FUNDAÇÃO ESCOLA DE COMÉRCIO ÁLVARES PENTEADO

FECAP

CENTRO UNIVERSITÁRIO ÁLVARES PENTEADO

MESTRADO EM CIÊNCIAS CONTÁBEIS

ROGÉRIO GUSTAVO PEREIRA DA SILVA

GESTÃO DE RISCOS E CONTROLES INTERNOS NO ENSINO SUPERIOR: UMA PROPOSTA DE FRAMEWORK PARA USO E PROTEÇÃO DE DADOS PESSOAIS EM UMA INSTITUIÇÃO DE ENSINO

São Paulo

2020

ROGÉRIO GUSTAVO PEREIRA DA SILVA

GESTÃO DE RISCOS E CONTROLES INTERNOS NO ENSINO SUPERIOR: UMA PROPOSTA DE FRAMEWORK PARA USO E PROTEÇÃO DE DADOS PESSOAIS EM UMA INSTITUIÇÃO DE ENSINO

Dissertação apresentada ao Programa de Mestrado em Ciências Contábeis do Centro Universitário Álvares Penteado, como requisito para a obtenção do título de Mestre em Ciências Contábeis.

Orientador: Prof. Dr. Ivam Ricardo Peleias

São Paulo

2020

Resumo

Silva, Rogério Gustavo Pereira. (2020). *Proteção de dados no ensino superior: uma proposta de framework para conformidade à Lei Geral de Proteção de Dados em uma instituição de ensino superior* (Dissertação de Mestrado). Centro Universitário Álvares Penteado, Fundação Escola de Comércio Álvares Penteado - FECAP, São Paulo, SP, Brasil.

A Lei Geral de Proteção de Dados, representa uma mudança na forma como a privacidade dos indivíduos é tratada, compreendendo assim um desafio para organizações de todos os segmentos. Diante disto, a presente pesquisa propõe um *framework* conceitual e funcional de adequação à lei em uma tradicional instituição de ensino superior (IES) da cidade de São Paulo. A metodologia adotada é a intervencionista que aproxima a dimensão teórica da prática, o que beneficia não apenas a instituição, como também colabora com o desenvolvimento de estudos em um setor ainda pouco explorado, o educacional. O trabalho contribui para o entendimento e *compliance* do uso e proteção de dados pessoais, na ordem de 83% junto aos times técnicos administrativos, com entregas articuladas de forma que permitam sua replicação em demais áreas não abrangidas. Alinham-se também achados à literatura de referência que assevera o desenvolvimento ainda embrionário de mecanismos de Gestão de Riscos e Governança de TI no segmento, similarmente beneficiados, corroborado de forma consoante e linear, pela alta gestão da IES.

Palavras-chave: Lei Geral de Proteção de Dados (LGPD). Ensino Superior. Controles Internos. Gestão de Riscos. Governança de TI (COBIT).

Abstract

Silva, Rogério Gustavo Pereira. (2019). *Data Protection in Higher Education: A Proposed Framework for Compliance with the General Data Protection Act in a Higher Education Institution* (Dissertação de Mestrado). Centro Universitário Álvares Penteado, Fundação Escola de Comércio Álvares Penteado - FECAP, São Paulo, SP, Brasil.

The General Data Protection Act, represents a change in the way privacy of individuals is treated, thus comprising a challenge for organizations of all segments. Therefore, this research proposes a conceptual and functional framework for compliance in a law. traditional higher education institution (HEI) in the city of São Paulo. The methodology adopted was the interventionist approach that approximates the theoretical dimension of practice, which benefits not only the institution, but also collaborates with the development of studies in a still unexplored sector, the educational. The work contributes to the understanding and compliance of the use and protection of personal data, in the order of 83% with the technical administrative teams, with articulated deliveries in a way that allows its replication in other areas not covered. Alignments are also aligned with the reference literature that asserts the still embryonic development of Risk Management and IT Governance mechanisms in the segment, similarly benefited, corroborated in a consonant and linear way by the high management of the HEI.

Key-words: Brazilian General Data Protection Act (LGPD). Higher education. Internal controls. Risk management. IT Governance (COBIT).

Lista de Figuras

Lista de Tabelas

Sumário

1 Introdução

A tecnologia da informação, tornou-se essencial ao crescimento e a sustentabilidade das organizações incluindo as do segmento educacional, especificamente do ensino superior, em que a infraestrutura tecnológica consiste em uma diversidade de aplicações e sistemas distintos, ou seja, recursos heterogêneos, voltados à suportar processos administrativos e acadêmicos, assim, exigindo uma estrutura efetiva de governança (Bianchi & Sousa, 2016; Coen & Kelly, 2007; Wu, Straub, & Liang, 2015).

Face a esta evolução tecnológica, a importância do *compliance* dos sistemas de informação nunca parou de crescer e, com o advento da internet e a sistematização de processos administrativos e contábeis, indivíduos e corporações esperam que estes sistemas sejam capazes de prever seu risco e apresentar estratégias para a redução destes (Jouini & Rabai, 2016) o impulso de informações organizacionais seguras deu início à necessidade de desenvolver melhores métricas para compreender o estado e o comportamento da segurança informacional na organização (The International Organization for Standardization and International Electrotechnical Commission 27005, 2011).

A segurança informacional, outrora favorável as organizações, é sensivelmente prejudicada por incidentes como fraudes e roubo de dados, os quais, ano após ano atingem índices alarmantes, favorecidos principalmente pelo alcance da internet, com isto, posicionando-se como o quarto maior risco organizacional do mundo em termos de probabilidade e registrando aumentos exponenciais nas violações de dados e seu intrínseco impacto financeiro (Global Risks Report, 2018).

Diante desta constatação, vários regulamentos entraram em vigor ou sofreram atualização recente, incluindo o Regulamento Geral de Proteção de Dados da União Europeia (GDPR - UE), Lei de Privacidade da Austrália (Notificable Data Breaches), Lei de Segurança Cibernética da China, em vigor desde 2017 e a Lei Geral da Proteção de Dados (LGPD – Brasil) buscando a regulação do risco informacional, particularmente no que tange à segurança de dados e privacidade (Tuttle, 2018).

À medida que mais violações levam os consumidores a exigir maior proteção e privacidade de seus dados, os reguladores aceleram o ritmo de resposta enquanto que as autoridades elaboram mais requisitos coercitivos, diferentes e complexos, portanto, a conformidade torna-se a cada dia mais complexa, dispendiosa e necessária (Privacy Governance Report, 2018).

Cada segmento enfrenta desafios únicos no gerenciamento da privacidade dos dados que possui, o ambiente aberto e colaborativo da maioria das Instituições de Ensino Superior (IES) é, muitas vezes, contrário ao controle necessário para o tratamento adequado de informações confidenciais. Instituições educacionais comumente abrigam altos indices de propriedade intelectual além de apresentam considerável volume de sistemas, segmentos lógicos, dispositivos e usuários o que prejudica sensivelmente a proteção, a privacidade e o compliance destas informações (Coffman, 2014).

Diante disto, as IES são, cada vez mais, vítimas de violações de segurança informacional e exposições de dados, diante disto, nenhuma instituição está imune, independentemente do tamanho, e, o que antes fora um problema ocasional agora é regular, assim, IES podem assumir as violações de privacidade como eventos quase certos, desta forma, um planejamento cuidadoso e uma implantação eficaz de recursos são cruciais para tratar este risco (Privacy Rights Clearinghouse, 2018).

Empresas têm que estimar as violações de segurança de seus sistemas porque as organizações que melhor gerenciam o risco da informação serão recompensadas por um mercado competitivo (Demchenko, Gommans, & Laat, 2000).

Lunardi, Becker, Maçada e Dolci (2014) e Weill e Ross (2004), evidenciam que as organizações adotam mecanismos formais de Governança de TI (GTI) para melhorar seu desempenho e lucro e ainda mitigar riscos informacionais, portanto uma governança efetiva de tecnologia auxilia as instituições a alcançar seus objetivos, aplicando os recursos relacionados de forma otimizada, com vistas, ao atingimento de bons resultados no desempenho organizacional (Grama, 2015).

Controles internos de TI são um componente importante do arsenal de conformidade de uma organização e ao compreender falhas de operacionais de tecnologia ou eventos de risco operacional de TI, como sinais das fraquezas do controle interno de TI, compreende-se também o impacto desses eventos nos próprios controles internos (Benaroch, Chernobai, & Goldstein, 2012; Firoiu, 2015; Mitra, Karathanasopoulos, Sermpinis, Dunis, 2015).

Em um mundo global e competitivo o sucesso a longo prazo requer uma forte conexão entre negócio e TI nas empresas, maximizando benefícios e reduzindo incertezas, desta forma, conferindo vantagem competitiva a estas organizações, por meio do uso de tecnologias com vistas ao aumento da eficácia e economia de tempo e custos (Calder, 2005; Grembergen, 2004).

Nesta direção, Instituições de Ensino Superior enfrentam, em grande parte, os mesmos "novos" e "convencionais" riscos de segurança e proteção de dados que demais setores da sociedade, entretanto, nas IES, estes representam uma ameaça mais estendida, com impactos

diretos à qualidade e continuidade das operações, comprometimento à continuidade do ensino e da pesquisa (Helsloot & Jong, 2006).

Um exemplo do problema da segurança no ensino superior é a vulnerabilidade dos sistemas de informação no ambiente virtual de aprendizagem, conduzindo a fragilidades de autenticidade, manipulação e roubo de informações, outra vulnerabilidade trata-se da infraestrutura física, ou seja, tudo que ocorre fora do âmbito computacional: roubos, incêndios e condições cada vez mais complexas de saúde e segurança (Ariff et al., 2014).

A ineficácia da Governança de TI afeta o desempenho da organização, a qualidade dos serviços, o gerenciamento de operações e de custos (Brown & Green 2012; Pang, 2014), além de ter negativamente afetadas: a qualidade do ensino, da pesquisa e do gerenciamento de processos internos, portanto, determinar mecanismos certos de TI é vital (Bianchi & Sousa, 2016).

Bichsel e Patrick (2014) preconizam que os programas de governança, gestão de risco e conformidade (GRC) de TI ainda estão em fase de desenvolvimento, onde poucas instituições têm todos os três pilares, acima, implementados e muitas mal têm definido por onde começar, além disto, não sabem se os programas de GRC devem ser desenvolvidos em paralelo ou separadamente, assim adotando várias abordagens para suportar a governança de TI, risco e, ou conformidade (Hicks, Pervan, & Perrin, 2012; Sabherwal & Kirs, 1994).

Associado ao estágio ainda embrionário que os programas de governança, gestão de risco e conformidade de tecnologia da informação estão, Tufano (2011) aponta que, a despeito, da existência de uma rica literatura nas áreas de gestão de risco, ainda há pouca pesquisa sobre práticas de gestão de risco e conformidade em relação às instituições de ensino superior.

Reconhecida por situar-se na fronteira do conhecimento, a educação superior revela: tendências, ideias e inovações que contribuem para o sucesso das organizações e da sociedade, todavia, as IES apresentam uma condição, ainda incipiente, do compliance de TI, do gerenciamento de risco e conformidade (Tufano, 2011), onde, observam-se dificuldades para implementação desta gestão além de dúvidas quanto a adoção de práticas mais adequadas ao cenário acadêmico (Ariff et al., 2014).

O fracasso dos mecanismos de governança corporativa e compliance, corrobora-se pela extraordinária sequência de escândalos comerciais que afetaram a economia global nos últimos 30 anos evidenciando a inadequação dos processos de governança quanto a prevenção de fraudes, controles internos e gerenciamento de riscos corporativos em geral (Rubino & Vitolla, 2014).

Diante disto, levando pesquisadores a refletir sobre a importância dos sistemas de governança e a ajudar o desenvolvimento de melhores modelos de gestão, desta forma, conduzindo as pesquisas relacionada a debater e evidenciar mais temas sobre controles internos e gestão de riscos (Enriques, & Volpin, 2007; Jensen, 1993; Power, 2004; Spira & Page, 2003) e profissionais (Committee of Sponsoring Organizations of the Treadway Commission [COSO], 1992, 2004 e 2013; Information Systems Audit and Control Association [ISACA], 2012).

Este é o cenário identificado em uma tradicional Instituição de Ensino Superior da cidade de São Paulo em função do exposto a questão de pesquisa segue adiante.

1.1 Questão de pesquisa

Diante do prazo de 18 meses previsto pela Lei Geral de Proteção de Dados do Brasil (LGPD, 13.709/18), sancionada em 14 de agosto de 2018, as empresas enfrentam a necessidade de assumirem as medidas pertinentes e cabidas para garantir o acato e cumprimento da lei.

Identifica-se, uma oportunidade de aliar o conhecimento acadêmico disposto sobre a prática coorporativa de controles internos e Governança de TI, ainda embrionária, no segmento educacional a ausência de um framework que ajuíze e implemente medidas de controle e governança aos termos da lei, desta forma, articulando a questão de pesquisa: **Como propor um framework conceitual e funcional para uso e proteção de dados pessoais em uma instituição de ensino superior?**

1.2 Objetivo geral

O presente trabalho propõe um framework conceitual e funcional para uso e proteção de dados pessoais em uma instituição de ensino superior, considerando a Lei Geral de Proteção de Dados do Brasil (LGPD – 13.709/2018) por meio de pesquisa intervencionista, em uma Instituição de Ensino Superior da cidade de São Paulo.

1.2.1 Objetivos específicos

Com vistas ao atingimento do objetivo geral, delineou-se uma relação de atividades, as quais são aqui estabelecidas como os objetivos específicos, apresentados em três momentos:

1. Pré implantação ao modelo de adequação:
    a. Compreender a Lei 13.709/18 – LGPD e suas implicações para as empresas sujeitas a sua ação;
    b. Mapear o estado atual de adequação à lei junto a IES estudada;

   c. Propor um modelo (framework) conceitual e funcional de adequação da IES, escolhida, aos termos da Lei 13.709/18 LGPD;
2. Momento de implantação do modelo de adequação:
   a. Dispor de forma estruturada o modelo de adequação junto a IES abordada;
3. Pós implantação do modelo proposto:
   a. Sobre o resultado, após aplicação do modelo, mapear todos os itens atendidos e não atendidos e propor potenciais tratativas;
   b. Avaliar se o framework foi efetivo e atendeu as imposições trazidas pela lei.

1.3 Justificativas e Contribuições

Diante da contribuição financeira e operacional que a Governança de TI agrega as instituições (Weill & Ross, 2004), da condição ainda embrionária no segmento educacional (Jairak & Praneetpolgrang, 2013; Tufano, 2011) e ainda face ao caráter coercitivo de conformidade a Lei Geral de Proteção de Dados aplicado a todas as empresas em território nacional que operem, dados de seus clientes, identifica-se a oportunidade de pesquisa para propor um modelo de adequação à regulamentação geral de proteção de dados do brasil (LGPD - 13.709/18) o qual atenda as exigências da lei em uma Instituição de Ensino Superior da cidade de São Paulo.

Desta forma, revisando, diagnosticando e propondo ajustes e melhorias aos controles internos, gerenciamento de riscos e governança de TI observados, contribuindo para o entendimento dos atuais níveis de governança, gestão de risco e conformidade (GRC) da IES estudada e sua relevância e impacto institucional, enquanto instrumento de desempenho organizacional e acadêmico (Ali & Green 2012; Bianchi & Sousa, 2016; Hicks et al., 2012; Pang, 2014; Sabherwal & Kirs, 1994). Além promover a aproximação da academia à prática de mercado (Suomala, Lyly-Yrjänäinen, Laine, & Mitchell, 2017).

Abaixo identificam-se e relacionam-se as seguintes contribuições de pesquisa.

Práticas:

1. Propor um Framework conceitual e funcional que apoie a implementação da conformidade à Lei 13.709/18 (LGPD) junto a uma IES, visto que até o momento final desta pesquisa não se localizou modelo de adequação dedicado ao segmento educacional;
2. Colaborar para adequação da IES escolhida para objeto de pesquisa a LGPD;
3. Possibilitar a implementação de práticas de Governança de TI na IES em questão;

4. Elevar o nível de maturidade de TI na IES promovido pela governança de TI implementada;

Acadêmicas:

5. Impulsionar o maior entendimento sobre Gestão de Riscos e Governança de TI em IES, o que ainda se mostra incipiente;
6. Alinhar percepções (variáveis observáveis) dos stakeholders envolvidos na intervenção ao referencial teórico versado (variáveis teóricas), quanto a controles Internos, Gestão de Risco e Governança de TI no segmento educacional;
7. Promover a aproximação do pensar científico, das práticas observáveis junto ao mercado de trabalho por meio da metodologia de pesquisa intervencionista, pesquisa-ação;
8. Incentivar futuras pesquisas sobre o segmento educacional, ainda pouco explorado pela literatura em específico junto as linhas de controles internos, gestão de riscos e governança de TI;

1.4 Limitações

O presente estudo limitar-se-á as análises de aspectos pertinentes a implementação dos controles necessários a adequação à lei 13.709/18 em um IES da cidade de São Paulo, escolhida para estudo, considerando: a) disponibilidade de informações; b) disposição dos stakeholders selecionados para realização dos trabalhos; c) porte da IES; d) relevância acadêmica; e) tempo hábil para a realização dos procedimentos e finalização do trabalho.

Outra limitação refere-se à impossibilidade de generalização dos achados e conclusões obtidos, diante do fato desse tratar de uma abordagem em uma única IES promovida pela estratégia de pesquisa adotada, a pesquisa intervencionista.

1.5 Estrutura do trabalho

Além da introdução, que apresenta a contextualização do problema, justificativa, do estudo realizado, seus objetivos, contribuições e limitações, o presente trabalho contará ainda com mais “n” capítulos, a saber: 2) Fundamentação teórica; 3) Metodologia; 4) Resultados e 5) Considerações finais.

O capítulo dois apresentará a fundamentação teórica, onde são abordados autores e obras sobre Governança de TI, Controles Internos, Gestão de Riscos e a Lei 13.709/18 em seus aspectos mais relevantes aplicados ao segmento educacional.

O capítulo três descreve a metodologia de pesquisa intervencionista. Pesquisa qualitativa, descritiva adotada neste estudo. Neste capítulo apresentar-se-á também o framework de implementação de ajustes aplicáveis a IES, mediante a avalição desta instituição realizada por meio de análises processuais, entrevistas, normas e literatura lograda.

Serão expostos também, os conceitos de entrevistas e questionários, como métodos e ferramentas para coleta de dados, os quais serão utilizados neste estudo.

No capítulo quatro, serão apresentadas e discutidas as informações derivadas das entrevistas com os usuários das informações, dos resultados obtidos na aplicação do framework proposto apreciando a estrutura da lei, suas reivindicações e ajustes realizados junto a estrutura da instituição. Oportunamente, apresentar-se-á a visão dos Reitores, gestores, e especialistas quanto a efetividade do framework proposto.

Por fim, o capítulo 5 traz considerações sobre os resultados alcançados na pesquisa, apoiando-se em estudos prévios e apresentados na fundamentação teórica. Após as considerações, serão listadas as referências, apêndices e anexos.

2 Referencial Teórico

2.1 Governança da tecnologia da informação em instituições de ensino superior

O termo “governança de tecnologia da informação” (GTI) deriva da “governança corporativa” (governança), destacando-se após vários escândalos financeiros em nível global em grandes corporações, tanto nos EUA quanto na Europa (Calder, 2005), e em sua definição mais básica, articula-se como o processo pelo qual as decisões são tomadas em torno dos investimentos em TI” (Brown & Nasuri, 2005).

Governança da Tecnologia da Informação é, a principal responsável por otimizar o uso de recursos de TI e gerenciar os riscos de projetos e processos, além do que, a GTI pode fornecer boas soluções para todas as organizações, sejam elas governamentais ou privadas, para otimizar os investimentos e práticas relacionadas e ainda equilibrar os riscos associados (Alreemy, Chang, Walters, & Wills, 2016).

O uso de TI como meio de desenvolver negócios tornou o processo de gerenciamento de sistemas corporativos e a medição de seu desempenho crítica, sistemas da organização devem garantir um fluxo adequado de informações para apoiar atividades relacionadas ao gerenciamento e controle da empresa, bem como apoiar os processos de governança corporativa (Bhattacharjya & Chang, 2007; Tiwana & Konsynski, 2010).

Nesse contexto, múltiplas motivações levam à aplicação de métodos de gerenciamento de TI: por um lado, a empresa diante dos custos crescentes precisa avaliar cuidadosamente os investimentos em tecnologia, por outro lado: percebe a crescente importância de mensurar a contribuição que os sistemas de TI fornecem à organização na busca de suas estratégias e metas (Weill & Ross 2004).

A informatização dos dados da empresa, portanto, exige que sua liderança preste mais atenção ao gerenciamento de serviços de TI para otimizar os investimentos em tecnologia, organizar a entrega de serviços de TI, monitorar o nível de qualidade dos serviços e alinhar os recursos de TI aos processos da empresa e as atividades de negócios (S. E. Abraham, 2012; Rubino & Vitolla, 2014).

A governança de TI ou sistemas de informação define a parte da governança corporativa que lida com o gerenciamento dos sistemas de TI de uma empresa, visando no gerenciamento de riscos de TI e o alinhamento dos sistemas corporativos aos propósitos dos negócios (Ko & Fink, 2010). Em essência, a governança de TI garante que os processos de gerenciamento de TI operem de maneira controlada e em conformidade para facilitar a obtenção dos benefícios

esperados, para apoiar as atividades de negócios atuais e suportar o sucesso de longo prazo da organização (Rubino & Vitolla, 2014).

Chang, Walters e Wills (2013) registram que a GTI se trata de uma estrutura que permite a compatibilidade entre os objetivos estratégicos da corporação e as iniciativas que ajudarão a empresa a alcançar um estágio satisfatório de risco, abrangendo diretrizes, ações, funções e tarefas organizacionais, portanto, auxiliando qualquer empresa a controlar e obter benefícios das práticas e investimentos em tecnologia

Definida por Calder e Moir (2009), a governança de TI otimiza o uso de investimentos em TI por meio de forte colaboração e comunicação entre os líderes de negócios, de TI e suas estratégias, portanto, pode-se traduzir a GTI como o grupo de processos que orientam e controlam os investimentos, decisões e práticas relacionadas à TI dentro da organização com vistas ao atingimento de seus objetivos.

Ao longo do tempo o tema Governança de TI evoluiu de estudos simples que mostravam certos aspectos específicos ligados à TI levaram à criação de uma ciência unitária. O termo governança de TI foi usado pela primeira vez por Henderson e Venkatraman (1993) e Loh e Venkatraman (1992) para descrever o conjunto de mecanismos indispensáveis para garantir a obtenção das capacidades de TI necessárias (Haes & Grembergen, 2005). Contudo, não foi muito significativo na literatura acadêmica até o final dos anos 1990, quando C. V. Brown (1997) e Sambamurthy e Zmud (1999) começaram a se referir a uma concepção de "estruturas de governança de sistemas de informação (SI) " e depois a "estruturas de governança de TI" em seus artigos (A. E. Brown & G. G. Grant, 2005).

Os principais tópicos que contribuíram para a criação do termo TI governança, como descrito por A. E. Brown e G. G. Grant (2005), estão listados, a saber:

a) Verificações de gerenciamento de sistemas de computador (Garrity, 1963);

b) verificações de serviços de informação (Olson & Chervany, 1980);

c) estrutura organizacional IS (Simson, 1995);

d) padrões da tecnologia da informação (Kayworth & Sambamurthy, 2000);

e) responsabilidades de tomada de decisão de TI (Boynton, Jacobs, & Zmud 1992);

f) arquitetura de TI gerenciamento e foco decisório de TI (Boynton et al., 1992);

g) papel organizacional e localização da responsabilidade dos sistemas de informação (C. V. Brown & S. L. Magill, 1994).

A tabela 1, estrutura a classificação das contribuições da pesquisa sobre Governança de TI do último decênio, classificadas por Novotny, Bernroider e Koch (2012) e ordenadas de acordo com a dimensão de governança de TI apreciada:

Tabela 1
Contribuições de pesquisa da GTI.

Dimensão da Governança de TI	Autores
Gestão de conformidade	Damianides (2005); Racz, Weippl e Seufert (2010); Raghupathi (2007).
Autoridade de decisão e responsabilidade	Bhattacharjya e Chang (2006); Lazic e Heinzl (2011); Peterson (2004); Schlosser, Wagner e Weitzel (2010); Simonsson e Johnson (2006); Tiwana e Konsynski (2010).
Desempenho e medição de qualidade	Bhattacharjya e Chang (2006); Raghupathi (2007); Ross e Weill (2005); Sambamurthy e Zmud (2000).
Gestão de investimentos	Haes e Grembergen, 2006; Luftman, (2003); Raghupathi, 2007).
Gerenciamento de recursos e capacidades	Dahlberg e Lahdelma (2007); Haes e Grembergen (2006); Schwarz e Hirschheim (2003).
Melhoria na governança	Dahlberg e Lahdelma (2007); Peterson, (2004); Schwarz e Hirschheim (2003).
Alinhamento ao negócio	Henderson e Venkatraman (1993); Luftman (2003); Reich e Benbasat (2000).
Entrega de valor comercial	Dahlberg e Lahdelma, (2007); Peterson, (2004); Raghupathi (2007).
Mecanismos de Governança na indústria	Almeida, Pereira e Silva (2013); Haes e Grembergen (2009); Pereira, Almeida e Silva (2014).
Entrega de valor e alinhamento estratégico	Chen, Sun, Helms e Jih (2008); Schobel e Denford (2013); Tallon (2007); Tallon e Pinsonneault (2011).
Gerenciamento de riscos	Bradley e Pratt (2011); Firoiu (2015)
Relação: TI e governança corporativa	Ko e Fink (2010)
Relação: TI e Gestão de Rico e *compliance*	Parent e Reich (2009); Wilkin e Chenhall (2010)

A governança da Tecnologia da Informação é um instrumento para controlar e gerenciar os recursos de TI, como a infraestrutura e pessoas em qualquer tipo de organização, incluindo universidades (Bajgoric, 2014; Haes & Grembergen, 2009; Hicks et al., 2012). Além do que, a GTI apoia a Governança Corporativa da organização a suportar a estratégia e a alcançar objetivos, metas e missão. Uma estrutura de governança de TI pode ser implantada com um conjunto de mecanismos, tais como estruturas, processos e instrumentos relacionais (Haes & Grembergen, 2004; Haes & Grembergen, 2009; Peterson, 2004; Weill & Ross 2004).

Em síntese o objetivo destes mecanismos é aprimorar o alinhamento entre o negócio e a tecnologia por meio da associação positiva do desempenho da governança de TI (Wu et al. 2015).

Bianchi e Sousa (2016) propõem que estruturas de GTI são responsáveis por definir papéis e responsabilidades institucionais, Comitês de direção são um exemplo das estruturas compostas por diretores, gerentes e executivos, ou seja, pessoas responsáveis pela tomada

decisória na organização (Haes & Grembergen, 2009; Webb, Pollard, & Ridley, 2006; Weill & Ross, 2004).

Desta forma, a Tabela 2 apresenta as diferentes estruturas da GTI observadas pela literatura e os pesquisadores que publicaram sobre:

Tabela 2
Estruturas de Governança de Tecnologia da Informação

Estruturas da Governança de Tecnologia da Informação	Autores									
	1	2	3	4	5	6	7	8	9	10
Comitê Estratégico de TI	x	x	x	x	x		x	x	x	x
Comitê de Auditoria de TI – alta gestão							x	x	x	x
Comitê Executivo – CIO	x	x								
Relatórios do CIO ao CEO e, ou COO		x			x		x	x	x	x
Comitê de direção de TI		x		x		x	x	x	x	x
Escritório de Governança de TI					x	x	x	x	x	x
Escritório de segurança/conformidade e risco							x	x	x	x
Comitê de projetos de TI							x	x	x	x
Comitê de segurança de TI							x	x	x	x
Comitê de arquitetura de TI						x	x	x	x	x
Integração de Governança / Alinhamento de tarefas, papeis e responsabilidades					x	x	x			x
Conselhos de TI					x	x				
Conselhos de lideranças de TI					x	x				
Estrutura organizacional de TI	x	x	x	x						
Centralizada					x		x			
Descentralizada						x		x		
Federal									x	x
Relação de gestores de TI e Negócio					x	x				

Nota: 1. Fraser e Tweedale (2003); 2. Albrecht e Pirani (2004); 3. Bhattacharjya e Chang (2006) 4. Aliyu, 2010; 5,6. Bhattacharjya e Chang 2006; 7. Zhen e Xin-yu (2007); 8. Wan e Chan (2008); 9. Fernández e Llorens (2009); 10. Ribeiro e Gomes (2009); CIO. Chief Information Officer; CEO. Chief Executive Officer; COO. Chief Operating Officer. Recuperado de "IT Governance mechanisms in higher education" de I. S. Bianchi e R. D. Sousa, 2016, *Procedia Computer Science, 100*, p. 3.

Bianchi e Sousa (2016) e Wu et al. (2015), sublinham que o alinhamento entre tecnologia e negócio se dá por meio de mecanismos relacionais, ou seja, uma comunicação apropriada e compartilhamento de conhecimento com aprendizagem e orientação (Haes & Grembergen, 2009; Webb et al., 2006; Weill & Ross, 2004).

A Tabela 3 articula os principais mecanismos relacionais ao alinhamento entre TI e as instituições, observados junto a literatura por Bianchi e Sousa (2016).

Tabela 3
Mecanismos relacionais de Governança de Tecnologia da Informação

Mecanismos Relacionais da Governança de Tecnologia da Informação	Autores									
	1	2	3	4	5	6	7	8	9	10
Posicionamento de TI e Negócio					x	x				
Treinamentos integrados				x			x	x	x	x
Gerenciamento do conhecimento	x		x		x	x				
Bons exemplos da alta gestão							x	x	x	x
Liderança de Tecnologia	x		x	x	x	x	x	x	x	x
Comunicação interna envolvendo TI					x	x				
Participação ativa dos Stakeholders					x	x	x	x	x	x
Colaboração entre os Stakeholders					x	x	x	x	x	x
Incentivos e recompensas de parcerias						x	x	x		
Entendimento compartilhado dos objetivos de TI e Negócio	x	x	x	x	x	x	x	x	x	x
Comunicação da alta gestão							x	x	x	x
Escritório do CIO e ITG					x	x	x	x	x	x

Nota: 1. Fraser e Tweedale (2003); 2. Albrecht e Pirani (2004); 3. Bhattacharjya e Chang (2006) 4. Aliyu, 2010; 5,6. Bhattacharjya e Chang 2006; 7. Zhen e Xin-yu (2007); 8. Wan e Chan (2008); 9. Fernández e Llorens (2009); 10. Ribeiro e Gomes (2009); Stakeholders. Partes interessadas; CIO. Chief Information Officer; ITG. Information Tecnology Governance. Recuperado de "IT Governance mechanisms in higher education" de I. S. Bianchi e R. D. Sousa, 2016, *Procedia Computer Science, 100*, p. 3

Processos de GTI referem-se ao planejamento de tomada de decisões estratégicas de TI apoiadas, recorrentemente, sobre práticas como COBIT ou Balance Scorecard (BSC), incluindo técnicas e ferramentas apropriadas para alinhar negócios e TI objetivando sempre um desempenho melhorado (Haes & Grembergen, 2013; Haes & Grembergen, 2009; Webb et al., 2006; Weill & Ross, 2004).

A Tabela 4 mostra os principais mecanismos de processos mais implementados pelas instituições, com destaque aos estudos de caso realizados em instituições de ensino de uma pesquisa da EDUCAUSE em 458 universidades dos EUA e Canadá por (Bichsel & Patrick, 2014).

Tabela 4
Mecanismos e artefatos de processos da GTI

Mecanismos e artefatos de processos da Governança de Tecnologia da Informação	Autores																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Planejamento estratégico de sistemas de TI	x	x	x	x	x	x														
Indicadores de desempenho de TI (BSC)	x		x	x								x	x	x	x		x			
Gestão de Portfólio – Projetos de TI	x				x	x						x	x	x	x					
Estornos (Chager back)	x														x					
Acordos de nível de serviço (SLA)															x					
Frameworks de Governança de TI					x										x					
ITIL					x	x	x	x	x		x	x	x	x	x	x				x
COBIT					x	x				x		x		x				x		x
ISO3850									x						x			x	x	x
BS7799, ISO17799 e ISO27001					x	x								x						x
People Capability Maturity Model (P-CMM)						x														
NIS																				x

Mecanismos e artefatos de processos da Governança de Tecnologia da Informação	Autores																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
NEISC																				x
OCTAVE																				x
Management of Risk (MoR)																				x
Garantia e auto avaliação da GTI												x	x	x	x					
Governança e metodologias de gestão de projetos de tecnologia	x	x		x	x	x						x								
Controle de orçamento de TI					x	x									x					
Gerenciamento de benefícios e relatórios					x															
Modelo de alinhamento Negócio/TI					x							x	x	x	x					
Modelo de Maturidade de TI (GTI-CMM)			x		x	x														
TI Sustentável – Green IT																			x	
Técnicas e ferramentas de software					x	x														
Análise de Riscos					x															

Nota: 1. Fraser e Tweedale (2003); 2. Albrecht e Pirani (2004); 3. Bhattacharjya e Chang (2006) 4. Aliyu, 2010; 5,6. Bhattacharjya e Chang 2006; 7. Zhen e Xin-yu (2007); 8. Wan e Chan (2008); 9. Fernández e Llorens (2009); 10. Ribeiro e Gomes (2009); 11. UCISA 12-15. Ko e Fink (2010); 16. Saleh e Almsafir (2013); 17. Jairak e Praneetpolgrang (2013); 18. Nugroho (2014); 19. Jairak et al. 2015; 20. Bichsel e Patrick (2014); SLA. Service Level Agreement. Recuperado de "IT Governance mechanisms in higher education" de I. S. Bianchi e R. D. Sousa, 2016, *Procedia Computer Science, 100*, p. 4.

Atualmente, a governança de TI e a segurança da informação são controlados por uma variedade de práticas, como ISO / IEC 38500, ISO / IEC 27001, COBIT e ITIL, no entanto, o COBIT agora é aceito como a estrutura preferida para a governança de TI e atualmente, em sua versão 5.0 e é apresentado como uma estrutura integrada única para governança de TI (Grembergen & Haes, 2010; Jairak & Praneetpolgrang, 2013).

2.1.1 COBIT 5.0 - estrutura e detalhes

O COBIT (*Control Objectives for Information and related Technology*) é uma estrutura de governança de TI desenvolvida pela ISACA (*Information Systems Audit and Control Association*), o framework surgiu a partir da iniciativa dos profissionais de auditoria que confrontavam ambientes cada vez mais automatizados.

O desenvolvimento inicial do COBIT foi uma estrutura dedicada a execução de atribuições de auditoria de TI, constituída ao redor de um conjunto abrangente de "Objetivos de Controle para os Processos de TI" (Haes, Grembergen, & Debreceny, 2013; International Accounting Standards Committee Fundation [IASCF], 1994; Klumb & Azevedo, 2014; Luciano & Testa, 2011).

Em sua quarta versão, fortaleceu o desenvolvimento de ferramentas para alinhar negócios, objetivos de TI e seu relacionamento com o suporte a processos de TI, estreitando a conexão com outros sistemas de governança relevantes (Haes et al., 2013; IT Governance Institute [ITGI], 2005).

Um aspecto importante do modelo é fornecer alinhamento estratégico da Tecnologia aos negócios, maximizando retornos, garantindo que os recursos de TI sejam usados com moderação e que os riscos associados à TI sejam mitigados (Klumb & Azevedo, 2014; Luciano & Testa, 2011).

Mais recentemente, o COBIT foi complementado com os frameworks "VAL IT" e "RISKIT", estes abordavam os processos de negócios e responsabilidades relacionados à TI na criação de valor (VAL IT) e gerenciamento de riscos (RISKIT), onde, em cada caso extraíram os principais conceitos e processos do COBIT e adicionaram orientação específica ao domínio (ISACA 2009c, 2010; Haes et al., 2013).

A Figura 1 mostra os principais marcos no desenvolvimento do COBIT.

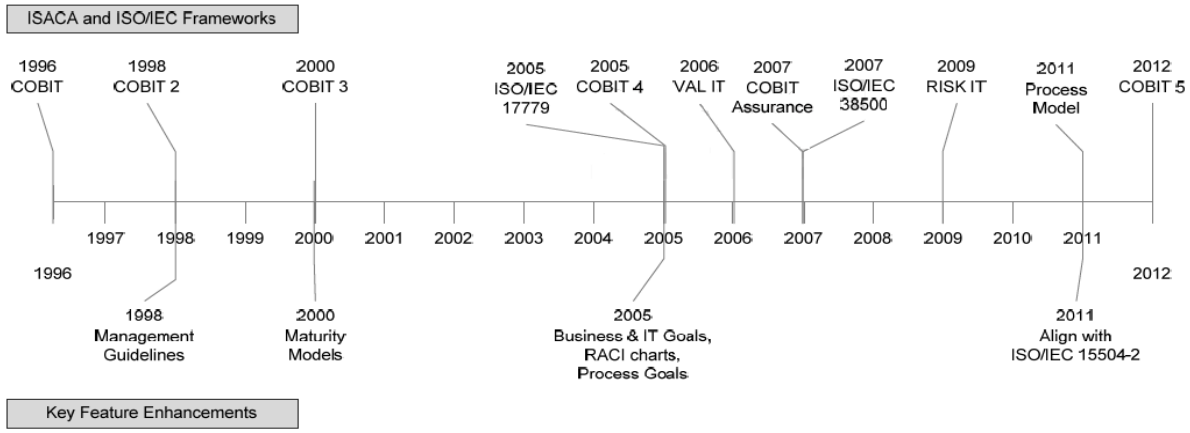

Figura 1. Time line Cobit até 2012.
Nota. Fonte: Adaptado de "COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities", de "S., de Haes, W. van Grembergen, & R. S. Debreceny (2013). *Journal of Information Systems, 27*.

O conceito de controle compreendido pelo COBIT baseia-se na literatura geral de controle de gerenciamento e sistemas de controle. A teoria do controle gerencial surgiu do comércio, particularmente com o desenvolvimento da corporação privada à medida que as empresas cresciam de tal forma que a propriedade se separava da administração (Berle & Means, 1932) e das teorias incluindo a teoria geral da administração de Fayol, teoria organizacional (Cyert & March, 1963; March & Simon 1958) e a cibernética de Stafford Beer (Beer 1959, 1972).

A definição de controle no COBIT, em sua terceira versão, é: "as políticas, procedimentos, práticas e estruturas organizacionais projetadas para fornecer uma garantia razoável de que os objetivos de negócios serão alcançados e que eventos indesejados serão evitados ou detectados e corrigidos" (International Accounting Standards Committee Fundation [IASCF], 2000; IT Governance Institute [ITGI], 2005).

Já em sua quinta versão, a mais recente, o termo controle outrora trazido enfaticamente é substituído por “boas práticas”, estabelecidas de forma altamente ativa e prescritiva, desta forma, podendo ser definidas como atividades ou processos usados, com sucesso, por diversas empresas e produzindo resultados confiáveis e satisfatórios (ISACA, 2012)

O COBIT 5 fornece um modelo abrangente que auxilia as organizações a atingirem seus objetivos de governança e gestão de TI, ou seja, auxilia a criar valor por meio da tecnologia mantendo o equilíbrio entre a realização de benefícios, a otimização dos níveis de risco e de utilização dos recursos disponíveis (ISACA, 2012).

Diante disto o COBIT 5 apresenta cinco princípios:

Figura 2. Os 5 princípios do COBIT.
Nota. Fonte: Adaptado de “COBIT 5: A Business Framework for the Governance and Management of Enterprise IT”, de Information Systems Audit and Control Association. Rolling Meadows, IL: ISACA. COBIT 5, 2012b, p. 19.

O COBIT, portanto, constitui uma ferramenta de governança de TI com a qual os gestores podem preencher a lacuna entre os requisitos de controle, sistemas de informação, problemas de TI e risco do negócio, para comunicar o nível de controle aos stakeholders (Brand, 2013).

Essa estrutura é desenvolvida para melhorar a qualidade dos produtos e serviços, a adequação do uso de recursos, investimentos e a conformidade com os requisitos de governança organizacional (ISACA, 2007), independentemente da plataforma de TI e, ou recursos técnicos

adotados pela empresa, uma vez que como já dito, seu uso é voltado para o negócio (Weill & Ross, 2004).

Diante disto o modelo COBIT, segundo o IT Governance Institute [ITGI], (2005), aplica-se a três níveis distintos dentro da organização, a saber:

I) 1º Nível - Gerentes: realizar a avaliação de riscos e controle de investimentos em TI;

II) 2º Nível – Usuários: Garantir a qualidade dos serviços prestados aos clientes internos e externos;

III) 3º Nível – Auditores: Avaliar no trabalho da gestão de TI e aconselhar e propor ajustes ao controle interno da organização;

Cada organização opera em um contexto diferente determinado por fatores externos (mercado, setor, geopolíticas, etc.) e internos (cultura, organização, inclinação ao risco, etc.), e exige um sistema de governança e gestão personalizado (ISACA, 2012b)

As necessidades das partes interessadas devem ser transformadas em uma estratégia exequível pela organização: “A cascata de objetivos da organização”, ou seja, um mecanismo de tradução das necessidades das partes em objetivos corporativos específicos, personalizados, exequíveis, objetivos de TI e metas, assim, permitindo configuração de objetivos específicos em cada nível e em cada área da organização e, portanto, apoiando efetivamente o alinhamento entre as necessidades corporativas e os serviços e soluções de TI (ISACA, 2012b, p. 19).

A cascata de objetivos do COBIT 5 é demonstrado, abaixo, junto a figura 03.

Figura 3. Cascata de objetivos do COBIT.
Nota. Fonte: Recuperado de "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT", de Information Systems Audit and Control Association. Rolling Meadows, IL: ISACA. COBIT 5, 2012b, p. 20).

A fim de alcançar uma melhor interação entre TI e negócios, a forma rígida da estrutura de TI deve adotar uma forma mais social e dinâmica (Schwarz & Hirschheim, 2003). Nesta direção, Weill e Ross (2004), afirmaram que identificar os direitos de decisão e responsabilidade do conselho pode encorajar comportamentos desejáveis no uso de TI. Uma combinação bem equilibrada de estruturas, processos e mecanismos relacionais possibilitará melhores resultados de governança (Haes & Grembergen, 2006).

Apoiado sobre a revisão da pesquisa de implementação de governança de TI, pode-se inferir que está relaciona-se não apenas à estrutura de governança de TI bem estabelecida, mas também à estratégia de TI e políticas bem comunicadas (Bowen et al., 2007).

O COBIT 5 não é prescritivo, mas defende que as organizações implementem seus processos de governança e gestão de forma que as principais áreas sejam contempladas, conforme abaixo demostrado na figura 4.

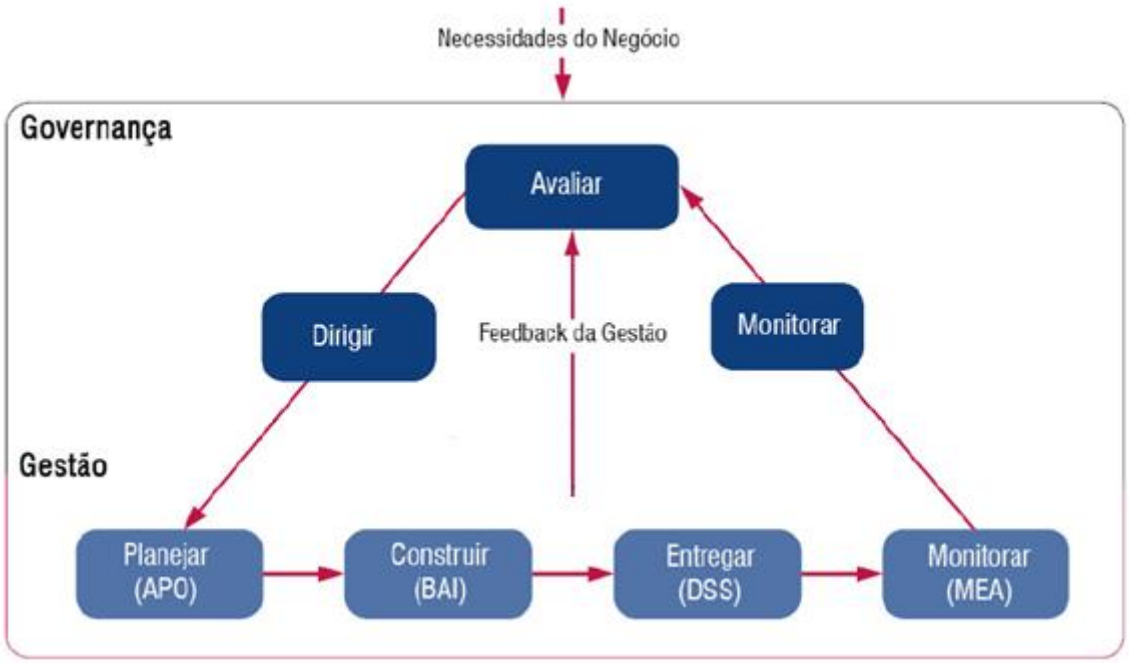

Figura 4. Áreas de governnça do COBIT
Nota. Fonte: Adaptado de "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT", de Information Systems Audit and Control Association. Rolling Meadows, IL: ISACA. COBIT 5, 2012b, p. 35).

O COBIT 5 divide os processos de governança e gestão de TI da organização em dois domínios de processo principais: 1) Governança: Contém cinco processos de governança; e dentro de cada processo são definidas práticas para Avaliar, Dirigir e Monitorar; 2) Gestão: Contém quatro domínios alinhados com as áreas responsáveis por planejar, construir, executar e monitorar, oferecendo cobertura de TI de ponta a ponta em consonância com as designações dessas áreas, e usam mais verbos para descrevê-las:

a) Alinhar, Planejar e Organizar (Align, Plan and Organise – (APO);
b) Construir, Adquirir e Implementar (Build, Acquire and Implement – (BAI);
c) Entregar, Serviços e Suporte (Deliver, Service and Support – (DSS);
d) Monitorar, Avaliar e Analisar (Monitor, Evaluate and Assess – (MEA).

A tabela 5 apresenta os critérios de dados e informações, abordados pelo COBIT, que transitam pelas organizações, independentemente de seu caráter.

Tabela 5
Critérios de dados e informações – COBIT 5

Critério	Conceito
Eficácia	A informação é eficaz se atender às necessidades do consumidor da informação que a utiliza para uma tarefa específica. Se o consumidor da informação puder realizar a tarefa com a informação, então a informação é eficaz. Isso corresponde às seguintes metas de qualidade da informação: valor adequado, relevância, compreensibilidade, interpretabilidade e objetividade.
Eficiência	Considerando que a eficácia leva em conta a informação como um produto, a eficiência se refere mais ao processo de obtenção e uso da informação, assim ela se alinha à visão de "informação como um serviço". Se a informação que atende às necessidades do consumidor da informação for obtida e usada facilmente (por exemplo, necessitar de poucos recursos – esforço físico, esforço cognitivos, tempo e dinheiro), então o uso da informação será considerado eficiente. Isso corresponde às seguintes metas de qualidade da informação: credibilidade, acessibilidade, facilidade de operação e reputação.
Integridade	Se a informação tiver integridade, então ela será exata e completa. Isso corresponde às seguintes metas de qualidade da informação: completude e exatidão.
Confiabilidade	A confiabilidade é frequentemente vista como sinônimo de exatidão; no entanto, também se pode dizer que a informação é confiável se ela for considerada verdadeira e confiável. Comparada com a integridade, a confiabilidade é mais subjetiva, mais relacionada à percepção, e não somente aos fatos. Ela corresponde às seguintes metas de qualidade da informação: credibilidade, reputação e objetividade.
Disponibilidade	A disponibilidade é uma das metas de qualidade da informação sob a orientação da acessibilidade e segurança.
Confidencialidade	A confidencialidade corresponde às metas de qualidade da informação no que diz respeito à restrição ao acesso.
Conformidade	conformidade no sentido de que a informação deve cumprir as especificações, impostas pelo ambiente (Direcionadores), é coberta por qualquer uma das metas de qualidade da informação, dependendo dos seus requisitos.

Nota. Fonte: Recuperado de "COBIT 5: A Business Framework for the Governance and Management of Enterprise IT", de Information Systems Audit and Control Association. Rolling Meadows, IL: ISACA., 2012b, p. 67.

Diante dos critérios da informação apresentados pelo COBIT, observa-se uma estreita relação com as prerrogativas do tratamento de dados pessoais apresentadas pela lei 13.709/18 em que se pese seus fundamentos, direitos dos titulares de dados e práticas de governança previstas em seus artigos, desta forma, alinhando-se com o objetivo geral da pesquisa aqui proposta: "Implementação um framework conceitual e funcional de adequação e acatação a lei 13.709/18 – LGPD por meio da pesquisa intervencionista, em uma IES da cidade de São Paulo".

2.2 Controles Internos e Gestão de Risco

Nos últimos anos, devido a inúmeras crises corporativas, a pesquisa em governança corporativa tem se concentrado no controle, tema que, tem recebido elevada atenção e volume de pesquisas superando, em alguns casos, a própria governança corporativa, aprimorando conceitos e estrutura para ser entendido como um processo iniciado dentro da organização, destinada a fornecer os meios mais adequados para alcançar objetivos predeterminados (Rubino & Vitolla, 2014).

Controle Interno, etimologicamente, remete à compreensão da fiscalização exercida sobre atividades e ações para que estas ocorram dentro das normas ou padrões pré-existentes,

entretanto, como todos os atos são humanos, observe-se então a inerente possibilidade de potencias riscos associados, o controle deve ser o conhecimento de como as pessoas conduzem as suas atividades e, a partir desse conhecimento, ser possível estabelecer, previamente, padrões de conduta adequados (Peleias, Caetano, Parisi, & Pereira, 2013; Cavalcante, Peter, & Machado, 2011; Lima, Maciel, & Libonati, 2008).

Peleias (2002) assevera controle interno como o conjunto de normas, procedimentos, instrumentos e ações adotadas de forma sistemática, os quais em constante evolução, asseguram o atingimento de resultados conforme objetivos preestabelecidos, protegendo o patrimônio e garantindo a transparência das operações.

No âmbito profissional, controle é versado pelo Relatório do COSO, publicado em inicialmente em 1992 e atualizado em 2004 com a publicação do Committee of Sponsoring Organizations of the Treadway Commission Entenprise Risk Management (COSO ERM), obra que colocou o conceito de sistema de controle interno lado a lado com o de gerenciamento de risco (Rubino & Vitolla, 2014).

O Comitê de Organizações Patrocinadoras da Comissão Treadway, é uma iniciativa conjunta das cinco organizações do setor privado, abaixo descritas, e dedica-se a fornecer liderança de pensamento por meio do desenvolvimento de estruturas e orientações sobre gerenciamento de riscos corporativos, controle interno e dissuasão de fraudes (COSO, https://www.coso.org/Pages/default.aspx, recuperado em 25 de novembro de 2019).

a) *American Accounting Association (AAA)* – Associação Americana de Contabilidade;
b) *American Institute of Certified Public Accountants (AICPA)*, Instituto Americano de Certificação de Contadores Públicos;
c) *Financial Executives International (FEI)* – Executivos Financeiros Internacionais;
d) *Institute of Internal Auditors (IIA),* - Instituto dos Auditores Internos, e;
e) *National Association of Accountants* – Associação nacional de Contadores, *(now the Institute of Management Accountants [IMA]*– Instituto de Contadores Gerenciais;

Segundo o comitê, Controle Interno "é um processo conduzido pela estrutura de governança, administração e outros profissionais da entidade, e desenvolvido para proporcionar segurança razoável com respeito à realização dos objetivos relacionados a operações, divulgação e conformidade" (COSO, 2013, p. 6).

De acordo com o COSO ERM, para alcançar os objetivos da empresa, um sistema de controle interno adequado deve ser estabelecido, portanto, a avaliação de risco é apenas um meio de ajustar adequadamente intensidade dos controles. A recente revisão do Relatório COSO de 2013 confirmou a importância do gerenciamento de riscos dentro do sistema de controle interno. À luz das mudanças que afetaram tanto as atividades comerciais quanto as

operacionais, o Relatório COSO, em sua nova função, expandiu os elementos sujeitos a observação, concentrando-se melhor nas tarefas relacionadas aos objetivos de relatórios e cumprimento.

Um progressivo fluxo de pesquisa em controles internos de tecnologia da informação (TI) foi motivado pela Lei Sarbanes-Oxley (SOX) de 2002, que exige das empresas divulgação dos pontos fracos do controle interno sobre os relatórios financeiros. Em linhas gerais, os controles de TI referem-se às "salvaguardas, contramedidas e medidas técnicas e de gerenciamento prescritas para um sistema de informações para proteger a confidencialidade, integridade e disponibilidade do sistema e suas informações" (Benaroch et al., 2012; National Institute of Standards and Technology [NIST], 2010).

O controle, em sua forma simples, propõe-se a influenciar como um indivíduo ou um grupo se comporta buscando alcançar objetivos prescritos. Um framework, por definição, é uma estrutura de várias camadas que define o curso de ação, assim, uma estrutura de controle em TI é uma estrutura em camadas que controla a maneira como os profissionais de TI se comportam em qualquer ambiente ou situação. Pode ser usado para categorizar mecanismos como: quem faz, o que e como o faz (Cram, Brohman, & Gallupe, 2016).

Por exemplo, na presença de uma ameaça, as pessoas se voltariam à estrutura de controle para buscar orientação sobre qual ação tomar entre ações alternativas (Chaxel, 2016). Sob a óptica de TI, as estruturas de controle são basicamente controles internos que ajudam a gerenciar riscos, portanto, para a implementação da segurança da informação, são empreendidos controles internos para proteger as informações contra acessos não autorizados (Chang, Yen, Chang, & Jan, 2014).

Coube ao Committee of Sponsoring Organizations (COSO), que atuou na elaboração do Treadway Report, articular, em setembro de 1992, no documento Internal Control - Integrated Framework (COSO 1), a seguinte definição (1994): o controle interno é um processo executado pelo conselho de administração, diretoria, gerência e outros profissionais, desenhado para promover razoável segurança de que alguns objetivos das empresas sejam atingidos: confiabilidade das demonstrações contábeis; eficácia e eficiência das operações; e adequado cumprimento das normas e regulamentos.

O COSO (Comitê de Organizações Patrocinadoras da Treadway Commission, 1996) é projetado para que as empresas possam usar com segurança os processos financeiros e promover a eficiência. Os principais componentes do COSO são:

a) O ambiente de controle interno;
b) Definição de objetivos;

c) Identificação de eventos;
d) Identificação de eventos;
e) Avaliação de riscos
f) Resposta a riscos;
g) Atividades de controle;
h) Informações e comunicação e monitoramento. (COSO, 2013)

De acordo com Chang, Walters e Wills (2013), o relatório sobre estruturas de controle divulgadas pelo COSO em 1992 falhou em termos de listagem de requisitos suplementares para a implementação e avaliação de controles de TI.

Assim, Pang e Li (2013), em sua pesquisa, analisam a necessidade de integrar o controle interno e a gestão de riscos onde afirmam que para garantir a eficácia e a eficiência das operações das empresas, são necessários: a) relatórios financeiros confiáveis; b) cumprimento da lei ou regulação; c) um sistema interno sólido; e estes são os objetivos fundamentais do gerenciamento de riscos.

A eficiência operacional prevê, entre outras coisas, a salvaguarda dos ativos da empresa, como testifica o COSO (2013) e Peleias (2012), declarando que controles internos objetivam preservar todo o patrimônio, uma vez que, este abrange todos os processos da empresa, sejam eles ligados ao ativo, ao passivo ou a geração de resultado.

O COSO possui dois modelos que estruturam suas diretrizes: o COSO I de 1992 que apresenta um modelo de Controles internos e o COSO II, de 2004, que traz um modelo de Riscos Empresariais, retratados por um cubo no qual as três faces visíveis representam: i) tipos de objetivos; ii) níveis da estrutura organizacional e iii) componentes.

A figura 5, abaixo, ilustra a comparação entre as estruturas do COSO, evidenciando suas características e dimensões:

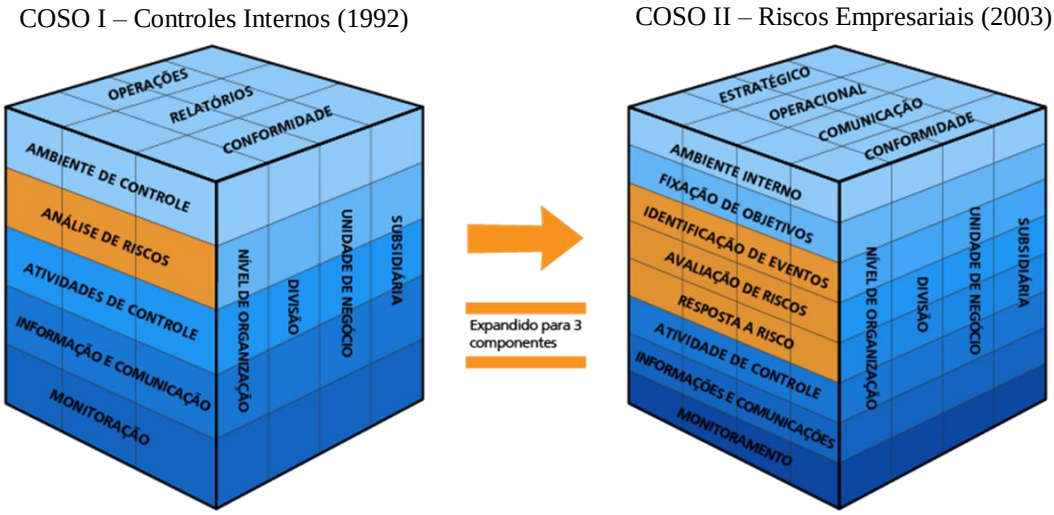

Figura 5. Comparação COSO I - 1992 e COSO II - 2003

Nota. Fonte: De "Modelos de referência de gestão corporativa de riscos", de "Tribunal de Contas da União", [2019]. Recuperado de https://portal.tcu.gov.br/planejamento-governanca-e-gestao/gestao-de-riscos/politica-de-gestao-de-riscos/modelos-de-referencia.htm

Observa-se que o cubo I, Controles Internos, é parte integrante do II, Riscos Empresariais, como um subconjunto do modelo de negócios, contextual e mais amplo, se concentrando nos objetivos estratégicos, uma vez que os Riscos Empresariais abrangem respostas múltiplas ao risco: evitar, aceitar, compartilhar e reduzir enquanto que o controle interno responde meramente sobre a redução de riscos (COSO, 2004).

O controle interno se trata da função da gestão que ajuda a controlar o antes e o depois dos objetivos de negócio e, neste sentido, finalmente recomendando que o controle interno e a gestão de riscos sejam organicamente integrados, pois beneficiariam o atingimento dos melhores resultados institucionais (Pang & Li, 2013).

2.2.1 Risco

Partindo da compreensão natural o termo "risco", surpreendentemente ainda não possui uma definição única e inequívoca que tenha o apoio absoluto de todos os especialistas no campo da "segurança" (Helsloot & Jong, 2006).

A constante busca por formas de minimizar riscos, muitas vezes, levam gestores e empresas a encara-los como oportunidades, adotando modelos mais adequados à gestão de riscos e ajustando também, suas ferramentas de controles internos (Peleias, Caetano, Parisi, & Pereira, 2013).

A norma ISO 31000 em sua edição de 2018, define risco como "efeito da incerteza sobre os objetivos e apoio à tomada de decisões levando em conta a incerteza e seu efeito no alcance dos objetivos e na avaliação da necessidade de qualquer ação", referindo-se à cultura, processos

e estruturas que são direcionados para a realização de oportunidades potenciais, ao mesmo tempo em que gerencia os efeitos adversos (ISO 31000, 2018).

A gestão de riscos é reconhecida como um aspecto proeminente da boa governança corporativa, onde a necessidade de uma estrutura eficaz de gerenciamento de riscos é amplamente reconhecida pela academia e pelo mercado, todavia, a gestão de risco em alguns setores como instituições públicas de ensino superior, parece ser significativamente menos desenvolvida (Ariff et al., 2014).

O gerenciamento de riscos empresariais é um processo amplo e comumente afetado pelo conselho de administração, pelo gerenciamento de resultados e pelos funcionários da organização. Aplicado junto a definição de estratégia e em toda a empresa, projetado para identificar possíveis eventos que possam afetar a entidade e ainda administrar o apetite institucional ao risco, garantindo razoável alcance dos objetivos da entidade (COSO, 2004).

Os problemas de gerenciamento de riscos são os desafios e oportunidades identificados e gerenciados por meio de plano, que vão desde a segurança e bem-estar dos indivíduos aos danos à reputação (Kenwood, & Rafferty, 2017).

Muitas das questões de gestão de risco enfrentadas pelas instituições de ensino superior são de natureza regulatória e financeira e frequentemente vinculadas a esforços de planejamento estratégico e compliance em toda a instituição (Fraser, Simkins & Narvaez, 2015).

No entanto, IES ainda enfrentam dificuldades com a implementação do gerenciamento de risco (Gallagher, 2013) por vários motivos, tais como: 1) ausência de atenção ou consideração de liderança sênior; 2) deficiência de compreensão, falta de treinamento e comunicação; 3) falta de esclarecimento de papéis e responsabilidades em toda a organização; e 4) ausência de identificação de riscos institucionais e de educação superior emergentes e relevantes; (Association of Governing Boards of Universities and Colleges [AGB], 2007).

O Gerenciamento de Riscos Empresariais é definido como um modelo de gestão de risco que aceita o risco como um princípio básico de operações e decisões, que se esforça para otimizar os resultados, identificando como os riscos podem afetar o desempenho geral da instituição, além das metas e planos estratégicos (Gallagher, 2013), exigindo que as partes interessadas estejam sintonizadas com a cultura de risco empresarial. Uma cultura consciente do risco é aquela em que as decisões tomadas em relação ao risco são baseadas em pessoas, sua participação e seu comprometimento com a organização (Hinton, 2012).

Pode-se pensar que uma instituição tenha uma cultura consciente do risco quando a liderança recompensa os esforços de identificação de risco, assume o risco e aspira a criar

estratégias de avaliação e mitigação de risco em cada departamento e em cada iniciativa do campus (J. M. Abraham, 2013).

No contexto do ensino superior, gestão de risco trata-se de um processo aplicado em toda a universidade, seja em sua dimensão acadêmica seja administrativa, projetado para: a) identificar e tratar possíveis eventos que possam afetar positiva ou negativamente a instituição; b) gerenciar os riscos para que estes estejam dentro do apetite ao risco institucional; c) criar e aferir indicadores-chave de desempenho; d) contribuir para a realização da missão e objetivos da universidade (Ariff et al., 2014).

Portanto, a crescente importância da gestão de risco nos mecanismos de governança corporativa é inferida, não apenas, a partir da análise dos principais quadros de controle, mas também, sobre o exame dos principais "Códigos de Governança Corporativa" emitidos por diversos países como:

a) Relatório Turnbull de 1999;

b) Código Combinado de 2008 e 2013;

c) King Report de 2009;

d) Código de Contrato da Bolsa de Valores da Itália de 2006 e 2015;

Observa-se tal relevância, por meio de normas regulatórias que legitimam a governança corporativa, em nível mundial, como: Lei Sarbanes-Oxley e Acordo de Basileia, evidenciando sua conotação estratégica como meio para atingir os objetivos da empresa respeitando, direitos e expectativas das partes interessadas (McWhorter, Matherly & Frizzell 2006; Rubino & Vitolla, 2014).

Significantes iniciativas da gestão de riscos são observadas ao redor do mundo, como: Austrália e Nova Zelândia (Padrão Australiano | Neozelandês de Gerenciamento de riscos - Princípios e diretrizes, 2009), França (Autorité des Marchés Financiers, Sistemas de gerenciamento de risco e controle interno - Estrutura de Referência, 2010) e no Reino Unido (Financial Reporting Council - Boards e Risk. Um resumo das discussões com empresas, investidores e consultores, 2011), desta forma, tornando obrigatória a implementação de sistemas de gestão de risco e conformidade em todas as empresas, mesmo as não listadas no Mercado de Ações (Rubino & Vitolla, 2012).

A literatura acadêmica disposta sobre a Gestão de Riscos, propõe e revisa diversos aspectos a serem considerados, primeiro: o posicionamento do risco de fraude junto ao gerenciamento da cadeia de valor; segundo: a discussão da fraude sob a perspectiva da gestão de risco; terceiro: a visão das abordagens de priorização de riscos na literatura, bem como

aquelas utilizadas junto a priorização de fraudes; e, finalmente, uma investigação empírica das abordagens desta priorização atualmente (Mu & Carroll, 2016).

Assim, o gerenciamento de riscos empresariais, propõe que as empresas abordem todos os seus riscos de forma abrangente e coerente, em vez de gerenciá-los individualmente (Beasley, Pagach, & Warr, 2008; Rubino & Vitolla, 2014).

A análise conjunta do quadro profissional de fontes reguladoras mostra que os temas de gestão de riscos e governança corporativa estão em curso de colisão, cada vez mais próximos, desta forma, propondo que uma ideal gestão de atividades empresariais se tornou sinônimo de um sistema amplo e formalizado de gerenciamento de riscos (Rubino e Vitolla, 2012). A gestão de riscos tornou-se agora um componente essencial de um sucesso o negócio, enquanto, por um lado, a crise financeira global de 2008 fortaleceu a importância de um sistema adequado de gestão de risco em apoio à governança corporativa, por outro lado, a globalização levou as empresas a uma revisão dinâmica de suas escolhas de gerenciamento de risco (Ashby, 2011; Kaplan & Mikes, 2012; Mikes & Kaplan, 2013).

A revisão sobre a implementação do Gerenciamento de risco indicou que a estrutura integrada de gestão de risco (COSO, 2004) e a IS0 31000: 2009 são amplamente adotadas, essas estruturas de gerenciamento de riscos descrevem princípios, práticas, diretrizes genéricas e processos envolvidos no gerenciamento de riscos. Desta forma, o Gerenciamento de Riscos Coorporativos (GRC) capaz de unificar práticas de esforço operacional e gestão de riscos para estabelecer o contexto, o parâmetro, a identificação, a análise e o perfil dos riscos, deste modo, determinando melhor a estratégia para seu tratamento.

Apesar de todo desenvolvimento observado junto a gestão de riscos em diversos segmentos, modelos e procedimentos dedicados ao ensino superior ainda são escassos, onde as práticas deste gerenciamento, ainda embrionárias, ocorrem comumente apoiadas sobre análises regulatórias do COSO (2004), IS0 31000: 2009 e MS ISO 31000: 2010 (Ariff et al., 2014)

Alguma padronização sobre o gerenciamento de riscos deve ser aplicada para que o método compulsório mínimo possa ocorrer, portanto, os padrões de gerenciamento de risco, como por exemplo, COSO e ISO 9001: 2009, podem ser considerados ao projetar uma estrutura para gerenciar riscos. Com base na revisão dessas normas, conforme apresentado na Tabela 1, as práticas de gerenciamento de risco desta devem ser considerar:

a) Governança de risco;
b) Política de risco;
c) Contexto de risco: identificação de risco e análise, avaliação, tratamento, comunicação, consulta, monitoramento e revisão do processo de gerenciamento de riscos;

d) Ferramentas e tecnologia;

e) Melhoria contínua.

Ferramentas e abordagens de gerenciamento de risco foram desenvolvidas para implementar práticas mais adequadas à esta gestão e ainda beneficiar o sucesso da organização (Kwak & Stoddard, 2004), portanto, sugere-se que nas instituições de ensino superior, as dimensões, acima trazidas, sejam tratadas de forma a entregar um efeito positivo e significativo junto as práticas relacionadas.

Tabela 6

Gestão de risco do COSO, IS0 31000: 2009, MS ISO 9001: 2010 e sua contribuição para práticas de gestão de risco dedicadas o ensino superior

COSO (2004)	ISO 31000:2009 / MS ISO 31000: 2010	Práticas Propostas de Gerenciamento de risco
Definição de objetivos, Ambiente interno, Ambiente processual e informacional	Mandato e compromisso Projeto de *framework* para gerenciamento de risco	1. Governança do Risco
	Política de Risco	2. Declaração de política de Risco
Identificação de Eventos Avaliação de risco Resposta ao Risco Atividades de controle Informação e comunicação Monitoramento	Implementação do gerenciamento de riscos - processos são idênticos aos tratados no AS / NZS 4360: 2007 (2004).	3. Processos de Gestão de Risco - Contexto de risco, avaliação de risco (identificação de risco, análise de risco, avaliação de risco), tratamento de risco, comunicação e consulta, monitoramento e revisão.
Ferramentas e técnicas	Ferramentas e técnicas	4. Ferramentas e tecnologia
Não especificamente abordado no *framework*, mas é mencionado no padrão	Melhoria contínua do *framework*	5. Melhoria contínua da estrutura de gerenciamento de riscos

Ariff et.al (2014), sugerem que as instituições de ensino devam criar sua própria estrutura metodológica, abordagem, práticas e diretrizes junto a gestão do risco e apoiado na revisão de pesquisas anteriores relacionadas ao gerenciamento de riscos, os seguintes processos de práticas de gerenciamento de riscos devem ser considerados: contexto de risco, identificação de riscos, análise e avaliação, tratamento de risco, consulta de risco e monitoramento e revisão de risco.

Um processo proativo de gerenciamento de riscos permite que os gestores pratiquem o gerenciamento adequado de riscos e resolvam possíveis problemas antes que ocorram e, portanto, contribuindo para o sucesso (Dey, Kinch, & Ogunlana, 2007; Kwak & Stoddard, 2004). Portanto conhecer os processos relacionados ao risco é condição essencial à sua gestão, isto dito a tabela 7, a seguir, elenca os principais processos da gestão de risco os relacionando aos autores de referência abrangidos.

Tabela 7
Pesquisadores dos Processos de Gerenciamento de Riscos

Processos da gestão de riscos	Pesquisadores e padrões								
	1	2	3	4	5	6	7	8	9
Contexto de risco	x								
Identificação de risco	x	x	x	x	x				x
Analise de risco	x	x				x	x		
Avaliação de risco	x	x				x		x	x
Tratamento de risco	x	x				x			x
Consulta de risco	x					x			
Monitoração e revisão de risco	x	x							

Nota: 1. ISO 31000:2009; 2. Kululanga and Kuotcha (2009); 3. Chapman (1997); 4. Tchankova (2002); 5. Cerevon (2006); 6. Ahmed et. al (2007); 7. Dey, Kinch e Ogunlana (2007); 8. Elkington et. al (2010); 9. Lee and Azlan (2002)

O Gerenciamento de Riscos corporativos, integrado a estratégia e desempenho organizacional realça a importância da gestão de riscos e sua incorporação em toda empresa, visto que o risco influencia e alinha estratégia e desempenho em todas os departamentos e funções (COSO, 2017).

A figura 6, apresenta o framework do COSO-ERM desenvolvido sob cinco componentes e vinte princípios, por estes distribuídos e adiante abordados:

Figura 6. Componentes do COSO-ERM.
Nota. Fonte: Recuperado de "*Gerenciamento de risco corporativos integrado com estratégias e performance: Sumário executivo*, " de Committee of Sponsoring Organizations of the Treadway Commission", 2017, p. 6.

Os cinco componentes do novo Framework se combinam em um conjunto de princípios, que abrangem desde a governança até o monitoramento e sua adoção pode trazer ao conselho e à administração a segurança de que a organização é capaz de gerenciar de modo aceitável os riscos associados à estratégia e aos objetivos de estratégicos (COSO, 2017).

Os cinco componentes, apresentados pelo framework, organizam-se em vinte princípios inter-relacionados, os quais percorrem desde a governança até o monitoramento, eles descrevem práticas que podem ser aplicadas de diferentes formas nas organizações, independentemente do seu tamanho, tipo ou setor econômico.

A tabela 8, abaixo distribui os vinte princípios através dos cinco componentes apreciados pelo framework.

Tabela 8
Componentes e Princípios do COSO-ERM

Componentes	Princípios
 Governança e Cultura	**1**. Exercícios de Supervisão do Risco da Diretoria; **2**. Estabelece Estruturas Operacionais; **3**. Define a Cultura Desejada; **4**. Demonstra Compromisso com os Valores Essenciais; **5**. Atrai, desenvolve e retém pessoas capacitadas;
 **Estratégia e definição de objetivos**	**6**. Analisa o Contexto do Negócio; **7**. Define Apetite ao Risco; **8**. Avalia Estratégias Alternativas; **9**. Formula Objetivos Empresariais;
 Desempenho	**10**. Identifica Risco; **11**. Avalia a gravidade do risco; **12**. Prioriza os riscos; **13**. Implementa Respostas de Risco; **14**. Desenvolve a Visão do Portfólio;
 Revisão e acompanhar	**15**. Avalia alteração substancial; **16**. Avaliações de Risco e Desempenho; **17**. Prossegue Melhoria no Gerenciamento de Riscos Corporativos;
 Informação comunicação e relatos	**18**. Aproveita Informações e Tecnologia; **19**. Comunica informações de risco; **20**. Relatórios sobre Risco, Cultura e Desempenho;

Nota. Fonte: Recuperado de "G*erenciamento de risco corporativos integrado com estratégias e performance: Sumário executivo*, " de Committee of Sponsoring Organizations of the Treadway Commission", 2017, p. 7.

2.3 Lei geral de proteção de dados (LGPD) do Brasil

Conhecida internacionalmente como "Brazilian GDPR" a Lei Geral de Proteção de Dados Pessoais (LGPD) é um regulamento que eleva significativamente o regime de proteção de dados do país, reforçando a sua postura de demonstrar adequação à norma europeia de proteção de dados e tornando o Brasil um dos poucos países a fornecer proteções de privacidade de dados comparáveis aos residentes da BRIC: Brasil, Rússia, Índia e China (Tuttle, 2018).

Aprovada em agosto de 2018, a Lei 13.709/18, Lei Geral de Proteção de Dados Pessoais (LGPD), versa sobre a proteção de dados pessoais visando assegurar que os princípios de respeito e proteção de dados não serão negligenciados, para tal, também altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet - MCI) assim gerando inúmeras interrogações nos agentes de mercado (KPMG, 2018).

Semelhantemente à GDPR, a lei brasileira firma um escopo amplo, reivindicando jurisdição extraterritorial sobre atividades de processamento de dados conduzidas não apenas no país, mas também qualquer associado a bens ou serviços oferecidos nacionalmente, como em sua predecessora europeia, a lei exige a notificação e obtenção do consentimento dos

consumidores e a adoção de uma abordagem baseada em riscos e controles internos para coletar, manipular e salvo-guardar dados (Tuttle, 2018).

Desta forma, a LGPD garantirá a todos os indivíduos maior controle sobre os seus dados pessoais, estipulando princípios basilares que nortearão qualquer hipótese de tratamento de dados pessoais, como, mas não só, as da internet, de relações de trabalho ou de consumo, desta forma, observando que a lei se aplica a um ampla gama de operações como trabalhista, consumerista e de prestação de serviços, sempre com observância na boa-fé das partes envolvidas (Mulholland, 2018; Sindicato dos Estabelecimentos de Ensino no Estado de São Paulo [SIEEESP], 2018).

As sanções previstas no regulamento são similares, mas não tão severas quanto as do GDPR, com multas máximas que chegam a 2% da receita global da empresa em relação ao ano anterior (comparado a 4% na UE) ou até 50 milhões de reais por infração, quase US$ 13 milhões (Baffa, Poggio, & Fachinetti, 2018; Deloitte, 2018; Maldonato, Blum, & Borelli 2019; Tuttle, 2018).

Todavia, a despeito das sanções previstas, essa política que busca proteger os cidadãos e as empresas, também impacta de forma positiva, as empresas brasileiras que buscam fazer, ou já fazem, negócios fora de suas linhas limítrofes territoriais e vice-versa, diante do aumento do nível de confiança, derivado da acatação da lei, para todos os seus públicos de relacionamento (Deloitte, 2018; Tuttle, 2018).

Portanto o escopo da lei, não é de todo negativo, pois além de garantir os direitos individuais, a LGPD busca estimular o desenvolvimento sustentável da economia e das empresas e suas transações de dados, com base nas melhores práticas internacionais (Bioni, 2019), o que representa, uma grande oportunidade para as empresas aperfeiçoarem suas regulações e controles internos em direção à obtenção de uma vantagem competitiva no uso desses dados, com um planejamento correto e aplicação de boas práticas de privacidade (Deloitte, 2018).

Globalmente, o tema proteção de dados vem sendo tratado há mais de 40 anos e sofre atualizações recorrentes a medida em que o processo de inovação tecnológica supera o desenho inicial do arcabouço proposto, um exemplo é a União Europeia, com regimento em vigor desde 1995 atualizou suas bases regimentais em 2018 para criar a General Data Protection Regulation (GDPR) (KMPG, 2018).

A Tabela 9, abaixo apresenta a síntese da visão geral da proteção e dados em outros países:

Tabela 9
Proteção de Dados: visão geral ao redor do mundo

Organization for Economic Cooperation and Development - **OECD**:	**União Europeia:**	**Reino Unido:**	**Japão:**	**Alemanha:**
Diretrizes sobre a Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais	Diretiva nº 95/45/ EC, substituída pela Regulamentação Geral de Proteção de Dados (GDPR)	Ato de Proteção de Dados	Ato de Proteção de Informações Pessoais	Ato Federal de Proteção de Dados (Bundesdatenschutzgesetz)
Em vigor desde 1980	Em vigor desde 1995	Em vigor desde 1998	Em vigor desde 2005	Em vigor desde 1998
Estados-membros devem ter legislação interna focada na proteção da privacidade e dos direitos individuais. Exigências de privacidade atingem entes públicos e empresas privadas.	Uniformiza diretrizes para proteção de dados pessoais em todos os Estados membros. Determina que direitos individuais devem ser protegidos e assegurados. Previne abusos.	Impõe regras relativas à proteção a dados pessoais e aos "dados sensíveis", que englobam informações como religião professada e etnia.	Empresas e demais organizações públicas ou privadas devem salvaguardar direitos e interesses dos indivíduos no processamento de seus dados. Prevê sanções penais em caso de desrespeito às disposições do Ato.	Protege os interesses individuais no que tange ao uso de dados pessoais. Uma curiosidade interessante: a primeira lei de proteção alemã a dados individuais data de 1977 e já estendia aos entes públicos e privados a responsabilidade pelo bom uso desses dados e respeito à privacidade.

Legenda:
OECD (Organização para Cooperação e Desenvolvimento Econômico): Irlanda, Estônia, Áustria, Austrália, Bélgica, Islândia, Polônia, Dinamarca, Alemanha, França, Finlândia, Coreia do Sul, Luxemburgo, Canadá, República Tcheca, Países Baixos, Estados Unidos, México, Noruega, Reino Unido, Chile, Portugal, Japão, Suécia, Suíça, Eslováquia, Eslovênia, Turquia, Espanha, Grécia, Nova Zelândia, Hungria, Israel, Itália e Letônia.
União Europeia: Alemanha, Áustria, Bélgica, Bulgária, Chipre, Dinamarca, Eslováquia, Eslovénia, Espanha, Estónia, Finlândia, França, Grécia, Hungria, Irlanda, Itália, Letónia, Lituânia, Luxemburgo, Malta, Países Baixos, Polónia, Portugal, Reino Unido, República Checa, Roménia, Suécia.
Reino Unido: Inglaterra, Escócia e País de Gales, Irlanda do Norte.

Nota. Fonte: Adaptado de "*Proteção de dados no Brasil e no mundo - Uma leitura do que vigora hoje, a importância da nova legislação e como as empresas e os entes públicos devem se preparar*", de KPMG, 2018, *44*, p.19

Não obstante, cabe a todas organizações, inclusas as de ensino, atentarem às diversas formas que a lei pode atingir seus processos de controle interno e gestão da informação, observando, inclusive, as questões éticas e jurídicas, especialmente ao que tange a responsabilidade civil, segurança do ambiente informático, privacidade e proteção de dados coletados e tratados durante a utilização de tais recursos (SIEEESP, 2018; Feferbaum & Lima, 2019).

A Lei estabelece um rol amplo a respeito do que é considerado tratamento de dados pessoais, a saber: "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. ” (Lei n. 13.709, 2018).

Diante disto, destaca-se, ainda, que a norma é aplicável a qualquer tratamento de dados pessoais realizado no território nacional ou destinado aos que aqui residem, independentemente da nacionalidade do titular dos dados ou do local em que o responsável pelo tratamento dos dados está localizado (SIEEESP, 2018).

Antes mesmo de tipificar o tratamento de dados pessoais, deve-se primordialmente entender o que são estes dados, segundo a LGPD, artigo 5º, inciso I, um dado pessoal é toda “informação relacionada à pessoa natural identificada ou identificável” (Lei n. 13.709, 2018). Infere-se, portanto, que a Lei adota um conceito amplo para “dados pessoais”, por meio do qual, as mais variadas informações são qualificadas como tal ou qualquer informação relacionada à pessoa identificada, como: dados biométricos, DNA ou um nome sem homônimos devem ser tratados como dados pessoais, assim como dados relacionados à pessoa, possivelmente, identificável, ou seja, aqueles dados que podem levar à identificação de uma pessoa, como: tipo sanguíneo, notas, esportes, práticas, meios de transporte utilizados, nome dos pais, ano letivo, e demais informações (Lei n. 13.709, 2018; Mulholland, 2018; SIEEESP, 2018).

Isto posto, é relevante observar que a Lei em seu artigo 5º, inciso II, distingue o conceito de dado pessoal sensível, como sendo:

> “. . . o dado pessoal 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” (Lei n. 13.709, 2018, p.2).

Nota-se, assim, que tais dados merecem atenção especial e ainda mais zelo e cuidado ao serem tratados, pois, por meio de tais dados pessoais, os titulares deles podem vir a ser discriminados, como dispõe artigo 11º da LGPD (SIEEESP, 2018).

Para compreender a norma em sentido amplo é salutar que o operador (responsável pelo tratamento de dados pessoais) se atente a boa-fé e aos princípios que norteiam a regulamentação, previstos junto ao artigo 6º da LGPD (Lei n. 13.709, 2018).

a) **Princípio da Finalidade**: determina que dado pessoal coletado deverá ser utilizado para o fim originariamente especificado ao usuário, sendo que qualquer alteração de sua finalidade deverá ser informada ao titular, inclusive se o dado for compartilhado com terceiros;
b) **Princípio da Adequação**: determina que o dado pessoal coletado deverá ser compatível com a finalidade informada ao titular;

c) **Princípio da Necessidade**: dispõe que a coleta deve se limitar ao mínimo de dados pessoais necessários para a realização de suas finalidades;
d) **Princípio do Livre Acesso**: para que os titulares dos dados possam consultar de forma gratuita e facilitada os dados pessoais coletados de sua titularidade;
e) **Princípio da Qualidade dos Dados**: que garante aos titulares que o tratamento dos dados pessoais ocorrerá com base em informações exatas, claras, relevantes e atualizadas dos dados, de acordo com a necessidade e finalidade de seu tratamento
f) **Princípio da Transparência**: garante aos titulares do tratamento de dados ser de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
g) **Princípio da Segurança**: utilização de medidas técnicas e administrativas para proteger de forma efetiva os dados coletados, tanto para se evitar a sua alteração como destruição;
h) **Princípio da Prevenção**: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
i) **Princípio da Não Discriminação**: o qual por meio de tal princípio, veda a utilização de dados pessoais para fins discriminatórios ou ilícitos;
j) **Princípio da Responsabilização e Prestação de Contas**: segundo o qual as empresas que realizam o tratamento de dados pessoais devem ser responsáveis por tal conduta de forma clara, assim como, devem prestar contas para os titulares dos dados pessoais a respeito do impacto que tal coleta representa.

Portanto, destaca-se que o tratamento de dados pessoais e as normas dispostas à LGPD estão diretamente atreladas às atividades das instituições de ensino, assim como de qualquer empresa, e devem ser objeto de adequação (Coffman, 2014; Feferbaum & Lima, 2019; SIEEESP, 2018).

A norma ainda contempla os dados pessoais de menores, alinhando-se e complementando as disposições do Estatuto da Criança e Adolescente (ECA), que promulgado há 28 (vinte e oito) anos não previa questões trazidas por novas tecnologias, e o Marco Legal da Primeira Infância onde em seu artigo 4º, inciso IX determinava que promover a formação da cultura de proteção e promoção da criança, com apoio dos meios de comunicação social (Lei n.13.257, 2016; Maldonado, Blum, & Borelli 2019; SIEEESP, 2018).

Deste modo, a LGPD, em respeito ao princípio universal do melhor interesse da criança (menores de 12 anos), e com base na falta de discernimento destes diante dos riscos,

consequências e garantias atreladas aos seus dados pessoais, regulamenta de forma específica, artigo 14, que "O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado em seu melhor interesse, nos termos deste artigo e da legislação pertinente", ou seja, deverá ser realizado com o consentimento específico e em destaque dado por, pelo menos, um dos pais ou pelo responsável legal (Lei n.13.709, 2018; Machado Meyer, 2018; SIEEESP, 2018).

Posto isto, junto ao artigo 5º, inciso XII, entende-se por consentimento "toda manifestação livre, informada e inequívoca pela qual o titular dos dados (país e-ou responsáveis legais), concordam com o tratamento de dados pessoais de crianças e de adolescentes, para uma finalidade determinada", devendo ser escrito ou expresso por meio que manifeste a inequívoca demonstração de vontade do titular ou responsável (Bioni, 2019; Pinheiro, 2018).

A base jurídica do consentimento exige total acessibilidade e transparência na forma de se obter os dados, ou seja, é fundamental que os propósitos da coleta estejam claramente definidos, de forma que o consentimento possa ser conscientemente dado pelo seu titular ou responsável legal, para cada uma das finalidades previstas (Bioni, 2019; Maldonado, Blum, & Borelli 2019; Pinheiro, 2018).

Contudo, o consentimento, por si só, não afasta em absoluto a responsabilidade de avaliar todos os riscos e prejuízos potenciais decorrentes do processamento destes dados, frisa-se, portanto, que o legislador não autoriza a coleta de dados pessoais para fins não autorizados pelos responsáveis, devendo estes serem consultados novamente caso surja uma nova finalidade para seu uso (Bioni, 2019; Mulholland, 2018; SIEEESP, 2018).

Infere-se, portanto, que ao dar especial atenção ao uso dos dados pessoais de crianças e adolescentes, a Lei Geral de Proteção de Dados visa assegurar o direito à proteção de dados pessoais, como fundamental inerente à sociedade da informação e do mundo conectado (Coffman, 2014; SIEEESP, 2018).

Compreendida a necessidade dos dados pessoais, e seu expresso consentimento de uso, para se formalizar qualquer relação contratual, sejam de trabalho entre a instituição de ensino e seus colaboradores (funcionários, professores, prestadores de serviços, etc.), sejam os contratos de prestação de serviços educacionais entre a instituição e os titulares de dados ou seus responsáveis legais, seja, entre a IES e empresas parceiras sob qualquer fim (Bioni, 2019; Coffman, 2014; Pinheiro, 2018; SIEEESP, 2018).

A lei caracteriza o Consentimento, enquanto apoio legal para o tratamento de dados, das seguintes formas (Lei n. 13.709, 2018):

a) Deve ser livre, informado e inequívoco, para uma finalidade determinada (art. 5º, inciso XII);
b) Deve constar de cláusula destacada das demais (art. 8º, parágrafo 1º);
c) Deve referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas (art. 8º, parágrafo 4º);
d) Será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca (art. 9º, parágrafo 1º).

Instituições de ensino obtêm de seus contratantes dados pessoais e sensíveis, que não necessariamente são imprescindíveis ao cumprimento contratual, tais como: origem étnica/racial de seus alunos; informações sobre crenças religiosas além de outras informações que relacionam o resultado de avaliações com o desempenho acadêmico do aluno, relatórios que podem rotular, identificar o aluno ou torná-lo identificável, portanto, devem ser exclusivamente direcionados ao aluno e aos seus responsáveis legais (Coffman, 2014). Tais dados devem ser tratados com cautela e conformidade com a LGPD, que não proíbe a coleta, mas exige transparência, expresso consentimento e cuidado junto a salvaguarda destes dados (Feferbaum & Lima, 2019; SIEEESP, 2018).

Sites, portais, blogs perfis institucionais em redes sociais, ou seja, toda informação veiculada em meios digitais, devem contemplar tão somente informações gerais e nunca relacionadas a um membro, determinado aluno ou seu responsável, sendo importante relembrar que a imagem e dados pessoais dos alunos em tais meios somente deverão ser utilizadas sob expressa autorização dos responsáveis (SIEEESP, 2018).

Portanto estes dados devem ser manipulados com extrema cautela, visto que sua violação pode gerar impacto reputacional na imagem da instituição, assim como a evasão de alunos e consequentes perdas financeiras, de modo que é de suma importância que a escola esteja comprovadamente engajada em ações para o devido enquadramento à lei e demais normas de proteção aos direitos da criança e do adolescente (Ariff et al., 2014; Coffman, 2014; Pinheiro, 2018).

Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas na Lei, sujeitam-se às seguintes sanções administrativas aplicáveis pela autoridade nacional de proteção e dados (ANPD), observadas junto a tabela 10, abaixo, que sintetiza as principais penalidades previstas (KPMG, 2018; Lei n. 13.709, 2018; Maldonodo, Blum, & Borelli, 2019; Pinheiro, 2018).

Tabela 10
LGDP: Sanções Administrativas Previstas

Inciso	Art. 52: Sanções Administrativas
I	advertência, com indicação de prazo para adoção de medidas corretivas;
II	multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
III	multa diária, observado o limite total a que se refere o inciso II;
IV	publicitação da infração após devidamente apurada e confirmada a sua ocorrência;
V	bloqueio dos dados pessoais a que se refere a infração até a sua regularização;
VI	eliminação dos dados pessoais a que se refere a infração;

Nota. Fonte: Adaptado de "*Lei n. 13.709*", 2018, recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Em dezembro de 2018, por meio de uma medida provisória (MP), a data da vigência da lei foi prorrogada para agosto de 2020, desta forma, empresas e o poder público ganham mais seis meses para se adaptarem, a mesma MP, ainda resgata a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei (Medida Provisória n. 869, 2018).

Adequar-se aos novos tempos será a melhor maneira das empresas atuantes no Brasil não serem atingidas pelas penalidades previstas e referido ajuste demandará ampliação de investimentos em tecnologia além da contratação de profissionais ou parceiros habilitados, traduzindo-se em investimento de tempo, dinheiro e energia.

Todavia, a nova lei não cria regras pontuais que poderiam, no futuro, tornar-se inadequadas, ao contrário, seus princípios alinham-se ao que existe de mais moderno no mundo contemporâneo, elevando o trato de dados no Brasil a patamares aptos a fazer frente aos maiores avanços tecnológicos (KPMG, 2018).

Diante da incerteza de impactos, positivos e-ou negativos, potenciais ao segmento adotado, um diagnóstico preliminar junto a instituição lócus faz-se premente, com vistas ao entendimento dos riscos inerentes e dimensão do esforço requerido ao seu processo de adequação.

3 Metodologia de Pesquisa

O presente estudo aplica como metodologia a pesquisa intervencionista que propõe a participação do pesquisador junto ao pesquisado na busca de soluções, apoiadas sobre a literatura, para a organização, desta forma, aliando revisão teórica à modelos práticos e assim tornando-se um instrumento concreto de mudança.

Desta forma esta obra apropria-se de uma abordagem qualitativa por meio da metodologia de pesquisa intervencionista, a qual, contribui para a subjetividade das

informações, muitas vezes não mensuradas exclusivamente por dados quantitativos, contribuindo assim à revelação da visão de mundo dos indivíduos (Gil, 2002; Vergara, 2006)

Buscou-se o desenvolvimento de um modelo de adequação de uma instituição de ensino superior da cidade de São Paulo à Lei Geral de Proteção de Dados do Brasil (Lei n. 13.709, 2018). A partir de uma revisão bibliográfica sobre Governança de TI, Controles Internos, Gestão de Riscos e a própria LGPD desenvolveu-se um modelo de intervenção que capta a situação atual, planeja e executa a intervenção e avalia os resultados, assim, aproximando perspectivas êmicas e éticas do trabalho pratico-acadêmico, permeado pelo rigor acadêmico previsto e evidenciando aspectos positivos da metodologia adotada (Atkinson & Shaffir, 1998; Baard, 2010).

3.1 Epistemologia de Bunge

Modelos científicos apresentam, em seu cerne, a avaliação dos processos de modelagem científica, em que, sua construção calcada em teorias gerais e objetivos-modelo não são suficientes se tais paradigmas não se submetem a um processo de validação que evidencie sua escala de validade, destarte, o caminho natural é o da contrastação empírica, entendida como um dos procedimentos primários da modelagem científica (Heidemann, Araujo, & Veit, 2016).

Segundo Bunge (1960), a reconstrução conceitual do mundo somente é possível por meio do empreendimento científico, assumido seu desenvolvimento paulatinamente mais amplo, profundo e detalhado, desta forma, alcançando no pensamento científico o único meio para compreensão e modelagem da realidade (Bunge, 1974).

Bunge (1960, 1974, 1983) propõe uma doutrina referente ao desenvolvimento científico, natureza e a tipologia da pesquisa em uma ciência social. Sua estrutura é construída sobre duas contribuições:

Primeiro, ele identifica dois tipos de programas na evolução do conhecimento científico, o programa de pesquisa em superfície e o programa de pesquisa em profundidade (Bunge, 1974). O programa de pesquisa na superfície envolve um crescimento no conhecimento de rotina. É um tipo de conhecimento prático, sem abrir mão do núcleo de suas crenças. Permite melhorar as teorias tradicionalmente aceitas de uma comunidade científica, resolvendo suas anomalias e aplicando-as a diversos campos. Já o programa de pesquisa aprofundada oferece um crescimento em larga escala de conhecimento. Ele fornece ideias substancialmente novas que sustentam novas visões e perspectivas a partir das informações disponíveis. Na história de uma ciência, existem períodos caracterizados pela predominância de um ou outro tipo de crescimento (Bunge, 1983).

Da perspectiva da Bunge, a pesquisa em ciências sociais pode ser definida como qualquer atividade ou trabalho realizado por um pesquisador com o objetivo de obter mais conhecimento sobre um fenômeno específico. Implica o uso de diversas versões teóricas para explicar, com mais ou menos sucesso, o fenômeno. A relação entre os sujeitos que lidam com o fenômeno acima mencionado no dia-a-dia também deve melhorar por meio de soluções, ideias, sistemas ou modelos técnicos (Bunge, 1974).

A modelização técnico-teórica de Bunge fornece uma fonte de informação e tratamento sobre lacunas, irregularidades ou peculiaridades que não foram tratadas nos projetos ou modelos utilitários empregados. Se o objetivo utilitário ou extrínseco da ciência for exagerado, aparecerá uma lacuna entre a atividade de pesquisa e a aplicação prática real, se os objetivos da ciência se concentrarem no conhecimento puro do sujeito em estudo (cognitivo), as soluções obtidas não permitirão obter maior controle sobre os diferentes problemas encontrados na prática, portanto, ambas as atividades devem ser desenvolvidas de maneira coordenada (Bunge, 1974, 1983).

Ainda que as teorias cientificas constituam o sistema central da Ciência, o entendimento da atividade científica moderna é fundamentado sobre o conceito de modelo (Bunge, 1974). Bunge, preconiza que os dois principais sentidos que devem ser considerados para o termo modelo, nas Ciências Fatuais da natureza e do homem, são: “o modelo enquanto representação esquemática de um objeto concreto e o modelo enquanto teoria relativa a esta idealização”.

Denominado como objeto-modelo, de um objeto (ou evento), concreto apresenta-se o primeiro sentido e o modelo teórico como segundo sentido, resume o entendimento do autor. Esse conceito, cujo protagonista é o objeto-modelo que lhe deu origem, é concebido como um sistema hipotético-dedutivo específico e deve ser representado por um conjunto de hipóteses e expressas de preferência em linguagem matemática. Mais adiante, será discutido como Bunge descreve a elaboração de modelos teóricos, também conhecidos como teorias específicas (Bunge, 1974).

Portanto, modelagem científica pode ser entendida como o abrangente processo de construção, validação, uso e revisão de modelos científicos, entendidos como representações simplificadas e idealizadas de sistemas, processos e fenômenos da natureza, aceitos por uma comunidade de cientistas (Brandão, Araujo, & Veit, 2011; Bunge, 1974; Develaki, 2007; Giere, Bickle, & Mauldin, 2006; Morgan & Morrison, 1999; Paty, 1995; Walliser, 1977).

Resumidamente o processo de modelagem científica sustenta-se sobre teorias gerais, que, hipoteticamente, não se pronunciam diretamente sobre a realidade, ao contemplarem

modelos conceituais, produzindo representações parciais da realidade (Brandão et al., 2011). Nas palavras de Bunge, o processo de modelagem:

> [...] deve-se distinguir as seguintes construções: o objeto-modelo "m" representando os traços-chave (ou supostos-chave) de um objeto concreto "r" (ou suposto concreto); o modelo teórico "Ts" especificando o comportamento e/ou o(s) mecanismo(s) interno(s) de "r" por meio de seu modelo "m"; e a teoria geral "Tg" acolhendo "Ts" (e muitas outras) e que deriva seu valor de verdade bem como sua utilidade de diversos modelos teóricos que podemos construir com o seu auxílio – mas jamais sem suposições e dados que a extravasam e recolhidos pelo objeto-modelo "m" (Bunge, 1974, p. 25).

A despeito do que preconiza o autor, é pertinente saber que diversas áreas do conhecimento ainda não apresentam teorias gerais e ideal maturidade de teórica, desta forma, a modelização tem início no extremo oposto, ou seja, a partir de hipóteses próximas dos dados empíricos derivados da observação e experimentação. Desta forma a modelagem de Bunge vem ao encontro do proposto pela pesquisa em que se pese as contribuições teóricas e práticas da observação e intervenção empírica colocada, com instâncias limítrofes dadas pela literatura de referência.

A tabela 12, abaixo, inspirada na modelagem de Bunge ilustra o mecanismo de modelagem científica, que relaciona elementos conceituais, "objetos-modelo", quando dispostos sobre teorias gerais, geram teorias específicas (Bunge, 1973; Pietrocola 1999):

Tabela 11

Situações a serem modeladas e modelos de Bunge

Situação a ser modelada	Objeto Modelo	Modelo teórico	Teoria Geral
Lua	Sólido esférico girando em torno do seu eixo, em rotação à volta de um ponto fixo, etc.	Teoria Lunar	Mecânica Clássica e Teoria Gravitacional
Luar	Onda eletromagnética polarizada plana	Equações de Maxwell para o vácuo	Eletromagnetismo Clássico
Pedaço gelo	Cadeia linear causal de contas	Mecânica estatística de cadeias causais	Mecânica Estatística
Cristal	Grade mais nuvem de elétrons	Teoria de Bloch	Mecânica Quântica

Nota. Fonte: Recuperado de "*Filosofia da Física"*, de M. Bunge, 1973, p. 53.

O objeto-modelo é uma representação de um objeto real, realidade observável, perceptível ou não, sendo este uma coisa[1] ou fato, nesta direção o modelo teórico e considerado um sistema hipotético-dedutivo capaz de gerar proposições plausíveis pois é comumente suportado por uma Teoria Geral que expressa o conhecimento sobre determinada realidade até então (Bunge, 1974).

[1] Elemento observado empiricamente junto a um ambiente real, realidade. (Bunge,1974)

Todavia, segundo o autor, modelos teóricos são aproximados e, portanto, parciais, desta forma, requerendo "objetos-modelo" para converter coisas concretas em imagens para alcançar a realidade. Assim, o termo modelo determina uma pluralidade de conceitos sob as teorias da natureza e do homem podendo assumir dois sentidos: a) enquanto representação esquemática de um objeto concreto e; b) enquanto teoria relativa a idealização de sistemas hipotético-dedutivos.

Assim a modelagem da realidade apoia-se em modelos conceituais e em seu processo de idealização permitindo-se elaborar um único objeto modelo sob a finalidade de representar uma classe inteira de objetos concretos ou esquematizar um único objeto concreto por meio de diversos modelos conceituais.

A figura 7, abaixo, expõe o axioma proposto por Bunge descrito anteriormente:

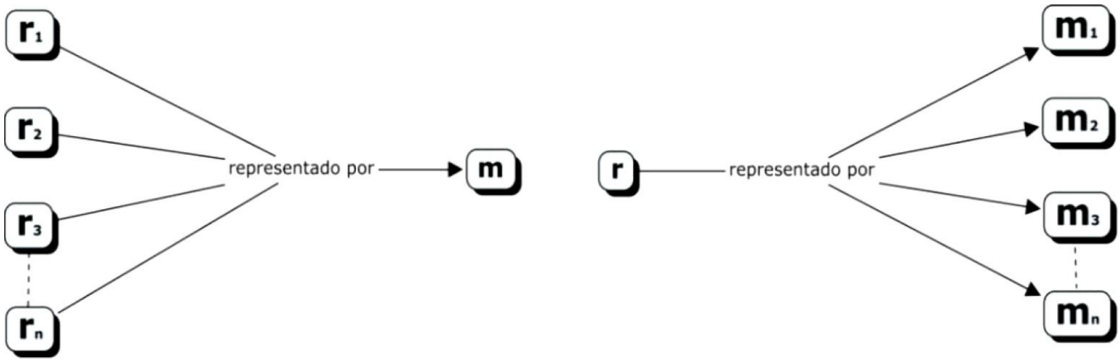

Figura 7. Esquemática da construção de modelos conceituais.

Nota. Fonte: Recuperado de "A modelagem científica vista como um campo conceitual", de R. V. Brandão, I. S. Araujo, & E. A. Veit, 2011, *Caderno Brasileiro de Ensino de Física, 28,* p.10.

À esquerda, "n" objetos concretos (r) distintos sendo representados por apenas um modelo conceitual (m); à direita, um objeto concreto (r) sendo representado por "n" modelos conceituais (m) distintos (Brandão et al., 2011).

Segundo Bunge o processo de teorização, consiste em trazer à realidade o plano conceitual, desta forma, podendo ser construídas teorias por meio de processos que investigam de forma esquemática a coisas e fatos, desta forma, construindo e entregando os "objetos-modelo" como representação máxima desta realidade.

Isto posto, o autor articula dois tipos de teorização: a) Teoria da Caixa Preta ou Teoria da Fenomenologia: construída por engenheiros para descrever certos sistemas elétricos, apresenta uma abordagem mais superficial considerando o comportamento sistêmico como unidade simples de entradas e saídas (*input* | *output*) sem observar o interior do mecanismo-meio, sem manipulação de variáveis internas, onde, apenas as externas seriam suficientes para

se atingir objetos-modelo ideais, e; b) Teoria da Caixa Translúcida ou Representacional: apresenta constructos hipotético-dedutivos com elementos que interferem nos mecanismos internos da "caixa", ou seja, "as variáveis internas do sistema, as quais, em sua linha limítrofe reagem a oscilação das variáveis externas, das entidades não observadas ainda pelo modelo, dos eventos e suas propriedades" (Bunge, 1974, p.18-25).

3.1.1 Modelo conceitual de Gestão de Riscos e Controles internos para uso e proteção de dados

Sobre a epistemologia brevemente apresentada do autor Mario Bunge e em consonância com sua proposta de teorização científica apresenta-se a modelização conceitual do *framework* de conformidade a Lei Geral de Proteção de Dados do Brasil em uma Instituição de Ensino Superior da cidade de São Paulo – SP, admitida para a pesquisa:

A tabela abaixo, 13, descreve a situação, apresentada pela pesquisa, a ser modelada, sobre a sistematização de Bunge:

Tabela 12
Situação de pesquisa a ser modelada

Situação a ser modelada	Objeto Modelo	Modelo teórico	Teoria Geral
Gestão de Riscos e Controles Internos no uso e proteção de dados pessoais	Instituições de Ensino	Modelo Conceitual Bunge & Catelli	Controles Internos e Gestão de Riscos Governança Coorporativa Civil Law, Constituição Federal, Código Civil e Código de Defesa do Consumidor

Nota: Adaptado de "*Filosofia da Física"*, de M. Bunge, 1973, p. 53.

Considerada a sucessão de variáveis internas indispensáveis a ideal operação do "objeto-modelo" proposto e ainda sua inter-relação com o ambiente externo (macro ambiente) que o permeiam, além de seu caráter hipotético-dedutivo, perante ao fato da lei ainda estar em *Vacatio Legis*[2] e assim ainda não haver disposições oficiais de instância governamental (ANPD[3]) pertinentes a sua adequação e fiscalização, a construção adotada é da Teoria da Caixa Translúcida ou Teoria Representacional:

- Teoria da Caixa Translúcida ou Representacional: apresenta constructos hipotético-dedutivos com elementos que interferem nos mecanismos internos da "caixa", ou seja, as variáveis internas do sistema, as quais, em sua linha limítrofe reagem a oscilação das variáveis externas, das entidades não observadas ainda pelo modelo, dos eventos e suas propriedades (Bunge, 1974, pp.18-25).

[2] Vacatio Legis ocorre quando nova lei foi publicada, mas ainda não se encontra em vigor;
[6.] Agência Nacional de Proteção de Dados (Art.38 – LGPD);

Estabelecidas as linhas limítrofes do modelo conceitual pela obra de Bunge, seu interior compõe-se disciplinado pelos modelos decisórios da gestão econômica (GECON) em que se prevê a otimização dos resultados da organização por meio da melhoria da produtividade e eficiência operacional (Catelli, 1999).

Sobre esta óptica a tomada decisória, em nível institucional, apresenta ideal relação entre os ciclos gerenciais de planejamento (estratégico e operacional), execução e controle abrangendo o relacionamento da empresa com o ambiente externo e tencionando a maximização da eficiência processual em questão (Catelli, 1999; Gerreiro, 1989).

Diante do exposto, apresenta-se a figura 8:

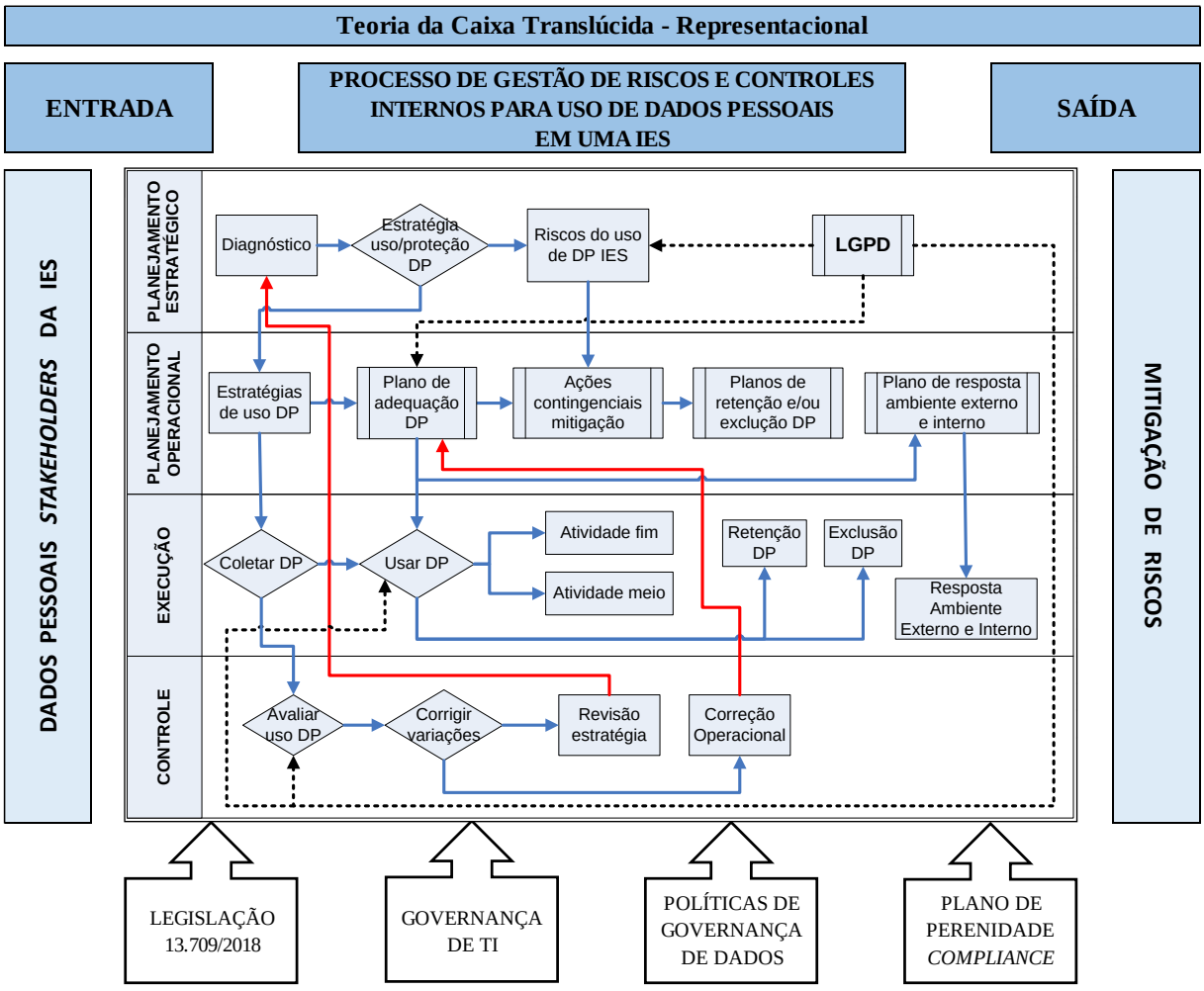

Figura 8. Modelo Conceitual de compliance à LGPD a luz de Bunge.

Delimitado pelo filósofo Carlos Bunge e sua Teoria Representacional, Caixa Translúcida, o modelo em seu cerne apresenta a estrutura de decisão da Gestão Econômica (GECON) preconizada pelo Professor Armando Catelli, (Bunge, 1974; Catelli, 1999).

O modelo compreende o processo de gestão de riscos e controles internos para o uso e proteção de dados pessoais dos titulares de dados de uma Instituição de Ensino Superior,

apresentando como entrada os dados pessoais dos *stakeholders* da IES e saída o tratamento do risco relacionado, aqui descrito como “mitigação”, ainda na linha limítrofe expressam-se variáveis internas e externas ao modelo que o afetam diretamente: Legislação, Governança e perenidade do estado de conformidade.

Diante da complexidade institucional e do próprio processo de gestão dos riscos relacionados, adicionando o impacto das variáveis internas e externas ao modelo, torna-se premente a necessidade de um framework que ajuíze as relações instituição, conformidade e macro ambiente, facilitando o entendimento da realidade, mensurando as alternativas de ação dedicadas ao processo em questão e promovendo seu controle e gerenciamento dos riscos.

Com leitura descendente, articula-se o primeiro nível: Planejamento Estratégico, onde sobre a caracterização da necessidade de decisão e o diagnóstico da instituição, definir-se-ão as estratégias de uso, ou não, de dados pessoais e os riscos deste uso, caso ocorra. Ainda nesta fase localiza-se a LGPD evidenciando assim o caráter estratégico que a legislação assume no processo.

Por conseguinte, o Planejamento Operacional, ocorre derivado do seu antecessor desdobrando as estratégias de uso dos dados pessoais em planos de ação, de adequação e de conformidade desta utilização ajustando-a ao disposto pela lei, desenvolvendo ações de resposta aos riscos mapeados, ao ambiente externo, sejam aos titulares de dados ou a ANPD e por fim desenvolvendo planos de retenção e exclusão destes dados.

O nível da Execução é onde ocorre a ação, abordado pelo Planejamento Estratégico e desenvolvido pelo Planejamento Operacional, neste momento ocorre o tratamento de fato (coleta e uso) de dados pessoais, orientados as atividades fim e meio, a execução dos planos de retenção e exclusão destes dados outrora desenhados junto a camada acima e ainda as respostas aos titulares e à autoridade nacional.

Não menos significativa a etapa do Controle ocorre sob o objetivo de avaliar o atual uso de dados pessoais da IES, ou seja, observando com periodicidade adequada a fase anterior, Execução, mapeiam-se conflitos e não conformidades existentes junto a este tratamento à luz da Lei Geral de Proteção de Dados e apontam-se ações de revisão de estratégia, junto ao Planejamento Estratégico e, ou correções operacionais residentes no Planejamento Operacional quando necessário.

3.2 IES lócus – Características relevantes

3.2.1 Histórico

Referência na área de Gestão de Negócios através do Pioneirismo e Excelência a serviço do desenvolvimento do país, são as marcas da IES lócus desta pesquisa. Criada por visionários de duas ilustres famílias em 1902, que enxergaram a necessidade de formação de profissionais contadores e guar-livros para a gestão das organizações, fator-chave para o aumento da produtividade e, consequentemente, do padrão de vida da população.

A instituição também foi a primeira a abrir os cursos superiores em Economia e em Contabilidade no país, atualmente oferece graduação, bacharelado, nas áreas de Administração, Ciências Contábeis, Ciências Econômicas, Publicidade e Propaganda, Relações Internacionais, Relações Públicas e Secretariado Executivo Trilíngue. Na Pós-Graduação Lato Sensu, são oferecidos cursos ligados às áreas de Gestão, Finanças e MBA com foco no desenvolvimento profissional. Na Pós-Graduação Stricto Sensu são oferecidos o Mestrado em Ciências Contábeis e o Profissional em Administração.

Concomitante ao Ensino Médio, a unidade do Colégio oferece Ensino Tradicional, bilíngue com certificação dupla Brasil–Canadá, e Técnico em diversas áreas, desde o técnico em Administração até o em Programação de Jogos Digitais, percorrendo Comercio Exterior, Multimídia, Hospedagem, Informática, Meio Ambiente, Produção de Áudio e Vídeo, Publicidade e, mais recentemente, Inteligência Artificial, sendo este o primeiro curso, desta modalidade, do país.

Composta por três Campi distribuídos pela cidade de São Paulo: Liberdade, Largo São Francisco e Pinheiros, ao longo dos anos, acumulou reconhecimento da qualidade de seus cursos, por meio de uma série de entidades, como o Índice Geral de Cursos (IGC), o qual seguidamente coloca a Instituição em destaque posicionando a IES entre as 1% das instituições privadas mais bem classificadas e entre os 2% das instituições públicas e privadas melhor classificadas de todo o Brasil.

A mídia especializada também a destaca, o Guia do Estudante, da Editora Abril, atribuindo o prêmio de melhor Centro Universitário do Brasil consecutivamente entre 2006 e 2008. Na edição de 2015 a 2019, todos os cursos da instituição foram estrelados.

Nesta direção, a excelência do trabalho educacional realizado pela Instituição também se expressa através do Prêmio Nacional de Gestão Educacional (PNGE) onde recebeu três vezes o “prêmio ouro”, duas vezes o “prêmio prata” e foi finalista em mais uma edição. Em tempo, A IES é uma das seis instituições em todo o país a ter seu MBA credenciado com o “padrão

global" da Associação Nacional de MBA (ANAMBA), demonstrando que o curso atende critérios internacionais de qualidade no ensino executivo. A Pós-Graduação conta, ainda, com premiações da revista Você S/A. Sua revista acadêmica, disseminadora da pesquisa acadêmica de ponta, tem uma das avaliações mais elevadas do Qualis, sistema brasileiro de avaliação de periódicos, mantido pela Coordenação de Aperfeiçoamento de Pessoal de Nível Superior – CAPES: A2. Outro indicador em que a revista é bem avaliada é o Journal Citation Reports (JCR) com fator de impacto de 0,875, o mais alto em periódicos de *management* da américa latina.

A gestão é baseada em pilares fundamentais, como foco no desenvolvimento dos alunos e manutenção de um corpo docente altamente qualificado, tanto no que se refere à formação acadêmica, quanto à experiência profissional e um ambiente meritocrático.

Para atingir seus objetivos, a Instituição também procura estabelecer parcerias com organizações de excelência, a exemplo da Cultura Inglesa, da Endeavor, entidade voltada para o fomento ao empreendedorismo, e do Bloomberg Institute. Atenta ao desejo de seus alunos em buscar experiências internacionais à necessidade de internacionalizar suas atividades, tem estabelecido parcerias com universidades localizadas nos Estados Unidos, Europa e América Latina.

3.2.2 Missão, Visão e Valores

Visão:

"Ser um centro de excelência em ensino e geração de conhecimento na área de negócios associando o rigor científico à aplicação dos conhecimentos e formando profissionais com princípios éticos transformadores do processo social, com visão humanística, crítica e reflexiva. "

Missão:

- ✓ Formar profissionais de nível superior, nas diferentes áreas de conhecimento, para participar no desenvolvimento da sociedade brasileira.
- ✓ Promover a pesquisa e a iniciação científica, visando colaborar no avanço da ciência e da cultura.
- ✓ Promover a extensão, facultada a participação da comunidade, para difundir as conquistas e os benefícios resultantes da produção científica e das pesquisas realizadas na Instituição.
- ✓ Estimular a criação cultural, por meio da promoção de eventos diversificados.
- ✓ Prestar serviços especializados à comunidade.

- ✓ Promover o aperfeiçoamento cultural, técnico, científico e profissional.

Valores:

- ✓ Competência técnica
- ✓ Senso crítico
- ✓ Atitude empreendedora
- ✓ Comportamento ético
- ✓ Autoconfiança

Desenvolver atividades para que os alunos incorporem esses valores como cidadãos e profissionais que irão colaborar com o desenvolvimento da sociedade por meio de sua competência e produtividade.

3.1.3 Organogramas

O primeiro organograma representa a organização hierárquica funcional da alta gestão, *board*, da IES, composta por seus conselhos administrativos, universitários, fiscais e Reitoria:

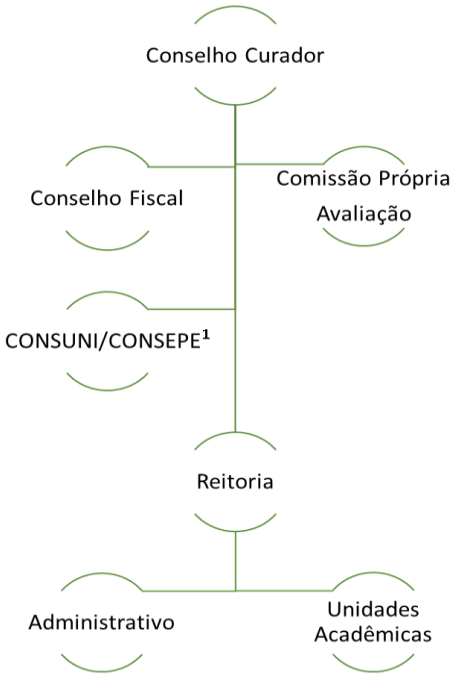

Figura 9. Organograma IES – Board

*Nota.*1.CONSUNI: Conselho Universitário; CONSEPE: Conselho Superior de Ensino, Pesquisa e Extensão.

Subordinado do Vice-Reitor da IES, o segundo organograma, descreve a estrutura hierárquico funcional da área administrava da instituição, ou seja, a empresa dentro da escola com departamentos técnico-administrativos e contábeis, semelhantemente a arcabouços de empresas de outros segmentos de mercado, que não o educacional:

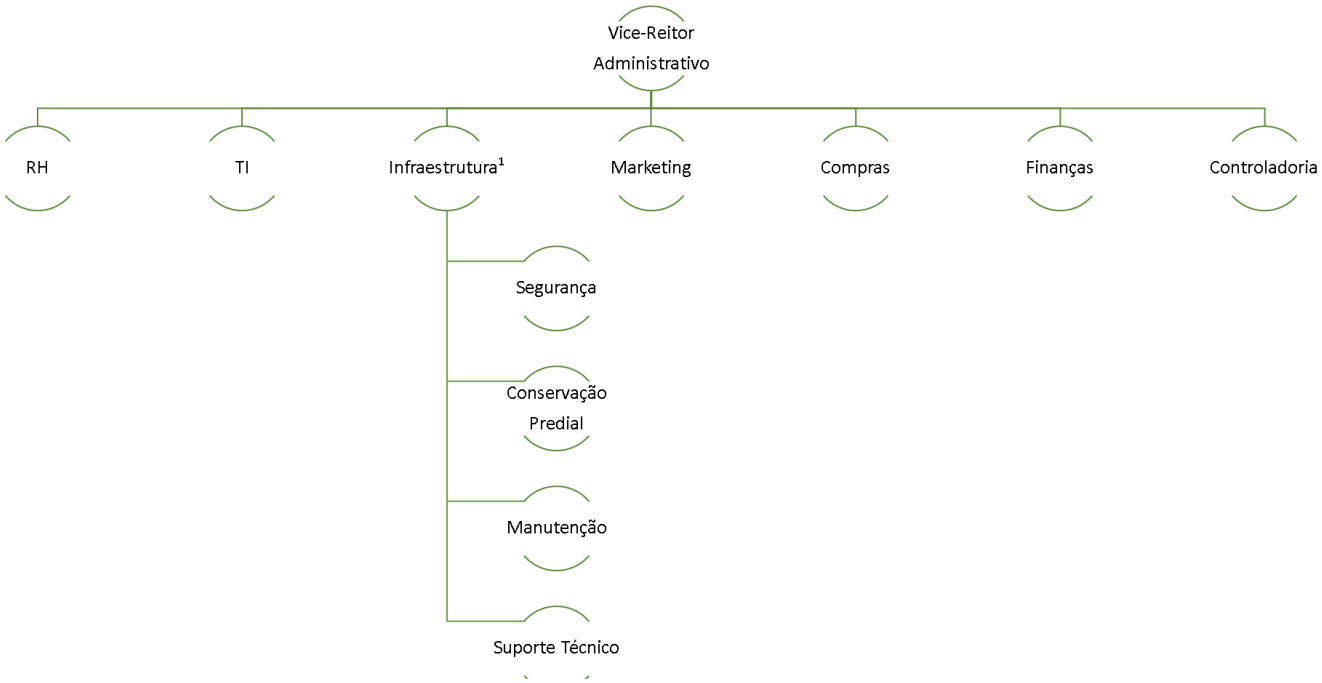

Figura 10. Organograma IES - Administrativo

*Nota.*1. Concatena áreas de *Facilities* (Segurança, Conservação Predial e Manutenção) e Infraestrutura de TI (Suporte Técnico) incluindo Segurança da Informação e de Redes de Computadores.

O terceiro e último organograma apresenta a estrutura hierárquica, formal e funcional da IES enquanto Centro Universitário, ou seja, ajuíza acerca da organização acadêmica, suas unidades de negócio: Colégio, Graduação, Pós (Lato e Stricto) e Extensão–EAD representadas por suas respectivas pró-reitoras, dispondo suas composições e fragmentos além das demais unidades dedicadas ao apoio acadêmico ao aluno como Biblioteca e Central de Atendimento ao aluno. Nesta dimensão do escopo institucional observa-se também a unidade dedicada ao Periódico Científico da instituição.

A Estrutura organizacional IES é especificada em seu Estatuto e a autonomia acadêmica é assegurada na medida em que os representantes docentes no CONSUNI têm maioria na sua composição e são escolhidos pelos seus pares. Compõem o CONSUNI o Reitor, seu Presidente, o Vice-Reitor, os Pró-Reitores, os representantes dos Professores, o representante do Corpo Técnico-Administrativo, o representante dos Alunos e o da Comunidade.

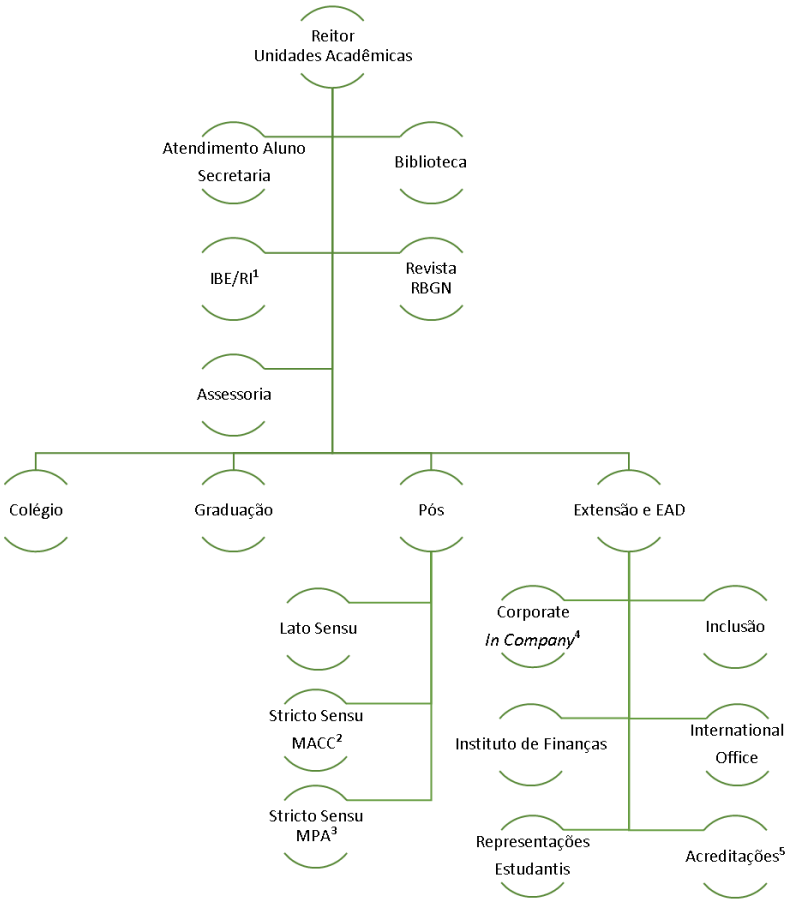

Figura 11. Organograma IES – Acadêmico.
*Nota.*1. IBE/RI: Programa de bolsas de estudos Ibero Americanas; 2. MACC: Mestrado Acadêmico em Ciências Contábeis; 3. MPA: Mestrado Profissional em Administração; 4. Unidade de Cursos "In Company"; 5. Unidade dedicada ao processo de adequação ao AACSB (The Association to Advance Collegiate Schools of Business).

3.1.4 Compliance Educacional & LGPD

Todos os setores da economia, de alguma forma e grau de intensidade submetem-se aos critérios de órgão regulares, seja, para avaliar sua qualidade destilada em forma de indicadores que mensuram a eficiência operacional até seus resultados, seja, para operar no segmento de ação escolhido adotado. O segmento educacional, não é distinto, especificamente o setor de educação superior privada do pais responde também responde a órgãos regulamentadores (Dimaggio & Powell, 1983).

De acordo com informações do Ministério da Educação (http://portal.mec.gov.br/secretaria-de-regulacao-e-supervisao-da-educacao-superior-seres, recuperado em 2 de janeiro de 2020), a Secretaria de Regulação e Supervisão da Educação Superior (Seres) é responsável pela formulação de políticas para a regulação e a supervisão de Instituições de Educação Superior (IES), públicas e privadas, pertencentes ao sistema federal de educação superior. A Seres foi criada em 17/4/2011 pelo Decreto nº 7.480/2011, absorvendo

competências antes da Sesu (Secretaria de Educação Superior), da Setec (Secretaria de Educação Profissional e Tecnológica) e da extinta Seed (Secretaria Estadual de Educação) do Ministério da Educação. É da sua alçada autorizar, reconhecer e renovar o reconhecimento de cursos de graduação (bacharelado, licenciatura e tecnológico) e de pós-graduação lato sensu, todos na modalidade presencial ou a distância. A Seres também é responsável pela Certificação de Entidades Beneficentes de Assistência Social na Área de Educação (Cebas-Educação). Entre outras atribuições, cabe à Seres também emitir parecer nos processos de credenciamento e recredenciamento de instituições de educação superior e supervisioná-las, bem como os cursos de graduação e sequenciais, com vistas ao cumprimento da legislação educacional e à melhoria da qualidade de educação superior. Também gerencia o *e*-MEC, sistema público de informações cadastrais em âmbito nacional dos cursos e instituições de educação superior promovido pelo Decreto nº 7.690 de 2012 e, posteriormente, pelo Decreto nº 8.066 de 2013 (Portaria n. 1342, 2012).

A este ambiente regulatório alia-se a legislação de proteção de dados, Lei nº 13.709/2018, que regimenta o tratamento de dados pessoais dos titulares de dados das empresas públicas e privadas nacionais e, portanto, as Instituições de Ensino Superior.

A Lei Geral da Proteção de Dados do Brasil é um marco normativo de grande impacto para todas as instituições privadas ou públicas do pais, que estejam ao seu alcance, portanto para garantir a exequibilidade da dimensão prática da pesquisa, considerando o tempo hábil para tal e a entrega de contribuições relevantes o framework proposto para uso e proteção de dados pessoais compreenderá o segmento ou unidade institucional mais exposta à legislação em estudo.

3.1.5 Atores IES & LGPD

O artigo 5 da lei 13.709/2018 apresenta em seu *caput* os elementos e termos utilizados no contexto dos dados pessoais com seus correspondentes conceitos, os quais são aqui abordados parcialmente com o objetivo de delimitar os principais elementos envolvidos com o escopo da lei junto a IES Lócus, presentemente tratados como “atores”.

A tabela 16, a seguir, articula o elemento ou termo, sua especificação da lei de proteção de dados, artigo 5 e seu representante ou ator junto a IES Lócus

Tabela 13
Atores IES e LGPD – Artigo 5

Inciso	Elemento Termo	Especificação	Ator(es) - IES
V	Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;	Alunos, funcionários, prestadores de serviço, professores, parceiros, visitantes e ex-alunos;
VI	Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;	IES Lócus: Reitor e Vice Reitor;
VII	Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;	Parceiros de negócios do Controlador: IES;
	Co-Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do operador;	Parceiros de negócios dos Operadores;
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);	Ainda não definido pela Gestão da IES;

A quantidade de Operadores variará de entre as organizações de acordo com o volume de parceiros que o Controlador possuir e estes deverão ter seu enlace organizacional balizado de forma tal que se garanta a proteção e privacidade dos dados pessoais relacionados bem como a responsabilização solidária caso estejam envolvidos em qualquer infração da lei, conforme previsto no artigo 42, parágrafo 1, inciso 1.

Não abordado pela lei brasileira, todavia, considerada a relação entre os Operadores com seus parceiros de negócio e os atuais modelos de uso de serviços de dados, o Co-Operador de Dados, é um elemento comum neste tipo de tratamento. Este "ator" surge toda vez que um Operador terceirizar os dados do Controlador para qualquer outro parceiro. Exemplo: hospedar e, ou armazenar os dados do Controlador fora de sua estrutura em *Cloud Computing*[4].

3.2 Pesquisa intervencionista

O ponto de ignição da pesquisa intervencionista é a visualização de um modelo ideal de produção com contribuições que não são apenas relevantes na prática, mas também teoricamente significativas, o que implica que um pesquisador intervencionista tem que ser eficaz nos domínios êmico e ético (Suomala, Lyly-Yrjänäinen, & Lukka, 2014; Suomala et al., 2017).

[4] *Cloud computing* ou computação em nuvem é a entrega da computação como um serviço ao invés de um produto, onde recursos compartilhados, software e informações são fornecidas, permitindo o acesso através de qualquer dispositivo conectado à Internet.

Um crescente entendimento na academia esclarece que a pesquisa científica pode ser conduzida por métodos intervencionistas e não intervencionistas (Lukka, 2005; Jönsson & Lukka, 2007) e embora parte da literatura sobre enfatize o objetivo de produzir soluções teoricamente fundamentadas para problemas práticos (Kasanen, Lukka, & Siitonen, 1993; Mattessich, 1995), estudos recentes sublinham o propósito mais acadêmico de tal pesquisa, ou seja, a necessidade de também apresentar contribuições teóricas (Labro & Tuomela, 2003; Lukka, 2000, 2003; Jönsson & Lukka, 2007). Desta forma encorajando a geração de novos conhecimentos em processos colaborativos entre pesquisadores e profissionais (Van de Ven, 2007; Van de Ven & Johnson, 2006).

Em 2006, o Chartered Institute of Management Accountants (CIMA) anunciou sua Iniciativa junto a Pesquisa Intervencionista, fornecendo financiamento para projetos relacionados. Como parte desta iniciativa de pesquisa intervencionista, o CIMA financiou uma obra focada em experiências práticas na condução de pesquisas de mestrado intervencionistas (Suomala & Lyly-Yrjänäinen, 2012), a obra ajuizou as lições aprendidas durante os dez anos de colaboração de pesquisa intervencionista com parceiros da indústria, focando nos processos da pesquisa intervencionista, força de intervenção e principalmente na contribuição para os domínios práticos da Contabilidade (Suomala et al., 2017).

Recentemente, surge uma corrente de literatura que procura examinar o potencial de combinar uma abordagem intervencionista com certas lentes teóricas, como o construtivismo pragmático e teoria da rede de atores, a fim de aumentar o impacto teórico e a relevância da pesquisa contábil (Laine, Korhonen, Suomala, & Rantamaa, 2016; Lukka & Vinnari 2017; Rautiainen, Sippola, & Matto, 2017). De acordo com Suomala et al. (2014), os estudos recentes destacam que o pesquisador intervencionista deve ser interpretado como um ator, com um papel multifacetado e ativo, o qual evolui ao longo do tempo (Laine et al. 2016; Lukka & Vinnari 2017).

O debate em torno da pesquisa intervencionista enfatiza a importância de assegurar contribuições teóricas, não apenas construtos relevantes na prática (Jönsson & Lukka, 2007; Lukka & Vinnari, 2017; Scapens 2014; Suomala & Lyly-Yrjänäinen, 2012). Diante disto, a pesquisa intervencionista pode ser vista como uma ferramenta não só para contribuir para a teoria e prática, mas também para impactar a sociedade de maneira mais geral. Como apontado por Flyvbjerg (2001), as ciências sociais não devem se concentrar em fornecer um espelho teórico para a sociedade, mas sim prover uma sociedade com conhecimento suficiente que possa ser usado como insumo para o diálogo sobre desafios e soluções sociais atuais.

Jönsson e Lukka (2007), Lukka e Vinnari (2017) e Scapens (2014), discutem a relevância pragmática da pesquisa intervencionista apontando as seguintes contribuições:

(1) Benefício às práticas observadas junto as empresas participantes desses estudos;
(2) Benefícios às práticas dos próprios mecanismos de pesquisa em contextos semelhantes aos estudos publicados;
(3) Produção de teorias com relevante conteúdo para academia e mercado;
(4) Impacto positivo nas empresas que participam dessas investigações empíricas ou gerentes que se encontram em decisões semelhantes;
(5) Teorização, com relevância e não apenas pragmática, mas também potencial para impactar a sociedade;
(6) Impacto positivo na sociedade de forma mais ampla;

Destaca-se a necessidade de melhorar a integração e a comunicação entre pesquisa e prática contábil, portanto, permanecendo continuamente envolvido em desafiar, repensar e refinar os fundamentos paradigmáticos da pesquisa no sentido de maior relevância na prática e consonância com a metodologia intervencionista (Baldvinsdottir, Mitchell, & Norreklit, 2010; Lukka & Vinnari, 2017; Mitchell, 2002; Norreklit, Norreklit, & Mitchell, 2010; Scapens 2014).

As contribuições teóricas dos projetos intervencionistas tendem a emergir de processos dinâmicos, nos quais o pesquisador demonstra competência nos domínios teóricos e práticos, portanto, o pano de fundo em torno das intervenções, é a oportunidade para a troca de conhecimento entre pesquisadores e profissionais, proporcionando um caminho potencial para a produção de novos conhecimentos (Suomala et al., 2014).

A pesquisa intervencionista, é uma abordagem de estudo de caso longitudinal variado, na qual a observação participante ativa é usada como um ativo de pesquisa e a abordagem é intrusiva, uma vez que o pesquisador intencionalmente busca produzir impacto sobre o mundo a fim de obter conhecimento (Aken, 2004; Argyris, Putnam, & McLain Smith, 1985; Jönsson & Lukka, 2007; Lewin, 1946, 1948; Lukka, 2003; Schein, 1987).

Nesta metodologia, a distinção entre o êmico e o ético (Pike, 1954, 1967) é significativa, onde, o ponto de vista êmico refere-se ao estudo do comportamento humano dentro do sistema, enquanto que a perspectiva ética significa examiná-lo de fora. Como o pesquisador intervencionista é um participante ativo no curso de eventos em tempo real no campo, ele está fadado a adotar a perspectiva êmica com base nos problemas em questão (Suomala et al., 2014).

A comunidade na qual o pesquisador realiza o trabalho de campo o aceita como um membro competente e digno de confiança, um "*insider*" e essa aceitação é crucial não somente

para compreender os significados e ações dos atores no campo, mas também para permitir que o pesquisador se comunique e aja junto com eles (Jönsson & Lukka, 2007).

Embora a adoção da abordagem êmica seja fundamental da pesquisa intervencionista, esta constitui apenas um aspecto do estudo, o pesquisador também deve assumir a posição ética, vinculando suas descobertas a um quadro teórico e contribuir para seu desenvolvimento, argumenta-se, portanto, que o uso equilibrado das perspectivas êmicas e éticas é essencial para justificar o uso dessa abordagem de pesquisa (Jönsson & Lukka, 2007).

Diferentemente dos modelos metodológicos tradicionais onde a coleta de dados normalmente ocorre após a definição do tema, referencial teórico, metodologia e instrumentos de coleta adotados o trabalho aqui proposto vale-se de estratégias não convencionais como a pesquisa-ação ou pesquisa intervencionista onde a coleta ocorre potencialmente em paralelo as demais etapas anteriores do estudo (Martins & Theophilo, 2009, p. 85).

Consoante com Daniballe (2017), Lima (2019), Malmi, Jarvinen e Llilrank (2004), quando se produz conteúdo capaz de resolver problemas práticos, considera-se o interesse teórico e se a solução for bem sucedida pode-se inferir a existência de uma teoria da Contabilidade Gerencial suportando o feito, assim, buscando maior robustez a aplicação da pesquisa será utilizada uma proposta de framework que ilustra um roteiro com as etapas principais do processo para a elaboração de uma pesquisa intervencionista estruturada conforme descrito na Figura 12.

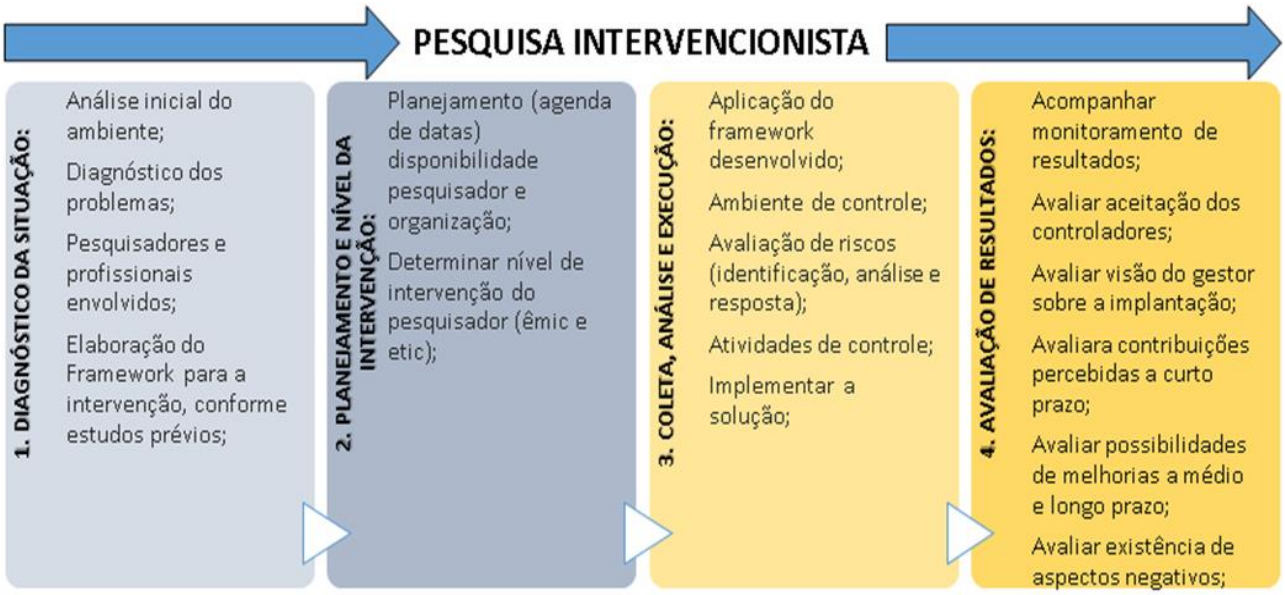

Figura 12. Framework da pesquisa intervencionista.

Nota. Fonte: Adaptado de "*Controles internos no 3º setor: uma proposta de framework para a casa Durval Paiva*. (Dissertação de Mestrado) ", de A. de A. P de Lima. Fundação Escola de Comércio Alvares Penteado – FECAP, São Paulo, SP, Brasil. 2019.

3.3 Diagnóstico da situação

3.3.1 Análise inicial do ambiente

Preliminarmente, realizaram-se contatos com a Instituição de Ensino Superior, com vistas a registrar o atual estágio de ciência sobre a lei 13.709/18 (LGPD), o grau de conformidade e as iniciativas de adequação correntes, nesta direção, mapearam-se ainda o presente estado de adesão as práticas de Governança de TI.

Procedeu-se, também, a análise e seleção de stakeholders diretamente envolvidos com a gestão da instituição e os representantes das unidades acadêmicas: ensino médio, graduação, pós-graduação Lato Sensu e Stricto Sensu, os quais foram submetidos a entrevistas semiestruturadas.

Concomitantemente, realizou-se, junto a literatura, um levantamento acerca de estudos que abordassem a aplicação de controles, medidas de conformidade e governança de TI em IES, examinando normas, processos de controle, melhores práticas, governança de TI (COBIT), além da própria Lei Geral de Proteção de Dados do Brasil.

3.3.1.1 Instrumento de coleta de dados – entrevista

Pretendendo atingir maior robustez no processo de coleta de dados e evidências, além de melhor captar a percepção dos stakeholders envolvidos sobre a temática relacionada, adotou-se o instrumento entrevistas semiestruturadas para o cumprimento desta fase da pesquisa. Entrevistas contribuem para o melhor domínio sobre a realidade e atuam como sustentáculo para as intervenções.

Consoante com Martins e Theóphilo (2016), a estratégia de pesquisa adotada determina o instrumento de coleta de dados, onde a coleta em trabalhos com estratégias convencionais ocorre após a definição do problema-tema, diante disto, e da característica desta fase de pesquisa, delimitada como convencional, adotou-se a entrevista como instrumento relacionado.

Mais que um simples colóquio a entrevista se trata de uma série de pergunta estruturadas de forma a coletar informações pertinentes e alinhadas com a literatura de referência (Cervo, Bervain, & Silva, 2007; Cooper & Schindler, 2003; Martins &Theóphilo, 2016).

Diante disto e do caráter teórico que a pesquisa intervencionista assume em alguns momentos de sua progressão, desenvolveu-se um quadro sinótico, disponível no **Apêndice A1**, compreendendo constructos dimensões, variáveis observáveis, assertivas perguntas e referências, desta forma alinhando a teoria disposta a percepção coletada dos stakeholders envolvidos.

3.3.2 Diagnóstico dos problemas

A finalidade desta etapa é, sobre a análise inicial do ambiente, identificar e qualificar o estágio atual observado, junto a instituição visitada, quanto ao processo de adequação à lei, elencando, de forma sistemática, os mais relevantes desvios e dificuldades observados. Ademais observou-se ainda os correntes níveis de Governança de TI presentes.

Diante disto, pode-se observar a ausência de um plano oficial de compliance a lei, um conhecimento raso sobre a legislação pertinente e um nível incipiente de adesão as práticas de Governança de TI.

3.3.3 Pesquisadores e profissionais envolvidos

Para execução da primeira etapa da pesquisa, foi realizado um contato inicial com a alta gestão da IES, Reitor e Vice-Reitor, quando foram esclarecidos propósitos, contribuições e demais detalhes esperados. Seguidamente submeteu-se uma solicitação formal de intervenção e após seu aceite os principais stakeholders administrativos e acadêmico da IES foram relacionados para posterior aplicação das entrevistas semiestruturadas e coleta inicial de dados.

Stakeholders administrativos: 6 colaboradores administrativos com funções de gestão, dos quais, 2 acumulam funções acadêmicas de gestão.

Stakeholder acadêmicos: 7 colaboradores acadêmicos com funções de gestão, dos quais 2 acumulam funções administrativas de gestão, e 4 representantes discentes (alunos) das unidades acadêmicas (Stricto Sensu, Lato Sensu, Graduação e Ensino Médio – Colégio).

Desta forma, contanto 17 stakeholders entrevistados: 6 administrativos, 7 academicos e 4 representantes discentes.

3.3.4 Elaboração do Framework para a intervenção

Diante dos achados iniciais orientados ao *compliance* da legislação que regulamenta a proteção de dados no pais, do grau atual de adesão da IES a Governança de TI propõe-se um *framework* disciplinado por Governança de TI, Controles Internos, Gestão de Riscos e a própria lei, com o objetivo de auxiliar no processo de entendimento e adequação a legislação que se impõe e ainda contribuir para a melhoria dos níveis atuais de Governança de TI.

Em tempo o *framework* propõe dois modelos: o primeiro Conceitual elaborado a luz da epistemologia de Bunge aqui apresentado no capítulo 2.5.1, e o segundo Funcional pautado sobre o modelo anterior, entretanto, com o viés prático do processo de adequação a lei, alinhando as ações pertinentes ao *compliance* a literatura de referência apontada para tal, observável junto ao tópico “3.3.2.3. Plano de Adequação e aplicação”.

3.4 Planejamento e nível da intervenção

3.4.1 Planejamento (agenda de datas) disponibilidade pesquisador e organização

Neste estágio apresentou-se a alta gestão da IES: Reitor (Superintendente Geral) e Vice-Reitor (Superintendente Adjunto) um cronograma com as atividades e datas relacionadas ao processo de intervenção, em que, se prevê ações de conformização a lei, derivados do framework desenvolvido e proposto.

A definição de datas será pautada por: a) disponibilidade dos envolvidos; b) impacto as atividades meio e fim da instituição; c) disponibilidade do pesquisador; d) sucessão das atividades de forma a se respeitar a ordem e prioridades destas;

3.4.2 Determinar nível de intervenção do pesquisador (êmic e etic)

A metodologia Intervencionista, registra uma distinção entre o êmico e o ético (Pike, 1954, 1967), onde, o ponto de vista êmico refere-se ao estudo do comportamento humano dentro do sistema, enquanto que a perspectiva ética significa examiná-lo de fora.

Assim, nesta fase, discute-se o nível do protocolo de intervenção adotado junto a instituição lócus e esta discussão determina a profundidade dos trabalhos que serão realizados em conformidade com as dimensões êmica e ética da literatura visitada.

Formulado sobre o Modelo Conceitual disponível no capítulo 2.5.1 do referencial teórico desta obra e sobre a tabulação e análise dos resultados obtidos na fase 1 da pesquisa intervencionista, vide capítulos 2.4, 4.2.1 e Apêndice B1 foi desenvolvido um Modelo Funcional de adequação e promoção do compliance a lei junto a IES lócus da intervenção.

3.4.2.1 Visão êmica

Trata-se de perspectiva interna do sistema verificado, considerando sua cultura, história e práticas, permitindo ao pesquisador intervencionista, uma visão mais próxima da realidade, por ser um participante ativo no curso de eventos em tempo real no campo, desta forma, adotando a perspectiva êmica com base nos problemas em questão (Suomala et al., 2014).

3.4.2.2 Visão ética

Embora a adoção da abordagem êmica seja fundamental da pesquisa intervencionista, esta constitui apenas um aspecto do estudo, o pesquisador também deve assumir a posição ética, visão externa do sistema estudado, vinculando suas descobertas a um quadro teórico e contribuir para seu desenvolvimento, argumenta-se, portanto, que o uso equilibrado das perspectivas

êmicas e éticas é essencial para justificar o uso dessa abordagem de pesquisa (Jönsson & Lukka, 2007).

3.4.2.3 Plano de adequação e aplicação

O plano proposto, orientado, pelo Modelo Conceitual e pela legislação de proteção de dados, além da literatura de referência apresenta componentes essenciais ao atingimento do *compliance* requerido. A imagem abaixo, figura 13, descreve os elementos e dimensões estabelecidos e direcionados ao processo de adequação buscado:

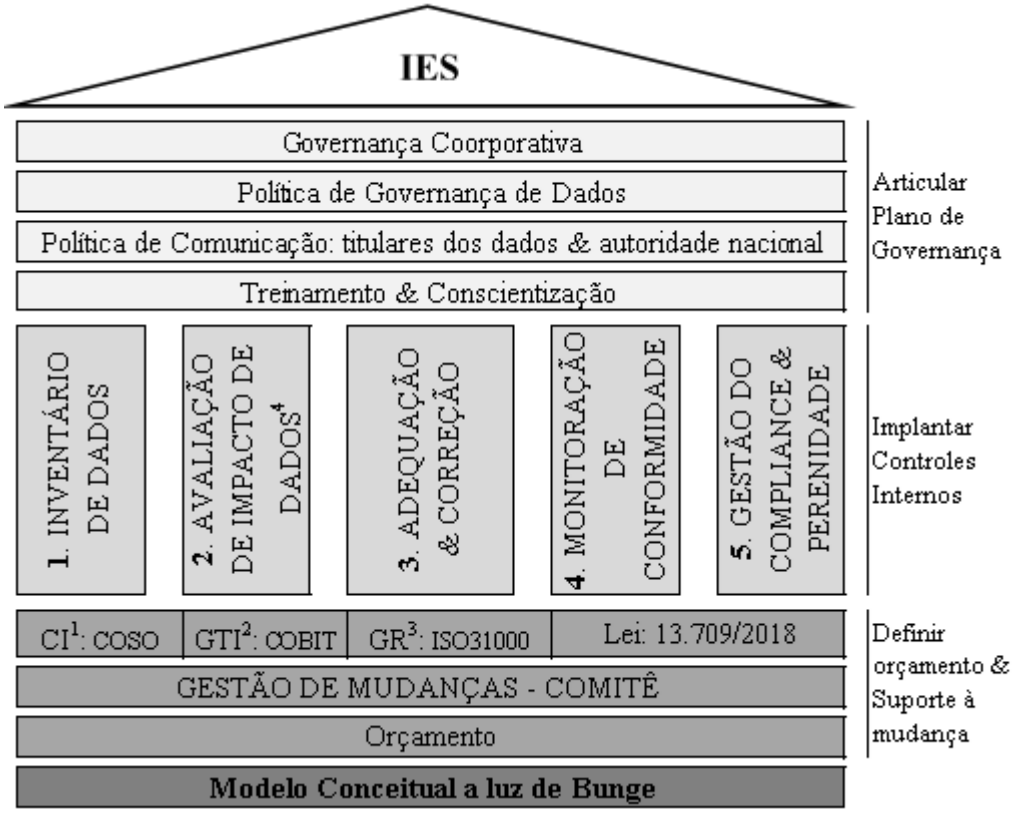

Figura 13. Plano de adequação a LGPD

Nota: 1. Controles Internos; 2. Governança de TI; 3. Gestão de Riscos; 4. Relatório de Impactos à Proteção de Dados (RIPD).

Desenvolvido sobre sua dimensão conceitual, o plano de adequação parte do pressuposto de que todo e qualquer processo de compliance produzirá impactos, operacionais e financeiros, à organização e estes devem estar previstos em orçamento, entretanto dada a característica metodológica adotada e objetivos da pesquisa a gestão orçamentária não será detalhada pelo modelo sendo apenas mencionado ao longo do escopo.

Fundamentalmente todo processo de *compliance* implica em mudanças, desta forma, quanto maior a dimensão da conformidade buscada e a força do isomorfismo coercitivo que se apresenta, maior a abrangência e imposição da mudança.

Sob o contexto organizacional toda mudança compreende alterações no comportamento humano, sejam: nos padrões de trabalho, rotinas, estruturas ou respostas a procedimentos e as pessoas, majoritariamente, são resistentes as forças de alteração de seu *status quo*, se opondo muitas vezes a alterações organizacionais, motivadas ora pela incapacidade de mudar, ora pela ausência de entendimento sobre os fatores motivadores da transformação (Armstrong, 1985; Herzog, 1991; Hong & Kim, 2002; Kirsch, Chelliah, & Parry, 2011; Kotter, 1995; Kotter, 2012; Wood, 1995).

Portanto o primeiro passo da adequação é atribuir a devida importância a gestão da mudança implícita no processo de *compliance* institucional, sendo assim, o modelo propõe a criação de um comitê com *stakeholders* que apoiarão as ações e atividades previstas. Elaborado sobre a obra seminal de Mitchell, Agle e Wood (1997) e Kotter (2012), propõe *stakeholders* relacionados de acordo com sua relevância na IES, no processo intervencionista e pautado sobre três pilares: poder, urgência e legitimidade:

a) Poder: refere-se a posicionamento hierárquico organizacional do stakeholder;
b) Urgência: qualifica a criticidade das ações dos stakeholders envolvidos na intervenção, comumente relacionada com fatores motivadores da mudança;
c) Legitimidade: aponta o caráter das ações enquanto desejáveis ou apropriadas no contexto organizacional;

Além de prover sustentação ao processo de mudança, o comitê, deterá também outras atribuições: a) legitimar os controles propostos; b) autorizar as incursões departamentais; c) reduzir barreiras burocráticas e processuais; d) validar treinamentos; e) ratificar agendamentos; f) propagar informações do processo intervencionista, e; g) adotar *compliance*;

O Modelo Funcional desenvolvido sobre a literatura disposta preconiza cinco estágios, abaixo esclarecidos na tabela abaixo:

Tabela 14
Descritivo fases operacionais – Plano de Adequação

FASE 01	**Nome**	INVENTÁRIO DE DADOS
	Descrição	Momento em que ocorre a coleta de todos os dados da organização os relacionando a uma série de variáveis relacionadas a lei
	Dados	Dados pessoais (art.05, incisos I, II, III) , tipo de dado (cadastral ou navegacional), classe do titular (aluno, professor, colaborador, prestador, fornecedor, visitante [prospect, suspect, lead]), finalidade da coleta (art.06), base legal para coleta (arts.07, 10 e 11), sistema interface da coleta,; localização do dado, retenção, exclusão e corresponsável (responsável solidário art.47) pelo processo (*corisk owner*-COSOERM);
	Instrumento	Matriz de inventário de dados: Apêndice X
	Empregável	Planilha em Excel
	Referencial	GDPR, LGPD, COSO - Inventário
FASE 02	**Nome**	AVALIAÇÃO DE IMPACTO DE DADOS
	Descrição	Relatório que relaciona os processos de tratamento de dados pessoais aos riscos gerados aos seus titulares, desenvolvido sobre o inventário de dados, etapa anterior, o diagnóstico apresenta as medidas e tratativas cabíveis e tangíveis para cada risco de dados levantado;
	Dados	Dados pessoais: FASE 01
	Instrumento	Relatório de Impacto de Dados Pessoais (RIDP) ou Data Protection Impact Assessment (DPIA): Apêndice Y
	Empregável	Planilha em Excel e gráficos (opcional)
	Referencial	LGPD: art. 5, inciso XVII, art. 10, parágrafo 3º, art. 38 e GPDR, art. 35, ISO27001, COSO-ERM
FASE 03	**Nome**	ADEQUAÇÃO & CORREÇÃO
	Descrição	Desenvolvimento e execução das ações que alinharão a IES ao *compliance* da lei: A) articular plano de respostas e procedimentos aos riscos apontados no RIPD; B) redigir política de governança de dados; C) criar plano de treinamentos para conscientização dos stakeholders; D) realizar dos treinamentos (item C); E) dispor canais de comunicação com os titulares de dados, autoridade nacional (ANPD) e comunidade em geral, F) criar de um plano de auditoria e perenidade do *compliance* do plano de adequação (item 5) ; G) propor ajustes processuais (*process and risk owners* – **art.47**); H) aditar contratos internos e externos; I) compor políticas de segurança da informação (TI); J) revisar políticas de becape de retenção e exclusão de dados; L) nomear de um encarregado de dados;
	Dados	Dados pessoais e processuais
	Instrumento	Políticas de Governança: 1) Política Institucional de Privacidade e Proteção de Dados Pessoais e; 2) Recomendações à contratos e consentimentos;
	Empregável	Documentos Word e planilhas Excel: Apêndice Z
	Referencial	LGPD, arts. 9, 15 ao 22, 37, 38, 41, 47 ao 51, COBIT, COSO-ERM, Gestão de Mudanças
FASE 04	**Nome**	MONITORAÇÃO DE CONFORMIDADE
	Descrição	Ocorre deste os primeiros momentos do modelo ainda na fase da Gestão de Mudanças em que se prevê a criação do Comitê de Proteção de Dados que irá acompanhar toda intervenção. Desta forma, uma vez que todos processos estejam desenhados e orientados ao atingimento de um estado de conformidade as ações impetradas serão acompanhadas e avaliadas, em algum grau, pela comissão. Nesta fase ocorrerá a confrontação dos resultados obtidos com os planejados.
	Dados	Datas, dados processuais (FASE 03) e Cronogramas
	Instrumento	Relatório de *Compliance*: planejado vs realizado, Matriz de responsabilidades;
	Empregável	Planilhas Excel: Apêndice N
	Referencial	Gestão de Mudanças, COSO

Continua

Conclusão

FASE 05	**Nome**	GESTÃO DO COMPLIANCE E PERENIDADE
	Descrição	Dedicada exclusivamente a perpetuidade do estado de compliance da instituição, esta fase se debruça sobre a adoção de meditas de segurança de dados, técnicas ou administrativas, ocorrer desde a fase de concepção do produto ou serviço até sua execução, ou seja, todo e qualquer produto ou serviço da organização deve estar, além de seu fim, orientado a privacidade de dados, edificada sobre sete princípios: 1º) Preventivo e não reativo; 2º) Privacidade como padrão (Privacy by Default); 3º) Privacidade incorporada ao desenho do projeto ou solução; 4º) Funcionalidade completa; 5º) Segurança ponta-a-ponto (End-to-end); 6º) Visibilidade e transparência; 7º) Respeito a privacidade do cliente;
	Dados	Processuais
	Instrumento	Privacy by Design, Gerenciamento de Processos de Negócio (BPM)
	Empregável	Políticas e proposta de desenhos de processos: Apêndice M
	Referencial	Privacy by Design: GPDR, art. 25, LGPD, art. 46, parágrafo 2, COSO

3.5 Coleta, análise e execução

3.5.1 Aplicação do framework desenvolvido

Buscando contribuir com o processo adequação a Lei Geral de Proteção de Dados do Brasil (13.709/18 – LGPD), um *framework*, foi aplicado em uma tradicional IES da cidade de São Paulo. O protocolo de intervenção derivado do *framework* proposto, respeitou as seguintes etapas:

3.5.1.1 Ambiente de controle

Para que o framework intervencionista proposto, faça o maior sentido possível e contribua com o máximo factível, variáveis endógenas e exógenas do ambiente em que se propõe a intervenção precisam ser mapeadas e observadas, diante disto, observaram-se mercado inserido, *Market share*, missão, visão, valores, indicadores de qualidade, infraestrutura física, estrutura organizacional e governança (COSO, 2013; COSO-ERM, 2017).

Em tempo, nesta etapa, procederam-se ainda:

a) Levantamento de dados (inventário de dados) em acordo com a definição da lei observada em seu Artigo 6º (LGPD, 2018);
b) Levantamento dos riscos aos quais a IES está exposta, vide Tabela 8 do Referencial Teórico desta obra (COSO-ERM, 2017, ISO 27001);
c) Levantamento descritivo dos atuais tratamentos de dados realizados pela IES em suas instâncias acadêmicas e administrativas, de acordo com as definições com o Inciso X do Artigo 5º da lei (LGPD, 2018);

3.5.1.2 Avaliação de riscos (identificação, análise e resposta)

Sob a compreensão da IES, por meio de suas variáveis e de seu inventário de dados, desenvolveu-se uma matriz de risco apoiada sobe o ISO 27001, COSO-ERM e NBC TA 330

(R1) onde os riscos identificados serão classificados de acordo com o tido de dado operado, conforme descrito pelo Artigo 5º da Lei, pela finalidade de tratamento, Artigo 2º, 6º e 7º da lei (LGPD, 2018). Desta forma, para cada risco mapeado foi relacionado impacto e suas potenciais tratativas de contenção, considerando sobretudo sua relevância e grau de impacto (amplitude: alto, médio, baixo).

3.5.1.3 Atividades de controle

Com a conclusão das fases anteriores, em que se mapeiam os dados da instituição, sua operação, seus riscos relacionados, impactos e tratativas, será desenvolvida uma proposta de controles para os ajustes destes, de forma que, se promova conformidade com a lei. Tal proposta será apresentada a diretoria da IES para análise e crivo.

A fim de garantir maior controle e efetividade ao processo será recomendado a formação de um comitê com, pelo menos, um membro de cada segmento (administrativo e acadêmico) e, indispensavelmente, o jurídico dedicado ao acompanhamento das intervenções e para o qual o pesquisador reportará suas ações, cronograma, informando assim os próximos atos e eventuais imprevistos, conforme já citado no Modelo Funcional e preliminarmente retratado junto ao item 3.3.2.3.

3.5.1.4 Informação e comunicação

O processo de implantação e manutenção de controles internos, sejam estes derivados do COSO ou do COBIT, têm na informação e a comunicação ferramentas vitais, por meio das quais, tais controles são disseminados à toda organização, permitindo a participação dos colaboradores nos processos, recebendo e transmitindo informações de qualidade e assim possibilitando o atendimento de requisitos (COSO, 2013; COSO, 2017).

Até o presente momento todos os gestores, administrativos e acadêmicos, da instituição de ensino passaram reuniões nas quais foram entrevistados e, preliminarmente, informados da pesquisa e sua proposta de atuação.

Com a desenvolvimento a etapa anterior (*3.4.1.3*) em que se prevê a formação do comitê proposto, rotinas de comunicação fundamentadas sobre a evolução dos trabalhos e impacto destes nas atividades da IES, colocarão informações necessárias à disposição das partes interessadas no momento adequado.

3.5.1.5 Atividades de monitoramento

Desenhada especificamente para acompanhar, revisar e regular o progresso da intervenção e o desempenho das atividades previstas pelo *framework*, esta etapa identifica todas as áreas e eventos nos quais serão necessários ajustes e iniciam as correções necessárias.

Controles pressupõem eficiência e eficácia e para que possam as entregar de forma efetiva seu contínuo acompanhamento e avaliação é condição indispensável, a monitoração permite a verificação e a análise da aplicação dos controles e sua efetividade diante das mudanças que se sucedem. (COSO, 2017)

Controles implantados, apresentam baixa efetividade sem um minucioso processo de verificação periódica, sem o devido monitoramento os colaboradores envolvidos podem não os aplicar de forma plena, assim, não cumprindo seu objetivo raiz, a mitigação de riscos. (Almeida, 2003)

Portanto, nesta etapa serão monitorados o cronograma da pesquisa e o escopo do *framework*, desta forma, procedendo-se:

a) Atualização da documentação da pesquisa relacionada ao cronograma;
b) Atualização da documentação da pesquisa relacionada ao escopo do *framework*;

3.6 Avaliação de resultados: Entrevistas, questionários e análise de entregas

Indicadores de desempenho, específicos a cada elemento da fase final, em título, foram adotados a ajuizar e avaliar os resultados:

3.6.1 Monitoramento de resultados iniciais

Para medir a compreensão dos times técnicos administrativos sobre privacidade de dados, a LGPD e como esta se beneficiou com o processo intervencionista, foi adotado a seguinte estratagema:

1. Aplicação de um questionário com respostas fechadas dispostas e escala *Likert*;
2. Realização de um treinamento com os times que responderam o questionário, acima referenciado;
3. Re-aplicação do mesmo questionário adotado junto ao item 1;
4. Avaliação estatística sobre a variação média das respostas dos indivíduos, antes e depois dos treinamentos, item 2,

Desta forma, possibilitando aferir, em alguma régua de medida, a distância percorrida entre o entendimento dos respondentes (times técnicos administrativos) do momento 0

(zero: "*ext-ant*"), anterior ao treinamento, ao momento 1 (um: "*ext-post*"), após o treinamento, com alguma acurácia (Anderson, Sweeney, & Williams, 2007).

Junto ao "**Apêndice A3**" é possível constatar as variáveis observáveis, adotadas por meio das assertivas aplicadas, antes e depois dos treinamentos, e sua relação com a literatura de referência visitada.

3.6.2 Avaliação dos controladores sobre a implantação "compliance"

O instrumento adotado para esta fase, foram as entrevistas semi-estruturadas, que favorecem respostas espontâneas e livres e distintas (Vergara, 2006), presentemente, aplicadas apenas aos stakeholders "chave": 1) Reitor – Superintendente Geral, e; 2) Vice-Reitor – Superintendente Adjunto; em tempo, já interpelados na fase I, após a implementação do modelo de conformidade.

O "**Apêndice A2**" apresenta as assertivas construídas para as entrevistas semi-estruturadas, as relacionando as variáveis observáveis, constructos da pesquisa e seu enlace como o refercial teórico abordado.

3.6.3 Contribuições percebidas a curto prazo

Apresentação dos resultados da adequação, entregáveis, consoantes com as etapas determinadas no plano de adequação, página 67:

a) Mapa de Risco da IES Lócus;
b) Inventário de Dados:
c) Relatório de Impacto à Proteção de Dados Pessoais:
d) Política Institucional de Privacidade e Proteção de Dados Pessoais:
e) Recomendações à contratos e consentimentos (coleta e gestão);

3.6.4 Possibilidade de melhorias a médio e longo prazo

Apresentar potenciais contribuições futuras alinhando circunstâncias acadêmicas, teoricamente significantes, aos aspectos práticos relevantes, desta forma, buscando expressividade nos domínios êmico e ético (Suomala, Lyly-Yrjänäinen, & Lukka, 2014; Suomala et al., 2017).

3.6.5 Avaliar existência de aspectos negativos

Revisitar limitações da pesquisa as complementando com aspectos negativos apreciados no processo intervencionista.

4 Resultados: Apresentação e Discussão dos Achados

A luz da fundamentação teórica adotada para pesquisa, do modelo intervencionista proposto e da análise inicial da fase I, “Diagnóstico da situação”, idealizar-se-á o modelo conceitual de adequação à Lei Geral de Proteção de Dados do Brasil orientado pela epistemologia de Mario Bunge (1974).

4.1 1ª Etapa: Entrevistas

Considerada a adoção da entrevista semiestruturada como instrumento de coleta de dados, para esta fase da pesquisa, a concepção das perguntas aos entrevistados foi sustentada pela literatura onde as variáveis observáveis apontavam as assertivas apoiadas pelo referencial teórico disposto, desta forma, foi criado um quadro de constructos de pesquisa disponível no **Apêndice A1**.

Com a aplicação da entrevista semiestruturada, observou-se que, a despeito da maioria dos gestores indicar algum conhecimento sobre a lei, uma compreensão ampliada ainda é escassa ou ausente, apenas a assessória jurídica demonstrou profundidade neste sentido. Desta forma, embora todos entendam, em algum grau, que há possibilidade de impacto, não conseguem articular os benefícios e, ou prejuízos da vigência da lei.

Paralelamente, não se identificou em instância alguma, acadêmica e administrativa, a presença de um plano ou projeto formal e oficial de adequação à LGPD na instituição.

Semelhantemente a percepção sobre a lei captada pelo instrumento de pesquisa, não obstante a todos entrevistados serem unânimes quanto a importância de TI para sustentabilidade financeira, sucesso e perenidade da IES, constatou-se um estágio embrionário de Governança de TI, o qual, por muitos, chega a ser interpretado como ausente, o que se alinha com a literatura disposta acerca (Bichsel & Patrick, 2014; Helsloot & Jong, 2006; Tufano, 2011).

O quadro com a tabulação dos achados parciais, com saturação, desta fase da pesquisa pode ser verificado junto ao **Apêndice B1**.

Elaborou-se a justaposição das respostas de todos os entrevistados para cada questão, onde se transportou fragmentos das respostas do stakeholders que respondiam sumariamente a assertiva em questão, a transcrição sintética com estes segmentos de respostas está disponível junto ao **Apêndice B2.**

Por fim a transcrição integral, das entrevistas com os stakeholders relacionados da IES lócus, segue em anexo um ao **Apêndice B3**.

4.2 2ª Etapa: Aplicação do protocolo intervencionista

4.2.1 Diagnóstico da situação

Diante dos achados iniciais, obtidos por meio de entrevistas semiestruturadas, com assertivas desenvolvidas sobre análise de constructos de pesquisa à partir da literatura visitada e disponíveis nos capítulos e apêndices à diante, os quais apontam que 88% da amostra afirma deter um conhecimento parcial ou superior a parcial sobre a lei e, em mesma medida, declara conhecer seus impactos, entretanto, 94% demonstra compreensão parcial ou inferior a parcial dos benefícios e prejuízos da legislação da IES abordada, consequentemente, demonstrando um viés de percepção sobre a lei e suas adjacências, apesar de, a amostra ser composta majoritariamente por gestores, com formação superior (especialistas, mestres e doutores) com mais de 3 anos mínimos de experiência nos cargos que desempenham.

Em continuidade, 100% é unânime quanto a instituição operar[5] dados pessoais de pessoas naturais[6], desta forma, deixando a escola ao alcance da lei, todavia, 65% expressa não conhecer iniciativas formais e oficiais de adequação.

Quanto a dimensão da Governança de TI as idiossincrasias se repetem quando, 100% da amostra reconhece o valor de TI e em mesmo percentual afirma que a Governança de TI apoia a compliance geral das IES, desta forma alinhando-se com a literatura disposta (Bianchi & Sousa, 2016; Coen & Kelly, 2007; Wu, Straub, & Liang, 2015).

Nesta perspectiva, a amostragem revela-se unânime, 100%, quanto a TI vulnerabilizar empresas de todos os segmentos (Ariff et al., 2014; Global Risks Report, 2018 ; ISO 27005, 2011; Privacy Governance Report, 2018) e, em 100% também, que o setor educacional é mais exposto a riscos informacionais (digitais e físicos), diante de algumas características endógenas como flexibilidade, colaboração e fomento à pesquisa, portanto novamente alinhando-se a teoria (Coffman, 2014; Helsloot & Jong, 2006; Privacy Rights Clearinghouse, 2018).

Todavia a despeito da percepção registrada acerca da TI, e sua governança, enquanto sustentáculo para o segmento educacional, contribuindo junto ao equilíbrio financeiro e longevidade organizacional, observou-se que: 76% dos entrevistados não percebem a presença de Governança de TI na IES *lócus*, ou a percebem em uma instância ainda incipiente, 100% é consoante quanto a inexistência da divulgação das políticas de Governança de TI. Por fim, 100% ajuíza a ausência de clareza do papel da TI na estratégia organizacional da IES (Hicks,

[5] Toda operação realizada com dados pessoais de pessoas naturais (LGPD, art. 5, inciso X);
[6] Titular dos dados, a quem os dados pessoais se referem (LGPD, art. 1);

Pervan, & Perrin, 2012; Jairak & Praneetpolgrang, 2013; Sabherwal & Kirs, 1994; Tufano 2011).

Ante ao exposto, observa-se uma estreita relação entre a literatura visitada e os achados iniciais que ajuízam:

a) Reconhecimento do valor[7] de TI para as organizações;
b) Vulnerabilização que a TI traz aos segmentos empresariais;
c) Maior exposição aos riscos do setor educacional por fatores endógenos;
d) Baixa e, ou incipiente adoção as melhores práticas de gestão de riscos e governança de TI na educação;

Isto dito, quadro abaixo, Tabela 11, estabelece uma relação entre os achados iniciais e a literatura visitada, expondo os constructos admitidos, as variáveis teóricas e suas disposições, as confrontando com o comportamento da amostra analisado para esta fase da pesquisa, ademais o apêndice B1 traz a tabulação integral destes dados e achados:

Tabela 15

Síntese dos achados – Fase I

Constructos	**Variáveis - Literatura**		**Comportamento da amostra**	**Literatura**
LGPD Lei 13.709/18	Ciência	Conhecimento	88% ≥ Parcial	Lei n. 13.709, (2018); SIEEESP, (2018); Mulholland, (2018); Tuttle, (2018); Global Risks Report, (2018); Privacy Governance Report, (2018); Privacy Rights Clearinghouse, (2014); Ariff, Zakuan, Tajudin, Ahmad, Ishak e Ismail, (2014); Pinheiro, (2018); (Bianchi & Sousa, 2016; Wu, Straub, & Liang, 2015; Coen & Kelly, 2007) (Global Risks Report, 2018; Privacy Governance Report, 2018; Ariff et al., 2014; ISO 27005, 2011) (Coffman, 2014; Privacy Rights Clearinghouse, 2018; Helsloot & Jong, 2006) (Jairak & Praneetpolgrang, 2013; Hicks, Pervan, & Perrin, 2012 ; Tufano 2011; Sabherwal & Kirs, 1994) (Jairak & Praneetpolgrang, 2013; Hicks, Pervan, & Perrin, 2012 ; Tufano 2011; Sabherwal & Kirs, 1994) (ISACA, 2010; COBIT, 2012)
		Compreenção dos impactos	88% ≥ Parcial	
	Importância	Compreenção sobre prejuízos e benefícios	94% ≤ Parcial	
	Conformidade	IES manipula dados	100% Sim	
		IES possui plano de compliance	76% Não	
	Relevância	TI é importante	100% sim	
Governança da Informação (TI)	Relevância Presença	TI vulnerabiliza IES	100% sim	
		IES mais expostas	94% sim	
		IES detem Gov.TI	76% ≤ Parcial	
	Presença Conformidade	IES divulga Gov.TI	100% ≤ Parcial	
		IES tem TI na estratégia	100% ≤ Parcial	
		Gov. TI apoia compliance	100% sim	

[7] Amparar sucesso organizacional (financeiro e operacional);

4.2.1.1 Análise inicial do ambiente

A IES lócus, a despeito da elevada qualificação observada em seus gestores administrativos e, ainda, da formação da gestão acadêmica, leia-se alta gestão, em 86% composta por doutores, apresenta uma incipiente compreensão sobre a lei, particularmente seus impactos, o que é relevante visto o cunho coercitivo de adequação imposto pelo poder público e o prazo de adequação datado para agosto de 2020.

Ademais, identificam-se ainda dois eixos que se distribuem em direções opostas quanto a Governança de TI, onde a amostra manifesta-se unânime, 100%, sobre a importância da TI para sustentabilidade e *compliance* geral da IES, por meio de sua governança, e em mesma escala, declara inexistente e, ou inobservável esta prática.

Achados finais, apontam em 100% que a TI, em sua evolução, vulnerabiliza as organizações, e, em tempo, que o segmento educacional se mostra mais exposto a riscos informacionais motivado por seu caráter colaborativo, de incentivo a pesquisa e desenvolvimento do conhecimento multidisciplinar. Portanto, requerendo o desenvolvimento de princípios e mecanismos de gestão de riscos eficazes, o que ainda se mostra embrionário na instituição.

Todos os achados da pesquisa, até então, alinham-se a literatura de referência visitada e podem ser observados junto a Tabela 11: "Síntese dos achados – Fase I", disposta no capítulo 2.4. "Diagnóstico – Fase I", junto a página 43 desta obra.

4.2.1.2 Diagnósticos dos problemas

Relacionam-se abaixo os principais pontos de atenção observados junto a avaliação realizada até o momento:

a) Exposição da IES a Lei Geral de Proteção de Dados: motivada pela modelo de seu negócio "empresa-consumidor" ou B_2C (*Business to Consumer*), em que o exercício de sua atividade meio e fim, impõe a coleta e tratamento dos dados pessoais de seus clientes, ou seja, titulares de dados;
b) Incipiente entendimento sobre a lei: apesar da exposição, do caráter coercitivo da lei e do prazo de adequação, as camadas gestoras não apresentam entendimento razoável aos impactos desta legislação;
c) Ausência de um projeto de adequação: ausência de um plano formal e oficial de *compliance* à lei;

d) Maior exposição ao risco informacional: como qualquer organização deste segmento ajuíza-se uma maior exposição ao risco, seja fundamentado pela TI em seu desenvolvimento e disseminação, seja, pelas características endógenas do setor;
e) Ausência de Governança de TI: não se observaram práticas, rotinas e, ou processos de governança da informação, TI, na IES, e, portanto, tão pouco sua divulgação;

4.2.1.3 Pesquisadores e profissionais envolvidos

Gestores acadêmicos: 1) Reitor (acumula função de Superintendente Geral); 2) Vice-Reitor (acumula função de Superintendente Adjunto); 3) Pró-Reitor de Graduação; 4) Pró-Reitor de Extensão; 5) Diretor da Pós-Graduação Lato e Stricto Sensu; 6) Diretor do Ensino Médio; 7) Secretário Geral.

Gestores Administrativos: 1) Superintendente Geral (acumula função de Reitor); 2) Superintendente Adjunto (acumula função de Vice-Reitor); 3) Advogada – Assessoria Jurídica; 4) Gerente Financeiro; 5) Supervisor de Compras; 6) Gerente Contabilidade; 7) Coordenador de TI – Sistemas; 8) Supervisor de TI – Infraestrutura.

Discentes: 1) representante mestrado (Stricto Sensu); 2) representante pós-graduação (Lato Sensu); 3) representante graduação; 4) representante ensino médio.

A tabulação de todos os dados pertinentes aos stakeholders entrevistados pode ser observada junto ao **Apêndice C1.**

4.2.1.4 Elaboração do Framework para a intervenção

Buscando contribuir com o processo adequação a Lei Geral de Proteção de Dados do Brasil (13.709/18 – LGPD), sancionada em agosto de 2018 e com início de vigência prevista para agosto de 2020, um framework, desenvolvido a luz da Governança de TI, Controles Internos, Gestão de Riscos e da própria legislação, foi aplicado em uma tradicional IES da cidade de São Paulo onde, achados iniciais, apontam uma baixa adesão as práticas de Governança de TI, limitada compreensão sobre a lei e seus impactos e ainda a ausência de planos formais e oficiais de compliance a lei.

O framework contribuirá com:

a) Conhecimento sobre a lei e seus potenciais impactos positivos e negativos;
b) Conformidade com a legislação que regulamenta a proteção de dados do pais;
c) Adoção de melhores práticas de Governança de TI;
d) Elevação dos níveis de Gestão de Riscos relacionados;

4.2.2 Planejamento e nível de intervenção

4.2.2.1 Planejamento: cronograma (agenda e datas para intervenção), disponibilidade do pesquisador e instituição

Estabelecido sobre a disponibilidade do pesquisador e da instituição, *stakeholders*, entre outras premissas, apresenta-se a proposta de cronograma do processo de intervenção que guiará as atividades de adequação com vistas ao compliance institucional à legislação de proteção de dados do pais.

A tabela 18 abaixo, cronograma, estratifica esta informação de forma macro analítica, reunindo informações das etapas articuladas para a intervenção e sua respectiva distribuição no tempo, desta forma, conferindo controle e gestão sobre cada ação praticada na direção dos ajustes pertinentes ao atingimento dos objetivos previstos sob aspectos práticos e teóricos (Leach, 1999).

Tabela 16

Estrutura analítica do processo de intervenção – Cronograma

ETAPA	AÇÃO	PERÍODO - PROJEÇÃO																																					
		NOV19				DEZ19				JAN20				FEV20				MAR20				ABR20				MAI20				JUN20				JUL20				AGO20			
		S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4	S1	S2	S3	S4
Diagnóstico Situação	Análise inicial ambiente																																						
	Diagnóstico problemas																																						
	Profissionais envolvidos																																						
	Elaboração framework																																						
Plano Intervenção	Planejamento (ações e datas)																																						
	Definir nível intervenção																																						
EXAME DE QUALIFICAÇÃO																																							
Ajustes exame de qualificação																																							
Coleta, análise e execução	Composição comitê																																						
	Fase 1: Inventário de dados																																						
	Fase 2: RIDP																																						
	Fase 3: Adequação																																						
Avaliação Resultados	Fase 4 : Monitoração																																						
	Fase 5 : Perenidade																																						
	Visão-aceitação da gestão																																						
	Contribuições curto prazo																																						
	Melhorias médio-longo prazo																																						
	Aspéctos em aberto																																						
	Aspectos negativos																																						
EXAME DE TITULAÇÃO																																							

4.2.2.2 Determinar nível de intervenção e participação do pesquisador (êmic e Etic)

Suomala e Yrjänäinen, (2010), apresentam uma escala contendo os níveis previstos de intensidade para “pesquisação” intervencionista, aqui compreendidos junto a tabela 19 abaixo:

Tabela 17
Escala dos níveis de intensidade previstos no trabalho intervencionista

Escala de níveis de intervenção **NÍVEL**	**PONTO FOCAL** (DE ACESSO)	**INTENSIDADE**
5	Intervenção exclusivamente em Contabilidade Gerencial / práticas / ferramentas	Colaboração forte, papel nativo 'um de nós'
4	Intervenção principalmente no Contabilidade Gerencial e em parte	Participação ativa e versátil, quase familiar
3	Equivalente enfoque em Contabilidade Gerencial e outros	Participação rica, mas de acesso interno limitado
2	Foco principal em outras disciplinas, também Contabilidade Gerencial	Especialista externo, participação limitada
1	Foco exclusivo em outros assuntos	Intervenção através da presença, participação muito limitada no processo

Diante disto e pela premente necessidade de ajuste imposto pela legislação concernente, adotou-se o nível 5 para os trabalhos, considerando que, após a apresentação dos processos mapeados, e ajustes propostos o pesquisador, atuará como ponto multiplicador: a) do conhecimento sobre a lei, e; b) das conformações processuais e comportamentais em direção ao *compliance* relato e sua perenidade.

4.2.3 Coleta, análise e execução: Aplicação do Framework desenvolvido

4.2.3.1 Ambiente de controle

Nesta etapa de pesquisa ocorreram:

a) Inventário de Dados: em acordo com a definição da lei observada em seu Artigo 6º (LGPD, 2018): desenvolvido sobre os seguintes instrumentos:
   a.1. Análise documental;
   a.2. Análise processual;
   a.3. Entrevistas;
b) Levantamento dos riscos aos quais a IES está exposta: apresentado adiante em "*Avaliação de riscos 4.2.3.2*";
c) Levantamento descritivo dos atuais tratamentos de dados realizados pela IES em suas instâncias acadêmicas e administrativas, de acordo com as definições com o Inciso X do Artigo 5º da lei (LGPD, 2018);

A maioria das fontes de dados e evidências científicas, independentemente do instrumento assumido para a pesquisa, apresentam de aspectos positivos e negativos, diante disto, é significativo garantir que não haja prevalência de uma técnica sobre as demais adotadas, mas sim a complementação destas (Gil, 1999, Gil, 2002, Yin, 2010).

A tabela 20, a seguir, articula os instrumentos adotados, partes envolvidas (“stakeholders”) e informações colhidas, analisadas e executadas nesta etapa da pesquisa:

Tabela 18
Stakeholders, instrumentos de pesquisa e metas

ÁREA	STAKEHOLDERS	INSTRUMENTOS	COLETA – ANÁLISE	META
Recursos Humanos	Gestor de RH Analistas de RH	Entrevistas Análise documental Análise processual	Ciclo de vida do dado pessoal do colaborador: do momento do processo seletivo ao desligamento do funcionário (administrativo e acadêmico), percorrendo todas as etapas deste trajeto	Mapear todos os processos relacionados ao ciclo de vida do dado pessoal: tipo de dado, tratamento, base legal - legitimação, políticas de armazenamento - retenção e riscos envolvidos
Relacionamento com candidato	Gestor da área		Ciclo de vida o dado pessoal do candidato: do momento da inscrição em processo seletivo ao momento ao momento da matrícula quando se torna aluno	
Central do Aluno	Gestor da área		Etapas percorridas pelos dados pessoais do aluno sobre a dimensão acadêmica: manutenção do ciclo de vida acadêmico do titular de dados	Mapear todos os processos e tratamentos relacionados a manutenção do ciclo de vida acadêmico do titular de dados
Central de carreiras e aconselhamento	Gestor da área		Etapas percorridas pelos dados pessoais quando o titular de dados, aluno, procurar à área	Mapear todos os processos e tratamentos de dados relacionados
Financeiro	Gestor da área		Etapas percorridas pelo dado pessoal do aluno sobre a dimensão financeira: manutenção do ciclo de vida financeiro do titular de dados	Mapear todos os processos e tratamentos relacionados a manutenção do ciclo de vida financeiro do titular de dados pessoal sobre o cunho financeiro
Segurança	Gestor da área	Entrevistas Análise documental Análise processual	Tratamentos de dados pessoais relacionados ao controle de acesso físico aos Campi	Mapear todos os processos e tratamentos de dados relativos aos titulares da dados com e sem vínculo com a IES
Tecnologia da Informação	Gestor da área Infraestrutura		Tratamentos de dados pessoais realizados no controle de acesso lógico (rede local, wi-fi e internet) dos titulares de dados	
	Gestor da área Desenvolvimento		Coleta de dados pessoais realizados sob interfaces (formulários) de software, armazenamento e demais tratamentos	
Compras	Gestor da área		Dados pessoais recebidos e, ou enviados a parceiros de	Mapear relação Controlador –

	negócio, caso haja, e os tratamentos de dados pertinentes	Operador da IES, os dados pessoais e tratamentos realizados

4.2.3.2 Avaliação de riscos (identificação, análise e resposta)

A gestão de riscos possivelmente seja a dimensão mais presente nesta obra, permeando aspectos teóricos e práticos pertinentes, desta forma, considerado os artigos 3 e 4 da Lei Geral de Proteção de Dados, que delimitam sua aplicabilidade a qualquer operação de tratamento realizado por pessoa natural ou jurídica (pública ou privada) do pais e em território nacional, com o objetivo de ofertar ou fornecer produto ou serviço com fins profissionais e, ou econômicos, não artísticos, não acadêmicos e, ou sem fins de segurança pública ou defesa nacional ou investigações a IES Lócus foi decomposta por unidade organizacional e, estas, avaliadas de acordo com seu grau de exposição à lei, ou seja consoante, com o grau de risco observado.

A tabela 14, abaixo apresenta o índice observado do tratamento atual de dados pessoais em cada unidade de negócio ou institucional, destacando o volume de titulares de dados e sua particular tratativa, caso haja.

Tabela 19

Matriz de exposição a Lei 13.709/2018 junto a unidades de negócio da IES Lócus.

UNIDADES DE NEGÓCIO	---------- Coleta, usa e-ou armazena ----------					Volume Titulares	Tempo	Politica(s): Privacidade e, ou Governança de Dados
	Dados Pessoais	Dados Pessoais Sensíveis	Dados menores de 18	Prospects, suspects, leads	Após término do contrato [1]			
Colégio	SIM	SIM	SIM	NÃO	SIM	738	3 anos	NÃO
Graduação	SIM	SIM	SIM [2]	NÃO	SIM	**2708**	4 anos	NÃO
Pós Lato Sensu	SIM	SIM	NÃO	NÃO	SIM	1176	1 ano	NÃO
Pós Stricto Sensu	SIM	SIM	NÃO	NÃO	SIM	142	2,5 anos	NÃO
Extensão	SIM	SIM	NÃO	NÃO	SIM	100	Dias	NÃO
Administrativo	SIM	SIM	SIM	SIM	SIM	400	Anos	NÃO

Nota. **1.** Mantem tratamento de dados pessoais após o termino do contrato de prestação de serviços educacionais; **2.** Refere-se aos *prospects* advindos do ensino médio para a graduação.

Considerado que o tratamento realizado decorre do exercício da atividade fim, ou seja, a prestação de serviços educacionais e todo seu desdobramento acadêmico e financeiro sobre o período em que o titular de dados mantiver este vinculo, fica inequívoco que a Graduação se mostra mais exposta que as demais unidades organizacionais, por meio de seu maior volume de titulares abrangidos, ainda que a unidade do Colégio apresente um número maior de titulares de menor idade, aqui admitido como menores de 18 anos, seu volume de titulares de dados é 72,7% inferior ao da Graduação.

Sobre a tabela de exposição das unidades de negócio da IES a lei, acima, e ainda sobre as diretrizes da gestão de risco observadas junto a ISO 31000, a Matriz de Ricos a seguir emoldura as unidades de negócio da instituição dentro do artefato de mensuração da probabilidade de concretização do risco versus seu impacto.

Tabela 20
Matriz de Risco: IES Lócus & LGPD

Matriz de Risco ISO31000		PROBABILIDADE				
		< 10% Rara	10 a 40% Baixo	40 a 60% Médio	60 a 80% Alto	> 80% Quase Certo
IMPACTO	Muito Alto			**Graduação**		
	Alto			**Colégio** **Pós Lato Sensu**		
	Médio			**Administrativo** **Pós Stricto Sensu**		
	Baixo			**Extensão**		
	Insignificante					

Fonte: De "*ISO 31000: Risk management. Principles and guidelines on implementation."* Geneva, 2009a. Recuperado de https://www.iso.org/standard/43170.html

Diante da incerteza e caráter ainda especulativo da ação governamental quanto ao processo de fiscalização, da inexistência índices históricos sobre incidentes e infrações da proteção de dados no país e, ainda, do comportamento dos titulares sobre o tratamento de seus dados pessoais, agravado pelo artigo 22 da LGPD que clarifica o exercício dos direitos e defesa dos titulares de dados permitindo este ser exercido individual ou coletivamente, a matriz apresentada é qualitativa para qual assumiu-se probabilidade alta, de 60% a 80%, de concretização para a unidade com mais titulares e, semelhantemente, atribui-se um maior impacto observando as mesmas premissas. As demais unidades, estabelecidas em probabilidade média, de 40% a 60%, tiveram seu grau de impacto distribuído de acordo com seu volume atual de titulares, exceto o Colégio que se posicionou como alto devido a tratar dados de menores, inclusive em seus mecanismos de prospecção de novos alunos.

A unidade com risco mais brando considerado é a Extensão, desta forma disposta por apresentar um baixo volume de titulares de dados, menor tempo de exercício da atividade fim e por estes serem majoritariamente compostos por alunos das demais unidades, os quais, tiveram a conformidade do tratamento de seus dados pessoais realizada nas instancias próprias a sua origem.

Os achados trazidos pelas matrizes pregressas alinham-se a literatura disposta asseverando caráter ainda incipiente no segmento educacional e sua maior exposição motivada primordialmente por fatores endógenos (Bichsel & Patrick, 2014; Helsloot & Jong, 2006).

Mediante a coleta e análise de dados, caracterizada como Inventário de Dados, dois Relatórios de Impacto à Proteção de Dados foram desenvolvidos considerando as três dimensões que materializam o risco das organizações a LGPD. A figura 14 e a Tabela 21, ambas abaixo, apresentam e descrevem estes pilares sua descrição medida de concentração em um programa de compliance:

Figura 14. LGPD: Dimensões dos Riscos - concentração

Tabela 21
LGPD: Dimensões dos Riscos - descrição

-TECNOLÓGICO-	-JURÍDICO-	-OPERACIONAL-
Representa todo tratamento de dados pessoais realizado sobre interfaces tecnológicas, da coleta, armazenamento e transmissão a exclusão. Baliza, comumente, a relação entre Controladores e Operadores de Dados e os mecanismos de segurança relacionados. Dimensão em que reside a Segurança da Informação, ISO27001 e a Governança de TI (COBIT)	Representa a sólida compreensão sobre a lei em seus artigos, *caputs*, incisos e parágrafos, percorrendo os artefatos e princípios propostos e seus respectivos impactos sobre as organizações principalmente sobre os titulares de dados e a garantia de preservação de seus diretos fundamentais. Dimensão que hospeda as leis 13.709/2018-LGPD, 12.965/2014 - MCI e GPDR - EU.	Representa do uso do dado pessoal pela organização (stakeholders) em si, o posicionamento junto a atividade fim ou atividade meio e seu propósito. Tange aos processos que tratam os dados pessoais e seu controle/*compliance.* Dimensão que abriga Governança Coorportativa[1] (*Accountability, Responsibility, Transparency e Fairness*), Gestão de riscos (ISO31000), Controles Internos (COSO e COSO-ERM).

Fonte Adaptado de "*Corporate governance as social responsibility: A research agenda*", de A. Gill, 2008, Berkeley J. Int'l L., 26, 452; de "Code of Corporate Governance", de T. Council, 2003, *Annual Review and Reporting, 5*; de "Corporate governance and internal control over financial reporting: A comparison of regulatory regimes", de U. Hoitash, R. Hoitash, & J. C. Bedard, 2009, *The accounting review, 84;* de "*Corporate governance: Principles and issues*", de D. Nordberg, 2010; de "*Corporate governance: Principles, policies, and practices*", de R. B. Tricker, & R. I. Tricker, 2015.

4.2.3.3 Atividades de controle, comunicação e monitoramento

Com o mapeamento dos riscos concluídos sobre o levantamento inicial (Inventário de Dados) um plano de resposta para cada ameaça foi estabelecido sob o desígnio de a mitigar, por meio da redução potencial da exposição e, em tempo, do tratamento dos impactos da verossímil concretização destes riscos.

Para garantir a eficácia de controles internos junto a mitigação de riscos com vistas a razoável certeza, confiança e fidedignidade dos dados aqui tratados o constante acompanhamento e comunicação são imprescindíveis, permitindo desta forma a participação de stakeholders nos processos relacionados aos tratamentos de dados realizados e permitindo o atendimento dos requisitos do *compliance* (Almeida, 2003; COSO, 2013; COSO, 2017).

Controles implantados, apresentam baixa efetividade sem um minucioso processo de verificação periódica, sem o devido monitoramento os colaboradores envolvidos podem não os aplicar de forma plena, assim, não cumprindo seu objetivo raiz, a mitigação de riscos. (Almeida, 2003).

Diante disto, a tabela 22, a seguir, pautada sobre o modelo de responsabilidades e comunicação de projetos (Feltus, Petit, & Dubois, 2009; Project Management Institute [PMI], 2017), apresenta o comitê de stakeholders composto para a intervenção, suas responsabilidades durante os trabalhos realizados, suas diretrizes de comunicação e, por fim, o controle atribuído em cada fase do ciclo de vida do dado pessoal mapeado dentro da IES lócus.

Tabela 22
Matriz de responsabilidades, comunicação e controle da intervenção

STAKEHOLDER	RESPONSABILIDADE	COMUNICAÇÃO	CONTROLE
Gestor de Recursos Humanos	Fornecer informações sobre a coleta de dados pessoais (DP) de colaboradores e todos os tratamentos posteriores.	Manter informado sobre o desenvolvimento desta fase exclusivamente	Risk-Owner sobre a coleta, tratamento, armazenamento de exclusão do dado pessoal dos colaboradores da IES
Gestor do Relacionamento Institucional	Proporcionar informações sobre a coleta de dados pessoais de candidatos e alunos.	Manter informado sobre o desenvolvimento desta fase exclusivamente	Risk-Owner sobre a coleta de dados de candidatos e alunos
Gestor da Central do Aluno e Gestor da Central de Carreiras e Aconselhamento	Fornecer informações detalhadas sobre todo tratamento acadêmico com DP de alunos	Manter informado sobre o desenvolvimento desta fase exclusivamente	Risk-Owners do tratamento realizado com dados pessoais de alunos
Gestor Financeiro	Munir pertinentes ao tratamento financeiro realizado com dados pessoais de alunos	Manter informado sobre o desenvolvimento desta fase exclusivamente	Risk-Owner do tratamento financeiro com dados pessoais de alunos
Gestor de Segurança Patrimonial	Fornecer informações sobre coleta e tratamento de dados pessoais de visitantes	Manter informado sobre esta fase da intervenção	Risk-Owner do tratamento realizado com DP dos visitantes

Gestores Tecnologia: 1) Infraestrutura; 2) Desenvolvimento;	Suprir informações acerca dos tratamentos realizados com DP de alunos, colaboradores e visitantes dentro da rede de computadores da IES e sob interfaces de software	Manter informados sobre esta dimensão do tratamento de DP de alunos e visitantes	Risk-Owners do tratamento de DP realizados nesta dimensão
Gestor de Compras	Suprir informações sobre tratamentos DP realizados por parceiros de negócio (fornecedores)	Manter informado sobre esta fase	Risk-Owner da relação Controlador e Operador
Reitores	Aprovar e facilitar o processo de intervenção	Manter informado sobre todas as fases da intervenção	Sponsosr[1] da pesquisa
Jurídico	Apresentar disposições consultivas acerca da dimensão jurídica pertinente a pesquisa	Manter informado sobre aspectos jurídicos junto a progressão da intervenção	Caráter Consultivo
Pesquisador	Realizar e promover a intervenção	Manter todas as partes informadas de acordo com disposto neste catálogo	Risk-Owner do *compliance* e sua perenidade

1. *Sponsor*: " pessoa ou grupo que fornece recursos e apoio ao projeto, programa ou portfólio e é responsável por possibilitar o seu sucesso" (PMI, 2017, p. 723).

4.2.4 Avaliação de resultados: Entrevistas, questionários e análise de entregas

4.2.4.1 Monitoramento de resultados iniciais

Um dos aspectos que se revela com a análise ambiental e diagnósticos de problemas, observado junto as entrevistas iniciais com o stakeholders, é a ausência de real entendimento acerca da legislação para qual se busca conformidade, vide "Apêndice B1", diante disto, como parte de processo de *compliance* e governança adotaram-se treinamentos dedicados, inicialmente, as partes envolvidas, por meio dos quais pretendeu-se apresentar:

a) Conceito de privacidade de dados, titulares de dados e seus direitos;
b) Contexto e elementos estruturais da Lei Geral de Proteção de Dados;
c) Impactos, positivos e negativos, da lei;
d) Processo de conformidade institucional e como cada stakeholder contribui;

Desta forma, cada gestor indicou uma parte de seu time para receber o treinamento desenvolvido remotamente com o pesquisador que aplicou questionários (*ext-ant* e *ext-post*) em escala *Likert* aos colaboradores participantes, os quais podem ser encontrados junto ao "**Apêndice A3**".

A tabela 23, abaixo, reuni e sumariza as respostas de todos os colaboradores que participaram dos treinamentos aplicados as áreas envolvidas, até então, no processo de intervenção com vistas ao *compliance* institucional à LGPD.

Tabela 23 - Respostas

Respostas sumarizadas dos treinamentos aos colaboradores da IES Lócus

Constructo Dimensão	Variáveis observáveis	Assertivas (antes e após) treinamento Stakeholders Técnico Administrativos		Área	Comportamento da amostra			Referências - Literatura
					ext-ant	*ext-post*	Δ%	
LGPD 13.709/18	Ciência	1	Qual seu grau de conhecimento ou entendimento sobre Privacidade de dados?	1	1,60	2,93	89%	Lei n. 13.709, (2018); SIEEESP, (2018); Mulholland, (2018); Tuttle, (2018); Global Risks Report, (2018); Privacy Governance Report, (2018); Privacy Rights Clearinghouse, (2014); Ariff, Zakuan, Tajudin, Ahmad, Ishak e Ismail, (2014); Machado Meyer, (2018); Pinheiro, (2018); Baffa, Poggio e Fachinetti, (2018); Maldonato, Blum e Borelli (2019); Feferbaum e Lima, (2019); Bioni, (2019);
				2	1,07	2,07	50%	
				3	1,47	2,67	72%	
		2	Qual seu grau de conhecimento da lei (LGPD)?	4	2,00	3,00	50%	
				5	2,22	3,56	89%	
	Importância & Impacto	3	Em qual grau, você entende que a IES pode estar exposta a lei?	6	1,00	2,67	139%	
				7	2,17	3,50	89%	
				8	2,67	4,00	89%	
				9	**1,69**	**2,94**	**83%**	

Nota: 1) Recursos Humanos; 2) Relacionamento Institucional (Matrículas); 3) Central do Aluno; 4) Central de Carreiras; 5) Financeiro; 6) Segurança e Risco; 7) Tecnologia; 8) Compras; 9) Variação total da amostra;

Sobre os valores posicionais apresentados, registra-se um índice geral de aproveitamento, na ordem de 83%, resultante da média dos percentuais de aproveitamento inferidos sobre cada área participante.

Aprecia-se também que a área da Segurança e Risco, apresentou maior variação da amostra atingindo 139% de aproveitamento, possivelmente motivada pelo total desconhecimento sobre o tema, 1,00, vide dados detalhados em **Apêndice A4**.

Relacionamento Institucional apresenta-se próximo da Segurança junto ao índice de entendimento anterior (*ext-ant*) com 1,07, entretanto diferentemente desta área, demonstra preocupante 50% de aproveitamento, o menor da amostra. Isto visto e considerada a ação da área junto ao tratamento inicial, coleta, de todo dado pessoal dos alunos da IES, faz-se premente um novo treinamento para área.

Compras, Tecnologia e Financeiro apresentaram o maior entendimento anterior (*ext-ant*) sobre a lei atingindo índices superiores a 50% do valor máximo apurável nesta variável, em tempo, maiores estudos sobre fatores endógenos as áreas fazem-se necessários para inferir a razão deste deslocamento.

Demais áreas expressam um comportamento próximo, com delta de aproveitamento oscilando entre 72 e 89%, o que, diante de toda a amostra é satisfatório à atual fase da pesquisa.

4.2.4.2 Avaliação dos controladores sobre a implantação "compliance"

Após a aplicação do modelo intervencionista orientado ao atingimento do compliance institucional ao uso e proteção de dados pessoais de todos os titulares de dados da IES lócus uma nova entrevista foi realizada com os "stakeholders chave" (controladores): 1) Reitor e Superintendente Geral, e; 2) Vice-Reitor e Superintendente Adjunto.

A caracterização dos entrevistados pode ser obtida junto ao "Apêndice C1" e as perguntas abordadas junto ao "Apêndice A2".

A tabela 24, a seguir, extrai a síntese das respostas dos reitores quanto aos benefícios e melhorias percebidas no processo de intervenção realizado até este instante da pesquisa, apresentando sua visão sobre a perspectiva da legislação, da governança e da própria pesquisa. A transcrição integral e a sintética da pesquisa podem ser observadas junto aos "Apêndices B4 e B5" respectivamente.

Tabela 24
Síntese e tabulação, entrevistas: Stakeholders chave (controladores)

	Perspectivas estimadas						
	PESQUISA	COMPLIANCE LGPD		GOVERNANÇA			PESQUISA
	Entendimento sobre a lei	Risco legal	Atividade meio e fim	Governança de TI	Controles internos	Risco informacional	Atendimento expectativas
E1	Sim: Maior compreensão sobre	Consciência melhorada no processo decisório	Maior conscientização de adequação	Processo decisório e estrutura de sistemas	Identificação de melhorias	Redução do nível de risco	Sim: mais tranquilidade no processo de ajuste da IES
E2	Sim	Melhor consciência do tratamento dados	Maior consciência de individualidade	Sim	Pontos de controle alinhados a atividade fim	Mitigação riscos pertinentes	Sim: valorização dos direitos individuais

Os reitores julgam haver benefício em todos os aspectos abrangidos pela pesquisa, melhorando a compreensão sobre a lei, a consciência sobre risco legal pertinente a preservação dos direitos fundamentais dos titulares de dados e melhorando os processos decisórios relativos.

Em tempo ajuízam uma melhora nos níveis de Governança de TI dispostos, apurados com baixos índices anteriores, favorecimento dos controles internos, seu alinhamento a atividade fim ao que tange a compliance proposto e ainda uma redução os níveis de exposição informacionais. Por fim são consoantes em expressar o atendimento de suas expectativas quanto a intervenção realizada trazendo tranquilidade e segurança no processo de ajuste da IES a lei.

Por fim, o "**Apêndice E1**" apresenta o panorama teórico da pesquisa identificando aspectos revelados pela análise ambiental e diagnóstico de problemas, variáveis ambientais relacionadas, contribuições alcançadas pela intervenção e instrumento aplicados, até este momento, e sua respectiva sustentação bibliográfica.

4.2.4.3 Contribuições percebidas a curto prazo:

Todo projeto, independentemente de seu escopo ou área de aplicação, apresenta um grupo de entregas (*deliverables*), podendo estas serem produtos ou serviços, sobre as quais indicadores de qualidade e desempenho são desenvolvidos e aplicados (Kerzner, 2017). Isto posto, o próprio processo de adequação a LGPD prevê, sob imposição legal, um grupo de saídas ou resultados iniciais, aqui apresentados, como: "curto prazo".

A tabela 25, a seguir, concatena e apresenta o catálogo de entregas inicias, relacionadas a pesquisa intervencionista desenvolvida, a integralidade destes deliverables está disponível junto aos apêndices e páginas desta obra e referenciados abaixo.

Tabela 25
Contribuições a curto prazo

	CONTRIBUIÇÃO - ENTREGÁVEL	LGPD	APÊNDICE/Ref.
1	Matriz de exposição da IES	Art.3 e Art.4	**Página 57**
2	Mapa de risco da IES	Art.2, Art.6, Art. 9, Art 17 ao 22	
3	Inventários de dados	Art. 37	**D1**
4	Relatório de Impacto a Proteção de Dados Pessoais	Art.5 XVII, Art.10 §3, Art.38	**D2**
		GPDR, Art.35 - DPIA	**D3**
5	Política Institucional de Privacidade e Proteção de Dados Pessoais	Art.47 e Art.50	**D4**
6	Política de *cookies* dos sítios eletrônicos institucionais		
7	Ajustes contratuais e consentimentos: coleta e gestão	Art.5 incisos VII e VIII, Art.8, Art.38 e 39	**D5**

Considerados: a) os baixos índices de adesão a gestão de risco no segmento educacional apontados pela literatura e, corroborados pela pesquisa aqui desenvolvida; b) a definição de qual unidade de negócio abordar junto a intervenção apoiar-se nestes artefatos; ambos são considerados como contribuição imediata.

Organizações que buscam conformidade à proteção de dados precisam mapear seus processos e fluxos de dados institucionais registrando, por meio destes, o clico de vida do dado pessoal de seus titulares (GPDR, *Article* 30). Este inventário é essencial ao cumprimento de todas as etapas da regulação imposta e, portanto, "pedra angular" de todo e qualquer processo que objetive aproximação ou atingimento do compliance relacionado.

Considerada a ausência de modelos relevantes disponíveis, foi desenvolvido um protótipo próprio para coleta e mapeamento de dados pessoais e seu ciclo de vida dentro da IES lócus, nesta direção, as seguintes variáveis foram consideradas para o modelo articulado:

1. PROCESSO INSTITUCIONAL: Processo por meio do qual o DP é tratado;
2. DADOS: Relação de todos os dados pessoais tratados;

3. TIPO: Categoria do DP (sensível, navegacional);
4. ORIGEM: forma de coleta do dado, se informado pelo titular ou não;
5. MEIO: Método da coleta, se físico (papel) ou digital (formulário online);
6. ARMAZENA: Quem e onde o dado é armazenado;
7. RETENÇÃO: Período de retenção do dado coletado;
8. RISK-OWNER: Responsável pelo risco do DP no processo institucional;
9. CoRISK-OWNER: Corresponsáveis pelo risco do DP no processo;
10. TRATAMENTO (Art.5): Tratamentos realizados com os DP no processo;
11. RAZÃO (Art.6): Fatores motivadores dos tratamentos realizados;
12. BASE LEGAL (Art.7): Hipótese de uso atribuída ao tratamento realizado;
13. OBRIGAÇÃO LEGAL (Art.7, II): Qual a lei que se acata, caso haja;
14. LEGÍTIMO INTERESSE (Art.10): Qual o legítimo interesse, caso haja;
15. DADOS PESSOAIS SENSÍVEIS (Art.11): Quais as hipóteses do tratamento;
16. COMPARTILHA: Se há compartilhamento e com quem;
17. TRANFERÊNCIA INTERNACIONAL: Se há transferências internacionais de DP;
18. ANONIMIZAÇÃO: Se o DP é anonimizado;
19. A18 (DIREITO DOS TITULARES): Se o processo mapeado permite o exercício dos direitos dos Titulares de Dados, previstos pelo Artigo 18;
20. IMPACTO: O impacto ao titular de dados em caso de incidente (concretização do risco) dentro de uma escala *Likert* (5 = máximo, 4 = alto, 3 = médio, 2 = baixo, 1 = ausente);

A despetio da não tipificação da remuneração, sálario, enquanto dado sensível pela Lei Geral de Proteção de Dados, este é tratado pela instituição lócus, como confidencial, apoiando-se, em parte, no Artigo 195, XI, da Lei de Proteção ao Segredo Industrial (Lei nº 9.279/96), que determina que comete crime quem "divulga, explora ou utiliza-se, sem autorização, de conhecimentos, informações ou dados confidenciais, utilizáveis na indústria, comércio ou prestação de serviços, excluídos aqueles que sejam de conhecimento público ou que sejam evidentes para um técnico no assunto, a que teve acesso mediante relação contratual ou empregatícia, mesmo após o término do contrato".

O inventário de dados, percorreu as oito áreas da IES lócus e mapeou todos os mecanismos, que tratam dados dos titulares, desta forma, atingindo um total de quarenta e três processos institucionais de tratamento de dados pessoais examinados, para cada qual, as dezenove variáveis acima foram aplicadas.

Um aspecto relevante ao Inventário de Dados é a temporalidade e destinação de documentos institucionais, ou seja, o tempo de retenção que os documentos oficiais, físicos ou digitais, que a IES gera e manipula, deve ser cumprido, conforme disposições governamentais e ou regulatórias. Destarte, relacionaram-se todos os instrumentos relativos a esta guarda e

conservação, emitidos pelo Arquivo Nacional e dispostos pelo Ministério da Justiça e Segurança Pública[8]:

Do Ministério da Fazenda – MF:

Portaria AN nº 290, de 22.11.2016 - DOU nº 225, seção 1, p. 24, de 24.11.2016. Código de Classificação e Tabela de Temporalidade e Destinação de Documentos relativos às atividades-fim do MF. Sítio eletrônico:

- ✓ http://www.siga.arquivonacional.gov.br/images/codigos_tabelas/00_CodigoClassificacao_MF.pdf

Da Secretaria da Receita Federal do Brasil – RFB:

Portaria AN/MJC nº 291, de 23.11.2016 - DOU nº 226, seção 1, p. 33, de 25.11.2016. Portaria AN nº 221, de 10.11.2014 - DOU nº 218, seção 1, p. 26, de 11.11.2014 [Revogada]. Tabela de Temporalidade e Destinação de Documentos de Arquivo relativos às atividades-fim da RFB. Sítio eletrônico:

- ✓ http://www.siga.arquivonacional.gov.br/images/codigos_tabelas/rfb_ttd_af.pdf

Das Instituições Federais de Ensino Superior – IFES:

O Ministério da Educação publicou Portaria MEC nº 1.261, de 23 de dezembro de 2013 sobre obrigatoriedade de uso do Código de Classificação e Tabela de Temporalidade e Destinação de Documentos de Arquivo relativos às Atividades-Fim pelas Instituições de Educação Superior, Portaria MEC nº 1.224, de 18 de dezembro de 2013, instituindo normas sobre a manutenção e guarda do Acervo Acadêmico das Instituições de Educação Superior (IES) pertencentes ao sistema federal de ensino. Portaria AN/MJ nº 092, de 23 de setembro de 2011 - DOU nº 185, seção 1, p. 26, de 26/09/2011. A Tabela de Temporalidade e Destinação de Documentos de Arquivo relativos às atividades-fim das IFES. Sítio eletrônico:

- ✓ http://www.siga.arquivonacional.gov.br/images/codigos_tabelas/portaria_n092_2011_tabela_de_temporalidade_e_destinao.pdf

Mais que um mero documento o RIPD é um processo desenhado para mapear e gerir os riscos aos direitos e liberdades fundamentais dos titulares de dados, apoiando Controladores a cumprir os requisitos da lei como também a demonstrar que foram tomadas as medidas apropriadas para garantir a conformidade, ou seja, trata-se de uma ferramenta valiosa para prestação de contas e respeito.

[8] http://www.siga.arquivonacional.gov.br/index.php/legislacao-e-normas/legislacao-portarias/31-gestao-de-documentos/resultado-das-atividades-de-gestao-documental/159-codigos-de-classificacao-e-tabelas-de-temporalidade-destinacao-de-documentos

Sobre o Inventário de Dados, construiu-se o Relatório de Impacto a Proteção de Dados Pessoais, o qual também não apresenta modelos expressivos disponíveis para adoção, diante disto, foram articulados dois documentos: 1) pautado sobre as premissas legais pertinentes a LGPD, derivado diretamente do inventário, observável junto ao "**Apêndice D2**"; 2) formulado sobre as diretrizes ao DPIA[9] (Data Protection Impact Assessment, prevista no artigo 35 da General Data Protection Regulation [GPDR]) proposto pelo EC[10] (European Commission) da União Europeia, observável junto ao "**Apêndice D3**";

Outra contribuição de curto prazo é a entrega de uma Política Institucional de Privacidade e Proteção de Dados Pessoais, ("**Apêndice D4**"), um dos instrumentos de implementação do *privacy by design*[11], fazendo parte da estrutura de documentos dedicada a proteção de dados, a política alvitra a visibilidade do tratamento de dados pessoais. Trata-se de um documento endereçado aos clientes diretos e indiretos das instituições, de serviços ou de sistemas, portanto, é uma declaração pública do compromisso da empresa com o respeito e preservação dos direitos fundamentais dos titulares de dados.

Sobre o compromisso como respeito aos direitos dos titulares de dados surge a Política de cookies da IES, que declara e tipifica a existência destes arquivos que coletam e armazenam dados dos usuários da internet, informando a razão destas ações e requerendo o consentimento para tal. Dito isto, a norma está disponível junto ao "**Apêndice D4**" em "TERMOS DE USO E SERVIÇO – Cookies. "

Como última contribuição de caráter imediato, anexa-se o "**Apêndice D5**" que articula e concatena os ajustes, fundamentados sobre a obra de Pinheiro e Weber (2019), pertinentes aos consentimentos e contratos que celebram as avenças entre as partes: a) IES (Controlador) e colaboradores (titulares de dados); b) IES (Controlador) e parceiros de negócio (Operadores); c) IES (Controlador) e alunos (titulares de dados); relacionando todos os termos de consentimento necessários a coleta e tratamento de dados pessoais, mapeados pela pesquisa, e apontando seus respectivos responsáveis imediatos (CORISKOWNERS: Corresponsáveis pelo risco inerente). A tabela 26, expõe todos os ajustes de ordem contratual e de consentimento realizados, indicando os atores que compartilharão a responsabilidade pelo cumprimento deste compliance:

[9] https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236
[10] Agência de Proteção de Dados - União Europeia: https://ec.europa.eu/info/about-european-commission_en
[11] ***Privacy by design***, ou privacidade desde a concepção, é uma abordagem ligada à Engenharia de Sistemas e que preza pela privacidade do usuário durante todo o processo de construção de uma solução

Tabela 26
Contratos, consentimentos e responsáveis

AJUSTES Contratos & Consentimentos	RESPONSÁVEIS CoRiskOwners
Consentimento: Termo de uso de dados pessoais para processo seletivo de vaga empregatícia (de trabalho) Contratos que celebrarão avenças entre IES Lócus (ESCOLA) e Titulares de dados (colaboradores contratados):	Departamento de Recursos Humanos Jurídico
Consentimento: Monitoramento e auditorias informacionais	Departamento de Recursos Humanos e Jurídico Departamento de Tecnologia e Informação
Consentimento: Termo de uso de dados pessoais para rede WI-FI da IES Lócus (ESCOLA) Consentimento: Termo de uso de dados pessoais (navegacionais) para Cookies de sítios eletrônicos da IES Lócus (ESCOLA) Consentimento: Termo de uso de dados pessoais para (pré) inscrição em vestibular da IES Lócus (ESCOLA)	Departamento de Tecnologia e Informação, Marketing e Jurídico
Contratos de prestação de serviços educacionais IES Lócus (ESCOLA) e Titulares de dados (ALUNO): matrícula	Departamento(s) de Matrícula(s), Secretaria Centro Universitário e Jurídico:
Contratos que celebrarão avenças entre IES Lócus (Controlador - Contratante) e Parceiro Externo (Operador - Contratada):	Departamento de Compras, Jurídico e Departamento demandante:

4.2.4.4 Possibilidade de melhorias a médio e longo prazo

Parte precípua da análise dos resultados refere-se as contribuições a médio prazo, aqui descritas como melhorias, a qual repousa sobre a compreensão dos benefícios não imediatos entregues pela pesquisa, pratica e teoricamente significativos.

Sob a perspectiva acadêmica, teórica, compõe-se o modelo conceitual, desenvolvido sobre a literatura de Gestão Econômica (Catelli, 1999) e a Filosofia da Modelagem (Bunge, 1974), que mimetiza o ambiente decisório das organizações, apoiando e orientando as estratégias de uso e proteção de dados pessoais por empresas de todos os seguimentos. A figura 15, abaixo, reapresenta o modelo desenvolvido e anteriormente demonstrado junto as páginas 43 a 48 desta obra:

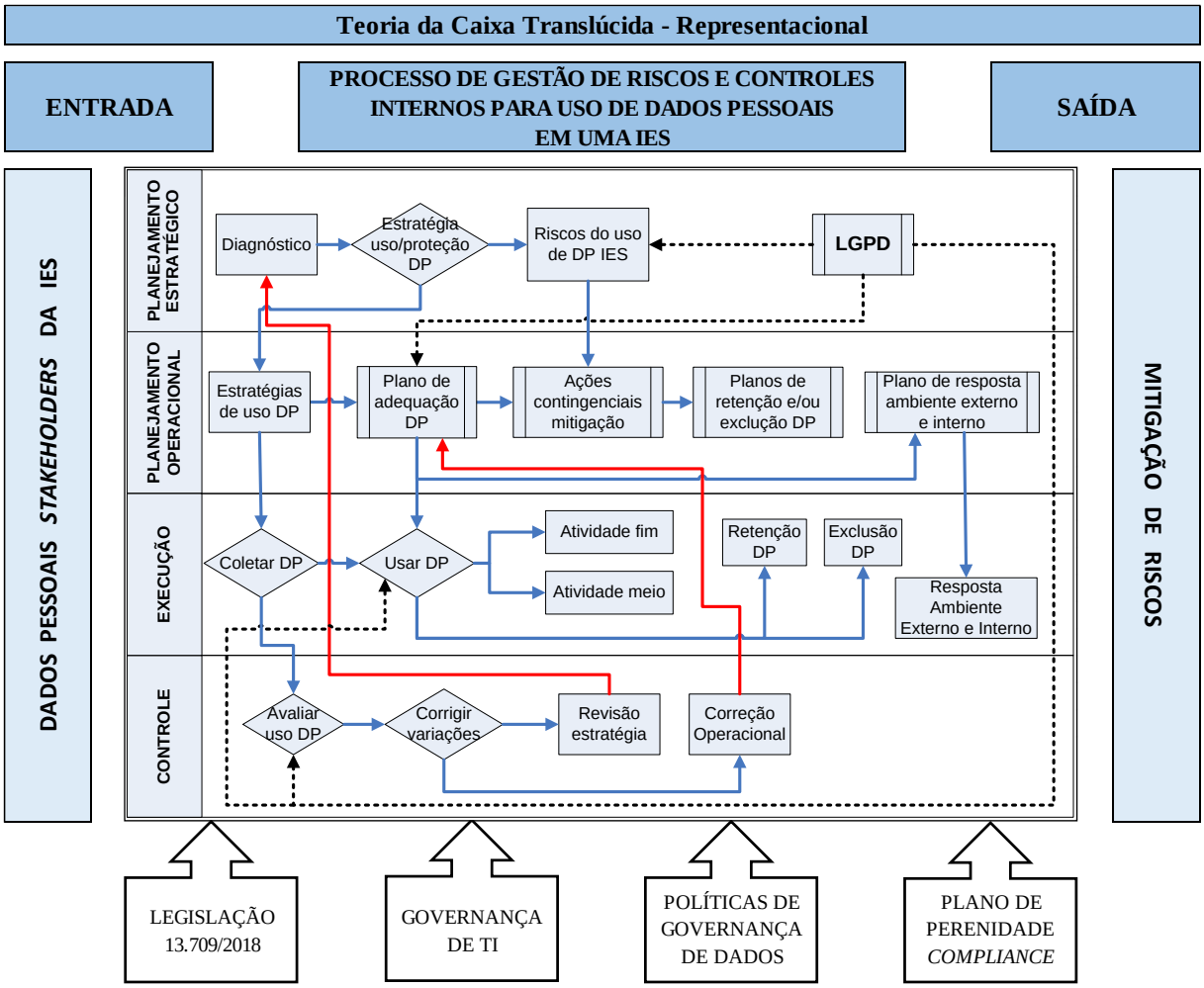

Figura 15. **Modelo Conceitual de compliance à LGPD a luz de Bunge.**

O modelo abrange o processo de gestão de riscos e controles internos para o uso e proteção de dados pessoais da IES lócus e apresenta como entrada os dados pessoais dos stakeholders e como saída o tratamento do risco relacionado, no modelo, descrito como "mitigação", na linha limítrofe alinham-se as variáveis internas e externas ao modelo que o afetam diretamente: Legislação, Governança e perenidade do estado de conformidade.

Sob o panorama prático, administrativo, a pesquisa apresenta o plano formal de *compliance*, como contribuição de médio prazo. O modelo operacionaliza a adequação organizacional pertinente a privacidade e proteção de dados pessoais, já apresentado e explorado junto as páginas 63 a 66 desta obra e abaixo reexposto, figura 16:

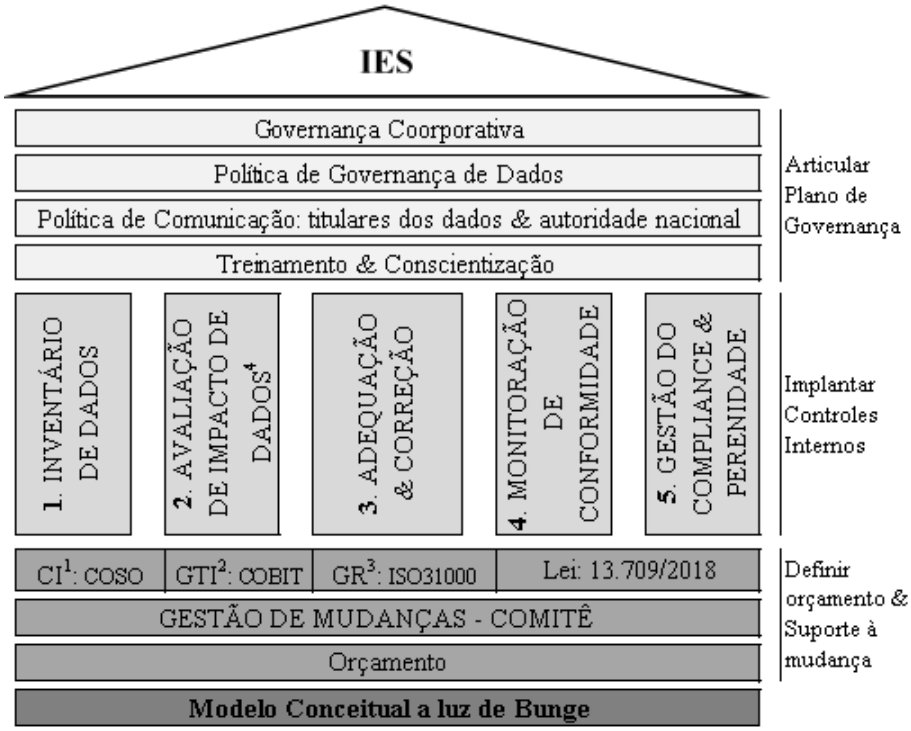

Figura 16. Plano de adequação a LGPD

O plano ergue-se sobre o modelo conceitual de Bunge e Catelli e baliza, os ajustes relacionados ao atingimento da regulação imposta, posicionando-se entre a estratégia institucional de uso de dados pessoais e a operacionalização e perenidade do *compliance* em todas as áreas da empresa.

Perante esta planificação a extensão da conformidade para demais departamentos administrativos e unidades de negócios da IES lócus, não abrangidas pela pesquisa, torna-se exequível sem maiores ou distintos esforços dos já empreendidos nesta direção. Nesta direção, a pesquisa aponta, sob caráter premente, algumas recomendações: a) nomear um Encarregado de Dados Pessoais; b) criar e publicar um sítio eletrônico dedicado a Proteção de Dados da IES; c) publicar, item “b”, os dados do Encarregado, canais de comunicação e a Política Institucional de Privacidade e Proteção de Dados; c) divulgar amplamente o sítio eletrônico, item “b”, junto aos canais digitais de comunicação com as comunidades administrativa, acadêmica (docente e discente), redes sociais e principal sítio eletrônico da instituição.

4.2.4.5 Avaliar existência de aspectos negativos

Todo método possui possibilidades e limitações (Vergara, 2006), o presente estudo circunscreve-se as análises de aspectos, teóricos e práticos, da intervenção junto a IES lócus, portanto, tornando inaplicável a generalização dos achados, alinhamento entre variáveis literárias versus observáveis e conclusão alcançados.

Alguns aspectos interferiram negativamente junto a execução da pesquisa intervencionista, assim sendo, a tabela 27 os apresenta seguidos de seus impactos e recomendações de tratamento:

Tabela 27
Aspectos negativos da pesquisa: impactos e recomendações

Aspectos Negativos	Impactos	Recomendações
- Dificuldade de compreensão dos *stakeholders* sobre a razão da presença e trabalho do pesquisador junto ao departamentos;	- Atraso nos processos de mapeamento de dados; - Imprecisão das informações coletadas; - Retrabalho;	- Reforçar comunicação da alta gestão (Reitores) com as áreas sobre a pesquisa; - Aplicar de início preleções aos times diretamente envolvidos;
- Resistência dos colaboradores em munir informações precisas sobre os processos e operação institucional;		- Aplicar preleções aos times (departamentos) diretamente envolvidos; - Desenvolver um senso de engajamento e pertencimento coma pesquisa; - Desenvolver (com o apoio da alta gestão) senso de emergência;
- Viés na visão, das áreas de TI, da proteção de dados pessoais (direitos dos titulares) com a segurança, "tecnológica", da informação;	- Atraso no processo de avaliação ambiental (inicial);	- Aplicar preleções aos times (departamentos) diretamente envolvidos;
- Indisponibilidade de agenda para entrevistas;	- Atraso no processo de avaliação ambiental (inicial e final)	- Explorar meios tecnológicos para reuniões remotas; - Propor horários mais flexíveis; - Desenvolver (com o apoio da alta gestão) senso de emergência;

Intervenção sugere mudança e todo mudança compreende alterações no comportamento humano sejam relativas a processos, rotinas ou ferramentas, entretanto pessoas são, majoritariamente, resistentes variações de seu *status quo*, muitas vezes se opondo a ajustes organizacionais, motivadas ora pela incapacidade de mudar, ora pela ausência de entendimento sobre os fatores motivadores da transformação (Armstrong, 1985; Herzog, 1991; Hong & Kim, 2002; Kirsch et al., 2011; Kotter, 1995; Kotter, 2012; Wood, 1995).

Por isso, estima-se que todo processo intervencionista, sob dimensão prática da pesquisa, possa ser sensivelmente beneficiado se, antes de qualquer ação do pesquisador, um plano maciço de comunicação institucional, da alta gestão aos gestores e colaboradores envolvidos, ocorra de forma estruturada, promovendo e fomentando: a) contato inicial com o

pesquisador com as áreas: palestra(s); b) engajamento e pertencimento à intervenção; c) senso de urgência e importância da pesquisa; d) legitimidade da ação.

5 Considerações Finais

A evolução tecnológica que há décadas impulsiona organizações, ao redor do globo, traz consigo uma maior exposição ao risco informacional, exigindo das nações regulamentações que alinhem esta evolução e escalada a privacidade e a proteção dos dados das pessoas, diante disto, o presente trabalho articula como questão de pesquisa e objetivo primordial a proposição de um framework conceitual e funcional para uso e proteção de dados em uma instituição de ensino superior.

Sobre uma estendida revisão bibliográfica abrangendo Controles Internos, Gestão de Riscos, Governança de TI e a Lei Geral de Proteção de Dados do Brasil, aliada, a Gestão Econômica preconizada por Armando Catelli e a Filosofia da Modelagem de Mario Bunge, desenvolveu-se a compreensão necessária para construção de um modelo que atendesse, com sucesso, o objetivo central desta pesquisa.

Os objetivos específicos, secundários, também foram atingidos: i) colaborar com o processo de compliance à lei; ii) elevar os níveis de governança da informação percebidos pela alta gestão (reitores); iii) alinhar conhecimento científico (variáveis teóricas [literatura]) com o conhecimento prático (variáveis observáveis [stakeholders]); iv) disseminar o conhecimento sobre Gestão de Riscos e Governança de TI, ainda incipientes no segmento educacional, na IES lócus.

Como principal contribuição a pesquisa entrega um modelo conceitual e funcional de uso da proteção de dados, o qual perfila estratégias de utilização destes dados pela atividade de meio e-ou fim da instituição com a operacionalização da proteção relativa, mimetizando o ambiente decisório sobre as variáveis endógenas e exógenas ao modelo. Com isto, permite-se seguir o processo de adequação a lei do ponto onde a pesquisa para sem maiores e ou distintos esforços dos já dedicados.

Semelhantemente relevantes, outros benefícios, dispostos pelo modelo tratam da perenidade do compliance atingido, ou seja, do exercício continuo e acrônico dedicado a manutenção do estado de adequação, ajustes e correções e da potencial aplicação do modelo em organizações de outros setores, que não o educacional, cabendo apenas ajustes quanto a temporalidade documentacional trazida pelos órgãos reguladores do segmento adotado.

Em um momento ainda embrionário da Regulamentação da Proteção de Dados no país e da ausência de literatura de referência sobre o tema, a pesquisa pretende contribuir com a

construção do entendimento científico sobre o uso e a proteção de dados das pessoas, provendo instrumentos que auxiliem no entendimento dos riscos relativos, orientando o percurso da adequação e provisionando artefatos multidisciplinares pertinentes a sua conformidade.

Como qualquer estudo científico, a pesquisa possui limitações e fragilidades, que versam tanto sobre a dimensão prática quanto a teórica: i) ausência de um modelo de mensuração ideal, pela escassez de tempo hábil para coletar e analisar dados após a implementação do framework construído, desta forma, consolidando as contribuições a médio e longo prazo sobre variáveis e indicadores quantitativos como: mitigação de riscos das respostas à incidentes dados e-ou a titulares de dados e-ou Agência Nacional de Proteção de Dados, percepção (*ext-ant* e *ext-post*) de mais stakeholders em cargos de gestão; ii) impossibilidade de generalizar achados acadêmicos concernentes ao alinhamento entre literatura e variáveis observáveis; iii) impossibilidade de implementar o plano de perpetuidade, dado a ausência de tempo hábil, desta forma encerrando a intervenção, previamente, com a conclusão da apuração dos resultados iniciais.

Para pesquisas futuras sugere-se o desenvolvimento dos temas Gestão de Risco e Governança de TI, aplicados ao segmento educacional, sob caráter ainda preambular, pouco explorado no Brasil e no mundo. Recomenda-se também a maior adoção da pesquisa intervencionista, que pode trazer contribuições teóricas relevantes e ainda melhorar a prática, promovendo a aproximação do pensar científico às atividades observáveis no mercado de trabalho. Por fim, considerada a ausência de literatura relevante sobre a Legislação de Proteção de Dados do nosso país, sua repercussão sobre as organizações e o caráter inédito desta obra, aconselha-se a exploração do tema e seus impactos, nas empresas.

Referências

Abraham, J. M. (2013). *Risk management and accountability guide for university and college boards*. Washington, DC: Association of Governing Boards of Universities and Colleges.

Abraham, S. E. (2012). Information technology, an enabler in corporate governance. *Corporate Governance, 12*(3), 281-291.

Abu-Musa, A. (2009). Exploring the importance and implementation of COBIT processes in saudi organizations: an empirical study. *Information Management Computer Security, 17*(2), 73–95. Available at: http://www.emeraldinsight.com/10.1108/09685220910963974

Anderson, D. R., Sweeney, D. J., & Williams, T. A. (2007). Estatística aplicada à administração e economia. São Paulo: Thomson Learning.

Ahmed, A., Kayis, B., & Amornsawadwatana, S. (2007). A review of techniciansfor risk management in projects. *Benchmarking International Journal*, *14*(1), 22-36.

Aken, J. E. van (2004). Management research based on the paradigm of the design sciences: the quest for field-tested and grounded technological rules. *Journal of management studies, 41*(2), 219-246.

Albrecht, B., & Pirani, J. A. (2004). Using an IT governance structure to achieve alignment at the University of Cincinnati. *EDUCAUSE Center for Applied Research*, Boulder, Colorado. Recuperado de https://library.educause.edu/resources/2004/5/using-an-it-governance-structure-to-achieve-alignment-at-the-university-of-cincinnati

Ali, S., & Green, P. (2012). Effective information technology (IT) governance mechanisms: An IT outsourcing perspective. *Information Systems Frontiers*, *14*(2), 179-193.

Almeida, R., Pereira, R., & Silva, M. (2013). It governance mechanisms patterns. In X. Franch, & P. Soffer (Eds.), *Advanced Information Systems Engineering Workshops* (pp. 156-161). Berlin: Springer Heidelberg.

Alreemy, Z., V. Chang, R. Walters, & Wills, G. (2016). Critical success factors (CSFs) for Information technology governance (ITG). *International Journal of Information Management, 36*(6), Part A, 907-916

Argyris, C., Putnam, R., & McLain Smith, D. (1985). *Action science*. San Francisco: Jossey-Bass.

Ariff, M. S. B. M., Zakuan, N., Tajudin, M. N. M., Ahmad, A., Ishak, N., & Ismail, K. (2014). A framework for risk management practices and organizational performance in higher education. *Review of Integrative Business and Economics Research, 3*(2), 422-432.

Armstrong, P. (1985). Changing management control strategies: the role of competition between accountancy and other organisational professions. Accounting, organizations and society, 10(2), 129-148.

Ashby, S. (2011). Risk management and the global banking crisis: lessons for insurance solvency regulation. *Issues and Practice, 36*(3), 330-347.

Association of Governing Boards of Universities and Colleges (2007). *Meeting the challenges of enterprise risk management in higher education*. National Association of College and University Business Officers. Recuperado de http:www.ucop.edu/enterprise-riskmanagement/_files/agb_nacubo_hied.pdf

Atkinson, A. A., & Shaffir, W. (1998). Standards for field research in management accounting. *Journal of Management Accounting Research, 10,* p. 41-68

Azira Ahmad (2014). Examining Risk Behaviour and Risk Management Practices In Oil And Gas Construction Industry. Unpublished Master Thesis, UTM.

Baard, V. (2010). A critical review of interventionist research. *Qualitative Research in Accounting & Management, 7*(1), 13-45.

Baffa, G., Poggio, G., & Fachinetti, A. (2018, agosto). Taxalert: Privacidade de Dados – Nova Lei Geral de Proteção de Dados Pessoais Brasileira. Ernest Yong. Recuperado de https://www.ey.com/Publication/vwLUAssets/TA-Agosto/%24File/TA-21082018-Privacidade-de-Dados.pdf

Bajgoric, N. (2014). Business continuity management: A systemic framework for implementation, *Kybernetes*, *43*(2), 156-177.

Baldvinsdottir, G., Mitchell, F., & Norreklit, H. (2010). Issues in the relationship between theory and practice in management accounting. *Management Accounting Research, 21*(2), 79–82.

Beasley, M., Pagach, D., & Warr, R. (2008). Information conveyed in hiring announcements of senior executives overseeing enterprise-wide risk management processes. *Journal of Accounting, Auditing & Finance, 23*(3), 311-332.

Berle, A. A., & Means, G. C. (1932). *The modern corporation and private property*. New York: The Macmillan Company.

Beer, S. (1959). *Cybernetics and management*. London: English Universities Press.

Beer, S. (1972). *Brain of the firm*. London: The Penguin Press.

Benaroch, M., Chernobai, A., & Goldstein, J. (2012). An internal control perspective on the market value consequences of IT operational risk events. *International Journal of Accounting Information Systems, 13*(4), 357-381.

Bhattacharjya, J., & Chang, V. (2006). Adoption and implementation of IT governance: Cases from Australian higher education. In *Proceedings of the Australasian Conference on Information Systems (ACIS '06)*, Adelaide. Recuperado de https://pdfs.semanticscholar.org/7e9e/2322e306172f8b404c4487e697e1e376b88b.pdf

Bhattacharjya, J., & Chang, V. (2007). Evolving IT governance practices for aligning IT with business – a case study in an Australian institution of higher education. *Journal of Information Science and Technology, 4*(1), 24-46.

Bianchi, I. S., & Sousa, R. D. (2016). IT Governance mechanisms in higher education. *Procedia Computer Science, 100,* 941-946. Recuperado de https://www.sciencedirect.com/science/article/pii/S187705091632422X

Bichsel, J., & Patrick, F. (2014, June). Getting your ducks in a row: It governance, risk, and compliance programs in higher education, Research Report. Louisville, CO: ECAR. Recuperado de https://library.educause.edu/-/media/files/library/2014/3/ers1402.pdf

Bioni, B. R. (2019). *Proteção de dados pessoais: a função e os limites do consentimento*. Forense.

Boynton, A. C., Jacobs, G. C., & Zmud, R.W. (1992). Whose responsibility is IT management? *Sloan Management Review, 33*(4). 32-38.

Bowen, P. L., Cheung, M. Y. D., & Rohde, F. H. (2007). Enhancing IT governance practices: A model and case study of an organization's efforts. International Journal of Accounting Information Systems, 8(3), 191-221.

Bradley, R.V., & Pratt, R. M. E. (2011). Exploring the relationships among corporate entrepreneurship, IT governance, and risk management. In *System Science, 44th Hawaii International Conference*, Kauai, HI, pp. 1-10.

Brand, J. C. (2013). The governance of significant enterprise mobility security risks (Doctoral dissertation, Stellenbosch: Stellenbosch University).

Brandão, R. V., Araujo, I. S., & Veit, E. A. (2011). A modelagem científica vista como um campo conceitual. *Caderno Brasileiro de Ensino de Física, 28*(3), 507-545.

Brow, A. E., & Grant, G. G. (2005), Framing the frameworks: A review of IT governance research. *Communications of the Association for Information Systems, 15,* 696-712.

Brown, C. V. (1997). Examining the emergence of hybrid IS governance solutions: Evidence from a single case site. *Information Systems Research, 8*(1), 69-94.

Brown, C. V., & Magill, S. L. (1994). Alignment of the is functions with the enterprise. *MIS Quarterly, 18*(4), 371-403.

Brown, W., & Nasuti, F. (2005). Sarbanes-Oxley and enterprise security: IT governance-what it takes to get the job done. *Information Systems Security, 14*(5), 15-28.

Bunge, M. (1960). La ciencia, su método y su filosofia. Buenos Aires: Ediciones Siglo Veinte, 1960. 110 p

Bunge, M. (1974). Os conceitos de modelo. Bunge M. Teoria e realidade São Paulo: Perspectiva, 11-40.

Bunge, M. (1983). La investigación cientıfica. Barcelona: Editorial Ariel.

Calder, A. (2005). *IT governance guildlines for directors*. United Kingdom: It Governance Publishing.

Calder, A., & Moir, S. (2009). *IT governance, implementing frameworks and standardsfor the corporate governance of IT*. United kingdom: IT Governance Ltd.

Catelli, A. (1999). Controladoria: uma abordagem da gestão econômica - GECON. São Paulo: Atlas.

Cavalcante, D. S., Peter, M. D. G. A., & Machado, M. V. V. (2013). Organização dos orgãos de controle interno municipal no estado do Ceará: Um estudo na região metropolitana de Fortaleza. *ASAA-Advances in Scientific and Applied Accounting*, *4*(1), 24-43.

Cervo, A. L., Bervian, P. A., & Silva, R. (2007). *Metodologia científica* (6a ed.). São Paulo: Pearson Prentice Hall.

Chang, S.-I., Yen, D. C., Chang, I.-C., & Jan, D. (2014). Internal control framework for a compliant ERP system. *Information and Management*, *51*(2), 187-205.

Chang, V., Walters, R. J., & Wills, G. (2013). The development that leads to the cloudcomputing business framework. *International Journal of InformationManagement*, 33(3), 524–538. doi: http://dx.doi.org/10.1016/j.ijinfomgt.2013.01.005

Chapman, C. (1997). Project risk analysis and management: PRAM the generic process. *International Journal of Project Management, 15*(5), 273-281.

Chaxel, A.-S. (2016). Why, when, and how personal control impacts information processing. *Journal of Consumer Research, 43*(1), 179-197.

Chen, R.-S., Sun, C.-M., Helms, M. M., & Jih, W.-J. (2008). Aligning information technology and business strategy with a dynamic capabilities perspective: A longitudinal study of a Taiwanese semiconductor company. *International Journal of Information Management, 28*(5), 366-378.

Coen, M., & Kelly, U. (2007). Information management and governance in Uk Higher Education Institutions: Bringing It in from the cold. *Perspectives: Policy and Practice in Higher Education, 11*(1), 7-11.

Coffman, D. (2014). Managing data protection in higher education. *Risk Management, 61*(7), 32-36.

Committee of Sponsoring Organizations of the Treadway Commission (1992). *Internal control: Integrated framework,* New York: American Institute of Certified Public Accountants.

Committee of Sponsoring Organizations of the Treadway Commission (2004). *Enterprise risk management – Integrated framework*. New York: American Institute of Certified Public Accountants.

Committee of Sponsoring Organizations of the Treadway Commission (2013). *Internal control: Integrated framework.* New York: American Institute of Certified Public Accountants.

Committee of Sponsoring Organizations of the Treadway Commission. (2017). *COSO Enterprise Risk Management: Integrating with Strategy and Performancement*. AICPA.

Council, T. (2003). Code of Corporate Governance. *Annual Review and Reporting, 5*, 52.

Cram, W. A., Brohman, K., & Gallupe, R. B. (2016). Information systems control: A review and framework for emerging information systems processes. *Journal of the Association for Information Systems*, *17*(4), 216-266.

Cyert, R. M., & March, J. G. (1963). *A behavioral theory of the firm*. Englewood Cliffs; New Jersey: Prentice-Hall, Inc.

Dahlberg, T., & Lahdelma, P. (2007). IT governance maturity and IT outsourcing degree: Na exploratory study. In *System Sciences, 40th Annual Hawaii International Conference*, Waikola, HI. Recuperado de https://ieeexplore.ieee.org/document/4076859

Damianides, M. (2005). Sarbanes-Oxley and IT governance: New guidance on IT control and compliance. *Information Systems Management*, *22*(1), 77-85.

Daniballe, R. G. (2017). *Modelo conceitual e funcional de identificação e acumulação de resultados para a mensuração de rentabilidade por cliente: uma proposta para empresa de saúde ocupacional.* (Dissertação de Mestrado). Fundação Escola de Comércio Alvares Penteado – FECAP, São Paulo, SP, Brasil.

Deloitte (2018, março 22). Lei Geral de Proteção de Dados: Nova regulamentação estabelece padrões sobre a gestão da privacidade de informações e permite que as empresas aumentem sua competitividade. Recuperado de https://www2.deloitte.com/br/pt/pages/risk/articles/lgpd.html

Demchenko Y, Gommans L, & Laat, C. (2000). Web services and grid security vulnerabilities and threats analysis and model. *Advanced Internet Research Group*. Amsterdam: University of Amsterdam. Recuperado de https://www.academia.edu/4307683/Web_services_and_grid_security_vulnerabilities_and_threats_analysis_and_model

Develaki, M. (2007). The model-based view of scientific theories and the structuring of school science programmes. Science & Education, 16(7-8), 725-749.

Dey, P. K., Kinch, J., & Ogunlana, S. O. (2007). Managing risk in software development projects: a case study. *Industrial Management & Data Systems*, *107*(2), 284-303.

Dimaggio, P., & Powell, W. The iron cage revised: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147-160, 1983.

Enriques, L., & Volpin, P. (2007). Corporate governance reforms in continental Europe. *Journal of Economic Perspectives*, *21*(1), 117-140.

Enterprise Risk Management - Integrated Framework, Executive Summary, Committee of Sponsoring Organizations of theTreadway Commission, September 2004. Online at: www.coso.org/documents/COSO_ERM_ExecutiveSummary.pdf

Feferbaum, M., & Lima, S. H. (2019). Lei Geral de Proteção de Dados Pessoias no setor educacional brasileiro. *Revista do Advogado (São Paulo), (144*), 99-106.

Feltus, C., Petit, M., & Dubois, E. (2009, November). Strengthening employee's responsibility to enhance governance of IT: COBIT RACI chart case study. In Proceedings of the first ACM workshop on Information security governance (pp. 23-32).

Fernández Martínez, A., & Llorens Largo, F. (2009). *An IT governance framework for universities in Spain*. Universidad de Alicante. Departamento de Ciencia de la Computación e Inteligencia Artificial. Recuperado de http://rua.ua.es/dspace/handle/10045/11216

Firoiu, M. (2015). General considerations on risk management and information system security assessment according to ISO/IEC 27005:2011 and ISO 31000:2009 standards. *Calitatea, 16*(149), 93-97. Retrieved from https://search.proquest.com/docview/1739063146?accountid=34586

Flyvbjerg, B. (2001). *Making social science matter: Why social inquiry fails and how it can succeed again.* Cambridge: Cambridge University Press.

Fraser, R. S., Simkins, B. J., & Narvaez, K. (2015). Implementing enterprise risk management case studies and best practices. Hoboken: NJ: Wiley & Sons, Inc.

Fraser, W., & Tweedale, R. (2003). It Governance at Qut. *EDUCAUSE in Australasia* [Working paper]. Adelaide, Australia. Recuperado de https://eprints.qut.edu.au/253/

Gallagher, A. J. (2013). *Collaborative risk management: "Risk management" vs. "managing risk"*. Gallagher Higher Education Practice. Recuperado de http://www.ajgrms.com/portal/server.pt/gateway/PTARGS_0_28406_584576_0_0_18/AJG%20HEP%20 Collaborative%20RM%20White%20Paper%202013.pdf

Garrity, J. (1963). Top management and computer profits. *Harvard Business Review, 41*(4), 6-13.

Giere, R. N., Bickle, J., & Mauldin, R. F. Understanding Scientific Reasonoing. 2006. Toronto: Thomson Wadsworth, 5.

Gill, A. (2008). *Corporate governance as social responsibility: A research agenda*. Berkeley J. Int'l L., 26, 452.

Gil, A. C. (2002). *Como elaborar projetos de pesquisa* (5a ed.). São Paulo: Atlas.

Gil, A. C. (1999). *Métodos e técnicas de pesquisa social* (5a ed.). São Paulo: Atlas.

Grama, J. L. (2015, february 22). Understanding It Grc in higher Education: It governance. *Educause review.* Recuperado de http://er.educause.edu/articles/2015/2/understanding-it-grc-in-higher-education-it-governance

Grembergen, W. van (2004). *Strategies for information technology governance*. Hershey: Idea Group Publishing. Recuperado de https://books.google.com.br/books?hl=pt-BR&lr=&id=IleHOs41iIMC&oi=fnd&pg=PP1&dq=Strategies+for+information+technology+governance+&ots=wX3CUFJcBN&sig=eg160h-l7_JODH2XOdp40A1tUiE#v=onepage&q=Strategies%20for%20information%20technology%20governance&f=false

Grembergen, W., van, & Haes, S., de (2010). A research journey into enterprise governance of IT, business/IT alignment and value creation. *International Journal of IT/Business Alignment and Governance, 1*(1), 1-13.

Haes, S., de, & Grembergen, W., van (2004). It Governance and Its Mechanisms. *Information Systems Control Journal*, *1*, 27-33.

Haes, S., de, & Grembergen, W., van (2005). IT governance structures, processes and relational mechanisms: Achieving IT/business alignment in a major belgian financial group. In Proceedings of the 38th Annual Hawaii International Conference on System Sciences, Track 8, Hawaii. Recuperado de https://www.researchgate.net/publication/221178165_IT_Governance_Structures_Processes_and_Relational_Mechanisms_Achieving_ITBusiness_Alignment_in_a_Major_Belgian_Financial_Group

Haes, S., de, & Grembergen, W., van (2006). Information technology governance best practices in belgian organisations. In *System Sciences, Proceedings of the 39th Annual Hawaii International Conference*, Hawaii. Recuperado de https://ieeexplore.ieee.org/abstract/document/1579688

Haes, S., de, & Grembergen, W., van (2009). An exploratory study into it governance implementations and Its impact on business/It alignment. *Information Systems Management, 26*(2), 123-137.

Haes, S., de, Grembergen, W., van, & Debreceny, R. S. (2013). COBIT 5 and Enterprise Governance of Information Technology: Building Blocks and Research Opportunities. *Journal of Information Systems*, *27*(1), 307–324. doi:10.2308/isys-50422

Heidemann, L. A., Araujo, I. S., & Veit, E. A. (2016). Modelagem Didático-científica: integrando atividades experimentais e o processo de modelagem científica no ensino de Física. Caderno Brasileiro de Ensino de Física, 33(1), 3-32.

Helsloot, I., & Jong, W. (2006). Risk management in higher education and research in the Netherlands. *Journal of Contingencies and Crisis Management, 14*(3), 142-159.

Henderson, J. C., & Venkatraman, N. (1993). Strategic alignment: Leveraging information technology for transforming organizations. *IBM Systems Journal, 32*(1), 4-16.

Herzog, J. P. (1991). People: the critical factor in managing change. Journal of systems management, 42(3), 6.

Hicks, M., Pervan, G., & Perrin, B. (2012). A study of the review and improvement of It governance in Australian Universities. *International Conference on Information Resources Management (CONF-IRM).* University Sector. Recuperado de https://pdfs.semanticscholar.org/5f66/f9240b3c7c4f31666a38013dcb17bc803603.pdf

Hinton, K. (2012). A practical guide to strategic planning in higher education. Society for College and University Planning. Retrieved 2015 from http://www.keene.edu/ksc/assets/files/19900/scpguideonplanning.pdf

Hoitash, U., Hoitash, R., & Bedard, J. C. (2009). Corporate governance and internal control over financial reporting: A comparison of regulatory regimes. *The accounting review, 84*(3), 839-867.

Hong, K. K., & Kim, Y. G. (2002). The critical success factors for ERP implementation: an organizational fit perspective. Information & management, 40(1), 25-40.

Information Systems Audit and Control Association (2007). *COBIT® 4.1*. Rolling Meadows, IL: Autor.

Information Systems Audit and Control Association (2009a). *Building the business case for COBIT® and Val IT™: Executive Briefing*. Rolling Meadows, IL: Autor.

Information Systems Audit and Control Association (2009b). *Implementing and continually improving IT Governance.* Rolling Meadows, IL: Autor.

Information Systems Audit and Control Association (2009c). *The Risk IT framework: RiskIT based on COBIT*. Rolling Meadows, IL: Autor.

Information Systems Audit and Control Association (2010). *Enterprise value: Governance of IT investments. The val IT framework 2.0.* Rolling Meadows, IL: Autor.

Information Systems Audit and Control Association (2012a). COBIT 5: *Implementation*. Rolling Meadows, IL: ISACA.

Information Systems Audit and Control Association (2012b). COBIT 5: *A Business Framework for the Governance and Management of Enterprise IT*. Rolling Meadows, IL: ISACA.

International Accounting Standards Committee Fundation (1994). *Control objectives for information and related technology: COBIT*. Rolling Meadows, Illinois: Autor.

ISO 31000: Risk management. *Principles and guidelines on implementation.* Geneva, 2009a. Recuperado de https://www.iso.org/standard/43170.html

ISO 31000: Risk management. G*uidelines.* Geneva, 2009b. Recuperado de https://www.iso.org/standard/65694.html

IT Governance Institute (2000). *COBIT*. Rolling Meadows, IL: Autor.

IT Governance Institute (2001*). Board Briefing on IT Governance*. Rolling Meadows, IL: Information Systems Audit and Control Foundation IT Governance Institute, 54.

IT Governance Institute (2005). *COBIT® 4.* Rolling Meadows, IL Autor.

IT Governance Institute (2006*). IT Control Objectives for Sarbanes-Oxley: The role of IT in the design and implementation of internal control over financial reporting* (2nd ed). Rolling Meadows, IL: IT Governance Institute.

Jairak, K., & Praneetpolgrang, P. (2013). Applying IT governance balanced scorecard and importance-performance analysis for providing IT governance strategy in university. *Information Management & Computer Security*, *21*(4), 228-249.

Jairak, K., Praneetpolgrang, P., & Subsermsri, P. (2015). Information technology governance practices based on sufficiency economy philosophy in the Thai university sector. *Information Technology & People*, *28*(1), 195-223.

Jensen, M. C. (1993). The modern industrial revolution, exit, and the failure of internal control systems. *Journal of Finance*, *48*(3), 831-880.

Jönsson, S., & Lukka, K. (2007). There and back again. Doing IVR in manage-ment accounting. In: C. Chapman, A. Hopwood, & M. Shields (Eds.), *Handbook of Management Accounting Research* (Vol. 1, pp. 373–397). Amsterdam: Elsevier.

Jouini, M., & Rabai, L. B. A. (2016). Comparative study of information security risk assessment models for cloud computing systems. *Procedia Computer Science, 83*, 1084–1089.

Kaplan, R. S., & Mikes, A. (2012). Managing risks: A new framework. *Harvard Business Review*, *90*(6), 48-60.

Kasanen, E., Lukka, K., & Siitonen, A. (1993). The constructive approach inmanagement accounting research. *Journal of Management Accounting Research, 5*, 241–264.

Kayworth, T., & Sambamurthy, V. (2000). Managing the information technology infrastructure. *Baylor Business Review*, *18*(1), 13-15.

Kenwood, P. A., & Rafferty, P. D. (2017). Exploring the culture of risk-awareness among the professoriate: the implementation of enterprise risk management in higher education. American association of university administrators, 32(1), 243-255.

Kerzner, H. (2017). Project management: a systems approach to planning, scheduling, and controlling. John Wiley & Sons.

Kirsch, C., Chelliah, J., & Parry, W. (2011). Drivers of change: a contemporary model. Journal of Business Strategy, 32(2), 13-20

Klumb, R., & Azevedo, B. M., de, (2014). A percepção dos gestores operacionais sobre os impactos gerados nos processos de trabalho após a implementação das melhores práticas de governança de TI no TRE/SC. *Revista de Administração Pública, 48*(4), 961–982.

Ko, D., & Fink, D. (2010). Information technology governance: An evaluation of the theory-practice gap. *Corporate Governance*, *10*(5), 662-674.

Kotter, J. P. (1995). Leading change: Why transformation efforts fail. Citado 7400

Kotter, J. (2012). The 8-step process for leading change. Kotter International.

Kululanga G., & Kuotcha W. (2010). Measuring project risk management process for construction contractors with statement indicators linked to numerical scores. *Engineering, Construction and Architectural Management, 17*(4), 336-351.

Kwak, Y. H., & Stoddard, J. (2004). Project risk management: Lessons learned from software development environment. *Technovation*, *24*(11), 915-920.

KPMG (2018). Proteção de dados no Brasil e no mundo - Uma leitura do que vigora hoje, a importância da nova legislação e como as empresas e os entes públicos devem se preparar. *KPMG Business Magazine*, *44*, 18-21.

Labro, E., & Tuomela, T. S. (2003). On bringing more action into management accounting research: process considerations based on two constructive case studies. *European accounting review*, *12*(3), 409-442.

Laine, T., Korhonen, T., Suomala, P., & Rantamaa, A. (2016). Boundary subjects and boundary objects in accounting fact construction and communication. *Qualitative Research in Accounting and Management, 13*(3), 303–329.

Lazic, M., & Heinzl, A. (2011). IT governance and business performance- A resource based analysis. In *Pacis 2011 Proceedings*, 103, Brisbane. Recuperado de https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1102&context=pacis2011

Leach, L. P. (1999). Critical chain project management improves project performance. Project Management Journal, 30(2), 39-51.

Lei n. 9.279, de 14 de maio de 1996. Regula direitos e obrigações relativos à propriedade industrial. Recuperado de http://www.planalto.gov.br/ccivil_03/leis/l9279.htm

Lei n. 13.257, de 8 março de 2016. Dispõe sobre as políticas públicas para a primeira infância e altera a Lei no 8.069, de 13 de julho de 1990 (Estatuto da Criança e do Adolescente), o Decreto-Lei no 3.689, de 3 de outubro de 1941 (Código de Processo Penal), a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei no 5.452, de 1o de maio de 1943, a Lei no 11.770, de 9 de setembro de 2008, e a Lei no 12.662, de 5 de junho de 2012. Recuperado de http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Lei/L13257.htm

Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). (Marco Civil da Internet). Recuperado de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm

Lewin, K. (1946). Action research and minority problems. In Lewin, G.W. (Eds.) (1948). *Resolving social conflicts: Selected paperson group dynamics* (pp. 201–216). New York: Harper and Brothers.

Lewin, G. W. (Eds.) (1948). *Resolving social conflicts: Selected paperson group dynamics*. New York: Harper and Brothers.

Lima, A. de A. P. de. (2019). *Controles internos no 3º setor: Uma proposta de framework para a casa Durval Paiva* (Dissertação de Mestrado). Fundação Escola de Comércio Alvares Penteado – FECAP, São Paulo, SP, Brasil.

Lima, D., Maciel, C., & Libonati, J. (2008). Os impactos gerados na adequação da estrutura de controles internos de uma empresa brasileira às exigências da seção 404 da Lei Sarbanes-Oxley: Um estudo de caso. *Anais do Encontro da Associação Nacional de Pós-Graduação e Pesquisa em Administração*, Rio de janeiro. RJ, Brasil, 32. Recuperado de http://www.anpad.org.br/admin/pdf/CON-B2629.pdf

Loh, L., & Venkatraman, N. (1992). Diffusion of information technology outsourcing: influence sources and the Kodak effect. *Information Systems Research, 3*(4), 334-359.

Luciano, E. M., & Testa, M. G. (2011). Controles de governança de tecnologia da informação para a terceirização de processos de negócio: uma proposta a partir do COBIT. *Journal of Information Systems and Technology Management (Online), 8*(1), 237-262. Recuperado de http://www.scielo.br/pdf/jistm/v8n1/a12v8n1.pdf

Luftman, J. (2003). Assessing IT/business alignment. *Information Systems Management*, *20*(4), 9-15.

Lukka, K., &Vinnari, E. (2017). Combining actor-network theory with interventionist research: Present state and future potential. *Accounting, Auditing & Accountability Journal*, *30*(3), 720–753.

Lukka, K. (2000). The key issues of applying the constructive approach tofield research. In T. Reponen (Ed.), *Management Expertise for theNew Millennium, in Commemoration of the 50th Anniversary of theTurku School of Economics and Business Administration* (pp. 113–128). Publications of the Turku School of Economics and Business Administration.

Lukka, K. (2003). The constructive research approach. In L. Ojala, O-P. Hilmola (Eds.), *Case Study Research in Logistics* (pp.83–101). Publications of the TurkuSchool of Economics and Business Administration.

Lukka, K. (2005). Approaches to case research in management accounting: The nature of empirical intervention and theory linkage. In S. Jönsson, J. Mouritsen (Eds.), *Accounting in Scandinavia – The Northern Lights* (pp. 375–399). Copenhagen: Liber & Copenhagen Business School Press.

Lunardi, G. L., Becker, J. L., Maçada, A. C. G., & Dolci, P. C. (2014). The impact of adopting it governance on financial performance: An empirical analysis among brazilian firms. *International Journal of Accounting Information Systems*, *15*(1), 66-81. doi: https://doi.org/10.1016/j.accinf.2013.02.001

Machado Meyer (2018, agosto). *Lei 13.709/18: Lei de proteção de dados pessoais*. Recuperado de https://www.machadomeyer.com.br/images/publicacoes/PDFs/Lei_Protecao_de_Dados_ebook_18.pdf

Malmi, T., Jarvinen, P., & Llilrank, P. (2004). A collaborative approach for managing project cost of poor quality. *European Accounting Review, 13*(2), 293-317

Maldonado, V. N., Blum, R. O., & Borelli, A. (2019). *LGPD: Lei geral de proteção de dados: comentada.* Revista dos Tribunais.

Martins, G. A., & Theophilo, C. R (2009). *Metodologia da investigação cientifica para ciências sociais aplicadas* (3a ed.). São Paulo: Atlas.

March, J., & Simon, H. (1958). *Organizations*. New York: John Wiley.

Mattessich, R. (1995). Conditional-normative accounting methodology: Incorporating value judgments and means-end relations of anapplied science. *Accounting, Organizations and Society*, *20*(4), 259–284.

McWhorter, L. B., Matherly, M., & Frizzell, D. M. (2006). The connection between performance measurement and risk management. *Strategic Finance, 87*(8), 50-55.

Medida Provisória n. 869. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá

outras providências. Recuperado de http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Mpv/mpv869.htm

Mikes, A., & Kaplan, R. (2013). *Managing risks: Towards a contingency theory of enterprise risk management*. [Working paper no. 13-063]. Boston: Harvard Business School.

Mitchell, F. (2002). Research and practice in management accounting: Improving integration and communication. *European Accounting Review, 11*(2), 277–289.

Mitchell, R. K., Agle, B. R., & Wood, D. J. (1997). Toward a theory of stakeholder identification and salience: Defining the principle of who and what really counts. Academy of management review, 22(4), 853-886.

Morgan, M. S., Morrison, M., & Skinner, Q. (Eds.). (1999). Models as mediators: Perspectives on natural and social science (Vol. 52). Cambridge University Press.

Mu, E., & Carroll, J. (2016). Development of a fraud risk decision model for prioritizing fraud risk cases in manufacturing firms. *International Journal of Production Economics, 173*, 30-42.

Mulholland, C. S. (2018). Dados pessoais sensíveis e a tutela de direitos fundamentais: uma análise à luz da lei geral de proteção de dados (Lei 13.709/18). *Revista de Direitos e Garantias Fundamentais, 19*(3), 159-180.

National Institute of Standards and Technology (2010). *Contingency planning for information systems: Updated guide for federal organizations.* Gaithersburg, Maryland, EUA: National Institute of Standards and Technology. Recuperado de https://ws680.nist.gov/publication/get_pdf.cfm?pub_id=906210

Nordberg, D. (2010). *Corporate governance: Principles and issues*. Sage.

Norreklit, H., Norreklit, L., & Mitchell, F. (2010). Towards a paradigmatic foundation for accounting practice. *Accounting, Auditing & Accountability Journal, 23*(6), 733–758.

Novotny, A., Bernroider, E., & Koch, S. (2012). Dimensions and operationalisations of IT governance: a literature review and meta-case study. In *Proceedings of the 2012 International Conference on Information Resource Management (Conf-IRM 2012*), University of Economics and Business, Vienna, pp. 1-13, Revuperado de http://epub.wu.ac.at/3660/1/novotny2012.pdf

Nugroho, H. (2014). Conceptual model of it governance for higher education based on cobit 5 framework. *Journal of Theoretical and Applied Information Technology, 60*(2), 216-221.

Olson, M. H., & Chervany, N. L. (1980). The relationship between organizational characteristics and the structure of the information services function. *MIS Quarterly, 4*(2), 57-69.

Pang, M. S. (2014). It Governance and business value in the public sector organizations - The role of elected representatives in IT governance and its impact on It Value in Us State governments. *Decision Support Systems, 59*, 274-285.

Pang, Y., & Li, Q. (2013). Game analysis of internal control and risk management. *International Journal of Business and Management, 8*(17), 103–112.

Parent, M., & Reich, B. H. (2009). Governing information technology risk. *California Management Review, 51*(3), 134-152.

Patty, M. (1995). A matéria roubada: a apropriação crítica do objeto da física contemporânea. São Paulo: Editora da Universidade de São Paulo, 82.

Peleias, I. R. (2002). *Falando sobre controle interno*. (IOB: Temática Contábil e Balanços). São Paulo: IOB Thomson

Peleias, I. R., Caetano, G., Parisi, C., & Pereira, A. C. (2013). Produção científica sobre controle interno e gestão de riscos no EnANPAD e Congresso USP: análise bibliométrica no período 2001-2011. *Revista Universo Contábil*, *9*(4), 29-49. Recuperado de http://proxy.furb.br/ojs/index.php/universocontabil/article/view/3323/2527

Peleias, I. R., Caetano, G., Parisi, C., & Pereira, A. C. (2013). Produção científica sobre controle interno e gestão de riscos no EnANPAD e Congresso USP: análise bibliométrica no período 2001-2011. Revista Universo Contábil, 9(4), 29-49.

Pereira, R., Almeida, R., & Silva, M. (2014). It Governance Patterns in the Portuguese Financial Industry. In *47th Hawaii International Conference on Systems Sciences, HICSS*, Hawaii, USA.: IEEE, pp. 4386-4395.

Peterson, R. (2004). Crafting information technology governance. *Information Systems Management, 21*(4), 7-22.

Pietrocola, M. (1999). Construção e realidade: o realismo científico de Mário Bunge e o ensino de ciências através de modelos. *Investigações em ensino de Ciências, 4*(3), 213-227.

Pike, K. L. (1954). Emic and etic standpoints for the description of behaviour. In K.L. Pike (Ed.), *Language in Relation to a Unified Theory of theStructure of Human Behaviour* (pp. 8–28). Summer Institute of Linguistics, Glen-dale.

Pike, K. L. (1967). *Language in relation to a unified theory of the structureof human behavior* (2nd ed.). Paris: Mouton.

Pinheiro, P. P. (2018). *Proteção de dados pessoais: Comentários à Lei n. 13.709/2018 (LGPD)*. São Paulo: Saraiva.

Pinheiro, P. P., Weber, S. T., & Neto, A. A. O. (2019). *Fundamentos dos Negócios e Contratos Digitais.* São Paulo: Thomson Reuters Revista dos Tribunais.

Portaria n. 1342, de 14 de novembro de 2012. O Ministério da Educação, no uso da atribuição que lhe confere o art. 87, parágrafo único, inciso II da Constituição e tendo em vista o disposto nos artigos 4º e 26 do Decreto no 7.690, de 2 de março de 2012, resolve. Recuperado de http://portal.mec.gov.br/index.php?option=com_docman&view=download&alias=13555-portaria-1342-de-14-11-2012-pdf&category_slug=junho-2013-pdf&Itemid=30192

Power, M. (2004). *The risk management of everything: Rethinking the politics of uncertainty*. London: Demos.

Project Management Institute. (2017). A guide to the project management body of knowledge (PMBOK guide) (Vol. 2). Project Management Institute.

Racz, N., Weippl, E., & Seufert, A. (2010, July). A process model for integrated IT governance, risk, and compliance management. In *Proceedings of the Ninth Baltic Conference on Databases and Information Systems (DB&IS 2010)* (pp. 155-170). Recuperado de http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.464.1936&rep=rep1&type=pdf

Raghupathi, W. (2007). Corporate governance of IT: A framework for development. *Communications of the ACM*, *50*(8), 94-99.

Rautiainen, A., Sippola, K., & Matto, T. (2017). Perspectives on relevance: The relevance test in the constructive research approach. *Management Accounting Research, 34*, pp. 19–29.

Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. *MIS quarterly*, 81-113.

Ribeiro, J., & Gomes, R. (2009). It governance using cobit implemented in a high public educational institution: A Case study. In G. Sirbiladze, A. Sikharulidze, I. Khutsishvili, T. Lominadze (Eds.). *Computing and computational intelligence: Proceedings of the European computing conference (ecc '09); Proceedings of the 3rd international conference on computational intelligence (ci '09)* (pp.41-52). Tbilisi, Georgia. Recuperado de https://www.researchgate.net/profile/Rui_Gomes6/publication/228656099_IT_governance_using_COBIT_implemented_in_a_high_public_educational_institution_a_case_study/links/55eda1a008ae3e12184829fb.pdf

Ross, J. W., & Weill, P. (2005). A matrixed approach to designing IT governance. *Sloan Management Review, 46*(2), 26-34.

Rubino, M. and Vitolla, F. (2012). Risk management, a key process of corporate governance: analysis of the related effects on organisational behavior. In D. Tipuric, & M. Dabic (Eds), *Management, Governance and Entrepreneurship* (Cap. 17, pp. 314-327). Darwen: New Perspectives and Challenges, Access Press.

Rubino, M., & Vitolla, F. (2014). Corporate governance and the information system: How a framework for IT governance supports ERM. *Corporate Governance*, *14*(3), 320-338.

Mitra, S., Karathanasopoulos, A., Sermpinis, G., & Dunis, C. (2015). Operational risk: Emerging markets, sectors and measurement. *European Journal of Operational Research, 241*(1), 122-132.

Sabherwal, R., & Kirs, P. (1994). The alignment between organizational critical success factors and information technology capability in academic institutions. *Decision Sciences*, *25*(2), 301-330.

Saleh, J. M., & Almsafir, M. K. (2013, December). The drivers of ITIL adoption in UNITEN. In *2013 International Conference on Advanced Computer Science Applications and*

Technologies (pp. 479-484). IEEE. Recuperado de https://ieeexplore.ieee.org/abstract/document/6836629

Sambamurthy, V., & Zmud, R. W. (1999). Arrangements for information technology governance: A theory of multiple contingencies. *MIS Quarterly, 23*(2), 261-290.

Sambamurthy, V., & Zmud, R.W. (2000). Research commentary: The organizing logic for an enterprise's IT activities in the digital era-a prognosis of practice and a call for research. *Information Systems Research, 11*(2), 105-114.

Scapens, R. W. (2014). My final editorial. *Management Accounting Review, 24*(4), 245–250.

Schein, E. (1987). *The clinical perspective in fieldwork*. Newsbury Park: Sage

Schlosser, F., Wagner, H.-T., Beimborn, D., & Weitzel, T. (2010). The role of internal business/IT alignment and IT governance for service quality in IT outsourcing arrangements. In *System Sciences (HICSS), 43rd Hawaii International Conference on System Sciences*, Honolulu, HI, pp. 1-10.

Schobel, K., & Denford, J. S. (2013). The chief information officer and chief financial officer dyad in the public sector: how an effective relationship impacts individual effectiveness and strategic alignment. *Journal of Information Systems, 27*(1), 261-281.

Schwarz, A., & Hirschheim, R. (2003). An extended platform logic perspective of IT governance managing perceptions and activities of IT. *Journal of Strategic Information Systems,12* (2), 129-166.

Sindicato dos Estabelecimentos de Ensino no Estado de São Paulo (2018). Impactos da nova lei de proteção de dados pessoais. *Escola Particular*, *22*(249), 4-10. Recuperado de https://www.sieeesp.org.br/uploads/sieeesp/imagens/revista/revista_249.pdf

Simonsson, M., & Johnson, P. (2006, June). Defining IT governance-a consolidation of literature. *Department of Industrial Information and Control Systems - Royal Institute of Technology* (EARP Working Paper MS103). Estocolmo, Suécia. Recuperado de http://citeseerx.ist.psu.edu/viewdoc/download;jsessionid=3A30474BC55C5C047B8436B1A1C8C7AD?doi=10.1.1.64.6388&rep=rep1&type=pdf

Spira, L., & Page, M. (2003). Risk management: The reinvention of internal control na the changing role of internal audit. *Accounting, Auditing and Accountability Journal*, *16*(4), 640-661.

Suomala, P., & Lyly-Yrjänäinen, J. (2012). *Management accounting researchin practice. Lessons learned from an interventionist approach*. NewYork: Routledge.

Suomala, P., Lyly-Yrjänäinen, J., Laine, T., & Mitchell, F. (2017). Interventionist management accounting research: Theory contributions with societal impact. New York: Routledge.

Suomala, P., Lyly-Yrjänäinen, J., & Lukka, K. (2014). Battlefield around interventions: A reflective analysis of conducting interventionist research in management accounting. *Management Accounting Research, 25*(4), 304-314.

Symons, C. (2005). IT governance framework. *Forrester Best Practices, 29*, 1-17. Recuperado de http://cba.co.nz/download/Forr051103656300.pdf

Tallon, P. P. (2007). A process-oriented perspective on the alignment of information technology and business strategy. *Journal of Management Information Systems*. *24*(3), 227-268.

Tallon, P. P., & Pinsonneault, A. (2011). Competing perspectives on the link between strategic information technology alignment and organizational agility: Insights from a mediation model. *MIS Quarterly*, *35*(2), 463-484.

Tchankova, L. (2002). Risk identification: Basic stage in risk management. *Environmental Management and Health,13*(3), 290 – 297.

Tiwana, A., & Konsynski, B. (2010), Complementarities between organizational IT architecture and governance structure. *Information Systems Research, 21*(2), 288-304.

Tricker, R. B., & Tricker, R. I. (2015). *Corporate governance: Principles, policies, and practices.* Oxford University Press, USA.

Tufano, P. (2011). Managing risk in higher education. *Forum Futures Symposium*, 2010. Aspen. Recuperado de http://forum.mit.edu/articles/managing-risk-in-higher-education/

Tuttle, H. (2018). Global regulation landscape: Data protection in 2018. *Risk Management*, *65*(11), 28-34.

Van de Ven, A. H. (2007). *Engaged scholarship: A guide for organizationaland social research*. Oxford: Oxford University Press.

Van de Ven, A. H., & Johnson, P. E. (2006). Knowledge for theory and practice. *Academy of Management Review, 31*(4), 802-821.

Vergara, S. C. (2006). *Projetos e relatórios de pesquisa em administração* (7a ed.). São Paulo: Atlas.

Simson, E. M., von (1995). The recentralization of IT. *Computerworld*, *29*(51), 1-5.

Walliser, B. (1977). Systèmes et modèles: introduction critique à l'analyse de systèmes. Editions du Seuil.

Wan, S. H. C., & Chan, Y.-H. (2008). *Improving service management in campus It operations*. *Campus-Wide Information Systems, 25*(1), 30-49.

Webb, P., Pollard, C., & Ridley, G. (2006, January). Attempting to define IT governance: Wisdom or folly?. *In Proceedings of the 39th Annual Hawaii International Conference on System Sciences* (HICSS'06) (Vol. 8, pp. 194a-194a). IEEE. Recuperado de https://ieeexplore.ieee.org/abstract/document/1579684

Weill, P., & Ross, J. W. (2004). *It governance: How top performers manage it decision rights for superior results.* Boston, Massachusetts: Harvard Business School Press.

Wilkin, C. L., & Chenhall, R. H. (2010). A review of IT governance: a taxonomy to inform accounting information systems. *Journal of Information Systems*, *24*(2), 107-146.

Wood Jr, T. (1995). Mudança organizacional: uma introdução ao tema. Organizacional, 1.

Wu, S. P.-J, Straub, D. W., & Liang, T.-P. (2015). How information technology governance mechanisms and strategic alignment influence organizational performance: Insights from a matched survey of business and IT managers. *MIS Quarterly, 39*(2), 497-518. Recuperado de http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=102375761&lang=pt-br&site=ehost-live

Yin, R. K. (2010). Estudo de caso: Planejamento e métodos (4a ed.). Sao Paulo: Bookman

Zhen, W., & Xin-yu, Z. (2007, August). An ITIL-based IT service management model for chinese universities. In *5th ACIS International Conference on Software Engineering Research, Management & Applications (SERA 2007)*. IEEE, pp. 493-497.

Apêndice A1 - Constructos da Pesquisa

Constructo Dimensão	Variáveis	Assertivas		Referências - Literatura
LGPD - 13.709/18	Ciência	1	Conhece ou já ouviu falar da Lei Geral de Proteção de Dados do Brasil?	Lei n. 13.709, (2018); SIEEESP, (2018); Mulholland, (2018); Tuttle, (2018); Global Risks Report, (2018); Privacy Governance Report, (2018); Privacy Rights Clearinghouse, (2014); Ariff, Zakuan, Tajudin, Ahmad, Ishak e Ismail, (2014); Machado Meyer, (2018); Pinheiro, (2018); Baffa, Poggio e Fachinetti, (2018); Maldonato, Blum e Borelli (2019); Feferbaum e Lima, (2019); Bioni, (2019);
		2	A instituição opera dados de seus clientes?	
		3	A instituição entende como pode ser impactada pela lei?	
	Importância	4	Acredita que a lei possa beneficiar e, ou prejudicar as instituições de ensino? Por que?	
	Conformidade	5	Há iniciativas que preveem adequação à lei, na instituição?	
Governança da Informação (TI)	Relevância	6	Acredita que a tecnologia seja importante para a sustentabilidade financeira institucional?	Ko e Fink, 2010; Benaroch, Chernobai e Goldstein (2012); Demchenko, Gommans e De Laat, (2000); Coffman, (2014); Weill e Ross (2004); Lunardi et al (2014); Grama, (2015); Benaroch, Chernobai e Goldstein, (2012); Mitra, Karathanasopoulos, Sermpinis e Dunis, (2015); Grembergen, (2004); Calder, (2005); Bichsel e Patrick (2014); Sabherwal e Kirs, (1994); Hicks et al., (2012); Ali e Green (2012); Pang, (2014); Bianchi e Sousa, (2016)
		7	A evolução tecnológica (ex.: internet) vulnerabiliza as instituições?	
		8	O ambiente acadêmico, por vezes flexível e colaborativo, pode vulnerabilizar as instituições?	
	Presença	9	A instituição possui processos de Governança de TI?	
		10	Estes processos estão claros e, ou divulgados?	
		11	A IES tem clareza quanto ao papel da TI em sua estratégia?	
	Conformidade	12	Controles Internos de TI (Governança TI) podem auxiliar a conformidade institucional?	

Apêndice A2 - Perguntas stakeholders "chave" (controladores) após adequação

Constructo Dimensão	Variáveis observáveis	Assertivas entrevistas semi-estruturadas: Stakeholders "chave" Reitor e Vice-Reitor		Referências - Literatura
LGPD 13.709/18	Ciência	1	Seu grau de entendimento sobre a lei foi, de alguma forma, melhorado com o processo de adequação?	Lei n. 13.709, (2018); SIEEESP, (2018); Mulholland, (2018); Tuttle, (2018); Global Risks Report, (2018); Privacy Governance Report, (2018); Privacy Rights Clearinghouse, (2014); Ariff, Zakuan, Tajudin, Ahmad, Ishak e Ismail, (2014); Machado Meyer, (2018); Pinheiro, (2018); Baffa, Poggio e Fachinetti, (2018); Maldonato, Blum e Borelli (2019); Feferbaum e Lima, (2019); Bioni, (2019);
	Conformidade	2	Sobre a dimensão de compliance a lei, você acredita que a IES foi beneficiada com a adequação?	
	Risco	A	Mitigação de riscos e sanções pertinentes à lei;	
	Importância	B	Atividade meio e fim da IES;	
Governança da Informação (TI)	Relevância	3	Sobre a dimensão de governança e controles internos você acredita que a IES foi favorecida?	(Global Risks Report, 2018; Privacy Governance Report, 2018; Ariff et al., 2014; ISO 27005, 2011) (Coffman, 2014; Privacy Rights Clearinghouse, 2018; Helsloot & Jong, 2006)
	Presença	A	Governança de TI (Informação): construção, exposição-divulgação;	(Jairak & Praneetpolgrang, 2013; Hicks, Pervan, & Perrin, 2012 ; Tufano 2011; Sabherwal & Kirs, 1994)
	Risco	B	Controles internos;	(Peleias, 2012; ISACA, 2010; COBIT, 2012, COSO-ERM, 2017; ISO31000, 2009; Kululanga & Kuotcha 2009)
		C	Gestão de riscos;	
	Conformidade	4	Suas expectativas enquanto (cargo do stakeholder) foram atendidas? O que comentaria?	

Apêndice A3 - Questionário (escala Likert) treinamentos - *workshops*

Constructo Dimensão	Variáveis observáveis	Assertivas (antes e após) treinamento Stakeholders Técnico Administrativos		Referências - Literatura
LGPD 13.709/18	Ciência	1	Qual seu grau de conhecimento ou entendimento sobre Privacidade de dados?	Lei n. 13.709, (2018); SIEEESP, (2018); Mulholland, (2018); Tuttle, (2018); Global Risks Report, (2018); Privacy Governance Report, (2018); Privacy Rights Clearinghouse, (2014); Ariff, Zakuan, Tajudin, Ahmad, Ishak e Ismail, (2014); Machado Meyer, (2018); Pinheiro, (2018); Baffa, Poggio e Fachinetti, (2018); Maldonato, Blum e Borelli (2019); Feferbaum e Lima, (2019); Bioni, (2019);
		2	Qual seu grau de conhecimento da lei (LGPD)?	
	Importância	3	Em qual grau, você entende que a IES pode estar exposta a lei?	
ESCALA**: 1 =** Ausente ou Nenhum**; 2 =** Baixo**; 3 =** Médio**; 4 =** Alto**;**				

Apêndice A4 - Extratificação das respostas de todos os participantes dos treinamentos

ÁREAS	COLABORADORES	1. Qual seu grau de conhecimento ou entendimento sobre Privacidade de dados?		2. Qual seu grau de conhecimento da lei (LGPD)?		3. Em qual grau, você entende que a IES pode estar exposta a lei?		Valor Mínimo apurável	Média Apurada		Valor Máximo apurável	Var % Média ext-ant ext-post
		ext-ant	ext-post	ext-ant	ext-post	ext-ant	ext-post		ext-ant	ext-post		
RECURSOS HUMANOS	1	1	3	2	3	3	4	1	2,00	3,33	4	89%
	2	1	3	2	3	2	3	1	1,67	3,00	4	89%
	3	1	3	2	3	2	3	1	1,67	3,00	4	89%
	4	1	3	2	2	2	3	1	1,67	2,67	4	50%
	5	1	3	1	2	1	3	1	1,00	2,67	4	139%
	Valores consolidados do comportamento da amostra:							**1**	**1,60**	**2,933**	**4**	**89%**
RELACIONA. INSTITUCIONAL	1	1	2	1	2	2	3	1	1,33	2,33	4	50%
	2	1	2	1	2	1	2	1	1,00	2,00	4	50%
	3	1	2	1	2	1	2	1	1,00	2,00	4	50%
	4	1	2	1	2	1	2	1	1,00	2,00	4	50%
	5	1	2	1	2	1	2	1	1,00	2,00	4	50%
	Valores consolidados do comportamento da amostra:							**1**	**1,07**	**2,07**	**4**	**50%**
CENTRAL DO ALUNO	1	2	3	2	3	3	3	1	2,33	3,00	4	22%
	2	1	2	1	3	2	3	1	1,33	2,67	4	89%
	3	1	2	2	2	2	3	1	1,67	2,33	4	22%
	4	1	2	1	3	1	3	1	1,00	2,67	4	139%
	5	1	2	1	3	1	3	1	1,00	2,67	4	139%
	Valores consolidados do comportamento da amostra:							**1**	**1,47**	**2,67**	**4**	**72%**
CENTRAL CARREIRAS	1	2	3	2	3	2	3	1	2,00	3,00	4	50%
	2	2	3	2	3	2	3	1	2,00	3,00	4	50%
	Valores consolidados do comportamento da amostra:							**1**	**2,00**	**3,00**	**4**	**50%**
FINANCEIRO	1	3	4	2	4	3	4	1	2,67	4,00	4	89%
	2	2	3	2	3	2	4	1	2,00	3,33	4	89%
	3	2	3	2	4	2	3	1	2,00	3,33	4	89%
	Valores consolidados do comportamento da amostra:							**1**	**2,22**	**3,56**	**4**	**89%**
SEGURANÇA	1	1	2	1	3	1	3	1	1,00	2,67	4	139%
	2	1	2	1	3	1	3	1	1,00	2,67	4	139%
	Valores consolidados do comportamento da amostra:							**1**	**1,00**	**2,67**	**4**	**139%**
TECNOLOGIA	1	3	4	3	4	3	4	1	3,00	4,00	4	50%
	2	2	4	3	4	2	4	1	2,33	4,00	4	139%
	3	2	3	2	3	2	3	1	2,00	3,00	4	50%
	4	1	2	2	3	2	3	1	1,67	2,67	4	50%
	5	2	3	2	4	2	4	1	2,00	3,67	4	139%
	6	2	3	2	4	2	4	1	2,00	3,67	4	139%
	Valores consolidados do comportamento da amostra:							**1**	**2,17**	**3,50**	**4**	**89%**
COMPRAS	1	3	4	2	4	3	4	1	2,67	4	4	89%
	Valores consolidados do comportamento da amostra:							**1**	**2,67**	**4**	**4**	**89%**

VALORES 1 = Ausente ou Nenhum; 2 = Baixo; 3 = Médio; 4 = Alto;

Apêndice B1 - Tabulação achados entrevistas semiestruturadas

Variáveis Observáveis - LGPD (13.709/18)						**Variáveis observáveis - GOVERNANÇA TI**							
Entrevistados	**Conhece**	**IES opera dados pessoais**	**Entende impactos da lei**	**Entende benefícios e prejuízos**	**Iniciativas para adequar**	**Valor de TI**	**TI vulnerabiliza IES**	**IES mais expostas risco**	**IES detém Gov.TI**	**IES divulga Gov.TI**	**Clareza de TI na estratégia**	**Gov.TI apoia compliance**	**STA[1]**
E1	Parcial	Sim	Sim	Parcial	Sim	Sim	Sim	Sim	Sim	Não	Parcial	Sim	
E2	Parcial	Sim	Sim	Parcial	Sim	Sim	Sim	Sim	Parcial	Não	Parcial	Sim	
E3	Parcial	Sim	Sim	Parcial	Não sabe	Sim	Sim	Sim	Parcial	Não	Parcial	Sim	
E4	Parcial	Sim	Sim	Parcial	Sim	Sim	Sim	Sim	Sim	Não	Parcial	Sim	
E5	Parcial	Sim	Sim	Parcial	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
E6	Parcial	Sim	Sim	Parcial	Não sabe	Sim	Sim	Parcial	Sim	Parcial	Parcial	Sim	
E7	Sim	Sim	Sim	Sim	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
E8	Parcial	Sim	Sim	Parcial	Não sabe	Sim	Sim	Sim	Não	Não	Parcial	Sim	
E9	Parcial	Sim	Sim	Parcial	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
E10	Parcial	Sim	Sim	Parcial	Não sabe	Sim	Sim	Sim	Sim	Parcial	Não	Sim	
E11	Não	Sim	Parcial	Parcial	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
E12	Parcial	Sim	Não	Parcial	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
E13	Parcial	Sim	Sim	Parcial	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
E14	Não	Sim	Não	Não	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
E15	Parcial	Sim	Sim	Parcial	Sim	Sim	Sim	Sim	Parcial	Não	Não	Sim	
E16	Parcial	Sim	Parcial	Não	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
E17	Parcial	Sim	Parcial	Não	Não sabe	Sim	Sim	Sim	Não	Não	Não	Sim	
SPA[2]	88% ≥ Parcial[3]	100%	88% ≥ Parcial[3]	94% ≤ Parcial[4]	76%	100%	100%	94%	76% ≤ Parcial[4]	100% ≤ Parcial[4]	100% ≤ Parcial[4]	100%	**93%**

Nota: 1. STA: Saturação Total da Amostra; 2. SPA: Saturação Parcial da Amostra; 3. ≥ (maior|igual) Parcial: compreende o "sim"; 4. ≤ (menor|igual) Parcial: compreende o "não";

Apêndice B2 - Transcrição sintética – entrevistas semiestruturadas

Q1: VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Entrevistado	Conteúdo
E1	Já ouvi falar sim da LGPD, vinda de uma regulamentação externa, estrangeria, acho que a Europa é a liderança nesta iniciativa;
E2	Já ouvi falar;
E3	Não posso dizer que conheço a fundo, já ouvi falar, mas nunca a li;
E4	Sim, já ouvi falar, já conversei internamente com algumas pessoas..., mas é assim eu nunca li a lei;
E5	Já ouvi falar em alguns eventos dos quais participei, mas não li a LGPD;
E6	Já ouvi falar. Conhecer, não posso dizer que sim, por que não li a lei, não conheço;
E7	Sim;
E8	Sim, já ouvi falar;
E9	Sim, não com profundidade, mas já ouvi falar.
E10	Sim, já ouvi falar. Não conheço com profundidade;
E11	Já ouvi falar, mas não conheço a fundo.
E12	Não só ouvi falar como tive um estudo mais aprofundado da lei;
E13	Sim, já tive a oportunidade e participar de workshops sobre a lei;
E14	Não, não conheço;
E15	Já ouvi falar, mas não conheço;
E16	Sim, já ouvi falar;
E17	Só ouvi falar...;

Q2: VOCÊ SABE DIZER SE A IES OPERA DADOS PESSOAIS?

Entrevistado	Conteúdo
E1	É opera, dados dos clientes, entendidos como alunos da IES. Opera sim, ela tem esses dados e utiliza esses dados em sua gestão...;
E2	Sim com altíssima frequência;
E3	Sim;
E4	Sim;
E5	Ele utiliza bastante;
E6	Muitos! Muitos, muitos dados né? Aí, por exemplo, vai desde a imagem do aluno, né, que está em nossas mãos, por exemplo a imagem do aluno que a gente veicula no impresso, na internet.
E7	Sim opera;
E8	Sim opera;
E9	Sim;
E10	Sim, sobretudo nas matrículas e captando “leads” e coisas deste tipo;
E11	Sim, tanto de alunos, funcionário e fornecedores;
E12	Ela opera sim e tem que operar por que é uma IES e todas suas informações são destinadas para pesquisa;
E13	Sim, a IES tem os acessos e dados de todos os clientes e colaboradores e de toda comunidade acadêmica da instituição;
E14	Não sei responder;
E15	Sim;
E16	Sim;
E17	Sim, quero dizer, acho que sim...sim;

Q3: SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

Entrevistado	Conteúdo
E1	Sim podemos ser impactos pela lei, todos os setores podem ser impactados pela lei. A gente tem que tomar o cuidado, na IES, com conformidade, então essa é uma preocupação grande nossa.
E2	Sim, enquanto cúpula, porém enquanto nível de gestão e colaboradores, não. Há assimetria;
E3	Entendo que sim;
E4	Entende, claro;
E5	Muito! Totalmente...;
E6	Então, essa é uma ponderação que deve partir da interação com a lei. Conhecer a lei, né? Não dá para falar agora você vai ajudar, vai atrapalhar, né, que eu ainda não conheço a lei detalhadamente.
E7	Não completamente, algumas pessoas (instâncias);
E8	Sim inclusive por que existe uma lei n. 13.826/2019 que informa que nós temos que divulgar os nomes e a classificação dos candidatos do processo seletivo...;
E9	Não, acredito que não;
E10	Eu acho que sim, eu espero que sim;
E11	Com certeza;
E12	No meu entendimento ainda não, eu acho que a IES precisa conhecer melhor a lei;
E13	Entendo que a IES tem uma visão parcial de que pode ser impactada pela Lei, a IES ainda carece de mais informações...;
E14	Não sei responder;
E15	Sim;
E16	Não em nível contábil, gerencial não sei responder;
E17	Acho que sim, mas não saberia descrever como e quanto;

Q4: SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Entrevistado	Conteúdo
E1	...eu acho que o resultado para escola pode ser positivo, nós somos uma escola muito cuidadosa... do ponto de vista mercadológico, em desvantagem em alguns momentos quando competíamos com outros players que não tem exatamente esse mesmo cuidado..., e, nesse sentido a gente pode ser beneficiado.
E2	Positivos, particularmente quanto ao impacto nos estudantes como um todo principalmente como cidadãos, há ainda uma questão de privacidade de dados que é muito débil nas organizações... então as escolas têm uma estrutura de dados muito completa que tem o raio x da vida de cada um, isso por si já é uma responsabilidade grande;
E3	Beneficiada no sentido de deixar em "pé de igualdade" com instituições de maior porte que de repente podem manipular, manipulam, de forma não tão ética e moral os dados e prejudicada por conta das sanções previstas caso não estejamos em conformidade;
E4	Ela (a lei) vai impactar a intuição. Beneficiar? Eu acho que alei vai trazer regulações e deixar claro para IES e as pessoas que se relacionam com a instituição como estas informações efetivamente deverão ser tratadas...;
E5	Prejudicar não. Se for falar de prejuízo é só de investimentos que precisam ser feitos, mas acho que é mais benefício, por que, dá mais se segurança para IES se ela for seguir rigidamente o que a lei pede;
E6	Não dá para falar agora você vai ajudar, vai atrapalhar, né, que eu ainda não conheço a lei detalhadamente. Agora a expectativa é que ajude...;
E7	Ela pode. As duas coisas, se a IES não tomar cuidado ela pode se prejudicar muito e se ela adotar uma boa governança...;
E8	É difícil eu te dizer se vai prejudicar a IES depende muito de como isso vai ser trabalhado, a estratégia a empresa;
E9	No primeiro momento, talvez prejudicada, a longo prazo talvez vem um benefício;
E10	Prejudicada se não souber manipular com toda certeza do mundo... Beneficiada, não sei se ela traz algum benefício..., mas eu acho que corre-se mais risco em não estar em compliance;
E11	Negativamente sim, positivamente só se existir um controle mais específico;

E12	Prejudicar eu não acredito... pelo contrário eu acho que vai ajudar bastante;
E13	Eu acredito que a proposta da lei é benéfica, ela tende a proteger o cidadão... eu entendo que as IES precisam ter essa noção e ajustar os seus processos para que lei seja cumprida como deve ser;
E14	Não sei responder;
E15	Prejudicar não, acredito que não, de alguma forma ela vem cobrar algo que é necessário;
E16	Beneficiada se souber usar e tratar os dados que possui. Prejudicada se trabalhar e operar à margem da lei, o que pode acabar trazendo alguma sanção para IES;
E17	Acho que não ser prejudicada é o que vale mais aqui... em se tratando de lei é bom estar regulado;

Q5: A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Entrevistado	**Conteúdo**
E1	Temos iniciativa de adequação com a lei, a nossa área de infraestrutura com o apoio do jurídico e outra outras áreas da escola que manejam estes dados...;
E2	Sim, porém não há uma formação estruturada da IES no momento...;
E3	Certamente há…eu não as conheço, não estou muito envolvido;
E4	Sim como eu falei anteriormente a advogada já tem esta demanda eu não sei como está o desenvolvimento, mas já faz um tempo que a gente conversou...;
E5	Ainda não, que tenha chegado até a mim, não!
E6	Eu acredito que sim. Tem uma pessoa aí Gestor de Infra de TI que, certamente, é o "Testa de ferro" aí para isso, né? E já tem mostrado preocupação, várias vezes, tem interesse
E7	O conhecimento que eu tenho é muito embrionário...;
E8	Olha... tem iniciativas, mas não tem, eu não conheço formalidades;
E9	Que eu saiba não;
E10	Não tenho conhecimento, formalizado não;
E11	Até hoje não, apenas comentários, mas não via ainda nenhum plano de ação a respeito;
E12	Não, não vi nenhuma iniciativa até o momento;
E13	Há algum tempo atrás foi levada a Superintendência/Reitoria a sugestão de criação de um comitê. Mas eu não sei qual é a evolução da criação deste comitê neste momento;
E14	Não sei responder;
E15	Sim, tem iniciativas sim;
E16	Não, até onde sei não conheço nenhum processo ou procedimento que faça isso;
E17	Não sei;

Q6: VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Entrevistado	**Conteúdo**
E1	Fundamental, essencial! Não há negócio ou virtualmente não deve haver negócio que não passe por TI, hoje em dia;
E2	Absolutamente. Importância total, "bone" da operação em particular em relação à novas tecnologias de aprendizagem que estão surgindo e a necessidade sim da gestão de custos fixos com base em processos tecnológicos;
E3	Certeza que sim, tecnologia hoje é base para tudo, tenho falado isso faz tempo: quando a gente nasce e a gente precisa falar para se comunicar, no mundo dos negócios precisa de tecnologia para tudo
E4	Com certeza, por que a tecnologia permite velocidade, segurança, comunicação. Então, no mundo que a gente vive de mobilidade de múltiplos canais de comunicação...;
E5	Eu até trocaria a palavra importante, para mim ela é fundamental, para mim tecnologia nas IES ainda mais como a nossa ela é estratégica e jamais poderia ficar em segundo plano...;
E6	Totalmente, absolutamente! Sim, a gente não pode mais prescindir da contribuição que a tecnologia dá a todos os processos...;
E7	Acredito que sim;
E8	Claro! Tecnologia é importante né;
E9	Sem dúvida, essencial;

E10	Eu acho que hoje não tem essa é uma condição necessária para se ter sucesso. A tecnologia é condição necessária...;
E11	Sem dúvida! Na realidade a TI é a parte mais importante de qualquer empresa, hoje qualquer IES depende 100% de TI, ponto. Não tenho dúvida quanto a isso;
E12	Sem dúvida nenhuma;
E13	100%! Acredito que a TI é importante para sustentabilidade financeira e para toda atividade fim e atividade meio da IES...;
E14	Fundamental;
E15	Total;
E16	Com certeza! Com a digitalização de todas informações financeiras e contábeis hoje em dia, sem a área de TI não há controles contábeis e financeiros efetivos;
E17	Acredito, como profissional de TI fica difícil de ver alguma escola sem tecnologia;

Q7: VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Entrevistado	Conteúdo
E1	Como negócio isso já acontece, porque, a TI ela trouxe a possibilidade a entrega educacional de forma diferente daquela que as escolas tradicionais... Do ponto de vista das suas operações, claro que o mundo caminha para digitalização de processos e de dados e isso pode trazer vulnerabilidade de segurança e de risco operacional para as escolas...;
E2	Ela (TI) pode ser risco, ameaça e oportunidade. Vulnerabiliza se a IES possui uma concepção antiga do que é universidade...;
E3	Com certeza sim, também. Considerando meu parco conhecimento você fica mais exposto com a internet, mas não somente o uso de softwares diversos você fica mais exposto há ataques hackers por exemplo...;
E4	Eu acho que sim e as escolas tem que se preparar para isso, por que, qualquer processo que você adote ele terá suas fragilidades, se você adota um processo que depende só de pessoas uma pessoa pode ficar doente e não aparecer, pode boicotar o processo...;
E5	Muito! Muito crescente isso, e muitas vezes a gente fica correndo atrás do rabo porque a evolução é mais rápida do que nossa capacidade de resposta.
E6	Claro! Ao mesmo tempo que beneficia, prejudica, ao mesmo tempo, com talvez a mesma facilidade e rapidez. É equivalente e ambíguo. Nós temos aqui a preocupação com o "bullying" o "bullying" virtual (CyberBulling)...;
E7	Também acho que pode;
E8	Pode sim, tão positivo quanto negativo;
E9	Acredito que sim, pelo fato de deixar mais expostas as IES e as mídias sociais, em algum momento, vai acabar prejudicando;
E10	Eu acho que sim;
E11	Acredito que sim. Aí são várias explicações desde "fake news" até vulnerabilidades técnicas;
E12	Ela tras risco para a IES!
E13	Sem dúvida alguma! Sim a evolução tecnológica traz essas vulnerabilidades cada vez mais ouve-se falar de fraude de ataques de sequestro de dados;
E14	Com certeza, acho a que a TI (internet) deixa as instituições muito expostas, da mesma forma em que ela é fundamental para empresa e o sucesso, ela expõe demais;
E15	Sim, todo processo tem risco, vale-se fazer a proteção destes riscos;
E16	Sim, porque dependendo do nível de segurança em que isso se aplica, ou seja, se os dados estão online se os dados estão em nuvem, isso tudo é suscetível a "hacking";
E17	Hackers? É sobre eles que esta falando? Se sim, todas as escolas estão em risco...se não, não vejo como...;

Q8: O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Entrevistado	Conteúdo
E1	Acho que pode sim, a gente quer na acadêmica o maior nível de liberdade possível, por que isso faz parte do processo educacional, no entanto isso pode gerar problema de segurança que você não tem no mundo de tijolos;
E2	Do que tange a lei e a privacidade de dados, é muito comum a troca de planilhas de informações sensíveis entre professores e colaboradores, nesse aspecto vulnerabiliza;

E3	Sim, por definição o ambiente acadêmico é mais aberto, você tem IES aqui em São Paulo mesmo no ensino privado que não tem nem portão, você pode entrar e ninguém vai te barrar, não tem nem catraca, então sem dúvida o ambiente acadêmico tende a ser mais flexível que os demais...;
E4	eu acho que é um ambiente menos visado... Mas há também o aluno e ele tem tempo para pensar em coisas incorretas se for o caso se tem casos (muitos casos) de invasão ocorrem dentro das universidades...;
E5	...ambiente acadêmico muitas vezes precisa ser flexível, tem que ser colaborativo porque a gente fala de pesquisas, de compartilhamento de conhecimento, então muitas vezes tem que trabalhar e operar em um ambiente meio que aberto, participativo e isso pode gerar um risco sim de vulnerabilidades, então é um tradeoff...;
E6	Depende das pessoas, da conscientização das pessoas. Isso É bem interessante. Então mesmo que haja a Lei e a regra senão há conscientização, eu acho que há o risco de falhar, senão há a lei e a regra, mas, a conscientização há o risco de funcionar!;
E7	Pode;
E8	Eu acho que sim, pode ter algum tipo de risco de imagem, por exemplo, mas eu acho também que pode trazer muitos benefícios;
E9	Acredito que sim, porque não a regras claras e há mudanças constantes, pode vir a prejudicar a IES;
E10	Torna o processo mais complexo dado você tem acesso de muitas outras pessoas aqui dentro, na sua rede, portanto que faz que você tenha que ter uma diligência maior nos seus processos e no seu compliance de TI;
E11	Sim, porque no ambiente empresarial são funcionário e produtos/serviços, na IES são serviços, funcionários e alunos e são muitos alunos;
E12	Sim!
E13	Sim, eu acredito que sim. O ambiente acadêmico ele é, por natureza, flexível, então acaba sendo mais fácil de ter uma pessoa, uma população circulante dentro Campus;
E14	Eu acho que ela está exposta ao risco, muitas vezes em função do diferente tipo de perfil que ela atende, diferentes pessoas dentro da instituição acadêmica então eu acho que ela está exposta ao risco;
E15	Sim é mais vulnerável, acho que tem muito mais mecanismos de saída, de acesso, o público é maior, acessos online bem maiores;
E16	Sim quanto mais liberdade você dá para quem acessa informações, maior o risco, então quanto maior a liberdade do aluno e do funcionário dentro da IES, maior é o risco que a instituição corre;
E17	Sim e não. Se não tiver boas tecnologias de segurança estará em risco;

Q9: VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Entrevistado	**Conteúdo**
E1	Possui sim, mas é assim a gente é uma IES de médio porte, então obviamente não temos a estrutura organizacional que uma empresa de grande porte tem, não temos escala para isso...;
E2	Se você aplicar a IES a uma escala de governança, de fato já aplicou, é muito baixa. Houve uma pequena evolução, mas ainda há muito pela frente;
E3	Se possui eu não conheço. Claramente há processos de governança, mas não há, nunca vi, uma política de governança;
E4	Eu acho que sim, o PDI (por exemplo) é um documento que deixa claro quais são as metas da área de TI ao longo de um período e essas metas estão relacionadas com aspectos de oferta de meios de comunicação de forma segura...;
E5	Então, pode ser que até a IES tenha, mas que é de conhecimento de uma forma formalizada, visível...eu desconheço.
E6	Tem! Claro que tem. Só considerando um exemplo que "tá" aí, né? O fato de eu acessar a internet hoje pela rede Wi-Fi como identificação pessoal é um processo de governança, né?;
E7	Ela tem, mas eu vejo como embrionário porque tem pessoas atuando nisso, mas a IES como um todo não enxerga a importância disso;
E8	Eu desconheço, existem manuais que foram disponibilizados na intranet, de acesso à laboratórios, por exemplo, mas algo de governança de fato, eu, desconheço;
E9	Não;

E10	No momento da contratação se assina o documento a respeito de governança, eles pensam de como manipular os dados e tudo mais, mas eu acho que se limita a isso;
E11	Ainda não;
E12	A instituição tenta ter uma governança de TI, porém está IES, tem uma característica, que eu costumo dizer, que a característica de vários chefes e quando você tem a situação de que cada departamento é um chefe, eles não estão preocupados com a governança;
E13	Não tanto quanto deveria, existem processos de TI, alinhados, um pouco, com governança, mas eu acho que ainda falta muita coisa;
E14	Não sei responder;
E15	Sim;
E16	Possui, mas não saberia explicar ou mencionar algum processo;
E17	Não sei;

Q10: ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Entrevistado	Conteúdo
E1	Não estão claros e divulgados na minha visão, na minha avaliação. Acho que a gente poderia ter um esforço e cuidado maior neste sentido;
E2	Não, o claro seria o pressuposto de um estágio mais avançado;
E3	Não estão claros, eles estão muito no conhecimento tácito das pessoas;
E4	Eu tenho percebo com o gestor do PDI, o cara que acompanha a metas, que a área de TI tem metas claras e ela tem trabalhado para cumprir estas metas, obviamente não só a área de TI como todas da IES...;
E5	Eu não conheço, não vi divulgado não.
E6	Sim, sim...parcialmente. Pode melhorar...;
E7	Não tenho conhecimento;
E8	Não;
E9	Não;
E10	Parcialmente;
E11	Não;
E12	Não;
E13	Eu entendo que a IES carece da gestão do conhecimento e que este conhecimento e que este conhecimento esteja em um repositório, formal, que nós tenhamos mais manuais, mais processos...;
E14	Não sei responder;
E15	Não, não muito claros;
E16	Não;
E17	Não sei;

Q11: A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Entrevistado	Conteúdo
E1	A alta gestão sim, com certeza, tem essa consciência essa clareza, mas, de novo, não está claro... quando você desce um nível, quando você desce do nível da alta Reitoria e Superintendência, perde-se essa clareza, essa consciência;
E2	Como cúpula sim, abaixo disto, enquanto corpo de colaboradores tenho dúvidas desta consciência. Não é simples comunicar estratégia e as pessoas compreenderem o papel de cada área e TI é muito fundamental, é base!
E3	Como membro do board, tem clareza total de que TI é mais de que um meio dentro da estratégia, eu falo isso direto: se a gente não colocar TI no centro do processo...;
E4	Tem, por que é o seguinte a escola tem um conselho que representa todos os setores: técnicos, administrativos, alunos, professores, gestores, esse conselho se reúne periodicamente para reportar o que aconteceu em todas as áreas...;
E5	Hoje não tem clareza, para mim TI é estratégico em qualquer organização, ainda mais na nossa área de instituições de ensino, mas eu acho que isso não está claro...;
E6	Acredito que sim, nós temos sim. Talvez não tanto como ainda podemos ter, mas estamos caminhando para isso...;
E7	Não, não tem;

E8	Creio que sim, principalmente agora com a troca de sistema, secretaria digital;
E9	Não, eu não tenho conhecimento de estratégias voltadas a TI;
E10	Com certeza! Com certeza tem porque o planejamento estratégico da instituição ele prevê em alguns cursos como economia, coisa do tipo, incluir programação nos cursos...;
E11	Os Superintendentes, eles têm uma ideia, mas eu não acredito que seja adequada;
E12	Não, eu não vejo que tenha a clareza...Ela, IES, sabe que tem importância, mas isso não é tão claro a ponto de dar tranquilidade que a governança precisa.
E13	Não, a clareza não é límpida;
E14	Não sei responder;
E15	Não;
E16	A IES até enxerga a necessidade da TI, só que não faz uso da aplicabilidade dela de forma correta;
E17	Não sei;

Q12: CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Entrevistado	**Conteúdo**
E1	Claro que sim, nós somos seres humanos falhamos e muitas vezes de forma não intencional e está bem claro, para mim...para todos, que em alguns aspectos e algumas atividades a tecnologia é superior (enquanto construída pelo ser humano, daqui a pouco, de forma mais hibrida) ela é superior...;
E2	TI presta o suporte total ao compliance, visto que ela tem como estabelecer regras de verificação de fraudes, detecção de situações que o processo humano pode gerar muitos problemas, como fraudes e falhas. Desta forma, o compliance com base em TI é vital para IES...;
E3	Certeza que sim, absolutamente sim;
E4	Claro que sim eu acho que se você não faz o controle interno com frequência e de forma sistematizada como se vai garantir o compliance...;
E5	Total, sou suspeito em falar pois minha formação é em controles internos...sabemos dos benefícios que tem os CI e são mais benefícios doque custos e é lógico não só auxilia, mas é necessário para manter a conformidade, não só com a legislação...;
E6	Sim, sem dúvida que podem. Precisa a sistematizar, organizar e atualizar. E há sim muitos recursos tecnológicos podem ajudar nesses processos de conformidade...;
E7	Eu acredito que sim, acho que faria um papel muito diferente, facilitaria processos, eu acho;
E8	Claro, muito! Senso, ENADE... a gente depende totalmente dos dados de TI;
E9	Sem dúvida! Com certeza absoluta, faz parte da transparência você ter um programa de compliance, as regras ficam bem definidas;
E10	Sim, eu acho que sim. Aliás eu acho que essa é a função principal da duas (controles internos e governança de TI);
E11	Sem dúvida, aqui na realidade pela atual conjuntura da IES, deveria redesenhar tudo, um monte de coisa, dentre eles o papel da TI;
E12	Sim, sem dúvida nenhuma...;
E13	Sim, sem dúvida alguma a literatura de Governança de TI é ampla, tem vários frames de governança que podem ser aplicados;
E14	Sem dúvidas ela é fundamental também;
E15	Sim, total. Total!
E16	Sim, com certeza, até por que provavelmente uma das próximas portarias do MEC serão sobre isso... quanto mais o tempo passa mais informatizado e digital fica, então para IES isso é primordial;
E17	Acho que sim, controles de TI são importantes. Não sei o quanto nas escolas, mas nas empresas não dá para ficar sem...;

Apêndice B3 - Transcrição Integral – entrevistas semiestruturadas

E1: Reitor e Superintendente Geral - IES

Caracterização:

CARGO ATUAL?

Superintendente Geral e Reitor.

TEMPO NO CARGO?

Reitor: 9 anos

SG: 4 anos

IDADE?

41

FORMAÇÃO

Administrador, Mestre e doutor em administração;

QUAL SUA RELAÇÃO COM A IES?

Mais de 20 de relacionamento com a IES, ou seja, aproximadamente metade da minha vida, começou como aluno, sou egresso do curso de ADM da instituição, e antes de concluir o curso iniciei profissionalmente milhas atividades na escola, tendo passado por várias e várias funções, especialmente no âmbito acadêmica, mas não só neste âmbito.

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Já ouvi falar sim da LGPD, vinda de uma regulamentação externa, estrangeria, acho que a Europa é a liderança nesta iniciativa;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

É opera, dados dos clientes, entendidos como alunos da IES. Opera sim, ela tem esses dados e utiliza esses dados em sua gestão. Dados pessoais e sensíveis também.

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI? Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Sim podemos ser impactos pela lei, todos os setores podem ser impactados pela lei. A gente tem que tomar o cuidado, na IES, com conformidade, então essa é uma preocupação grande nossa. Mas eu acho que o resultado para escola pode ser positivo, nós somos uma escola muito cuidadosa, zelosa com os dados nossos alunos, mas não só com esses dados, e talvez isso tenha colocado, do ponto de vista mercadológico, em desvantagem em alguns momentos quando competíamos com outros players que não tem exatamente esse mesmo cuidado, então acho que o resultado da lei pode ser o de nivelamento do campo da competição, e, nesse sentido a gente pode ser beneficiado.

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Temos iniciativa de adequação com a lei, a nossa área de infraestrutura com o apoio do jurídico e outra outras áreas da escola que manejam estes dados tem estudo o temo e tem buscado identificar as iniciativas que a gente tem de colocar em prática para adequação a lei.

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Fundamental, essencial! Não há negócio ou virtualmente não deve haver negócio que não passe por TI, hoje em dia. Claro que a gente, nós somos uma IES sem finalidade lucrativa mas a gente tem que sobreviver, então a pergunta da questão financeira, a gente tem duas possíveis formas que a IT pode apoias a perenidade da escola: 1) por um processo inevitável de digitalização das suas atividades meio, isso é importante porque implica em eficiência, implica em você ter uma nível de serviço superior aliado a um custo mais baixo e esse é o melhor dos mundos; e por outro lado, 2) a gente tema certeza também que do ponto de vista da atividade fim, seja na experiência que o aluno tem na IES seja na capacitação desse aluno em TI que é uma competência que não dá para fugir, pois estamos no século 21, ou seja, ele não vai conseguir ser produtivo na sociedade sem ele não tenha está competência aliada a de capacidade de análise de dados, não importa em que área ele venha atuar, não importa o curso que ele executa aqui na IES, se a gente não providenciar este tipo de experiência e não preparar nossos alunos nessas competências é a gente não vai fazer nosso serviço correto e não estará cumprindo nossa missão e TI obviamente tá no centro disso tudo. Eu acho que as organizações de uma forma geral elas precisam mudar a forma como encaram TI, não podem ignorar TI, eu acho que TI não pode ser uma área isolada ela tem que estar dentro as áreas de negócios da escola, operando conjuntamente, no nosso caso TI e gestão e acadêmica, TI e gestão administrativa também, mas principalmente coma gestão acadêmica. Encontrando junto as soluções, juntos, em equipes multi-interdisciplinares;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Como negócio isso já acontece, porque, a TI ela trouxe a possibilidade a entrega educacional de forma diferente daquela que as escolas tradicionais, então elas estão sofrendo uma concorrência que não existia a 10, 15 anos atrás então elas estão sendo, o termo usado é o da disrupção, o setor está sofrendo uma disrupção, usando este termo de uma forma conceitual correta onde a gente usa na área de estratégia, então algumas escolas, novos players começaram a usar TI para entrega de educação com uma qualidade inferior a aquilo que se faz normalmente, só que foi havendo desenvolvimento e as escolas incumbentes tranquilas passivos assistiram ou não enxergaram a evolução que essas tecnologias foram desenvolvendo ao longo do tempo e hoje as curvas estão se encontrando em termos de qualidade de ensino, ou seja, ou você acelera agora e usa seus recursos que escolas totalmente digitais não tem, como instalações, corpo docente, tradição e você alia isso com TI e isso pode ser uma vantagem para escola ou você vai correr um sério risco de sair do mercado. Então do ponto de vista de negócio há essa vulnerabilidade.

Do ponto de vista das suas operações, claro que o mundo caminha para digitalização de processos e de dados e isso pode trazer vulnerabilidade de segurança e de risco operacional para

as escolas, então se precisa tomar um cuidado técnico nesta frente para evitar essa exposição sem inibir o avanço no uso dessas ferramentas então deve-se buscar um equilíbrio nesta questão;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Acho que pode sim, a gente quer na acadêmica o maior nível de liberdade possível, por que isso faz parte do processo educacional, no entanto isso pode gerar problema de segurança que você não tem no mundo de tijolos. Então você precisa ter equilíbrio e compreensão dos dois lados acho que o processo de comunicação aí é fundamental, porque muitas vezes quem está do outro lado: o professor, o aluno, ele não tem conhecimento sobre a fato de que aquela liberdade vai trazer vulnerabilidade e que pode ser prejudicial a ele mesmo e de outro lado também você tem que pensar em formas de criar ambientes que blindem o que é essencial e deem liberdade naquilo que vá trazer um menor nível de risco possível, dados por exemplo, a proteção aos dados tem que ser forte, de preferência que essas coisas não se misturem embora a gente saiba que nem sempre isso é possível, mas tem que se buscar essa blindagem.

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Possui sim, mas é assim a gente é uma IES de médio porte, então obviamente não temos a estrutura organizacional que uma empresa de grande porte tem, não temos escala para isso, mas isso não significa que os processos de governança não ocorram, no limite, estes estão sob liderança de uma pessoa que compõe o "top management" da escola. Esses processos existem, mas não em uma estrutura específica, não vamos encontrar um gerente, um diretor de governança de TI na IES. Não temos escala para isso, acho que nem sei se é necessário.

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não estão claros e divulgados na minha visão, na minha avaliação. Acho que a gente poderia ter um esforço e cuidado maior neste sentido. Eu digo até que na falta dessa clareza talvez por parte aí, um "mea culpa" por parte da alta gestão da escola ea falta dessa clareza traga problemas que se vê no avanço dos recursos tecnológicos da escola, exemplo: a troca de sistema de gestão que está ocorrendo neste momento, isso foi comunicado mas...eu tenho um princípio que quando as pessoas não sabem não tem conhecimento a falha é do emissor, sempre do emissor....a gente não tomou cuidado, não fez, não emprenhou o máximos dos esforços para cuidar deste processo de comunicação.

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

A alta gestão sim, com certeza, tem essa consciência essa clareza, mas, de novo, não está claro... quando você desce um nível, quando você desce do nível da alta Reitoria e Superintendência, (Reitor e Vice/ Superintendente Geral e Adjunto), perde-se essa clareza, essa consciência, mas, acho que como a gente está nesse processo de construção do plano estratégico da escola "nome-da-IES Futuro" essa é grande oportunidade de deixar isso mais transparente e fazer mais gente se engajar com essa ideia e esse conceito.

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Claro que sim, nós somos seres humanos falhamos e muitas vezes de forma não intencional e está bem claro, para mim...para todos, que em alguns aspectos e algumas atividades a tecnologia é superior (enquanto construída pelo ser humano, daqui a pouco, de forma mais hibrida) ela é superior e pode, em conjunto com o ser humano, com a capacidade do ser humano de racionar de forma mais sistêmica, identificar pontos de conexo entre áreas, ela pode trazer alguns "flags" que do ponto de vista individual, da atuação das pessoas seria mais difícil, então sim pode, e acho que bem colocado tem que ter um esforço para que essa avaliação de conformidade ela não seja feita exclusivamente em relação a lei, então a escola tem, como toda organização, uma cultura, seus próprios regramentos e isso tudo deveria, em um nível crescente de complexidade, estar dentro do escopo de um trabalho de conformidade como apoio de TI. Então, vou dar um exemplo aqui: a gente não tolera o plágio, isso não é uma questão legal, necessariamente, é uma questão moral...talvez como uso de IT, com certeza com o uso de TI já mais fácil de se identificar o plágio do que isoladamente pelo ser humano, aliás existem ferramentas para isso. Mas não precisa ser plágio direto, ou a famosa cola, talvez com o uso de TI você consiga identificar similaridade, por exemplo, em respostas, linhas de pensamento em resposta, em provas feitas por uma mesma turma e isso seja um indicador de um problema que pode estar havendo de conformidade no sentido amplo, com a cultura, com o regulamento com os regramentos internos da escola, com o código de ética da escola. Então vai além de você pensar em atender a LGPD, de você pensar em atender a conformidade no sentido de se cumprir prazos e regras governamentais, mas a própria checagem das práticas cotidianas e rotineiras da escola como apoio de TI, podendo ser acelerada nos próximos anos, provavelmente a gente vai ter, talvez daqui a 20, 30 anos, talvez antes...algoritmos que estejam avaliando coisas como que falei...originalidade na produção acadêmica, intensidade na condução das aulas...será que os professores estão fazendo aquilo que eles deveriam fazer a gente tem pontos de checagem que a TI ajuda, exemplo: provas institucionais, mas daqui a pouco você vai ter, pode ter, e ai tem uma questão de privacidade que tem que ser tradada e considera, você vai ter câmeras instaladas em salas de aula com um algoritmo observando o que está acontecendo e isso vai gerar informação de conformidade de gestão, então...sim já ajuda e vai ajudar muito. O contraponto é que isso é cada vez mais invasivo e no ambiente acadêmico isso é muito importante, nós deveremos os primeiros na sociedade em defender a privacidade das pessoas e até que ponto vamos conseguir esse tipo de recurso sem quebrar regras seculares de ética e de moral que o ambiente acadêmico deveria ser o primeiro a promover.

E2: Vice-Reitor e Superintendente adjunto (Administrativo-financeiro) - IES

Caracterização:

CARGO ATUAL?

Vice-Reitor

Superintendente Administrativo Financeiro (Adjunto)

TEMPO NO CARGO?

Vice-Reitor: 9 anos

Superintendente: 4 anos

Superintendente Adjunto: 4 anos

IDADE?

40 anos

FORMAÇÃO

Administrador, Mestrado e Doutorado em Administração;

QUAL SUA RELAÇÃO COM A IES?

Ex-aluno colégio, faculdade e Mestrado, Professor da Graduação desde 2001 e atuando em posições de gestão em diversas frentes;

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Sim, já ouvi falar;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim com altíssima frequência;

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Sim, enquanto cúpula, porém enquanto nível de gestão e colaboradores não. Há assimetria;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Positivos, particularmente quanto ao impacto nos estudantes como um todo principalmente como cidadãos, há ainda uma questão de privacidade de dados que é muito débil nas organizações, quest,ões de invasão de privacidade, então esta lei deve ajudar bastante e o pais como um todo em particular as IES a informações muito sensíveis com relação a performance de estudantes e com relação a perfil e informações de etnia e sócio econômicas, então as escolas têm uma estrutura de dados muito completa que tem o raio x da vida de cada um, isso por si já é uma responsabilidade grande.

Quanto ao que pode beneficiar, eu vejo mais o público de estudantes e das pessoas que participam da IES em ter uma melhor privacidade das suas informações;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Sim, porém não há uma formação estruturada da IES no momento, há um comitê em desenho, mas o movimento estratégico anterior de migrar de desenvolvimento interno para estar de acordo o ERP de nível nacional para trazer soluções externas já nos coloca numa situação de compliance que o fornecedor vai ter que se adequar. Agora a gente vai precisar do corpo de gestores nosso consciente da utilização dos dados;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Absolutamente. Importância total, “bone” da operação em particular em relação à novas tecnologias de aprendizagem que estão surgindo e a necessidade sim da gestão de custos fixos com base em processos tecnológicos;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES? Ex. INTERNET.

Ela (TI) pode ser risco, ameaça e oportunidade. Vulnerabiliza se a IES possui uma concepção antiga do que é universidade: “eu sou dono do conhecimento e as pessoas tem que vir aqui beber desse conhecimento” só que este conhecimento está disponível na internet, na realidade as IES são “hubs” de troca de informações de network, então se for essa visão as IES vão se beneficiar da Internet;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Do que tange a lei e a privacidade de dados, é muito comum a troca de planilhas de informações sensíveis entre professores e colaboradores, nesse aspecto vulnerabiliza;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Se você aplicar a IES a uma escala de governança, de fato já aplicou, é muito baixa. Houve uma pequena evolução, mas ainda há muito pela frente;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não, o claro seria o pressuposto de um estágio mais avançado;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Como cúpula sim, abaixo disto, enquanto corpo de colaboradores tenho dúvidas desta consciência. Não é simples comunicar estratégia e as pessoas compreenderem o papel de cada área e TI é muito fundamental, é base!

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

TI presta o suporte total ao compliance, visto que ela tem como estabelecer regras de verificação de fraudes, detecção de situações que o processo humano pode gerar muitos problemas, como fraudes e falhas. Desta forma, o compliance com base em TI é vital para IES, como automatizar processos e ter um nível mais maduro de TI vai ajudar a IES como um todo não incorrer em erros de conformidade;

E3: Pró-reitor de Graduação - IES

Caracterização:

CARGO ATUAL?

Pró-reitor de Graduação e Coordenador de Ciências Contábeis;

TEMPO NO CARGO?

Pró-reitor de Graduação: 5;

Coordenador de Ciências Contábeis: 12 anos

IDADE?

42 anos

FORMAÇÃO

Graduação em Ciências Contábeis, Mestrado em Ciências Contábeis, Doutorado em Educação;

QUAL SUA RELAÇÃO COM A IES?

Professor, pai de aluno colégio, pai de aluno Graduação, pró-reitor e coordenador;

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Não posso dizer que conheço a fundo, já ouvi falar, mas nunca a li;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim;

Q3. SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

Entendo que sim;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Beneficiada no sentido de deixar em "pé de igualdade" com instituições de maior porte que de repente podem manipular, manipulam, de forma não tão ética e moral os dados e prejudicada por conta das sanções previstas caso não estejamos em conformidade;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Certamente há…eu não as conheço, não estou muito envolvido. Com certeza há, mas não posso dizer que sei quais são. Então para ser direto, há, mas não sei;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Certeza que sim, tecnologia hoje é base para tudo, tenho falado isso faz tempo: quando a gente nasce e a gente precisa falar para se comunicar, no mundo dos negócios precisa de tecnologia para tudo seja para sustentabilidade financeira, comunicação, etc., então de maneira objetiva para resposta é sim;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Com certeza sim, também. Considerando meu parco conhecimento você fica mais exposto com a internet, mas não somente o uso de softwares diversos você fica mais exposto há ataques hackers por exemplo, neste sentido, a evolução tecnológica cada vez mais você vai entregando

dados, ficando mais exposto, colocando mais a sua cara a tapa sem dúvida que vulverabiliza as IES;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Sim, por definição o ambiente acadêmico é mais aberto, você tem IES aqui em São Paulo mesmo no ensino privado que não tem nem portão, você pode entrar e ninguém vai te barrar, não tem nem catraca, então sem dúvida o ambiente acadêmico tende a ser mais flexível que os demais, uma organização empresarial no topo da governança e uma instituição acadêmica no topo da governança, elas estão superprotegidas, o ambiente acadêmico é mais flexível (vulnerável) do que a outra;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Se possui eu não conheço. Claramente há processos de governança, mas não há, nunca vi, uma política de governança;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não estão claros, eles estão muito no conhecimento tácito das pessoas;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Como membro do board, tem clareza total de que TI é mais de que um meio dentro da estratégia, eu falo isso direto: se a gente não colocar TI no centro do processo, não necessariamente o principal (foco), mas no centro do processo a gente não vai para lugar algum. De novo como board tem clareza.

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Certeza que sim, absolutamente sim;

E4: Pró-reitor de Extensão - IES

Caracterização:

CARGO ATUAL?

Pró-reitor de Extensão

TEMPO NO CARGO?

10 anos

IDADE?

52 anos

FORMAÇÃO?

Engenheiro, Administrador, Bacharel em Química, Mestrado em Eng. Da Produção, Doutorado em Administração, Doutorado em Educação.

QUAL SUA RELAÇÃO COM A IES?

Além de Pró-reitor sou professor;

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Sim, já ouvi falar, já conversei internamente com algumas pessoas com você com o Ronaldo (Pró-reitor de Graduação), coma Maria Carolina que advogada e também está discutindo esta questão, então, mas é assim eu nunca li a lei;

Q2. VOCÊ SABE DIZER SE A IES OPERA DADOS DOS SEUS CLIENTES?

Sim;

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Entende, claro;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU IMPACTADA PELA LEI?

Ela (a lei) vai impactar a intuição. Beneficiar? Eu acho que alei vai trazer regulações e deixar claro para IES e as pessoas que se relacionam com a instituição como estas informações efetivamente deverão ser tratadas, então eu acredito que se a lei for bem entendida e aquilo que ela preconizar for bem trabalhado aqui dentro ela trará benefícios pois ela dará segurança para as partes envolvidas acerca das informações de todo mundo.

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Sim como eu falei anteriormente a advogada já tem esta demanda eu não sei como está o desenvolvimento, mas já faz um tempo que a gente conversou. Por que como a gente tem um projeto de ensino à distância aqui, a gente precisa muitas vezes que os dados das pessoas cheguem até aqui de forma digital, a gente precisa garantir que estes dados sejam preservados, então já faz mais de um ano que a área jurídica e a área técnica vem discutindo maneiras de se adequar a esta lei. Não sei exatamente o prazo, (agosto de 2020), então daqui menos de um ano tudo mundo vai ter que se adequar, a escola está se mexendo e espera-se que no prazo estipulado a gente esteja preparado.

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Com certeza, por que a tecnologia permite velocidade, segurança, comunicação. Então, no mundo que a gente vive de mobilidade de múltiplos canais de comunicação a escola que não tiver preparada tecnologicamente para esses canais junto a seus clientes ela não vai se sustentar, acho que ela não vai existir. Uma escola não pode ficar à margem disco.

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Eu acho que sim e as escolas tem que se preparar para isso, por que, qualquer processo que você adote ele terá suas fragilidades, se você adota um processo que depende só de pessoas uma pessoa pode ficar doente e não aparecer, pode boicotar o processo. Quanto você tem tecnologia você depende de infraestrutura, você depende de conhecimento, proteção, então certamente alguns setores ai desta tecnologia precisam ser protegidos, por que a forças do mal existiram e sempre existirão, gente querendo tirar vantagem. O que vai desde um aluno tentando invadir o sistema para mudar uma nota, criar um diploma falso.

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Eu acho que sim, apesar de que o que tem dentro do ambiente universitário são coisas de interesse dos estudantes, interesses relacionados a sua formação, então a maior parte das informações vão estar ligadas a desempenho, a trilha que eles percorreram aqui dentro, talvez o lado financeiro é a mensalidade do cara, ele entrar no sistema e dar baixa no boleto por exemplo. Mas eu acho que é um ambiente menos visado do que o de determinados ambientes como lojas de produtos, bancos e outras coisas assim. Mas há também o aluno e ele tem tempo para pensar em coisas incorretas se for o caso se tem casos (muitos casos) de invasão ocorrem dentro das universidades, então eu acho que é um ambiente menos propício mas tem isso também.

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?
Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Eu acho que sim, o PDI (por exemplo) é um documento que deixa claro quais são as metas da área de TI ao longo de um período e essas metas estão relacionadas com aspectos de oferta de meios de comunicação de forma segura, então não adianta você prover uma rede que todo consiga entrar, então, não faz sentido. Eu tenho percebo com o gestor do PDI, o cara que acompanha a metas, que a área de TI tem metas claras e ela tem trabalhado para cumprir estas metas, obviamente não só a área de TI como todas da IES como de outras escolas essas metas de planos de longo prazo dependem muito de recursos, então, em um cenário com dificuldades macro econômicas que acabam chegando até nós, como desemprego, menos alunos, menor entrada de dinheiro em caixa, acaba limitando vários projetos, mas até onde me lembro os de tecnologia estão sendo cumpridos;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Tem, por que é o seguinte a escola tem um conselho que representa todos os setores: técnicos, administrativos, alunos, professores, gestores, esse conselho se reúne periodicamente para reportar o que aconteceu em todas as áreas e periodicamente também as metas do plano de desenvolvimento institucional essas metas são reportadas pelo gestor da área e esse cara nesse reporte ele explica por que a meta foi alcança ou não e quais foram as dificuldades. Especificamente no caso de TI isso é mostrado para todos os representantes de todas as áreas, então dessa forma há um reporte institucional, inclusive para o conselho de curadores e isso está disponível para a comunidade, então eu acho que nesse sentido há uma preocupação da escola divulgar o que está acontecendo inclusive nesta área que você está me perguntando;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Claro que sim eu acho que se você não faz o controle interno com frequência e de forma sistematizada como se vai garantir o compliance, você tem que ter processos de controle interno bem definido e bem conhecido pelos operadores, gestores, então, acredito que sim;

E5: Pró-reitor de Pós-graduação (Lato e Stricto Sensu)

Caracterização:

CARGO ATUAL?

Pró-reitor de Pós-graduação

TEMPO NO CARGO?

6 meses

20 anos com professor e Coordendor da Pós-graduação – Lato Sensu

IDADE?

49 anos

FORMAÇÃO?

Contador (graduado), Mestrado em Contabilidade e Doutorado em Administração.

QUAL SUA RELAÇÃO COM A IES?

Além de Pró-reitor sou professor;

Constructos:

Q1. CONHECE OU JÁ OUVIU FALAR DA LEI DA PROTEÇÃO GERAL DE DADOS DO BRASIL?

Já ouvi falar em alguns eventos dos quais participei, mas não li a LGPD.

Q2. A INSTITUIÇÃO OPERA MANIPULA DADOS DOS SEUS CLIENTES DOS SEUS ALUNOS?
Ele utiliza bastante, aliás é uma instituição cujos dados são praticamente todos de clientes, 99% do que deve transitar em termos de informações são dados relacionados a clientes.

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Muito! Totalmente, tem que ter mecanismos urgentes para adotar a lei porque o impacto é grande.

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Prejudicar não. Se for falar de prejuízo é só de investimentos que precisam ser feitos, mas acho que é mais benefício, por que, dá mais se segurança para IES se ela for seguir rigidamente o que a lei pede, os procedimentos que são pedidos, benefícios para até evitar a exposição de dados de clientes, então claro que é um benefício seguir a lei e o prejuízo é mais uma questão de investimento, a relação de custo benefício aí é mais para o benefício do que para o custo.

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Ainda não, que tenha chegado até a mim, não! Oficial que está se adequando a lei, ainda não.

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Eu até trocaria a palavra importante, para mim ela é fundamental, para mim tecnologia nas IES ainda mais como a nossa ela é estratégica e jamais poderia ficar em segundo plano, ela tem que ser decidida e tratada e discutida como são discutidas decisões financeiras da IES, tecnologia tinha que ter o mesmo nível de importância.

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Muito! Muito crescente isso, e muitas vezes a gente fica correndo atrás do rabo porque a evolução é mais rápida do que nossa capacidade de resposta.

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Aí eu volto na questão de custo benefício, esse ambiente acadêmico muitas vezes precisa ser flexível, tem que ser colaborativo porque a gente fala de pesquisas, de compartilhamento de conhecimento, então muitas vezes tem que trabalhar e operar em um ambiente meio que aberto, participativo e isso pode gerar um risco sim de vulnerabilidades, então é um tradeoff que precisa ser acompanhado, ter controles alternativos, mas essa flexibilidade essa colaboração é necessária no ambiente acadêmico sim.

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Então, pode ser que até a IES tenha, mas que é de conhecimento de uma forma formalizada, visível...eu desconheço.

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Eu não conheço, não vi divulgado não.

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Hoje não tem clareza, para mim TI é estratégico em qualquer organização, ainda mais na nossa área de instituições de ensino, mas eu acho que isso não está claro desde o órgão máximo da IES, o conselho de curadores por exemplo, está muito distante.

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Total, só suspeito em falar pois minha formação é em controles internos...sabemos dos benefícios que tem os CI e são mais benefícios do que custos e é lógico não só auxilia, mas é necessário para manter a conformidade, não só com a legislação, com os procedimentos as regras, as políticas internas. Quando a gente fala controle interno ele é mais visível e palpável para se colocar em prática e ocorre mais no nível operacional, enquanto que a GR é mais gerencial e ainda pouco adotada e praticada nas escolas e o GTI enviesada pelo nome porque as pessoas nas organizações acham que é responsabilidade exclusiva da TI quando é de todos, então acho que o nome está errado precisaria mudar mais até melhorar a adesão.

E6: Diretor do Ensino Médio (Colégio) **- IES**

Caracterização:

CARGO?

Diretor do colégio;

5 anos;

47 anos

Pós Doutorando em Ciência da Informação. Doutor, Mestre e Graduado.

Qual sua relação com a instituição?

10 anos de vínculo com a IES, exercendo a função de professor nos cursos de graduação e desde tenho exercido a função de diretor do colégio. Também já tem outras funções da instituição de coordenação de atividades como por exemplo a comissão própria de avaliação e o programa de iniciação científica então, experiência aí em atividades de coordenação executiva;

Constructos:

Q1. CONHECE OU JÁ OUVIU FALAR DA LEI DA PROTEÇÃO GERAL DE DADOS DO BRASIL?

Já ouvi falar. Conhecer, não posso dizer que sim, por que não li a lei, não conheço. Se me perguntar para citar algum dispositivo da Lei, eu não vou saber falar, né? Mas claro que uma noção geral da lei eu tenho e sei da importância;

Q2. A INSTITUIÇÃO OPERA MANIPULA DADOS DOS SEUS CLIENTES DOS SEUS ALUNOS?
VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Muitos! Muitos, muitos dados né? Aí, por exemplo, vai desde a imagem do aluno, né, que está em nossas mãos, por exemplo a imagem do aluno que a gente veicula no impresso, na internet. É a pessoa do aluno que está exposta à outras pessoas. Então de certa forma aí como sendo um dado. A gente gera muito dado a partir do nosso relacionamento com os alunos no trabalho, por exemplo, de orientação Educacional a gente tem o conteúdo dessas conversas muitas vezes são conteúdos extra sala de aula e diz respeito à vida pessoal do aluno, como problemas familiares, problemas pessoais, atitudinais. E toda essa informação a gente tem que lidar de uma forma organizada por que não pode ficar só escuta do profissional a gente tem que ter um registro disso tem que ter uma consolidação disso até por uma questão de histórico, né, e isso é muito sério e complexo. Sério porque diz respeito a individualidade então tem uma questão de confidencialidade, né? E complexo que é você garantir, né? Essa preservação da confidencialidade desse dado, né, não permitir em uma escola tão grande. Quando nós trabalhamos aqui todo mundo junto ao mesmo tempo, que isso também não se divulgue. E depois da nota do aluno é dado não é na verdade, né? Então o que o aluno hoje está vendo postando na internet é dado. Então a gente tem que se preocupar com tudo isso.

Q3. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Então, essa é uma ponderação que deve partir da interação com a lei. Conhecer a lei, né? Não dá para falar agora você vai ajudar, vai atrapalhar, né, que eu ainda não conheço a lei detalhadamente. Agora a expectativa é que ajude, obviamente, mas que venha para ajudar sobretudo para esclarecer, né? Aquelas situações que ainda não há clareza. Hoje, por exemplo, o uso de imagem: já tem legislação para isso. Então a gente é "cego" à legislação que nos protege e isso é importante. Eu posso tranquilamente fotografar meus alunos no pátio e publicar, do ponto de vista legal eu estou protegido, então a lei está meu favor. Obviamente que a gente tem que sempre que pensar em outra forma. Porque uma vez todo aluno que faz parte da escola já está no contrato escolar dele, que ele concorda com o uso da imagem, mas, pode ter alguém que muda de ideia por algum motivo e falar: quero minha imagem seja veiculada, então, a gente tem que ter também esse outro olhar e ajustar e de dar a pessoas direito também dela querer que a gente não use o dado dela;

Q4. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Eu acredito que sim. Tem uma pessoa aí chamada Rogério Gustavo que, certamente, é o "Testa de ferro" aí para isso, né? E já tem mostrado preocupação, várias vezes, tem interesse então sem dúvida que você representa essa preocupação aqui na escola isso eu acho bem positivo, legal, muito bom;

Q5. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Totalmente, absolutamente! Sim, a gente não pode mais prescindir da contribuição que a tecnologia dá a todos os processos, seja o, da facilidade das operações como do ponto de vista, da rapidez nas operações, então, a gente não pode, hoje em dia, mais abrir mão da TI como recurso e também como objetivo como a escola, como instituição de educação a gente tem que pensar inclusive nisso, né, de ensinar como usar a tecnologia a favor;

Q6. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Claro! Ao mesmo tempo que beneficia, prejudica, ao mesmo tempo, com talvez a mesma facilidade e rapidez. É equivalente e ambíguo. Nós temos aqui a preocupação com o "bullying" o "bullying" virtual (CyberBulling) que é a utilização de um dado alheio de forma virtual, ou por meio da exposição em rede social, por exemplo, é um aluno com outro mas nós não podemos nos isentar disso e isso acontece por meio da tecnologia e às vezes de uma forma, até assim, inocente ou até superficial de um menino a menina acha que essa foi só uma brincadeira não foi por mal, mas compromete uma imagem, expõe, acabar às vezes caluniando, difamando e ele não sabe que isso, inclusive, é crime. Ele não tem essa noção, os grupos presentes também em rede social, já tem lei para isso agora né? Não é só quem posta, quem administra o grupo, se não se responsabiliza, também responde por isso. Então "tá" no pacote, né? Já gente tem uma campanha aqui no colégio que é uma campanha de conscientização para os alunos. Inclusive adequarem o uso do Smartphone, e a campanha é: entrou na sala desliga o smartphone. A campanha está adesivada nas costas das portas aí: a partir daqui celular off, conhecimento on! Parece um contrassenso, né? Claro que a tecnologia está à favor e ajuda, nesses tempos, e a gente falar para desligar, mas é que ainda o smartphone na mão dos alunos, ele é uma grande potencialidade de ser mal-usado, porque, ele tem uma função de dispersor da atenção e não recurso de aprofundamento do conhecimento. Se o aluno usasse o celular, todo dia, como a

gente usa muitas vezes, por exemplo, você está em uma palestra a pessoa fala alguma coisa, você já está rastreando que ela falou para saber...se você tivesse na palestra sobre a lei geral de dados o que eu faria é pegar e buscar no Google sobre a lei. Enquanto você está falando...eu, já estaria vendo a lei para acompanhar. Na verdade, a gente usa a tecnologia A favor em casa, né? A gente tem que fazer alguma coisa e, não sabe, a gente vai lá no YouTube e busca um tutorial que mostra como fazer né? Isso é extremamente útil, mas para o aluno, para adolescente, que a gente tem aqui na escola, o sujeito aqui da escola, ele é muito imaturo e ele vê daí na tecnologia como recurso de entretenimento e interação e não de conhecimento, e isso é positivo, muito bom, eu também gosto, né, mas precisa equilibrar né? Senão até acaba desvirtuando, né a finalidade ou não usando todas as potencialidades;

Q7. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Tem duas coisas aí. Primeira coisa: a existência da lei da regra e da punição garante alinhamento de Conduta? Em uma parte, sim, por temor (!), as pessoas falam o que eu não quero é sofrer as penas, mas a gente sabe que se fosse isso suficiente estarão resolvidos os problemas do mundo, né? Porque não haveria violência, não haveriam problemas, porque às leis estão aí com regras e sanções, mas a gente sabe que não funciona, por que muita gente mesmo sabendo que existe lei e regra infringem e pronto e ponto final. Por outro lado, às vezes, a ausência de lei e regras têm condutas alinhadas porque o que faz diferença não é a imposição externa, mas a convicção interna de fazer aquilo que é certo e desejado. Então o fato de ter ausência das regras ou a presença de uma coerção mais forte pode comprometer e vulneráveis mais? Depende das pessoas, da conscientização das pessoas. Isso É bem interessante. Então mesmo que haja a Lei e a regra senão há conscientização, eu acho que há o risco de falhar, senão há a lei e a regra, mas, a conscientização há o risco de funcionar! Uma coisa assim ambígua, né? E a vulnerabilidade ela existe em todos os contextos e em todos os ambientes, eu acredito;

Q8. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Tem! Claro que tem. Só considerando um exemplo que "tá" aí, né? O fato de eu acessar a internet hoje pela rede Wi-Fi como identificação pessoal é um processo de governança, né? Isso é, o fato de a gente ter dispositivos contratuais para alunos e até para funcionários, que garante por exemplo o uso de imagem é um dispositivo de governança que prevê essa gestão do uso de dados né? Então, e até por exemplo do uso de câmeras na instituição é isso também, são vários exemplos de dispositivos de governança preocupados com isso, né com a gestão de informação dos dados.

Q9. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?
Sim, sim...parcialmente. Pode melhorar, né? Dá para dar um exemplo: Alunos de sexto semestre, para quem eu dou aula, ainda não sabem todos os recursos que podem usar para prática da sua atividade acadêmica, como por exemplo os notebooks da Google (ChromeBooks) e assim por diante. Dá para melhorar ainda e muito ainda, né? Mas temos sim;

Q10. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Acredito que sim, nós temos sim. Talvez não tanto como ainda podemos ter, mas estamos caminhando para isso, tem gente estudando tem gente pesquisando. A gente precisa desenvolver e obviamente que a gente tem ainda limitações, mas já temos também bastante conquistas, né?

Seja do ponto de vista da infraestrutura disponível, seja por conta dos processos já em andamento, né? Então para dizer que, realmente, nós temos bastante clareza: em investimentos, em processos, né? Mas temos limitações e desafios para aprimorar e o resultado ganho em termos de aprendizado acadêmico;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sim, sem dúvida que podem. Precisa a sistematizar, organizar e atualizar. E há sim muitos recursos tecnológicos podem ajudar nesses processos de conformidade, né? Então obviamente nós temos também uma lição de casa muito grande a cumprir nesse sentido, né? Porque nós não temos isso, né de forma organizada na instituição, né? E há muita coisa a ser feita em todos os sentidos, né? Quer ver te dou um exemplo: o seu trabalho de pesquisa, ele não está adequado, em conformidade com as regras. Por que, veja só você, não sabe mas se nós tivéssemos um programa em comitê de ética em pesquisa aqui na instituição antes de você fazer entrevista comigo, você teria submetido seu projeto ao comitê de pesquisa com esse instrumento com termo de consentimento livre e esclarecido que existe que é dado pelo Conselho Nacional de ética em pesquisa. E aí você me daria esse termo de consentimento. Queria ler eu iria assinar, entendeu? Depois do comitê já teria aprovado o seu projeto, entendeu? E aí você faria preciso comigo, então eu estaria seguro, não pela confiança na sua palavra, mas um processo se isso é um processo que já existe instalado desde 1996 que são as diretrizes do CONEP (Comitê de Ética em Pesquisa). Você não sabe, mas existisse isso em pesquisa e nós fazemos pesquisas e não temos um comitê de ética em pesquisa.

E7: Advogada (Assessoria Jurídica) - IES

Caracterização:

CARGO ATUAL?

Advogada e Professora;

TEMPO NO CARGO?

10 anos

IDADE?

39 anos

FORMAÇÃO?

Especialista – Pós-Graduação

QUAL SUA RELAÇÃO COM A IES?

Advogada, Professora (Lato Sensu e Graduação) e aluna (Mestrado Acadêmico em Ciências Contábeis);

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Sim;

Q2. VOCÊ SABE DIZER SE A IES OPERA DADOS DOS SEUS CLIENTES?

Sim opera;

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Não completamente, algumas pessoas (instâncias);

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU IMPACTADA PELA LEI?

Ela pode. As duas coisas, se a IES não tomar cuidado ela pode se prejudicar muito e se ela adotar uma boa governança em relação a essa lei ela vai sair na frente em relação as outras. As empresas, em um todo no Brasil, não estão dando a importância que precisa para este assunto;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

O conhecimento que eu tenho é muito embrionário. Houve um começo de conversa sobre o assunto e ele morreu;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Acredito que sim;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Também acho que pode;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Pode;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Ela tem, mas eu vejo como embrionário porque assim tem pessoas atuando nisso, mas a IES como um todo não enxerga a importância disso;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não tenho conhecimento;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Não, não tem;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Eu acredito que sim, acho que faria um papel muito diferente, facilitaria processos, eu acho.

E8: Secretário Geral IES

Caracterização:

CARGO ATUAL?

Secretária Geral e Pesquisadora institucional

TEMPO NO CARGO?

9 anos

IDADE?

38 anos

FORMAÇÃO

Especialista

QUAL SUA RELAÇÃO COM A IES?

Ex-aluna, Coordenadora do PróUni, Supervisora da Central do Aluno

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Sim, já ouvi falar;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim opera;

Q3. SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

Sim inclusive por que existe uma lei n. 13.826/2019 que informa que nós temos que divulgar os nomes e a classificação dos candidatos do processo seletivo e a gente não sabe exatamente... porque ela dá conflito com esta lei dos dados;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

É difícil eu te dizer se vai prejudicar a IES depende muito de como isso vai ser trabalhado, a estratégia a empresa. Que os dados precisam ser protegidos eu acredito que sim, agora como isso vai ser feito aí pode ser que prejudique eu não sei te dizer exatamente;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Olha... tem iniciativas, mas não tem, eu não conheço formalidades. A gente não passa informações do aluno por telefone, nem para terceiros, etc. e tal, as vezes empresas entram em contato para saber se um aluno foi aprovado ou não, tudo isso ainda não tem um processo tão claro, muita gente vem me perguntar o que fazer, se pode ou não informar;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Claro! Tecnologia é importante né;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Pode sim, tão positivo quanto negativo;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Eu acho que sim, pode ter algum tipo de risco de imagem, por exemplo, mas eu acho também que pode trazer muitos benefícios;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Eu desconheço, existem manuais que foram disponibilizados na intranet, de acesso à laboratórios, por exemplo, mas algo de governança de fato, eu, desconheço;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Creio que sim, principalmente agora com a troca de sistema, secretaria digital;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Claro, muito! Senso, ENADE... a gente depende totalmente dos dados de TI;

E9: Gerente Financeiro - IES

Caracterização:

CARGO ATUAL?

Gerente Financeiro;

TEMPO NO CARGO?

3 anos

IDADE?

39

FORMAÇÃO?

Superior em Administração, Contabilidade, Especialização em Gestão Empresarial e Didática do Ensino Superior;

QUAL SUA RELAÇÃO COM A IES?

Ex-aluna, Aluna Mestrado e colaboradora;

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Sim, não com profundidade, mas já ouvi falar.

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim;

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Não, acredito que não;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA E, OU PREJUDICADA PELA LEI?

No primeiro momento, talvez prejudicada, a longo prazo talvez vem um benefício;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Que eu saiba não;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Sem dúvida, essencial;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES? EX. Internet

Acredito que sim, pelo fato de deixar mais expostas as IES e as mídias sociais, em algum momento, vai acabar prejudicando;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Acredito que sim, porque não a regras claras e há mudanças constantes, pode vir a prejudicar a IES;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Não;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Não, eu não tenho conhecimento de estratégias voltadas a TI. Conheço de outras abordagens, mas não voltadas a TI;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sem dúvida! Com certeza absoluta, faz parte da transparência você ter um programa de compliance, as regras ficam bem definidas, para o cliente externos traz segurança e

internamente quando você conhece os processos há uma grande possibilidade de você mitigar riscos. Então, tanto interno quanto externo traz benefícios;

E10: Gestor de Compras - IES

Caracterização:

CARGO ATUAL?

Supervisor de Compras

TEMPO NO CARGO?

4 anos

IDADE?

29 anos

FORMAÇÃO?

Mestre em Administração e Finanças

QUAL SUA RELAÇÃO COM A IES?

Ex-aluno (Graduação e Mestrado), gestor como já dito e Professor auxiliar;

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Sim, já ouvi falar. Não conheço com profundidade;

Q2. VOCÊ SABE DIZER SE A IES OPERA DADOS DOS SEUS CLIENTES?

Sim, sobretudo nas matrículas e captando “leads” e coisas deste tipo;

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Eu acho que sim, eu espero que sim;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Prejudicada se não souber manipular com toda certeza do mundo, desde que tenha uma supervisão também, da parte dos órgãos regulamentadores. Beneficiada, não sei se ela traz algum benefício, até por que meu conhecimento não é tão profundo a respeito do assunto, mas eu acho que corre-se mais risco em não estar em compliance. Talvez no processo haja algum benefício, sim há benefício neste processo, aí sim é um benefício;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Não tenho conhecimento, formalizado não;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Eu acho que hoje não tem essa é uma condição necessária para se ter sucesso. A tecnologia é condição necessária para que tem a sustentabilidade no seu negócio como um todo e financeira também;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Eu acho que sim;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Eu acho mais complexo, torna o processo mais complexo dado você tem acesso de muitas outras pessoas aqui dentro, na sua rede, portanto que faz que você tenha que ter uma diligência maior nos seus processos e no seu compliance de TI;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?
Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Que eu saiba sim e no momento da contratação se assina o documento a respeito de governança, eles pensam de como manipular os dados e tudo mais, mas eu acho que se limita a isso;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Com certeza! Com certeza tem porque o planejamento estratégico da instituição ele prevê em alguns cursos como economia, coisa do tipo, incluir programação nos cursos. Então eu acho que que tem essa clareza assim na demanda do mercado hoje é muito forte nesse sentido e ela se adequou;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sim, eu acho que sim. Aliás eu acho que essa é a função principal da duas (controles internos e governança de TI);

E11: Gerente Contabilidade - IES

Caracterização:

CARGO ATUAL?

Gerente de Controladoria

TEMPO NO CARGO?

4 anos

14 anos de IES

IDADE?

56

FORMAÇÃO

Contábil, Administrador e MBA em controladoria

QUAL SUA RELAÇÃO COM A IES?

Funcionário e ex-aluno

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Já ouvi falar, mas não conheço a fundo;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim, tanto de alunos, funcionário e fornecedores;

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Com certeza;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Negativamente sim, positivamente só se existir um controle mais específico;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Até hoje não, apenas comentários, mas não via ainda nenhum plano de ação a respeito;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Sem dúvida! Na realidade a TI é a parte mais importante de qualquer empresa, hoje qualquer IES depende 100% de TI, ponto. Não tenho dúvida quanto a isso;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Acredito que sim. Aí são várias explicações desde “fake news” até vulnerabilidades técnicas;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Sim, porque no ambiente empresarial são funcionário e produtos/serviços, na IES são serviços, funcionários e alunos e são muitos alunos;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Ainda não;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Bom vou falar como *Controller* e como amigo pessoal dos Superintendentes, eles têm uma ideia, mas eu não acredito que seja adequada;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sem dúvida, aqui na realidade pela atual conjuntura da IES, deveria redesenhar tudo, um monte de coisa, dentre eles o papel da TI;

E12: Coordenador de Tecnologia da Informação (Desenvolvimento de Sistemas) - IES

Caracterização:

CARGO ATUAL?

Coordenador de Desenvolvimento de Sistemas;

TEMPO NO CARGO?

10 anos;

IDADE?

53

FORMAÇÃO

Graduado em Matemática, Pós-Graduado em Gestão de TI e Segurança da Informação e Mestrado em Ciências da Computação;

QUAL SUA RELAÇÃO COM A IES?

Iniciou como consultor, Gestor, pai de ex-aluno e alunos do ensino médio;

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Não só ouvi falar como tive um estudo mais aprofundado da lei, isso por que eu fiz uma pós-graduação em Segurança da Informação onde este tema foi amplamente abordado, participei de diversos workshops também sobre a lei, então eu tenho um conhecimento razoável sobre;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Ela opera sim e tem que operar por que é uma IES e todas suas informações são destinadas para pesquisa e isso é uma das coisas que sempre tive uma dúvida muito grande com esta lei, por que, como serão tratados os dados dos alunos na pesquisa, são dados pessoais, entre outros;

Q3. SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

No meu entendimento ainda não, eu acho que a IES precisa conhecer melhor a lei, as pessoas ficam esperando a informação chegar até elas do que vai acontecer com a lei sendo implantada, uma noção de que o impacto vai ser grande, as consequências são grandes, além de que no mundo o roubo de dados é cada vez mais recorrente, felizmente a IES ainda não passou por isso;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Prejudicar eu não acredito, por que devido a obrigatoriedade dos documentos e a informação está lá, ela não vai deixar de existir, o que vai acontecer é que a IES vai se adequar e se acostumar com situações que ocorrerão à partir da lei, pelo contrário eu acho que vai ajudar bastante no que diz respeito à o que fazer em caso de roubo de informação ou o que fazer se por algum motivo a IES teve que passar dados, para um pesquisador por exemplo, e estes vazarem;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Não, não vi nenhuma iniciativa até o momento, existem algumas ideias a respeito, mas iniciativa propriamente dita, eu não vi;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Sem dúvida nenhuma! Hoje nós estamos vivendo uma situação que é a seguinte: uma realidade que diz respeito a educação o EAD não pode ser ignorado, algumas IES estão se rendendo a possibilidade de não terem mais ensino presencial, fora do Brasil o MIT por exemplo está colocando todos os seus cursos na WEB, para que as pessoas tenham acesso...porque esse é caminho que o jovem profissional de hoje busca ele não tem mais aquela situação de ficar horas dentro de uma sala de aula, ele quer estudar do escritório dele, da forma como ele quiser, como ele puder...e a estrutura disto, que permite isto é TI, falando apenas o básico. Seja local seja na nuvem você precisa ter segurança da informação e estrutura para manter isso rodando...isso é TI não tem como fugir deste tipo de coisa. Por outro lado, os alunos hoje estão na sala de aula vendo se o que o professor está falando é verdade ou não no celular e como você consegui lidar com isso sem preparar o professor para lidar com TI.

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Ela tras risco para a IES! Prova disso é algumas instituições de renome que tiveram os dados de alunos vazados e a consequência não foi nada agradável, agora o que tem que ser feito com relação a isso é um trabalho forte de segurança, não diria tanto em hardware, mas com certeza em sistemas por que a vulnerabilidade é grande e não podemos pensar que você resolve um problema hoje e amanhã "está tudo certo! ". Existe uma profissão chamada hoje no mercado de "*hacker*" que eles estão ganhando para burlar o que as empresas adotam de segurança.

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Vamos pensar na seguinte situação: (escola versus empresa) seria aceitável no banco Itaú um funcionário ter a senha do seu coordenador para acessar um sistema por que o coordenador não está presente para poder resolver uma situação? Isso por si só já responde à pergunta. Então.... Sim!

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

A instituição tenta ter uma governança de TI, porém está IES, tem uma característica, que eu costumo dizer, que a característica de vários chefes e quando você tem a situação de que cada departamento é um chefe, eles não estão preocupados com a governança. A TI ela tem uma

responsabilidade tão forte na IES que isto é uma responsabilidade de todos na IES e se você tem pessoas que não concordam e não contribuem com isto você não tem governança.

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não.

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Não, eu não vejo que tenha a clareza...Ela, IES, sabe que tem importância, mas isso não é tão claro a ponto de dar tranquilidade que a governança precisa.

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sim, sem dúvida nenhuma, a gente pode por exemplo os métodos ágeis de desenvolvimento...você pode implementar estes métodos ágeis dentro do seu dia a dia em qualquer parte da IES o problema é adequar as pessoas a essas conformidades, mas é possível sim.

E13: Supervisor de Tecnologia da Informação (Suporte e Infraestrutura) - IES

Caracterização:

CARGO ATUAL?

Supervisor de Infraestrutura e Suporte de TI;

TEMPO NO CARGO? TEMPO NA IES, EM NÍVEL DE GESTÃO?

1 ano;

5 anos;

IDADE?

36 anos;

FORMAÇÃO?

Bacharel em Ciências da Computação e Pós-graduado (especialista) em Gestão Estratégica de Pessoas;

QUAL SUA RELAÇÃO COM A IES?

Ex-aluno, Professor do ensino médio técnico e colaborador;

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Sim, já tive a oportunidade e participar de workshops sobre a lei;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim, a IES tem os acessos e dados de todos os clientes e colaboradores e de toda comunidade acadêmica da instituição;

Q3. SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

Entendo que a IES tem uma visão parcial de que pode ser impactada pela Lei, a IES ainda carece de mais informações sobre essa lei e imagino que até o mercado como um todo carece um pouco de maiores esclarecimentos;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Eu acredito que a proposta da lei é benéfica, ela tende a proteger o cidadão e as IES acho que elas precisam se alinhar, principalmente na questão comercial, hoje é comum que as IES disparem seus processos de captação, busquemos seus alunos através de meios onde a privacidade desses dados não é tratada como a lei prevê que deveriam ser, então neste formato eu entendo que as IES precisam ter essa noção e ajustar os seus processos para que lei seja cumprida como deve ser;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Há algum tempo atrás foi levada a Superintendência/Reitoria a sugestão de criação de um comitê. Mas eu não sei qual é a evolução da criação deste comitê neste momento;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

100%! Acredito que a TI é importante para sustentabilidade financeira e para toda atividade fim e atividade meio da IES, então há mais a possibilidade de "tocar o negócio" sem que a TI não prevaleça. A gente tem TI em todos os sentidos da operação;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Sem dúvida alguma! Sim a evolução tecnológica traz essas vulnerabilidades cada vez mais ouve-se falar de fraude de ataques de sequestro de dados enfim é muito comum e sabemos que tudo isso está ligado a evolução tecnológica então, sim, acredito que sim e as IES precisam investir e evoluir aí no caminho da segurança da informação para protege-la.

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Sim, eu acredito que sim. O ambiente acadêmico ele é, por natureza, flexível, então acaba sendo mais fácil de ter uma pessoa, uma população circulante dentro Campus e, neste sentido, eu acredito que a vulnerabilidade se torna muito maior, não só tecnológica, mas humana mesmo;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Não tanto quanto deveria, existem processos de TI, alinhados, um pouco, com governança, mas eu acho que ainda falta muita coisa. Eu acho que a IES pode e deve evoluir na questão de governança de TI de governança total;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Eu acho que essa é uma das grandes questões associadas a esses processos, eu entendo que a IES carece da gestão do conhecimento e que este conhecimento e que este conhecimento esteja em um repositório, formal, que nós tenhamos mais manuais, mais processos de treinamento, enfim acho que dá para evoluir bastante nessa questão da clareza dos processos. É muito comum o processo existir, mas somente na cabeça que executa aquela função;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Não, a clareza não é límpida, tão sólida quanto deveria ser, por vezes eu tenho a sensação de que TI é visto como um segmento que executa as tarefas dadas, a sensação que eu tenho é que ao definira estratégia: ok, TI vai conseguir executar, mas não é questionada, não é trazida à mesa para efetivamente perguntar: "e aí TI o que é para que essa estratégia...", então eu tenho essa sensação de que TI é deixada de lado em relação a estratégia;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sim, sem dúvida alguma a literatura de Governança de TI é ampla, tem vários frames de governança que podem ser aplicados, e sim eu imagino que TI pode tomar aí uma dianteira e ter um papel de liderança na aplicação de governança nesse formato mais amplo, aqui citado, eu acho que os controles internos de TI podem e devem ser utilizados e servir de exemplo de governança para IES como um todo;

E14: Representante discente do Mestrado - IES

Caracterização:

CARGO ATUAL?

Supervisora Contábil;

TEMPO NO CARGO?

6 Meses;

QUANTO TEMPO VOCÊ TRABALHA COM CONTABILIDADE EM NÍVEL DE GESTÃO?

3 anos mais ou menos;

IDADE?

30 anos

FORMAÇÃO

Contadora

QUAL SUA RELAÇÃO COM A IES?

Aluna do Mestrado Acadêmico em ciências contábeis.

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Não, não conheço;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Não sei responder;

Q3. VOCÊ SABE DIZER SE A INSTITUIÇÃO PODE SER IMPACTADA PELA LEI?

Não sei responder;

Q4. SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

Não sei dizer;

Q5. SABE DIZER SE A IES PODE SER BENEFICIADA OU IMPACTADA PELA LEI?

Não sei responder;

Q6. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Não sei responder;

Q7. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Fundamental;

Q8. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Com certeza, acho a que a TI (internet) deixa as instituições muito expostas, da mesma forma em que ela é fundamental para empresa e o sucesso dela, desempenho dela, eu também acho que ela expõe demais, então...está exposto ao risco essa questão de tecnologia e internet;

Q9. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Eu acho que ela está exposta ao risco, muitas vezes em função do diferente tipo de perfil que ela atende, diferentes pessoas, então você não sabe o tipo de pessoa que você está lidando dentro da instituição acadêmica então eu acho que ela está exposta ao risco;

Q10. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Não sei responder;

Q11. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não sei responder;

Q12. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Não sei responder;

CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sem dúvidas ela é fundamental também;

E15: Representante discente Pós-Graduação (Latu Senso) - IES

Caracterização:

CARGO ATUAL?

Supervisor Manutenção;

TEMPO NO CARGO?

2 anos

IDADE?

37 anos;

FORMAÇÃO

Especialista;

QUAL SUA RELAÇÃO COM A IES?

Aluno, ex-aluno, Pai de aluno ensino médio e colaborador;

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Já ouvi falar, mas não conheço;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim;

Q3. SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

Sim;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Prejudicar não, acredito que não, de alguma forma ela vem cobrar algo que é necessário;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Sim, tem iniciativas sim;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Total;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Sim, todo processo tem risco, vale-se fazer a proteção destes riscos;

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Sim é mais vulnerável, acho que tem muito mais mecanismos de saída, de acesso, o público é maior, acessos online bem maiores do que as instituições não educacionais, empresas;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Sim;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não, não muito claros;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Não;

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sim, total. Total!

E16: Representante discente da Graduação - IES

Caracterização:

CARGO ATUAL?

Analista Contábil

TEMPO NO CARGO?

2 anos

IDADE?

20 anos

FORMAÇÃO

Graduando em Ciências Contábeis na IES abordada;

QUAL SUA RELAÇÃO COM A IES?

Aluno e colaborador da IES

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Sim, já ouvi falar;

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim;

Q3. SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

Não em nível contábil, gerencial não sei responder;

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Beneficiada se souber usar e tratar os dados que possui. Prejudicada se trabalhar e operar à margem da lei, o que pode acabar trazendo alguma sanção para IES;

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Não, até onde sei não conheço nenhum processo ou procedimento que faça isso;

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Com certeza! Com a digitalização de todas informações financeiras e contábeis hoje em dia, sem a área de TI não há controles contábeis e financeiros efetivos, principalmente em uma instituição de educação;

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Sim, porque dependendo do nível de segurança em que isso se aplica, ou seja, se os dados estão online se os dados estão em nuvem, isso tudo é suscetível a "hacking". Antigamente era suscetível a roubo do que estava no papel, então, existe uma dificuldade, esse problema, a probabilidade de que aconteça, não sei, pois, depende dos outros.

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Sim quanto mais liberdade você dá para quem acessa informações, maior o risco, então quanto maior a liberdade do aluno e do funcionário dentro da IES, maior é o risco que a instituição corre;

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Possui, mas não saberia explicar ou mencionar algum processo;

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não;

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

A IES até enxerga a necessidade da TI, só que não faz uso da aplicabilidade dela de forma correta.

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Sim, com certeza, até por que provavelmente uma das próximas portarias do MEC serão sobre isso. O MEC nos próximos anos, ainda que se pese a lentidão do Brasil, mas as próximas visitas do MEC, as próximas avaliações do MEC com certeza abordarão a proteção de dados dos alunos, dos professores dos funcionários da IES, por que esse é o caminho, porque quanto mais o tempo passa mais informatizado e digital fica, então para IES isso é primordial;

E17: Representante discente da Colégio (pai de aluno) - IES

Caracterização:

CARGO ATUAL?

Gerente de TI

TEMPO NO CARGO?

5 anos

IDADE?

40 anos

FORMAÇÃO

Graduando em Análise de Sistemas;

Pós-graduado (LatuSenso) em Tecnologia;

QUAL SUA RELAÇÃO COM A IES?

Pai de aluno do Colégio da IES

Constructos:

Q1. VOCÊ CONHECE JÁ OUVIU FALAR DA LEI DE PROTEÇÃO DE DADOS DO BRASIL?

Só ouvi falar...algumas empresas têm feito “barulho” sobe essa lei aí...

Q2. VOCÊ SABE DIZER SE A IES MANIPULA OS SEUS DADOS PESSOAIS? OU SEJA, COLETA OU FAZ ALGUM TIPO DE USO DOS SEUS DADOS PESSOAIS?

Sim, quero dizer, acho que sim...sim.

Q3. SABE DIZER SE A IES PODE SER IMPACTADA PELA LEI?

Acho que sim, mas não saberia descrever como e quanto.

Q4. SABE DIZER SE A IES PODE SER BENEFICIADA OU PREJUDICADA PELA LEI?

Acho que não ser prejucada é oque vale mais aqui, quero dizer, em se tratando de lei é bom estar regulado, nos conformes....mas não sei como pode ser bom para escola sem ser isso.

Q5. A IES POSSUI INICIATIVAS QUE PREVEEM A ADEQUAÇÃO OU COMPLIANCE À LEI?

Não sei.

Q6. VOCÊ ACREDITA QUE TI SEJA IMPORTANTE PARA A SUSTENTABILIDADE FINANCEIRA DA INSTITUIÇÃO?

Acredito, como profissional de TI fica difícil de ver alguma escola sem tecnologia, fica para tras, sabe? A tecnologia esta aí né (?) e cada vez mais presente em todo canto.

Q7. VOCÊ ACREDITA QUE A TECNOLOGIA POSSA VULNERABILIZAR AS IES?

Hackers? É sobre eles que esta falando? Se sim, todas as escolas estão em risco...se não, não vejo como, quero dizer, não saberia como...mas é complicado.

Q8. O AMBIENTE DAS INSTITUIÇÕES DE ENSINO, MUITAS VEZES FLEXÍVEL E COLABORATIVO, COMO TEM QUE SER, ELE PODE VULNERABILIZAR ESSAS INSTITUIÇÕES?

Sim e não. Se não tiver boas tecnologias de segurança estará em risco, se fechar muito pode complicar para o aluno e professor, acho que tem que procurar um meio termo aí... flexibilidade demais traz junto perigo em TI. É complicado.

Q9. VOCÊ SABERIA DIZER SE A IES POSSUI PROCESSOS DE GOVERNANÇA DE TI?

Não sei

Q10. ESSES PROCESSOS ESTÃO CLAROS OU DIVULGADOS?

Não sei

Q11. A IES TEM CLAREZA QUANTO AO PAPEL DA TI EM SUA ESTRATÉGIA?

Não sei

Q12. CONTROLES INTERNOS DE TI (GOVERNANÇA TI) PODEM AUXILIAR A CONFORMIDADE INSTITUCIONAL?

Acho que sim, controles de TI são importantes. Não sei o quanto nas escolas, mas nas empresas não dá para ficar sem...é complicado e perigoso.

Apêndice B4 -Transcrição Integral – entrevistas stakeholdes chave (controladores) após aplicação da intervenção:

E1: Reitor e Superintendente Geral;
E2: Vice-Reitor e Superintendente Adjunto;

1. SEU GRAU DE **ENTENDIMENTO SOBRE A LEI** FOI, DE ALGUMA FORMA, MELHORADO COM O PROCESSO DE ADEQUAÇÃO (PESQUISA INTERVENCIONISTA), ATÉ AQUI DESENVOLVIDO E APRESENTADO?

E1: Sim, foi aprimorado. A pesquisa permitiu a aquisição de compreensão mais aprofundada e técnica sobre a lei.
E2: Sim.

2. SOBRE A DIMENSÃO DE **COMPLIANCE A LEI**, VOCÊ ACREDITA QUE A IES FOI BENEFICIADA COM A ADEQUAÇÃO?

A. MITIGAÇÃO DE RISCOS E SANÇÕES PERTINENTES À LEI:

E1: Sim. A pesquisa trouxe maior nível de conscientização da alta gestão sobre o tema, o que influenciou o processo decisório.
E2: Sim. Houve aumento de consciência e de responsabilização individual e institucional quanto à manipulação de dados e comunicações entre indivíduos e organizações.

B. ATIVIDADE MEIO E **FIM** DA IES:

E1: Sim. Estamos em processo de disseminação do tema na instituição e, naturalmente, as lideranças estão considerando a disposições legais. Nossa expectativa, com o avanço do trabalho, é a de que todas as camadas da estrutura sejam conscientizadas e adequem as suas práticas.
E2: Sim. Há consciência de que informações individuais dadas à organização devem ser dedicadas única e exclusivamente aos fins acordados com o prestador da informação; trata-se de princípio de liberdade e respeito à individualidade.

3. SOBRE A DIMENSÃO DE **GOVERNANÇA E CONTROLES INTERNOS** (COBIT, COSOERM), VOCÊ ACREDITA QUE A IES FOI FAVORECIDA?

A. GOVERNANÇA DE TI (INFORMAÇÃO): CONSTRUÇÃO, EXPOSIÇÃO-DIVULGAÇÃO:

E1: Sim, certamente. A maior conscientização sobre o tema tem ajudado no processo decisório sobre a arquitetura de sistemas da Instituição, assegurando a conformidade com a Lei.
E2: Sim.

B. CONTROLES INTERNOS:

E1: Sim. Já identificamos melhorias com algumas mudanças feitas tendo a conformidade com a Lei em mente.
E2: Sim. A aplicação de pontos de controle e auditorias atende ao fim.

C. GESTÃO DE RISCOS;

E1: Sim. A mudança das práticas tem trazido menor nível de risco. E esperamos avançar com a gestão de riscos.
E2: Sim. Mitigação de risco de invasões e vazamentos de informações por imperícia.

4. SUAS **EXPECTATIVAS** ENQUANTO (REITOR) FORAM **ATENDIDAS**? O QUE COMENTARIA?

E1: Minhas expectativas estão sendo atendidas. Como gestor, me sinto mais tranquilo ao saber que temos na nossa equipe um especialista no tema e que o tema está sendo disseminado institucionalmente.
E2: Foram atendidas. Agradecemos o trabalho e adequação da Instituição para a bem pensada LGPD. É um movimento individual de defesa da individualidade e deve ser valorizado.

Apêndice B5 - Transcrição Sintética – entrevistas stakeholders chave (controladores) após aplicação da intervenção

1. Seu grau de entendimento sobre a lei foi, de alguma forma, melhorado com o processo de adequação (pesquisa intervencionista), até aqui desenvolvido e apresentado?	
Reitor	"Sim...permitiu a aquisição de compreensão mais aprofundada sobre a lei".
Vice-reitor	"sim"
2. Sobre a dimensão de compliance a lei, você acredita que a ies foi beneficiada com a adequação?	
A	Mitigação de riscos e sanções pertinentes à lei:
Reitor	"Sim...maior nível de conscientização da alta gestão...influenciou oprocesso decisório"
Vice-reitor	"sim... Aumento de consciência e de responsabilização individual e institucional"
B	Atividade meio e fim da ies:
Reitor	"Sim...Nossa expectativa, ... É a de que todas as camadas da estrutura sejam conscientizadas e se adequem"
Vice-reitor	"sim... Há consciência de que informações individuais dadas à organização devem ser dedicadas única e exclusivamente aos fins acordados com o prestador da informação... Respeito à individualidade"
3. Sobre a dimensão de governança e controles internos (cobit, cosoerm), você acredita que a ies foi favorecida?	
A	Governança de TI (informação): construção, exposição-divulgação:
Reitor	"Sim, certamente. A maior conscientização sobre o tema tem ajudado no processo decisório"
Vice-reitor	"sim"
B	Controles internos:
Reitor	"Sim. Já identificamos melhorias com algumas mudanças feitas"
Vice-reitor	"Sim. A aplicação de pontos de controle e auditorias atende ao fim."
C	Gestão de riscos;
Reitor	"Sim. A mudança das práticas tem trazido menor nível de risco..."
Vice-reitor	"Sim. Mitigação de risco de invasões e vazamentos de informações..."
4. Suas expectativas enquanto (reitor) foram atendidas? O que comentaria?	
Reitor	"Minhas expectativas estão sendo atendidas. Como gestor, me sinto mais tranquilo ao saber... Que o tema está sendo disseminado institucionalmente."
Vice-reitor	"Foram atendidas. Agradecemos o trabalho e adequação da instituição para a bem pensada lgpd..."

Apêndice C1 - Tabulação dados dos stakeholders entrevistados

Representantes acadêmicos

Entrevistado	Sexo	Data da Entrevista	Cargo	Tempo no Cargo em anos	Formação	Relação com IES
E1	Masculino	05/09/2019	Reitor e Superintendente Geral	10 e 4	Doutorado	Ex-Aluno, Reitor, Superintendente Geral e Professor
E2	Masculino	05/09/2019	Vice Reiror e Superintendente Adjunto	10 e 4	Doutorado	Ex-Aluno, Reitor, Superintendente Geral e Professor
E3	Masculino	10/09/2019	Pró Reitor Graduação e Coordenador Ciências Contábeis	5 e 12	Doutorado	Pró Reitor e Professor
E4	Masculino	29/08/2019	Pró Reitor Extensão	10	Doutorado	Pró Reitor e Professor
E5	Masculino	30/10/2019	Pró Reitor Pós Graduação (Latu e Structu Senso)	20	Doutorado	Diretor e Professor
E6	Masculino	29/08/2019	Diretor Colégio	5	Doutorado	Diretor e Professor
E7	Feminino	12/09/2019	Secretário Geral	9	Especialista	Gestora e ex-aluna
	86% Masculino	86% Masculino		100% ≥ 5 anos	86% Doutorado	

Representantes Administrativos

Entrevistado	Sexo	Data da Entrevista	Cargo	Tempo no Cargo em anos	Formação	Relação com IES
E8	Feminino	30/08/2019	Advogada	10	Especialista	Acessora Jurídica, Professora e Aluna Mestrado
E9	Feminino	06/09/2019	Gerente Financeiro	3	Especialista	Gestora e Aluna Mestrado
E10	Masculino	28/08/2019	Supervisor Compras	3	Mestrado	Gestor e Professor
E11	Masculino	06/09/2019	Gerente Contabilidade	4	Especialista	Gestor e ex-aluno
E12	Masculino	16/09/209	Coordenador TI Sistemas	10	Mestrado	Gestor
E13	Masculino	06/09/2019	Supervisor TI Infraestrutura	1	Especialista	Gestor e Professor
	67% Masculino			33% = 10 50% ≥ 3 17% = 1	67% Especialistas	

Representantes Discentes

Entrevistado	Sexo	Data da Entrevista	Cargo	Tempo no Cargo em anos	Formação	Relação com IES
E14	Feminino	27/08/2019	Supervisora Contábil	3	Graduada	Representante discente Mestrado
E15	Masculino	06/09/2019	Analista Contábil	2	Graduando	Representante discente Graduação
E16	Masculino	13/09/2019	Supervisor Operações	1	Especialista	Representante discente Pós-Graduação
E17	Masculino	21/10/2019	Gestor de TI	5	Especilista	Representante discente ensino médio
	75% Masculino			25% = 5,3,2,1	50% Especialistas	

Apêndice D1 - Inventário de Dados (1a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
1. Centro Universitário: **Requisição de pessoal** - recrutamento interno	Nome e função (se substituição)	Pessoal	Coletado pelo Controlador	Físico: papel	Físico: Arquivo DRH	5 anos - Lei 5.452/1945 (CLT), art. 11;	Controlador	Encarregado de Dados e Recursos Humanos
2. Centro Universitário: Processo de **Seleção de Candidatos** à vagas de emprego em aberto	**Pretensão:** Cargo e salário pretendidos, disponibilidade laboral (segunda a sábado); **Dados cadastrais:** nome, estado civil, data de nascimento, idade, endereço, sexo, e-mail pessoal, transporte e tempo de deslocamento para o trabalho; **Dados acadêmicos:** formações, escolaridade, qualificações; **Dados empregatícios:** emprego atual e anteriores: empresa, endereço da empresa, cargo inicial e final, salário atual e anteriores, atividades e motivo da saída; **Dados familiares:** pai, mãe, conjugue, filhos; **Dados Financeiros:** residência, aluguel, automóvel-prestação, demais rendas e valores; **Documentação:** Carteira de Trabalho, RG, Título de Eleitor; CPF, Certificado de Reservista, CNH;	Pessoal	Informado pelo candidato em formulários fisicos/digitais e por envio de *Curriculum Vitae*	Físico: papel; Digital: formulário online;	Físico: Arquivo DRH; Digital: Banco de Dados do Controlador;	Contratados: 05 anos Lei 5.452/1945 (CLT), art. 11; Não contratados: 01 ano;	Controlador	Encarregado de Dados, Recursos Humanos e Departamento de Tecnologia e Informação;
	Dados raciais: Etnia, raça, cor; **Dados de saúde**: Relação de problemas de saúde, relação de tratamentos;	Sensível						
3. Centro Universitário: Processo de **Admissão de candidato**	Gestor, nome completo, Instrução (escolaridade), contato, cargo, departamento, horário de trabalho, data admissão, regime de contratação (CLT, estágio, RPA, PJ e salário), vigência da contratação (determinada ou indeterminada), CPF, RG, endereço residencial, PIS, Reservista, Título de eleitor, Certidão de casamento, Carteira profissional, Documentos escolares (histórico), Currículo, Documentos bancários (Santander);	Pessoal	Informado e coletado junto ao candidato	Físico: papel	Físico: Arquivo DRH	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos
	Dados Biométricos: Foto 3x4 e cópia da carteira de trabalho com foto; Dados Médicos: Exame médico admissional; Dados de menores: Carteira de vacinação filhos menores de 14 anos, Certidão nascimento filhos menores de 14 anos;	Sensível						

Apêndice D1 - Inventário de Dados (1b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
1. Centro Universitário: **Requisição de pessoal** - recrutamento interno	Coleta, arquivamento e eliminação;	Execução de processo de recrutamento	IX. Legitimo interesse do controlador;	NA	I. Apoio a atividades do controlador: recrutamento interno; e II. Prestação de benefício ao funcionário: admissão;	NA	Não	Não	Não	Sim	2. Baixo
2. Centro Universitário: Processo de **Seleção de Candidatos** à vagas de emprego em aberto	Coleta, classificação, avaliação, arquivamento e eliminação;	Execução de processo de seleção	I. Consentimento; IX. Legitimo interesse do controlador;	NA	I. Apoio a atividades do controlador: Processo Seleção; e II) Prestação de benefício ao candidato: contratação;	NA	Não	Não	Não	Sim	3. Médio
						I. Consentimento				Sim	4. Alto
3. Centro Universitário: Processo de **Admissão de candidato**	Coleta, classificação, avaliação, arquivamento e eliminação;	Execução de processo admissional;	II. Obrigação Legal; V. Execução de contrato, de trabalho, pelo Controlador; IX. Legitimo interesse do controlador;	1) Decreto-lei nº 5.452, de 1º de maio de 1943; 2) Constituição da República Federativa do Brasil de 1988, artigo 7 ; 3) Emenda constitucional nº 28, de 25 de maio de 2000; 4) Emenda constitucional nº 72, de 2 de abril de 2013; 5) Decreto nº 8.373, de 11 de dezembro de 2014; 6) Lei 13.467/2017 (Reforma Trabalhista);	I. Apoio a atividades do controlador: Processo Admissional; e II. Prestação de benefício ao candidato: contratação;	NA	Não	Não	Não	Sim	3. Médio
						Cumprimento de obrigação legal				Sim	4. Alto

Apêndice D1 - Inventário de Dados (2a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
4. Centro Universitário: **Cadastro Sistêmico** de Admissão - **TOTVS ERP**	Nome, nome social, estado natal, cidade, naturalidade, data nascimento, estado civil, sexo, nacionalidade, grau de instrução, tipo sanguíneo, e-mail profissional, CPF, RG, título de eleitor, carteira de trabalho, CNH, certificado reservista, PIS/PASEP; endereço residencial (rua, número, CEP, bairro, telefones (residencial e celular); departamento alocado, salário; jornada; dados bancários (banco, agência e conta corrente), dependentes (pai, mãe, conjugue e filhos), data admissão (FGTS), plano de saúde; dados de acesso ao local de trabalho - controle de jornada (REP);	Pessoal	Cadastro pelo DRH em software de parceiro externo, TOTVS	Digital: Interface de software de parceiro externo, TOTVS	Digital: Base de Dados do Controlador	05 anos Lei 5.452/1945 (CLT), art. 11; FGTS: 30 anos art. 23, § 5º, Lei 8036/90 e Súmula 362 TST ; Folha de Pagamento: 10 anos art. 225, I e § 5º, Dec. 3048/99;	Controlador	Encarregado de Dados e Recursos Humanos e Departamento de Tecnologia e Informação
	RAIS (cor, raça); Dados Biométricos: digital, foto; Dados dos filhos, se, menores, Filiação Sindical;	Sensível						
5. Centro Universitário: Cadastro de **Conta Salário - Santander**	Nome, CPF, residência, função/cargo e salário;	Pessoal	Informado pelo Controlador a Banco Privado do Sistema Bancário Brasileiro	Físico: Papel	Físico: Arquivo DRH	Folha Pagamento: 10 anos art. 225, I e § 5º, Dec.3048/99	Controlador	Encarregado de Dados e Recursos Humanos
6. Centro Universitário: **Assinatura Ficha de** Registro de **Empregado**	Nome, Filiação (nome dos pais), Carteira de trabalho, Reservista, Título de eleitor, CNH, RG, data de nascimento, estado civil, sexo, escolaridade, nacionalidade, naturalidade, dependentes; Se estrangeiro: data da chegada, conjugue, identidade, tipo de visto, número registro geral, decreto, naturalizado, validade identidade, validade carteira de trabalho, número de filhos;	Pessoal	Informado pelo funcionário	Físico: Papel	Físico: Arquivo DRH	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos

Apêndice D1 - Inventário de Dados (2b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
4. Centro Universitário: **Cadastro Sistêmico** de Admissão - **TOTVS ERP**	Coleta, classificação, utilização, acesso, transmissão, processamento, armazenamento, eliminação;	Execução de processo admissional;	II. Obrigação Legal; V. Execução de contrato, de trabalho, pelo Controlador; IX. Legitimo interesse do controlador;	1) Decreto-lei nº 5.452, de 1º de maio de 1943; 2) Constituição da República Federativa do Brasil de 1988, artigo 7 ; 3) Emenda constitucional nº 28, de 25 de maio de 2000; 4) Emenda constitucional nº 72, de 2 de abril de 2013; 5) Decreto nº 8.373, de 11 de dezembro de 2014; 6) Lei 13.467/2017 (Reforma Trabalhista);	I. Apoio a atividades do controlador: Processo Admissional; e II. Prestação de benefício ao candidato: contratação;	NA	Sim: Banco Privado do Sistema Bancário Brasileiro (Santander); Empresa Privada Assistência Médica (AMIL); Empresa Privada Corretora de Seguros (TRR); Empresa Privada de Seguro de Vida e Previdência (MetLife); Empresa Privada de Medicina do Trabalho (WorkLife); Empresa Privada de Software de Medicina Ocupacional (ProClinic); Ministério da Economia - Secretaria Especial de Previdência e Trabalho (eSocial);	Não	Sim	Sim	3. Médio
						Consentimento e cumprimento de obrigação legal;				Sim	4. Alto
5. Centro Universitário: Cadastro de **Conta Salário - Santander**	Coleta, utilização, transferência, armazenamento e eliminação;	Execução de processo admissional;	II. Obrigação Legal; V. Execução de contrato, de trabalho, pelo Controlador; IX. Legitimo interesse do controlador;	Resoluções 3.402 e 3.424/06 - Conselho Nacional Monetário;	I. Apoio a atividades do controlador: recrutamento interno; e II. Prestação de benefício ao funcionário: pagamento salário;	NA	Sim: Banco Privado do Sistema Bancário Brasileiro (**Santander**);	Não	Não	Sim	3. Médio
6. Centro Universitário: **Assinatura Ficha de** Registro de **Empregado**	Coleta, utilização, impressão, coleta de assinatura, armazenamento e eliminação;	Execução de processo admissional;	II. Obrigação Legal; V. Execução de contrato, de trabalho, pelo Controlador; IX. Legitimo interesse do controlador;	1) Decreto-lei nº 5.452, de 1º de maio de 1943; 2) Lei 13.467/2017 (Reforma Trabalhista);	I. Apoio a atividades do controlador: processo de contratação;	NA	Não	Não	Não	Sim	3. Médio

Apêndice D1 - Inventário de Dados (3a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
7. Centro Universitário: **Assinaturas Contratos:** Trabalho (experiência e posterior), Acordo individual de compensação de horas, e Cessão de uso de imagem e declarações;	Nome, CPF, residência, função/cargo, assinatura;	Pessoal	Informado pelo funcionário	Físico: Papel	Físico: Arquivo DRH	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos
8. Centro Universitário: Processo de Nomeação e, ou alteração de Beneficiário do **seguro de vida** institucional (**TRR** e **MetLife**)	Nome, CPF, estipulante, subestipulante, número da apólice, nome do beneficiário, percentual de participação da apólice e grau de parentesco;	Pessoal	Informado pelo funcionário	Físico: Papel; Digital: E-mail	Físico: Arquivo DRH; Digital: Base de dados do parceiro / provedor de e-mail (MS)	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos
9. Centro Universitário: Processo de **Adesão e movimentação** no cadastro de beneficiários pessoa jurídica **Assistência Médica** e Dental (**AMIL**)	Titular: Nome, CPF, número do cartão médico e odontológico, data de nascimento, número do cartão do sistema único de saúde (SUS), sexo, estado civil, endereço, telefones para contato; Dependentes: nome, CPF, número do cartão do SUS, número da declaração de nascido vivo (à partir de 2010), data de nascimento, grau de parentesco, nome da mãe, sexo, estado civil, IMC, assinatura;	Pessoal	Informado pelo funcionário	Físico: Papel	Físico: Arquivo DRH; Digital: Base de dados do parceiros de software	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos
	Declaração de saúde (Titular e dependentes), se portador ou se já sofreu de doenças: do aparelho cardio circulatório, endócrinas, metabólicas, do sangue, imunológicas, do colágeno, autoimunes, do sistema nervoso, cerebrovasculares, do aparelho respiratório, do ouvido, do nariz, da garganta, ortopédicas, tumorizações malignas (câncer), do aparelho urinário, aparelho reprodutor (masculino ou feminino), qualquer outra doença não relacionada anteriormente ou que tenha gerado internação;	Sensível						

Apêndice D1 - Inventário de Dados (3b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
7. Centro Universitário: **Assinaturas Contratos:** Trabalho (experiência e posterior), Acordo individual de compensação de horas, e Cessão de uso de imagem e declarações;	Coleta, utilização, impressão, coleta de assinatura, armazenamento e eliminação;	Execução de processo admissional;	I. Consentimento; II. Obrigação legal; V. Execução de contrato, de trabalho, pelo Controlador; IX. Legitimo interesse do controlador;	1) Decreto-lei nº 5.452, de 1º de maio de 1943; 2) Lei 13.467/2017 (Reforma Trabalhista);	I. Apoio a atividades do controlador: processo de contratação;	NA	Não	Não	Não	Sim	3. Médio
8. Centro Universitário: Processo de Nomeação e, ou alteração de Beneficiário do **seguro de vida** institucional (**TRR** e **MetLife**)	Coleta, utilização, impressão, coleta de assinatura, transmissão, armazenamento e eliminação	Execução de processo admissional;	II. Obrigação legal; V. Execução de contrato, de trabalho, pelo Controlador; IX. Legitimo interesse do controlador;	1) Decreto-lei nº 5.452, de 1º de maio de 1943; 2) Lei 13.467/2017 (Reforma Trabalhista);	I. Apoio a atividades do controlador: processo de contratação; II. Benefício do titular: Seguro de vida;	NA	Sim: Empresa Privada de Seguro de Vida (**MetLife**) e Corretora de Seguros (**TRR**)	Não	Não	Sim	3. Médio
9. Centro Universitário: Processo de **Adesão e movimentação** no cadastro de beneficiários pessoa jurídica **Assistência Médica** e Dental (**AMIL**)	Coleta, classificação, utilização, acesso, transmissão, processamento, armazenamento, eliminação;	Execução de processo admissional;	V. Execução de contrato, de trabalho, pelo Controlador; IX. Legitimo interesse do controlador;	NA	I. Apoio a atividades do controlador: admissão de funcionário; e II. Prestação de benefício ao funcionário: contratação de plano de saúde privado;	NA	Sim: Empresa Privada de Assistência Médica Dental (**AMIL**)	Não	Não	Sim	3. Médio
			Consentimento;			Consentimento e cumprimento de obrigação legal;				Sim	4. Alto

Apêndice D1 -Inventário de Dados (4a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
10. Centro Universitário: Processo de Operação e Manutenção da Medicina do Trabalho (SST: Saúde e Segurança do Trabalho) (**WorkLife**)	Nome , RG, cargo, setor, assinatura, idade;	Pessoal	Informado pelo funcionário	Físico: Papel	Físico: Arquivo DRH; Digital: Base de dados do parceiros de software	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos
	Atestados de saúde ocupacionais: Exames médicos Admissionais, demissionais, periódicos e a critério médico que incorram em afastamento;	Sensível	Obtido junto a parceiro Particular de Medicina Laboral contratada;					
11. Centro Universitário: Processo de **cadastro e gestão de Medicina Ocupacional** (SST: Saúde e Segurança do Trabalho) (**ProClinic**)	Nome, sexo, estado civil, data nascimento, idade, salário, função, CFP, datas (admissão, demissão e afastamento), contatos telefônicos, endereço residencial, matrícula e qualificação;	Pessoal	Informado pelo funcionário		Digital: Base de dados do parceiro de software de Medicina Ocupacional, ProClinic;	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos
	Exames médicos (passado e presente), GHE (Grupo Homogêneo de Exposição), exames (a vencer e vencidos), apto e inapto ao trabalho;	Sensível	Obtido junto a parceiro Particular de Medicina Laboral contratada;					
12. Centro Universitário: **Envio de dados** funcionários para Governo (**TOTVS TAF**, **ProClinic** e **eSocial**)	Nome, CPF, NIS, Sexo, Estado Civil, Grau de Instrução, Data de nascimento, pais de nascimento, pais de naturalidade, UF, município, nome da mãe e do pai, regime trabalhista, regime previdenciário, cargo, função, CBO (classificação Brasileira de Ocupação), data, razão e verbas rescisórias;	Pessoal	1. informado pelo funcionário; 2. atribuído pela empresa ao funcionário; 3. coletado junto ao parceiros de segurança e medicina do trabalho;	Digital: base de dados Operador	Digital: Base de dados dos parceiro de software de Medicina Ocupacional, ProClinic; Físico: Prontuário funcionário;	NA	Controlador	Encarregado de Dados e Recursos Humanos
	Raça, exames admissionais, exames complementares (de acordo com os riscos aos quais o trabalhador está exposto), exames de retorno ao trabalho e exames periódicos;	Sensível		Físico: papel e Digital: base de dados Operador				

Apêndice D1 - Inventário de Dados (4b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
10. Centro Universitário: Processo de Operação e Manutenção da Medicina do Trabalho (SST: Saúde e Segurança do Trabalho) (**WorkLife**)	Coleta, utilização, classificação, transmissão, armazenamento e eliminação;	Execução de processo admissional;	I. Consentimento ; II. Obrigação Legal; V. Execução de contrato, de trabalho, pelo Controlador; IX. Legitimo interesse do controlador: admissão funcionário;	CLT - Decreto Lei nº 5.452 de 01 de Maio de 1943, artigo 168; Lei nº 7.855, de 24/10/1989; Lei 13.467/2017;	I. Apoio a atividades do controlador: admissão de funcionário; e II. Prestação de benefício ao funcionário: avaliação médica;	NA	Sim: Empresa Privada de Segurança e Medicina do Trabalho (**WorkLife**)	Não	Não	Não	3. Médio
						Consentimento e cumprimento de obrigação legal;				Não	4. Alto
11. Centro Universitário: Processo de **cadastro e gestão de Medicina Ocupacional** (SST: Saúde e Segurança do Trabalho) (**ProClinic**)	Coleta, utilização, classificação, transmissão, armazenamento e eliminação;	Execução de processo de gestão laboral	II. Obrigação Legal; V. Execução de contrato, de trabalho, pelo Controlador;	CLT - Decreto Lei nº 5.452 de 01 de Maio de 1943, artigo 168; Lei nº 7.855, de 24/10/1989; Lei 13.467/2017;	NA	NA	Sim: parceiro de software de Medicina Ocupacional, (**ProClinic**);	Não	Não	Sim	3. Médio
						Consentimento e cumprimento de obrigação legal;				Sim	4. Alto
12. Centro Universitário: **Envio de dados** funcionários para Governo (**TOTVS TAF**, **ProClinic** e **eSocial**)	Coleta, utilização, classificação, transmissão, armazenamento e eliminação;	Execução de processo de gestão laboral e Obrigação Legal	II. Obrigação Legal;	CLT - Decreto Lei nº 5.452 de 01 de Maio de 1943, artigo 168; Lei nº 7.855, de 24/10/1989; Lei 13.467/2017;	NA	NA	Sim: Ministério da Economia, Secretaria Especial de Previdência e Trabalho (**eSocial**)	Não	Não	Não	3. Médio
						II. Obrigação legal;				Não	4. Alto

Apêndice D1 - Inventário de Dados (5a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
13. Centro Universitário: Processo de **desligamento**	Nome, Endereço, CTPS, CPF, RG, nascimento, nome da mãe, causa do afastamento, cargo, remuneração, datas: admissão, aviso prévio, afastamento, verbas rescisórias, dependentes, saldo FGTS,	Pessoal	Informado pelo funcionário	Digital: base de dados Operador	Digital: Base de dados dos parceiro de software de Medicina Ocupacional, ProClinic; Físico: Prontuário funcionário;	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos
	Filiação Sindical, Atestado de saúde ocupacional (demissional)	Sensível	Coletado junto à parceiro de segurança e medicina do trabalho	Físico: papel e Digital: base de dados Operador				
14. Centro Universitário: Processo de **armazenamento externo**: **Iron Mountain**	Nome, Filiação (nome dos pais), Carteira de trabalho, Reservista, Título de eleitor, CNH, RG, data de nascimento, estado civil, sexo, escolaridade, nacionalidade, naturalidade, dependentes; Se estrangeiro: data da chegada, conjugue, identidade, tipo de visto, número registro geral, decreto, naturalizado, validade identidade, validade carteira de trabalho, número de filhos;	Pessoal	Informado pelo funcionário	Físico: Papel	Físico: Armazém de Empresa Privada de Guarda e Gestão de documentos	05 anos Lei 5.452/1945 (CLT), art. 11; Constituição Federal art. 7º, XXIX;	Controlador	Encarregado de Dados e Recursos Humanos
	Atestados de saúde ocupacionais: Exames médicos Admissionais, demissionais, periódicos e a critério médico que incorram em afastamento;	Sensível	Coletado junto à parceiro de segurança e medicina do trabalho					
15. Centro Universitário: Processo de **inscrição** para **vestibular**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais;	Pessoal	Informado pelo candidato	Digital: formulário web de parceiro: CRM Educacional	Digital: Base de dados de parceiro: CRM Educacional	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Área de Relacionamento Institucional
16. Centro Universitário: Processo de **transmissão de dados** do inscrito para o **Controlador**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais;	Pessoal	Informado pelo candidato	Digital: formulário web de parceiro: CRM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação;

Apêndice D1 - Inventário de Dados (5b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
13. Centro Universitário: Processo de **desligamento**	Coleta, utilização, classificação, armazenamento e eliminação;	Execução de processo demissional;	II. Obrigação Legal;	CLT - Decreto Lei nº 5.452 de 01 de Maio de 1943, artigo 168; Lei nº 7.855, de 24/10/1989; Lei 13.467/2017;	NA	NA	Sim: Banco Privado do Sistema Bancário Brasileiro (**Santander**); Empresa Privada Assistência Médica (**AMIL**); Empresa Privada Corretora de Seguros (**TRR**); Empresa Privada de Seguro de Vid e Previdência (**MetLife**); Empresa Privada de Medicina do Trabalho (**WorkLife**); Empresa Privada de Software de Medicina Ocupacional (**ProClinic**); Ministério da Economia - Secretaria Especial de Previdência e Trabalho (**eSocial**);	Não	Não	Sim	3. Médio
						II. Obrigação legal;				Sim	4. Alto
14. Centro Universitário: Processo de **armazenamento externo**: **Iron Mountain**	Coleta e Armazenamento	Execução de processo de Gestão Laboral	II. Obrigação Legal; V. Execução de contrato, de trabalho, pelo Controlador;	CLT - Decreto Lei nº 5.452 de 01 de Maio de 1943, artigo 168; Lei nº 7.855, de 24/10/1989; Lei 13.467/2017;	NA	NA	Sim: Empresa Privada de Guarda e Gestão de documentos, **Iron Mountain**	Não	Não	Sim	3. Médio
						II. Obrigação legal;				Sim	4. Alto
15. Centro Universitário: Processo de **inscrição** para **vestibular**	Coleta, classificação, utilização e armazenamento	Execução de processo de inscrição para vestibular	I. Consentimento; II. Obrigação Legal;	Portaria Normativa nº 40/2007, republicada em 29/12/2010	NA	NA	Sim: Empresa Privada de Gestão Educacional, **CRM Educacional**	Não	Não	Sim	3. Médio
16. Centro Universitário: Processo de **transmissão de dados** do inscrito para o **Controlador**	Coleta, transmite e armazena;	Transporte e detenção local dos dados dos titulares inscritos em processo seletivo	I. Consentimento;	NA	NA	NA	Sim: Empresa Privada de Gestão Educacional, **CRM Educacional**	Não	Não	Sim	3. Médio

Apêndice D1 - Inventário de Dados (6a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
17. Centro universitário: Processos de **contato e relacionamento** com o **inscrito** em **processo seletivo** graduação;	Nome, e-mail, celular;	Pessoal	Informado pelo candidato	Digital: formulário web de parceiro: CRM Educacional	Digital: Base de dados do Controlador e parceiro: CRM Educacional;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Área de Relacionamento Institucional;
18. Centro Universitário: Processo de **matrícula Graduação**;	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	Pessoal	Informado pelo candidato	Digital: formulário web ou local e parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Área de Relacionamento Institucional;
	Nome social, digital, foto;	Sensível						
19 Centro Universitário: transporte dados para Secretaria da Graduação - **Arquivo vivo aluno;**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	Pessoal	Informado pelo candidato	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Física: Pasta do aluno; Digital: Base de dados do Controlador e de parceiro de gestão eletrônica de documentos, TOTVS DocExpress;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Secretaria da Graduação;
	Nome social, digital, foto;	Sensível						
20. Centro Universitário: **controle de acesso físico** aos Campi	Nome	Pessoal	Informado pelo candidato	Digital: formulário web de parceiro: TOTVS RM Educacional integração programa	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação, Departamento de Segurança e Risco e Secretaria da Graduação;
	Foto e, ou digital;	Sensível						

Apêndice D1 - Inventário de Dados (6b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
17. Centro universitário: Processos de **contato e relacionamento** com o **inscrito** em **processo seletivo** graduação;	Classificação, utilização	Comunicação com o titular de dados inscrito no processo seletivo graduação;	I. Consentimento;	NA	NA	NA	Sim: Empresa Privada de Gestão Educacional, **CRM Educacional**	Não	Não	Sim	3. Médio
18. Centro Universitário: Processo de **matrícula Graduação**;	Coleta, utilização, classificação, transmissão, armazenamento e eliminação;	Matricular candidato em curso de formação superior - Graduação, emitir crachá de acesso físico às instalações da IES;	I. Consentimento; II. Obrigação Legal;	Lei nº 9.394/1996 (LDB); Lei nº 11.741, de 2008; Portaria MEC nº 230/2007;	NA	I. Consentimento;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**	Não	Não	Sim	3. Médio
										Sim	4. Alto
19 Centro Universitário: transporte dados para Secretaria da Graduação - **Arquivo vivo aluno;**	Coleta, utilização, classificação, transmissão, armazenamento e eliminação;	Gerar repositório de registro da atividade acadêmica do aluno;	I. Consentimento; V. Execução de contrato;	NA	NA	I. Consentimento;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional Secretaria Digital**	Não	Não	Sim	3. Médio
										Sim	4. Alto
20. Centro Universitário: **controle de acesso físico** aos Campi	Coleta, utilização, classificação, armazenamento e eliminação;	Controlar o acesso aos Campi e a presença, do aluno, em sala de aula, por meio do software, legado, "ChamadaOnLine";	I. Consentimento, VII. Proteção da vida ou da incolumidade;	NA	NA	I. Consentimento;	Sim: Empresa Privada de Gestão de Controle de Acesso, **Sualtech**	Não	Não	Sim	3. Médio
										Sim	4. Alto

Apêndice D1 - Inventário de Dados (7a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
21. Centro Universitário: atribuição de **grade acadêmica** ao aluno;	Nome	Pessoal	Informado pelo aluno	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Secretaria da Graduação;
22. Centro Universitário: **Comunicação** acadêmica **com aluno**;	Nome e telefone (whatsapp)	Pessoal	Informado pelo aluno	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Reitoria;
23. Centro Universitário: Processo de **avaliação acadêmica**;	Nome	Pessoal	Informado pelo aluno	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Física: pasta do aluno; Digital: Base de dados do Controlador e do parceiro de gestão de avaliações acadêmicas, ProvaFácil;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Secretaria da Graduação;
24. Centro Universitário: Processo de **orientação** e **aconselhamento** de **carreira;**	Nome, e-mail, celular;	Pessoal	Informado pelo aluno	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e FECAP+;
25. Centro Universitário: Processo de **gestão** e controle da **evasão;**	Nome, e-mail, celular;	Pessoal	Informado pelo aluno	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e FECAP+;

Apêndice D1 - Inventário de Dados (7b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
21. Centro Universitário: atribuição de **grade acadêmica** ao aluno;	Coleta, utilização, classificação;	Associar ao aluno: turma, sala, disciplinas, professores, ano letivo;	I. Consentimento; V. Execução de contrato;	NA	NA	NA	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**	Não	Não	Sim	3. Médio
22. Centro Universitário: **Comunicação** acadêmica **com aluno**;	Coleta, utilização;	Informar disposições acadêmicas ao aluno;	I. Consentimento; V. Execução de contrato;	NA	NA	NA	NA	Não	Não	Sim	3. Médio
23. Centro Universitário: Processo de **avaliação acadêmica**;	Coleta, utilização, classificação, armazenamento;	Gerar, aplicar, corrigir, divulgar, armazenar provas para alunos da graduação;	I. Consentimento; V. Execução de contrato;	NA	NA	NA	Sim: Empresa Privada de Gestão de avaliações acadêmicas, **ProvaFácil**	Não	Não	Sim	3. Médio
24. Centro Universitário: Processo de **orientação** e **aconselhamento** de **carreira;**	Coleta, utilização, classificação, armazenamento;	Planejar carreira com vistas ao ingresso ou recolocação no mercado de trabalho;	I. Consentimento;	NA	NA	NA		Não	Não	Sim	3. Médio
25. Centro Universitário: Processo de **gestão** e controle da **evasão;**	Coleta, utilização, classificação, armazenamento;	Entender fatores motivadores, da evação, e buscar soluções;	I. Consentimento;	NA	NA	NA	NA	Não	Não	Sim	3. Médio

Apêndice D1 - Inve ntário de Dados (8a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
26. Centro Universitário: Processo de **apoio psicopedagógico** ao **aluno;**	Nome, e-mail, celular;	Pessoal	Informado pelo aluno	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e FECAP+;
	Laudos e análises psicopedagógicas	Sensível	Sessões de aconselhamento psicopedagógicas	Fisico: papel; Digital: Documento eletrônico (MS.Word)	Físico: pasta do aluno; Digital: repositório de rede da IES			
27. Centro Universitário: Processo de **suporte acadêmico (Central do Aluno)**	Nome, telefone, responsável legal (financeiro e, ou acadêmico),	Pessoal	Informado e, ou coletado junto ao aluno	Físico: entrega de cópia de atestados; Digital: interface de software parceiro TOTVS RM Educacional e Aplicativo IES;	Física: Pasta do aluno; Digital: Base de dados do Controlador e de parceiro de gestão eletrônica de documentos, TOTVS DocExpress;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Central do Aluno;
	Atestados médicos (de saúde), nome social, laudos psicológicos;	Sensível						
28. Centro Universitário: **Rematrícula**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	Pessoal	Informado pelo candidato	Digital: formulário web de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Área de Relacionamento Institucional;
	Nome social, digital, foto;	Sensível						
29. Centro Universitário: **Emissão de Diploma**	Nome, CPF, RG	Pessoal	Informado pelo candidato	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Física: Pasta do aluno; Digital: Base de dados do Controlador e de parceiro de gestão eletrônica de documentos, TOTVS DocExpress;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Informação e Secretaria da Graduação;

Apêndice D1 -Inventário de Dados (8b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
26. Centro Universitário: Processo de **apoio psicopedagógico** ao **aluno;**	Coleta, utilização, classificação, armazenamento;	Apoiar aluno no processo de autoconhecimento e desenvolvimento pessoal, social e profissional;	I. Consentimento;	NA	NA	I. Consentimento;	NA	NA	Não	Não	3. Médio
										Não	4. Alto
27. Centro Universitário: Processo de **suporte acadêmico (Central do Aluno)**	Coleta, utilização, classificação, armazenamento e eliminação;	Atuar como apoiador e facilitador da vida acadêmica e financeira do aluno da IES: emissão de documentos, abono de ausências justificadas, revisão de avaliações, negociações financeiras, etc.;	I. Consentimento; V. Execução de contrato;	NA	NA	I. Consentimento;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional Secretaria Digital**	Não	Não	Sim	3. Médio
										Sim	4. Alto
28. Centro Universitário: **Rematrícula**	Coleta, utilização, classificação, transmissão, armazenamento e eliminação;	**Re**matricular candidato em curso de formação superior - Graduação;	I. Consentimento; II. Obrigação Legal;	Lei nº 9.394/1996 (LDB); Lei nº 11.741, de 2008; Portaria MEC nº 230/2007;	NA	I. Consentimento;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**	Não	Não	Sim	3. Médio
										Sim	4. Alto
29. Centro Universitário: **Emissão de Diploma**	Coleta, utilização, classificação, armazenamento;	Emitir, imprimir diploma de graduação do aluno	I. Consentimento; II. Obrigação Legal;	Lei nº 9.394/1996 (LDB); Lei nº 11.741, de 2008; Portaria MEC nº 230/2007;	NA	NA	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional Secretaria Digital**	Não	Não	Sim	3. Médio

Apêndice D1 - Inventário de Dados (9a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
30. Centro Universitário: **emissão** de **boletos**	Nome, endereço, CPF, Responsável Financeiro	Pessoal	Informado pela aluno e coletado junto ao sistema	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Base de dados do Controlador	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;
31. Centro Universitário: **declaração** de **adimplência**	Nome, CPF	Pessoal	Informado pela aluno e coletado junto ao sistema	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador e de parceiro de gestão eletrônica de documentos, TOTVS DocExpress;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;
32. Centri Universitário: **conbrança** (**inadimplência**)	Nome, CPF, E-mail, teefone, endereço	Pessoal	Informado pela aluno e coletado junto ao sistema	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;
33. Centro Univesitário: **Confissão de dívida**	Nome, endereço, CPF, e-mail	Pessoal	Informado pela aluno e coletado junto ao sistema	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;
34. Centro Universitário: **reenbolso**	Nome, CPF, dados bancário para reenbolso;	Pessoal	Informado pela aluno e coletado junto ao sistema	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;

Apêndice D1 - Inventário de Dados (9b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
30. Centro Universitário: **emissão** de **boletos**	Coleta, utilização, classificação, armazenamento;	Gerar boletos para pagamento dos serviços educacionais contratados;	I. Consentimento; II. Obrigação Legal; V. Execução de contrato;	Circular nº 3.598/2012 - Banco Central do Brasil (BACEN)	NA	NA	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**; Banco Privado do Sistema Bancário Brasileiro (**Santander**)	Não	Não	Sim	Médio
31. Centro Universitário: **declaração** de **adimplência**	Coleta, utilização, classificação, armazenamento;	Emitir declaração de adimplência do aluno;	I. Consentimento; II. Obrigação Legal;	Lei nº 12.007/2009	NA	NA	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional;** Empresa Privada de comunicação por mensagens de texto**, ChatBot**	Não	Não	Sim	3. Médio
32. Centri Universitário: **conbrança** (**inadimplência**)	Coleta, utilização, classificação, armazenamento;	Informar aluno sobre não pagamento de mensalidade e negociar formas de quitação destas;	I. Consentimento; II. Obrigação Legal; X. Proteção ao crédito;	Lei nº 15.659/2015; Lei nº 12.414/2011 (formação de histórico de crédito); Lei 10.406/2002 (Código Civil) artigo 188, inciso I; Lei 8078/1990 (Código de Defesa do Consumidor) artigo 43;	NA	NA	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional;** Empresa Privada de comunicação por mensagens de texto**, ChatBot;** Empresa Privada de pagamentos eletrônicos no varejo, **CIELO;** Serviço Central de Proteção ao Crédito **Boa Vista SCPC;** Empresa Privada de recuperação de crédito,	Não	Não	Sim	4. Alto
33. Centro Univesitário: **Confissão de dívida**	Coleta, utilização, classificação, armazenamento;	Negociar dívida com aluno;	I. Consentimento; II. Obrigação Legal; X. Proteção ao crédito;	Lei nº 10.406/2002 (Código Civil); Lei n º 8.078/ 1990 (Código de Defesa do Consumidor); Lei 13.105/2015 (Código do Processo Civil), art.784;	NA	NA	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**; Banco Privado do Sistema Bancário Brasileiro (**Santander**)			Sim	
34. Centro Universitário: **reenbolso**	Coleta, utilização, armazenamento;	Restituir valor ao aluno por serviço não realizado;	I. Consentimento; V. Execução de contrato;	NA	NA	NA	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**; Banco Privado do Sistema Bancário Brasileiro (**Santander**)	Não	Não	Sim	3. Médio

Apêndice D1 - Inventário de Dados (10a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
35. Centro Universitário: **Financiamentos Próprios**	Aluno e Fiador: Nome, CPF, RG, endereço (rua, número, bairro, cep, cidade, estado - UF), profissão, nacionalidade, telefone, estado civil, data de nascimento;	Pessoal	Informado pela candidato e coletado junto ao sistema	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;
	Aluno e Fiador: Renda (salário);	Sensível	Informado pelo aluno;					
36. Centro Universitário: **assistência financeira**	Aluno e responsável financeiro: nome, RG, CPF, endereço;	Pessoal	Informado pela aluno e coletado junto ao sistema	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;
	Quando cabido: Termo de rescisão contrato de trabalho, carteira de trabalho, certidão de óbito responsável financeiro, Laudo médico atestando a invalidez permanente e total, informando as sequelas deixadas pelo acidente, discriminando cada órgão ou membros lesados, do responsável financeiro, Relatório Médico informando o motivo e o período de afastamento das atividades laborais do aluno;	Sensível	Informado pelo aluno e, ou responsável financeiro;					
37. Centro Universitário: **PROUNI**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	Pessoal	Informado pelo candidato;	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;
	Nome social, digital, foto, salário (holerite);	Sensível						
38. Centro Universitário: **FIES**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	Pessoal	Informado pelo candidato;	Digital: formulário web ou local de parceiro: TOTVS RM Educacional	Digital: Base de dados do Controlador;	Tabela de teporalidade para IES: Portaria MEC nº 1.224/2013;	Controlador	Encarregado de Dados e Departamento de Tecnologia e Departamento Financeiro;
	Nome social, digital, foto, salário (holerite);	Sensível						

Apêndice D1 - Inventário de Dados (10b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
35. Centro Universitário: **Financiamentos Próprios**	Coleta, utilização, classificação, armazenamento;	Possibilitar pagamento parcial dos valores das mensalidades da graduação ao final do curso;	I. Consentimento; V. Execução de contrato;	NA	NA	I. Consentimento;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**;	Não	Não	Sim	3. Médio
										Sim	4. Alto
36. Centro Universitário: **assistência financeira**	Coleta, utilização, classificação, armazenamento;	Garantir a continuidade de estudos, em caso da perda de renda por desemprego, falecimento ou invalidez por acidente ou perda de renda por afastamento médico do responsável financeiro do contrato de prestação de serviços educacionais	I. Consentimento; V. Execução de contrato;	NA	NA	I. Consentimento;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**;	Não	Não	Sim	3. Médio
										Sim	4. Alto
37. Centro Universitário: **PROUNI**	Coleta, utilização, classificação, transmissão, armazenamento e eliminação;	Oferecer bolsas de estudo, integrais e parciais (50%) governamentais, em instituições particulares de educação superior;	I. Consentimento; II. Obrigação Legal;	Lei nº 11.096/2005	NA	I. Consentimento; II.a. Obrigação Legal;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**;	Não	Não	Sim	3. Médio
										Sim	4. Alto
38. Centro Universitário: **FIES**	Coleta, utilização, classificação, transmissão, armazenamento e eliminação;	Fundo de Financiamento Estudantil (Fies), é uma ação do Ministério da Educação que financia cursos superiores não gratuitos;	I. Consentimento; II. Obrigação Legal;	Lei nº 10.260/2001; Lei nº 13.530/2017; Portaria nº 209, de 7 março de 2018	NA	I. Consentimento; II.a. Obrigação Legal;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**;	Não	Não	Sim	3. Médio
										Sim	4. Alto

Apêndice D1 - Inventário de Dados (11a_de_11)

PROCESSO INSTITUCIONAL	DADOS	TIPO	ORIGEM	MEIO	ARMAZENA	RETENÇÃO	RISK OWNER	RISK CO OWNER
39. Centro Universitário: **Controle de acesso VISITANTE, PRESTADOR DE SERVIÇO E USUÁRIOS SEM VÍNCULO**	RG, CPF, CNH, RNE (Registro Nacional de Estrangeiros), nome, e-mail, telefone, nascimento, idade;	Pessoal	Informado pelo visitante, prestador de serviço ou usuário em vínculo;	Digital: formulário de sistema de parceiro SUAL TECH	Digital: Base de dados do Controlador;	05 anos da data da coleta	Controlador	Encarregado de Dados e Departamento de Segurança e Gestão de Riscos
	Foto e, ou digital	Sensível						
40. Centro Universitário: **Controle** de **acesso** a rede sem fio, **WI-FI** (Wireless Fidelity)	Dados de redes sociais: Google e Facebook; **ou** Dados cadastrais: nome, endereço, e-mail, data de nascimento, sexo, RG, CPF;	Pessoal	Informado pelo usuário	Digital: Formulário online	Base de dados do Operador	01 ano da data da coleta	Controlador	Encarregado de Dados, Departamento de Tecnologia e de Marketing
41. Centro Universitário: **Cookies** do **site** do controlador	Dados navegacionais: Identificação sobre o usuário (endereço IP, dispositivo, navegador) , Operadora: *Internet Service Provider* , comportamento de navegação e preferências para um site(s) específico(s) da IES locus;	Pessoal	Coletado junto a navegação de internet do titular de dados, exclusivamente no site da IES locus;	Digital: Cookies;	Base de dados do Operador	Enquanto durar o tratamento dos dados coletados.	Controlador	Encarregado de Dados e Departamento de Marketing
42. Centro Universitário: **Registros** de **Navegação** de **Internet**	Dados Navegacionais: Informações sobre sistema operacional e navegador do dispositivo, Endereço IP, Geolocalização (se ativada), Conteúdo e tempo navegado, Dados técnicos do dispositivo utilizado, Registros de interações com a plataforma (cookies);	Pessoal	Coletado junto a navegação de internet do titular de dados;	Digital: ferramenta de coleta, armazenamento e análise de dados navegacionais;	Base de dados do Controlador	01 ano da data da coleta	Controlador	Encarregado de Dados e Departamento de Tecnologia
43. Centro Universitário: **Acesso** a **rede** administrativa e, ou acadêmica enquanto **visitante**	Informações sobre o sistema operacional, aplicativos utilizados, acessos a recursos da rede local (LAN): diretórios e impressoras - se disponível, tempo de sessão (*logout - login*), criação e edição de arquivos;	Profissional	Coletado junto a sessão de rede do titular de dados;	Digital: ferramenta de coleta, armazenamento	Base de dados do Controlador	Enquanto se manter o vículo empregatício com o titular de dados	Controlador	Encarregado de Dados e Departamento de Tecnologia

Apêndice D1 - Inventário de Dados (11b_de_11)

PROCESSO	TRATAMENTO	RAZÃO	LEGITIMAÇÃO				COMPARTILHA	TRANS	ANONI	A18	IMP.
INSTITUCIONAL	ART.5.X.	ART.6	BL.ART.7	ART.7.II.OL.	LI.ART. 10	DPS. ART.11		INTERN			
39. Centro Universitário: **Controle de acesso VISITANTE, PRESTADOR DE SERVIÇO E USUÁRIOS SEM VÍNCULO**	Coleta, armazenamento e eliminação;	Dispor acesso fisico às dependências dos Campi da IES	VII. Proteção da vida ou da incolumidade;	NA	NA	II.e. Proteção da vida ou da incolumidade;	Sim: Empresas Privada de Controle de Acesso, **Sual Tech;**	Não	Não	Sim	3. Médio
										Sim	4. Alto
40. Centro Universitário: **Controle** de **acesso** a rede sem fio, **WI-FI** (Wireless Fidelity)	Coleta, armazenamento, classificação, comunicação, armazenamento e eliminação;	Dispor acesso a rede mundial de computadores ao aluno	I. Consentimento;	NA	NA	NA	NA	Não	Não	Sim	3. Médio
41. Centro Universitário: **Cookies** do **site** do controlador	Coleta, armazenamento, classificação, comunicação, armazenamento e eliminação;	Melhorar a experiência de navegação no site do Controlador e divulgar produtos e serviços próprios;	I. Consentimento;	NA	NA	NA	NA	Não	Não	Sim	2. Baixo
42. Centro Universitário: **Registros** de **Navegação** de **Internet**	Coleta, classificação, armazenamento e eliminação;	Dispor acesso a rede mundial de computadores ao aluno	I. Consentimento; II. Obrigação Legal;	Lei 12.965/2014 Marco Civil da Internet	NA	NA	NA	Não	Não	Sim	2. Baixo
43. Centro Universitário: **Acesso** a **rede** administrativa e, ou acadêmica enquanto **visitante**	Coleta, armazenamento e eliminação;	Segurança da Informação	IX. Legitimo interesse do controlador;	NA	Manutenção de perenidade das práticas e política de segurança da informação	NA	NA	Não	Não	Sim	1. Ausente

Apêndice D2 - Relatório de Impacto a Proteção de Dados (1_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
1. Centro Universitário: **Requisição de pessoal** - recrutamento interno	Nome, função (se substituição)	**P**	Coletado pelo Controlador em papel	Físico: Arquivo DRH	Execução de processo de recrutamento	Não	2. Baixo	1. Prever e tratar (consentimento) este uso em contrato CLT; 2. Revisar retenção; 3. Treinar time em questões pertinentes; 4. Considerar uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP);
2. Centro Universitário: Processo de **Seleção de Candidatos** à vagas de emprego em aberto	**Pretensão:** Cargo e salário pretendidos, disponibilidade laboral (segunda a sábado); **Dados cadastrais:** nome, estado civil, data de nascimento, idade, endereço, sexo, e-mail pessoal, transporte e tempo de deslocamento para o trabalho; **Dados acadêmicos:** formações, escolaridade, qualificações; **Dados empregatícios:** emprego atual e anteriores: empresa, endereço da empresa, cargo inicial e final, salário atual e anteriores, atividades e motivo da saída; **Dados familiares:** pai, mãe, conjugue, filhos; **Dados Financeiros:** residência, aluguel, automóvel-prestação, demais rendas e valores; **Documentação:** Carteira de Trabalho, RG, Título de Eleitor; CPF, Certificado de Reservista, CNH;	**P**	Informado pelo candidato em formulário papel, formulário online "trabalhe conosco" e, ou envio de *Curruculum Vitae*	Físico: Arquivo DRH	Execução de processo de seleção	Não	3. Médio	1. Adicionar termo de esclarecimento e consentimento junto aos formulários (fisico e digital) de dados coletados sendo específico e claro quanto aos dados pessoais sensíveis relacionados; 2. Revisar retenção; 3. Treinar time em questões pertinentes; 4. Considerar uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP);
	Dados raciais: Etnia, raça, cor; **Dados de saúde**: Relação de problemas de saúde, relação de tratamentos;	**S**					4. Alto	

Apêndice D2 - Relatório de Impacto a Proteção de Dados (2_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
3. Centro Universitário: Processo de **Admissão de candidato**	Gestor, nome completo, Instrução (escolaridade), contato, cargo, departamento, horário de trabalho, data admissão, regime de contratação (CLT, estágio, RPA, PJ e salário), vigência da contratação (determinada ou indeterminada), CPF, RG, endereço residencial, PIS, Reservista, Título de eleitor, Certidão de casamento, Carteira profissional, Documentos escolares (histórico), Currículo, Documentos bancários (Santander);	**P**	Informado e coletado junto ao candidato em formulário papel	Físico: Arquivo DRH	Execução de processo admissional;	Não	3. Médio	1. Adicionar clausulas de esclarecimento e consentimento (explicitando dados sensívies) junto ao contrato de trabalho assinado pelo funcionário; 2. Revisar retenção para contratados e <u>não</u> contratados; 3. Treinar time em questões pertinentes; 4. Considerar uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP);
	Dados Biométricos: Foto 3x4 e cópia da carteira de trabalho com foto; Dados Médicos: Exame médico admissional; Dados de menores: Carteira de vacinação filhos menores de 14 anos, Certidão nascimento filhos menores de 14 anos;	**S**					4. Alto	
4. Centro Universitário: **Cadastro Sistêmico** de Admissão - **TOTVS ERP**	Nome, nome social, estado natal, cidade, naturalidade, data nascimento, estado civil, sexo, nacionalidade, grau de instrução, tipo sanguíneo, e-mail profissional, CPF, RG, título de eleitor, carteira de trabalho, CNH, certificado reservista, PIS/PASEP; endereço residencial (rua, número, CEP, bairro, telefones (residencial e celular); departamento alocado, salário; jornada; dados bancários (banco, agência e conta corrente), dependentes (pai, mãe, conjugue e filhos), data admissão (FGTS), plano de saúde; dados de acesso ao local de trabalho - controle de jornada (REP);	**P**	Cadastro pelo DRH em software de parceiro externo, TOTVS	Digital: Base de Dados do Controlador	Execução de processo admissional;	Sim: Banco Privado do Sistema Bancário Brasileiro (Santander); Empresa Privada Assistência Médica (AMIL); Empresa Privada Corretora de Seguros (TRR); Empresa Privada de Seguro de Vida e Previdência (MetLife); Empresa Privada de Medicina do Trabalho (WorkLife); Empresa Privada de Software de Medicina Ocupacional (ProClinic); Ministério da Economia - Secretaria Especial de Previdência e Trabalho (eSocial);	3. Médio	1. Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD)
	RAIS (cor, raça); Dados Biométricos: digital, foto; Dados dos filhos, se, menores, Filiação Sindical;	**S**					4. Alto	

Apêndice D2 - Relatório de Impacto a Proteção de Dados (3_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
5. Centro Universitário: Cadastro de **Conta Salário - Santander**	Nome, CPF, residência, função/cargo e salário;	**P**	Informado pelo Controlador a Banco Privado do Sistema Bancário Brasileiro em papel	Físico: Arquivo DRH	Execução de processo admissional;	Sim: Banco Privado do Sistema Bancário Brasileiro (Santander);	3. Médio	Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD)
6. Centro Universitário: **Assinatura Ficha de** Registro de **Empregado**	Nome, Filiação (nome dos pais), Carteira de trabalho, Reservista, Título de eleitor, CNH, RG, data de nascimento, estado civil, sexo, escolaridade, nacionalidade, naturalidade, dependentes; Se estrangeiro: data da chegada, conjugue, identidade, tipo de visto, número registro geral, decreto, naturalizado, validade identidade, validade carteira de trabalho, número de filhos;	**P**	Informado pelo funcionário papel	Físico: Arquivo DRH	Execução de processo admissional;	Não	3. Médio	Risco tratado em contrato de trabalho da IES com a adequação deste nos termos na Lei Geral de Proteção de Dados
7. Centro Universitário: **Assinaturas Contratos:** Trabalho (experiência e posterior), Acordo individual de compensação de horas, e Cessão de uso de imagem e declarações;	Nome, CPF, residência, função/cargo, assinatura;	**P**	Informado pelo funcionário papel	Físico: Arquivo DRH	Execução de processo admissional;	Não	3. Médio	Risco tratado em contrato de trabalho da IES com a adequação deste nos termos na Lei Geral de Proteção de Dados

Apêndice D2 - Relatório de Impacto a Proteção de Dados (4_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
8. Centro Universitário: Processo de Nomeação e, ou alteração de Beneficiário do **seguro de vida** institucional (**TRR** e **MetLife**)	Nome, CPF, estipulante, subestipulante, número da apólice, nome do beneficiário, percentual de participação da apólice e grau de parentesco;	**P**	Informado pelo funcionário papel e e-mail	Físico: Arquivo DRH; Digital: Base de dados do parceiro / provedor de e-mail	Execução de processo admissional;	Sim: Empresa Privada de Seguro de Vida (**MetLife**) e Corretora de Seguros (**TRR**)	3. Médio	Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD)
9. Centro Universitário: Processo de **Adesão e movimentação** no cadastro de beneficiários pessoa jurídica **Assistência Médica** e Dental (**AMIL**)	Titular: Nome, CPF, número do cartão médico e odontológico, data de nascimento, número do cartão do sistema único de saúde (SUS), sexo, estado civil, endereço, telefones para contato; Dependentes: nome, CPF, número do cartão do SUS, número da declaração de nascido vivo (à partir de 2010), data de nascimento, grau de parentesco, nome da mãe, sexo, estado civil, IMC, assinatura;	**P**	Informado pelo funcionário em formulário papel	Físico: Arquivo DRH; Digital: Base de dados do parceiros de software	Execução de processo admissional;	Sim: Empresa Privada de Assistência Médica Dental (**AMIL**)	3. Médio	Risco tratado em contrato de trabalho da IES com a adequação deste nos termos na Lei Geral de Proteção de Dados
	Declaração de saúde (Titular e dependentes), se portador ou se já sofreu de doenças: do aparelho cardio circulatório, endócrinas, metabólicas, do sangue, imunológicas, do colágeno, autoimunes, do sistema nervoso, cerebrovasculares, do aparelho respiratório, do ouvido, do nariz, da garganta, ortopédicas, tumorizações malignas (câncer), do aparelho urinário, aparelho reprodutor (masculino ou feminino), qualquer outra doença não relacionada anteriormente ou que tenha gerado internação;	**S**					4. Alto	1. Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD); 2. Incluir termo de esclarecimento e consentimento para cessão de dados pessoais relacionados;

Apêndice D2 - Relatório de Impacto a Proteção de Dados (5_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
10.Centro Universitário: Processo de Operação e Manutenção da Medicina do Trabalho (SST: Saúde e Segurança do Trabalho) (**WorkLife**)	Nome , RG, cargo, setor, assinatura, idade;	**P**	Informado pelo funcionário papel	Físico: Arquivo DRH; Digital: Base de dados do parceiros de software	Execução de processo admissional;	Sim: Empresa Privada de Segurança e Medicina do Trabalho (**WorkLife**)	3. Médio	Risco tratado em contrato de trabalho da IES com a adequação deste nos termos na Lei Geral de Proteção de Dados
	Atestados de saúde ocupacionais: Exames médicos Admissionais, demissionais, periódicos e a critério médico que incorram em afastamento;	**S**	Obtido junto a parceiro Particular de Medicina Laboral contratada em papel				4. Alto	Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD)
11.Centro Universitário: Processo de **cadastro e gestão de Medicina Ocupacional** (SST: Saúde e Segurança do Trabalho) (**ProClinic**)	Nome, sexo, estado civil, data nascimento, idade, salário, função, CFP, datas (admissão, demissão e afastamento), contatos telefônicos, endereço residencial, matrícula e qualificação;	**P**	Informado pelo funcionário: contratação	Digital: Base de dados do parceiro de software de Medicina Ocupacional, ProClinic;	Execução de processo de gestão laboral	Sim: parceiro de software de Medicina Ocupacional, (**ProClinic)**;	3. Médio	Risco tratado em contrato de trabalho da IES com a adequação deste nos termos na Lei Geral de Proteção de Dados
	Exames médicos (passado e presente), GHE (Grupo Homogêneo de Exposição), exames (a vencer e vencidos), apto e inapto ao trabalho;	**S**	Obtido junto a parceiro Particular de Medicina Laboral contratada: papel				4. Alto	Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD)

Apêndice D2 - Relatório de Impacto a Proteção de Dados (6_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
12. Centro Universitário: **Envio de dados** funcionários para Governo (**TOTVS TAF**, **ProClinic** e **eSocial**)	Nome, CPF, NIS, Sexo, Estado Civil, Grau de Instrução, Data de nascimento, pais de nascimento, pais de naturalidade, UF, município, nome da mãe e do pai, regime trabalhista, regime previdenciário, cargo, função, CBO (classificação Brasileira de Ocupação), data, razão e verbas rescisórias;	**P**	Informado pelo funcionário na contratação	Digital: Base de dados dos parceiro de software de Medicina Ocupacional, ProClinic; Físico: Prontuário funcionário;	Execução de processo de gestão laboral e Obrigação Legal	Sim: Ministério da Economia, Secretaria Especial de Previdência e Trabalho (**eSocial**)	3. Médio	Risco tratado em contrato de trabalho da IES com a adequação deste nos termos na Lei Geral de Proteção de Dados
	Raça, exames admissionais, exames complementares (de acordo com os riscos aos quais o trabalhador está exposto), exames de retorno ao trabalho e exames periódicos;	**S**	Coletado junto ao parceiros de segurança e medicina do trabalho;				4. Alto	
13. Centro Universitário: Processo de **desligamento**	Nome, Endereço, CTPS, CPF, RG, nascimento, nome da mãe, causa do afastamento, cargo, remuneração, datas: admissão, aviso prévio, afastamento, verbas rescisórias, dependentes, saldo FGTS,	**P**	Informado pelo funcionário na contratação	Digital: Base de dados dos parceiro de software de Medicina Ocupacional, ProClinic; Físico: Prontuário funcionário;	Execução de processo demissional;	Sim: Banco Privado do Sistema Bancário Brasileiro (**Santander**); Empresa Privada Assistência Médica (**AMIL**); Empresa Privada Corretora de Seguros (**TRR**); Empresa Privada de Seguro de Vida e Previdência(**MetLife**); Empresa Privada de Medicina do Trabalho (**WorkLife**); Empresa Privada de Software de Medicina Ocupacional **ProClinic**); Ministério da Economia - Secretaria Especial de Previdência e Trabalho (**eSocial**);	3. Médio	Risco tratado em contrato de trabalho da IES com a adequação deste nos termos na Lei Geral de Proteção de Dados
	Filiação Sindical, Atestado de saúde ocupacional (demissional)	**S**	Coletado junto à parceiro de segurança e medicina do trabalho papel e digital				4. Alto	

Apêndice D2 - Relatório de Impacto a Proteção de Dados (7_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
14. Centro Universitário: Processo de **armazenamento externo**: **Iron Mountain**	Nome, Filiação (nome dos pais), Carteira de trabalho, Reservista, Título de eleitor, CNH, RG, data de nascimento, estado civil, sexo, escolaridade, nacionalidade, naturalidade, dependentes; Se estrangeiro: data da chegada, conjugue, identidade, tipo de visto, número registro geral, decreto, naturalizado, validade identidade, validade carteira de trabalho, número de filhos;	**P**	Informado pelo funcionário ato da contratação	Físico: Armazém de Empresa Privada de Guarda e Gestão de documentos	Execução de processo de Gestão Laboral	Sim: Empresa Privada de Guarda e Gestão de documentos, **Iron Mountain**	3. Médio	Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD)
	Atestados de saúde ocupacionais: Exames médicos Admissionais, demissionais, periódicos e a critério médico que incorram em afastamento;	**S**	Coletado junto à parceiro de segurança e medicina do trabalho				4. Alto	
15. Centro Universitário: Processo de **inscrição** para **vestibular**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais;	**P**	Informado pelo candidato: formulário digital	Digital: Base de dados de parceiro: CRM Educacional	Execução de processo de inscrição para vestibular	Sim: Empresa Privada de Gestão Educacional, **CRM Educacional**	3. Médio	1. Adicionar termo de esclarecimento e consentimento junto ao formulário de dados coletados; 2. Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD);
16. Centro Universitário: Processo de **transmissão de dados** do inscrito para o **Controlador**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais;	**P**	Informado pelo candidato: formulário digital ato da inscrição vestibular	Digital: Base de dados do Controlador;	Transporte e detenção local dos dados dos titulares inscritos em processo seletivo	Sim: Empresa Privada de Gestão Educacional, **CRM Educacional**	3. Médio	Risco tratado em termo de esclarecimento e consentimento do formulário de inscrição para vestibular;

Apêndice D2 - Relatório de Impacto a Proteção de Dados (8_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
17. Centro universitário: Processos de **contato e relacionamento** com o **inscrito** em **processo seletivo** graduação;	Nome, e-mail, celular;	**P**	Informado pelo candidato: formulário digital, ato da inscrição vestibular	Digital: Base de dados do Controlador e parceiro: CRM Educacional;	Comunicação com o titular de dados inscrito no processo seletivo graduação;	Sim: Empresa Privada de Gestão Educacional, **CRM Educacional**	3. Médio	1. Treinar time em questões pertinentes; 2 Contemplar no termo de inscrição em vestibular este contato;
18. Centro Universitário: Processo de **matrícula Graduação**;	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	**P**	Informado pelo candidato: formulário digital	Digital: Base de dados do Controlador;	Matricular candidato em curso de formação superior - Graduação, emitir crachá de acesso físico às instalações;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**	3. Médio	1. Adicionar clausulas de esclarecimento e consentimento (explicitando dados sensívies) junto ao contrato de prestação de serviços educacionais; 2. Revisar retenção relacionada; 3. Treinar time em questões pertinentes; 4. Considerar uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP); 5. Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD);
	Nome social, digital, foto;	**S**					4. Alto	
19. Centro Universitário: transporte dados para Secretaria da Graduação - **Arquivo vivo aluno;**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	**P**	Informado e coletado junto ao candidato/aluno: formulário digital e papel	Física: Pasta do aluno; Digital: Base de dados do Controlador e de parceiro de gestão eletrônica de documentos, TOTVS DocExpress;	Gerar repositório de registro da atividade acadêmica do aluno;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional Secretaria Digital**	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais; 2. Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD);
	Nome social, digital, foto;	**S**					4. Alto	

Apêndice D2 - Relatório de Impacto a Proteção de Dados (9_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
20. Centro Universitário: **controle de acesso físico** aos Campi	Nome	**P**	Informado pelo candidato: formulário digital ato da matrícula	Digital: Base de dados do Controlador;	Controlar o acesso aos Campi e a presença, do aluno, em sala de aula, por meio do software, legado, "ChamadaOnLine";	Sim: Empresa Privada de Gestão de Controle de Acesso, **Sualtech**	3. Médio	1. Prever e considerar este uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP); 2. Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD);
	Foto e, ou digital;	**S**					4. Alto	
21.Centro universitário: atribuição de **grade acadêmica** ao aluno;	Nome	**P**	Informado pelo aluno: formulário digital ato da matrícula	Digital: Base de dados do Controlador;	Associar ao aluno: turma, sala, disciplinas, professores, ano letivo;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**	3. Médio	Risco tratado ao contrato de prestação de serviços educacionais
22. Centro Universitário: **Comunicação** acadêmica **com aluno**;	Nome e telefone (whatsapp)	**P**	Informado pelo aluno: formulário digital ato da matrícula	Digital: Base de dados do Controlador;	Informar disposições acadêmicas ao aluno;	NA	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais; 2. Treinar times em questões pertinentes;
23. Centro Universitário: Processo de **avaliação acadêmica**;	Nome	**P**	Informado pelo aluno: formulário digital ato da matrícula	Física: pasta do aluno; Digital: Base de dados do Controlador e do parceiro de gestão de avaliações acadêmicas, ProvaFácil;	Gerar, aplicar, corrigir, divulgar, armazenar provas para alunos da graduação;	Sim: Empresa Privada de Gestão de avaliações acadêmicas, **ProvaFácil**	3. Médio	Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados;

Apêndice D2 - Relatório de Impacto a Proteção de Dados (10_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
24. Centro Universitário: Processo de **orientação** e **aconselhamento** de **carreira;**	Nome, e-mail, celular;	**P**	Informado pelo aluno: formulário digital ato da matrícula	Digital: Base de dados do Controlador	Planejar carreira com vistas ao ingresso ou recolocação no mercado de trabalho;		3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais; 2. Treinar times em questões pertinentes;
25. Centro Universitário: Processo de **gestão** e controle da **evasão;**	Nome, e-mail, celular;	**P**	Informado pelo aluno: formulário digital ato da matrícula	Digital: Base de dados do Controlador	Entender fatores motivadores, da evação, e buscar soluções;	NA	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais; 2. Treinar times em questões pertinentes;
26. Centro Universitário: Processo de **apoio psicopedagógico** ao **aluno;**	Nome, e-mail, celular;	**P**	Informado pelo aluno: formulário digital ato da matrícula	Digital: Base de dados do Controlador	Apoiar aluno no processo de autoconhecimento e desenvolvimento pessoal, social e profissional;	NA	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais; 2. Treinar times em questões pertinentes;
	Laudos e análises psicopedagógicas	**S**	Sessões de aconselhamento psicopedagógicas: papel e posterior formulário digital	Físico: pasta do aluno; Digital: repositório de rede da IES			4. Alto	1. Adicionar termo de esclarecimento e consentimento antes no início das sessões de análise psicopedagógicas; 2. Treinar time em questões pertinentes; 3. Considerar uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP);

Apêndice D2 - Relatório de Impacto a Proteção de Dados (11_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
27. Centro Universitário: Processo de **suporte acadêmico (Central do Aluno)**	Nome, telefone, responsável legal (financeiro e, ou acadêmico),	**P**	Informado pelo aluno formulário digital ato da matrícula	Física: Pasta do aluno; Digital: Base de dados do Controlador e de parceiro de gestão eletrônica de documentos, TOTVS DocExpress;	Atuar como apoiador e facilitador da vida acadêmica e financeira do aluno da IES: emissão de documentos, abono de ausências justificadas, revisão de avaliações,	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional Secretaria Digital**	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais; 2. Treinar times em questões pertinentes;
	Atestados médicos (de saúde), nome social, laudos psicológicos;	**S**	Coleto em papel				4. Alto	
28.Centro Universitário: **Rematrícula**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	**P**	Informado pelo candidato em formulário digital no ato da matrícula	Digital: Base de dados do Controlador;	**Re**matricular candidato em curso de formação superior - Graduação;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais; 2. Treinar os times envolvidos em questões pertinentes;
	Nome social, digital, foto;	**S**					4. Alto	
29. Centro Universitário: **Emissão de Diploma**	Nome, CPF, RG	**P**	Informado pelo candidato em formulário digital no ato da matrícula	Física: Pasta do aluno; Digital: Base de dados do Controlador e de parceiro de gestão eletrônica de documentos, TOTVS DocExpress;	Emitir, imprimir diploma de graduação do aluno	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional Secretaria Digital**	3. Médio	Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados;

Apêndice D2 - Relatório de Impacto a Proteção de Dados (12_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
30. Centro Universitário: **emissão** de **boletos**	Nome, endereço, CPF, Responsável Financeiro	**P**	Informado pela aluno ato da matrícula e coletado junto ao sistema	Base de dados do Controlador	Gerar boletos para pagamento dos serviços educacionais contratados;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**; Banco Privado do Sistema Bancário Brasileiro (**Santander**)	Médio	1. Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados; 2. Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD);
31. Centro Universitário: **declaração** de **adimplência**	Nome, CPF	**P**	Informado pela aluno ato da matrícula e coletado junto ao sistema	Digital: Base de dados do Controlador e de parceiro de gestão eletrônica de documentos, TOTVS DocExpress;	Emitir declaração de adimplência do aluno;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional;** Empresa Privada de comunicação por mensagens de texto**, ChatBot**	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados; 2.Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD);
32. Centri Universitário: **conbrança** (**inadimplência**)	Nome, CPF, E-mail, telefone, endereço	**P**	Informado pela aluno ato da matrícula e coletado junto ao sistema	Digital: Base de dados do Controlador;	Informar aluno sobre não pagamento de mensalidade e negociar formas de quitação destas;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional;** Empresa Privada de comunicação por mensagens de texto**, ChatBot;** Empresa Privada de pagamentos eletrônicos no varejo, **CIELO;** Serviço Central de Proteção ao Crédito **Boa Vista SCPC;** Empresa Privada de recuperação de crédito**, TECHCOB;**	4. Alto	1. Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados; 2.Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD);

Apêndice D2 - Relatório de Impacto a Proteção de Dados (13_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
33. Centro Univesitário: **Confissão de dívida**	Nome, endereço, CPF, e-mail	**P**	Informado pela aluno ato da matrícula e coletado junto ao sistema	Digital: Base de dados do Controlador;	Negociar dívida com aluno;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**; Banco Privado do Sistema Bancário Brasileiro (**Santander**)	4. Alto	1. Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados; 2.Aditar contratos de parceiros (Operadores de Dados) relacionados, contemplando proteção dos dados pessoais compartilhados nos termos da Lei Geral de Proteção de Dados (13.709/2018 - LGPD);
34. Centro Universitário: **reenbolso**	Nome, CPF, dados bancário para reenbolso;	**P**	Informado pela aluno ato da matrícula e coletado junto ao sistema	Digital: Base de dados do Controlador;	Restituir valor ao aluno por serviço não realizado;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**; Banco Privado do Sistema Bancário Brasileiro (**Santander**)	3. Médio	Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados;
35. Centro Universitário: **Financiamentos Próprios**	Aluno e Fiador: Nome, CPF, RG, endereço (rua, número, bairro, cep, cidade, estado - UF), profissão, nacionalidade, telefone, estado civil, data de nascimento;	**P**	Informado pela candidato e coletado junto ao sistema	Digital: Base de dados do Controlador	Possibilitar pagamento parcial dos valores das mensalidades da graduação ao final do curso;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**;	3. Médio	1. Adicionar clausulas de esclarecimento e consentimento (explicitando dados sensívies) junto ao contrato de financioamento próprio; 2. Revisar retenção relacionada; 3. Treinar time em questões pertinentes; 4. Considerar uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP);
	Aluno e Fiador: Renda (salário);	**S**	Informado pelo aluno;				4. Alto	

Apêndice D2 - Relatório de Impacto a Proteção de Dados (14_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
36. Centro Universitário: **assistência financeira**	Aluno e responsável financeiro: nome, RG, CPF, endereço;	**P**	Informado pela aluno ato da matrícula e coletado junto ao sistema	Digital: Base de dados do Controlador; Fisico: pasta do aluno	Garantir a continuidade de estudos, em caso da perda de renda por desemprego, falecimento ou invalidez por acidente ou perda de renda por afastamento médico do responsável financeiro do contrato de prestação de serviços educacionais	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**;	3. Médio	1. Adicionar clausulas de esclarecimento e consentimento (explicitando dados sensívies) junto ao contrato ou termo de adesão à assistência financeira; 2. Revisar retenção relacionada; 3. Treinar time em questões pertinentes; 4. Considerar uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP);
	Quando cabido: Termo de rescisão contrato de trabalho, carteira de trabalho, certidão de óbito responsável financeiro, Laudo médico atestando a invalidez permanente e total, informando as sequelas deixadas pelo acidente, discriminando cada órgão ou membros lesados, do responsável financeiro, Relatório Médico informando o motivo e o período de afastamento das atividades laborais do aluno;	**S**	Informado pelo aluno e, ou responsável financeiro em papel				4. Alto	
37. Centro Universitário: **PROUNI**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	**P**	Informado e coletado junto ao candidato/aluno ato da matrícula;	Digital: Base de dados do Controlador;	Oferecer bolsas de estudo, integrais e parciais (50%) governamentais, em instituições particulares de educação superior;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**;	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados; 2. Treinar times relacionados; Prever tratamento em RIPDPP;
	Nome social, digital, foto, salário (holerite);	**S**					4. Alto	

Apêndice D2 - Relatório de Impacto a Proteção de Dados (15_de_15)

PROCESSO INSTITUCIONAL	Descrição DADOS: (**P**essoais; **S**ensíveis)		COLETA	GUARDA	RAZÃO	SHARE	IMP	TRATAMENTO: RESPOSTA AO RISCO
38. Centro Universitário: **FIES**	CPF, nome, RG, data de nascimento, e-mail, celular, endereço (CEP, rua/avenida, número, bairro, cidade, unidade fiscal - UF), necessidades especiais, sexo, nacionalidade, naturalidade, pai/mãe (nome, CPF, data de nascimento, RG, data de nascimento, naturalidade e estado natal), fiador, CPF fiador, titulo de eleitor, reservista, responsável financeiro, responsável acadêmico	**P**	Informado e coletado junto ao candidato/aluno ato da matrícula;	Digital: Base de dados do Controlador;	Fundo de Financiamento Estudantil (Fies), é uma ação do Ministério da Educação que financia cursos superiores não gratuitos;	Sim: Empresa Privada de Gestão Educacional, **TOTVS RM Educacional**;	3. Médio	1. Risco tratado ao contrato de prestação de serviços educacionais e base legal realacionada, vide inventário de dados; 2. Treinar times relacionados; Prever tratamento em RIPDPP;
	Nome social, digital, foto, salário (holerite);	**S**					4. Alto	
39. Centro universitário: **Controle de acesso VISITANTE, PRESTADOR DE SERVIÇO E USUÁRIOS SEM VÍNCULO**	RG, CPF, CNH, RNE (Registro Nacional de Estrangeiros), nome, e-mail, telefone, nascimento, idade;	**P**	Informado pelo visitante, prestador de servicço e usuário em vínculo;	Digital: Base de dados do Controlador;	Dispor acesso fisico às dependências dos Campi da IES	Sim: Empresas Privada de Controle de Acesso, **Sual Tech;**	3. Médio	1. Revisar retenção relacionada; 2. Treinar time em questões pertinentes; 3. Considerar uso em Política Institucional de Proteção de Dados Pessoais e da Privacidade (PIPDPP);
	Foto e, ou digital	**S**					4. Alto	

Apêndice D3 - Relatório de Impacto a Proteção de Dados (1_de_2)

Décalogo de Princípios	Riscos	Impacto	Tratativa(s)
(1) Finalidade: legitimidade de tratamento;	Finalidade específica	Médio	Garantir que os dados coletados serão inalterados e exclusivamente utilizados para o fim declarado: mapear para cada dado coletado a razão desta coleta, documentar e revisar com as partes dietamente envolvidas;
	Uso de imagem dos titulares de dados	Alto	Tratar este uso em instumento jurídico de contratação de prestação de serviços educacionais e, ou empregatício;
(2) Adequação: tratamento compativel com a finalidade;	Tratamento de dados pessoais	Médio	Adequar tratamento a Lei por meio de um adequado processo de conformidade
	Tratamento de dados pessoais sensíveis	Alto	Obter consentimento e, ou Base legal para tal tratamento, na ausência não tratar
(3) Necessidade: apenas dados necessários a Finalidade;	Limitação de dados pessoais	Médio	Coletar apenas os dados pessoais estritamente necessários a execução do processo institucional relacionado
(4) Livre acesso: garantia de acesso aos titulares à seus dados pessoais;	Direito a informação	Médio	Informar dados coletados; finalidade; Base legal; tratamentos realizados; **direitos do titular de dados**; períodos de retenção; compartilhamento (Operadores de Dados) caso haja; canais e meios de comunicação com a IES sobre;
(5) Qualidade de dados;	Classificação, **incorreta**, de dados pessoais	Alto	Treinar times que tratam e, ou tem acesso a dados pessoais
(6) Transparência: informações devem ser claras, precisas e verdadeiras;	Consentimento de uso	Alto	Criar mecanismos de esclarecimento e coleta de consentimento: claros, específicos e registrados. Termos (textos) fisicos e digitais de consentimento
	Bases jurídicas de uso	Alto	Relacionar todas as bases jurídicas adotadas e aplicáveis ao uso de dados pessoais da IES as relacionando com os processos em que ocorrem os devidos tratamentos

Apêndice D3 - Relatório de Impacto a Proteção de Dados (2_de_2)

Décalogo de Princípios	Riscos	Impacto	Tratativa(s)
(7) Segurança: garantir segurança dos dados coletados; (8) Prevenção: medidas prévias para evitar a ocorrência de danos em virtude do tratamento de dados pessoais	Incidentes de Dados Pessoais: perda de dados pessoais e violações de confidencialidade e integridade	Alto	Ajustar: a) segurança de rede de computadores; b) segurança de sistemas informáticos; c) políticas de segurança da informação institucional; d) Privacy by Design;
	Compartilhamento - Operadores de Dados	Alto	Aditar contratos com Operadores de Dados nos termos da Lei 13.709/2018 - LGPD
	Retenção e Eliminação de dados pessoais	Médio	Rever todos os períodos de retenção e criar políticas de eliminação de dados pessoais
(9) Não discriminação:	Divulgação de dados pessoais	Alto	Garantir a não divulgação e quando tiver que ocorrer a apoiar em consentimento e, ou base legal. Exemplo: Divulgação de resultados de vestibular
(10) Responsabilização e Prestação de Contas:	Encarregado de dados (*Data Protection Officer* - GDPR): responsabilidades e prestação de contas	Alto	Nomear um Encarregado de Dados e tornar públicas formas e meios de contato
BOA FÉ:	Fiscalização, Compliance e Perenidade	Alto	Desenvolver conformidade/Governança de dados; Treinar departamentos envolvidos; Implantar linhas de resposabilidade;

Apêndice D4 - Política Institucional de Privacidade de Proteção de Dados

Política Institucional de Privacidade de Proteção de Dados

IDENTIFICAÇÃO:

Instituição de Ensino Superior:	Centro Universitário Escola - SIGLA
Mantenedora:	Fundação Escola – SIGLA
Endereço – Campus Matriz:	Avenida, número, Bairro
Cidade / Estado:	São Paulo, SP
CEP:	número
CNPJ:	número
Cadastro – Ministério da Educação e Cultura (MEC):	Link http do mec

INTRODUÇÃO:

A presente Política tem, como finalidade, esclarecer o compromisso que o Centro Universitário Escola – SIGLA, doravante nomeado apenas ESCOLA, de buscar a preservação máxima da privacidade e proteção de todos aqueles que, em algum momento, tiverem, seus dados pessoais tratados pela instituição, acatando e cumprindo a Lei Geral de Proteção de Dados do Brasil (Lei 13.709/2018 – LGPD) que dispõe sobre o tratamento de dados pessoais, sobre todos os meios, inclusos os digitais, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade das pessoas.

ARCABOUÇO LEGAL:

A presente Política sustenta-se sobre:

- Lei Geral de Proteção de Dados, 13.709/18 (PLANALTO, 2018a), promulgada em 14 de agosto de 2018.
- Lei Geral de Proteção de Dados, 13.853/19 (PLANALTO, 2018a), promulgada em 08 de julho de 2019, alterando a Lei original 13.709/18.
- Projeto de lei, PL, n° 1179 de 2020, aprovado em 03 abril de 2020, alterando a Lei original 13.709/18.
- Lei 12.965, de 28 de novembro de 2011, conhecida como Marco Civil da Internet.

GLOSSÁRIO:

Controlador:

> Pessoal Natural ou Jurídica, pública ou privada, a quem competem as decisões referentes ao tratamento de dados pessoais.

Dado Pessoal:

Dado relacionado a qualquer pessoa identificada ou identificável.

Operador:

Pessoal Natural ou Jurídica, pública ou privada, que realiza tratamento de dados pessoais, em nome do Controlador.

Agentes de tratamento de dados:

Refere-se, primordialmente ao Controlador e Operador, e designa a pessoas jurídicas que tratam os dados pessoais.

Titular:

Pessoa natural a quem se referem os dados, objeto do tratamento. O "dono" do dado.

Tratamento:

Toda e qualquer operação que se realize com o dado pessoal.

Encarregado de Dados - DPO:

Pessoa indicada pelo Controlador para atuar como canal de comunicação entre o próprio, os titulares de dados e a Autoridade Nacional de Proteção de Dados. Adiante este profissional será analisado em maiores detalhes.

Pessoa Natural:

Pessoa natural é o ser humano capaz de direitos e obrigações na esfera civil. Todo ser humano, assim, recebe a denominação de pessoa, natural ou física, para ser denominada como sujeito do direito, ente único, do qual e para o qual decorrem normas.

PRINCÍPIOS:

O Centro Universitário, alinhando missão e valores institucionais à proteção dos diretos fundamentais de seus alunos, professores, colaboradores e comunidade, considera sua privacidade é um bem de valor inestimável.

Para preservar este bem, a escola assume as medidas necessárias recomendadas por lei e pelas boas práticas de privacidade de dados e segurança da informação, apoiando-se nos seguintes princípios:

1. Princípio da Finalidade: Os dados coletados devem ter um objetivo específico e o tratamento destes deve ater-se a tal fim;
2. Princípio da Adequação: A relação entre a finalidade e quais dados serão coletados deve ser consoante e preservada;
3. Princípio da Necessidade: A coleta dos dados deve apresentar uma justificativa plausível alinhada a finalidade de uso;

4. Princípio do Livre Acesso: É assegurado ao titular de dados, consulta gratuita e facilitada aos seus dados pessoais, as formas de tratamento que estes recebem ou receberão e períodos de retenção seja pelo Controlador e, ou Operador. Todos os titulares de dados podem obter informações relacionadas procedendo solicitações específicas ao **Encarregado de Dados** da instituição, devidamente identificado e descrito nesta política;
5. Princípio da Qualidade de Dados: É garantido ao titular que seus dados serão tratados com clareza, exatidão e atualização de acordo com o item 1 e 3 destes princípios;
6. Princípio da Transparência: Todos os dados e tratamentos ocorridos devem ser informados de forma clara, precisa e transparente;
7. Princípio da Segurança: Garante-se a adoção de medidas técnicas, administrativas e processuais dedicadas à proteção dos dados pessoais e ao afastamento de potenciais incidentes como acessos não autorizados e, ou eventos ilícitos;
8. Princípio da Prevenção: Relacionado ao item anterior, afirma adoção de medidas para prevenir ocorrência de danos em virtude do tratamento de dados pessoais;
9. Princípio da Não Discriminação: Impossibilidade de realização de tratamento dos dados pessoais, para fins discriminatórios, ilícitos ou abusivos;
10. Princípio da Responsabilização e Prestação de Contas: O agente de tratamento de dados deve ser capaz, a qualquer momento, de demonstrar a adoção de medidas que comprovem a observância e cumprimento das normas de proteção de dados pessoais e sua eficácia.

Diante disto, a Instituição busca cumprir com todos os princípios, zelando, sempre pela privacidade de seus clientes e comunidade.

São consideradas exceções a aplicabilidade, ou seja, não se aplicam aos dados que:

a) Sejam considerados públicos por determinação legal, ou tenham de ser processados para cumprimento de obrigação legal e, ou regulatória;
b) Sejam públicos para o tratamento e uso compartilhado para execução de políticas públicas de caráter coercitivo;
c) Sejam objeto de decisão judicial transitada em julgado, pela divulgação ou exibição dos mesmos;
d) Se destinem a procedimentos relacionados à segurança, passiva ou ativa (incolumidade[12]);
e) Já forem considerados dados públicos por outros meios;
f) Destinarem-se a tutela de saúde, à proteção da vida ou incolumidade física das pessoas (titulares de dados);
g) Sejam pertinentes a relação contratual ou vínculo empregatício com a escola e preservem os princípios anteriormente trazidos;

[12] Incolumidade: A incolumidade pública significa evitar o perigo ou risco coletivo, tem relação com a garantia de bem-estar e segurança de pessoas indeterminadas ou de bens diante de situações que possam causar ameaça de danos. TJDFT - Tribunal de Justiça do Distrito Federal e dos Territórios: https://www.tjdft.jus.br/institucional/imprensa/campanhas-e-produtos/direito-facil/edicao-semanal/incolumidade-publica;

h) Dedicados para fins, exclusivamente, acadêmicos, considerando a cautela na publicação do trabalho científico e, sempre que possível, a aplicação de anonimização[13], desta forma, dissociando o dado de seu titular.

CONFORMIDADE:

A escola, declara aderência aos princípios supracitados estabelecendo como prioridade sua conformidade com o arcabouço legal, neste documento trazido, sincronicamente em que manifesta seu compromisso de incessante esforço na manutenção do *compliance*[14] e adequação ante as referidas leis e toda sua estrutura informacional.

Para tal a escola mantem, atualizado, um Inventário de Dados em consonância com o nível de privacidade e hipótese de tratamento, prevista em lei (13.709/18), identificando com clareza os métodos adotados, o tratamento realizado e a retenção aplicada.

Em que se pesem os procedimentos de Segurança da Informação e resposta a incidentes, a instituição, é consciente de que a privacidade de dados representa um desafio e que a despeito dos cuidados dedicados, da contínua atualização dos times de segurança e privacidade, o risco informacional é permanente e paulatino.

Diante disto para eventuais incidentes, a escola, possui um protocolo de mitigação de riscos, seguido do correspondente Relatório de Impacto aos Dados Pessoais que identifica as principais ameaças e seus danos (impactos), estabelecendo sobre estes um plano de resposta, aqui apresentado.

PLANO DE RESPOSTA À INCIDENTES DE DADOS:

Assim que identificado indesejável evento (acesso desautorizado, destruição, perda, alteração ou qualquer tratamento de cunho ilícito) a escola, por meio de seu Encarregado de Dados:

1. Comunicará, de imediato, o titular de dados;
2. Comunicará a Autoridade Nacional de Proteção de Dados (**ANPD**), informando:
    a. Dada do incidente;
    b. Dados relacionados;
        i. Categoria e Sensibilidade destes dados;
    c. Natureza e escopo do tratamento realizado com os dados atingidos;
    d. Titulares de dados relacionados;
    e. Riscos relacionados ao incidente;
    f. Gravidade do ocorrido: impacto do incidente ao titular;
    g. Operadores e demais agentes de tratamento envolvidos, caso haja;

[13] Anonimização: Ato ou efeito de Anonimizar, tornar anônimo. Aqui refere-se a aplicação de métodos técnicos razoáveis e disponíveis no momento do tratamento dos dados, por meio dos quais, perde-se a possibilidade de associação direta ou indireta a um indivíduo natural, titular dos dados, em trato;

[14] Conjunto de disciplinas a fim de cumprir e se fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da instituição ou empresa.

h. Indicação das medidas técnicas e administrativas de segurança dedicadas a proteção dos dados;
i. Razões da demora, caso a comunicação não tenha sido imediata;
j. Medidas que foram, são e serão adotadas para impedir futuras ocorrências de mesmo gênero;
k. Medidas que foram, são e serão adotadas para reverter e mitigar os efeitos do prejuízo;
l. Reincidência, ou não, do incidente.

3. Assumirá todas as medidas cabíveis e disponíveis para sanar o impacto do incidente e sua recidiva futura, em qualquer prazo, de acordo com o disposto junto as alíneas "j" e "k" do item 2 deste, acima trazido.

ENCARREGADO DE DADOS – *DATA PROTECTION OFFICER (**DPO):***

A principal função do Encarregado de Dados ou apenas DPO (*Data Protection Officer*) como é conhecido no Regulamento Geral de Proteção de Dados da União Europeia (GPDR, em inglês) é garantir que a instituição processe (trate) os dados pessoais da organização: equipes, clientes, fornecedores ou quaisquer outros indivíduos (também chamados de titulares de dados), em conformidade com as regras de proteção de dados aplicáveis.

Nas instituições e órgãos do Brasil, a Lei Geral de Proteção de Dados (13.709/2018) obriga a nomeação de um DPO a partir de 01 de janeiro de 2021, conforme Projeto de lei, PL, n° 1179 de 2020, que altera esta lei. Portanto cada controlador terá que divulgar, em seu sítio eletrônico[15], a identidade e informações de contato de seu Encarregado de Dados de forma clara e objetiva.

As atividades do encarregado consistem em:

I) Aceitar reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;
II) Receber comunicações da Autoridade Nacional de Proteção de Dados e adotar providências;
III) Orientar os funcionários e os contratados da entidade a respeito das práticas as serem adotadas em relação a proteção de dados pessoais;
IV) Executar demais atribuições determinadas pelo controlador ou estabelecidas em normas complementares, entre outras, a saber:
   a. Garantir que as regras de proteção de dados sejam conhecidas, entendidas e respeitadas dentro da escola;
   b. Garantir que o controlador e titulares dos dados sejam informados sobre seus direitos, obrigações e responsabilidades pertinentes;
   c. Assegurar a conformidade e perpetuidade da proteção de dados da instituição seja atingida e mantida;

[15] Sítio Eletrônico: Refere-se ao website do controlador.

d. Manter a instituição alinhada à ANPD ao que tange novos dispostos sobre a lei e práticas de governança e segurança de dados-informação.

Pelo exposto, o Centro Universitário (escola), nesta Política, identifica e declara, para os efeitos da Lei Geral de Proteção de Dados, que reconhece e atribui as correspondentes responsabilidades de Encarregado de Dados, conforme especificações a saber:

Encarregado de Dados – IES:	Nome Sobrenome
Endereço:	Avenida ou rua, número, Bairro, CEP-SP
Telefone:	(DDD) número
e-Mail:	dpo@escola.br
Página WEB – Sítio eletrônico:	lgpd.escola.br

DIRETOS DOS TITULARES DE DADOS, segundo a LGPD:

O titular de dados, pessoa natural a quem os dados pessoais se referem, possui direitos específicos trazidos pela legislação, os quais a escola acata garantindo ao titular, mediante requisições formais e por escrito:

I) Confirmação da existência de tratamento de dados;
II) Acesso aos dados;
III) Correção de inconsistências e atualizações;
IV) Eliminação de dados desnecessários, excessivos;
V) Portabilidade observado segredo comercial disposto;
VI) Eliminação dos dados pessoais tratados, excesso nas hipóteses de:
   a. Cumprimento de obrigação legal ou regulatória pela escola;
   b. Estudo por órgão de pesquisa, garantida anonimização, sempre que possível;
   c. Uso exclusivo do controlador, vetado a terceiros e anonimizado;
VII) Informação das entidades (públicas e privadas: Operadores) onde houve e, ou há compartilhamento de dados;
VIII) Revogação do consentimento, visto e excetuado, quando condição à execução de contrato pelo controlador, obrigação legal e regulatória, anonimização do dado, utilização por e para órgão de pesquisa;
IX) Temporalidade do tratamento dos dados e a retenção destes;
X) Informação sobre as consequências do não fornecimento do consentimento, caso opte em não o prover.

Todos os pedidos dos titulares serão recebidos por meio eletrônico, seguro e idôneo junto a conta de e-mail do Encarregado de Dados nomeado pelo Controlador:

dpo@escola.br

A resposta à solicitação do Titular de Dados será providenciada em formato simplificado por meio de declaração clara e completa em um prazo de até 15 (quinze) dias, contados da data do requerimento do titular.

A escola poderá ainda, antes de término do prazo inicial, contatar o titular informando as medidas assumidas e sobre uma justificativa concreta e pertinente noticiar um novo prazo para apresentar sua resposta, não superior a 30 (trinta) dias, contatos da data do requerimento pelo titular.

TERMOS DE USO E SERVIÇO:

Todos os serviços da Instituição, são subordinados aos princípios gerais desta Política, sem prejuízo às disposições específicas constantes em contratos firmados. Há ausência de normas específicas para quaisquer serviços observados junto ao *Portfólio* da escola ou na presença de conflitos entre os demais dispositivos normativos (regras ou contratos anteriores) a vigente Política prevalecerá.

- **Coleta de dados:**
  A escola coleta dados que considera indispensáveis à operação de suas atividades educacionais e correlatas. Sendo algumas destas informações (grupos de dados) absolutamente necessárias à realização de transações comerciais com seus clientes (alunos, professores, colaboradores e prestadores de serviço terceirizados) por razões de cumprimento às legislações pertinentes, como: civil, educacional, trabalhista, tributária entre outras.

  Outros dados, como e-mail e demais contatos, podem ser requeridos por motivos de interesse legítimo, sob a finalidade de Marketing e ou registro de potenciais clientes. Em quaisquer das possibilidades, o titular será previamente avisado sobre tal coleta de dados com clareza e assertividade e poderá fornecer ou não seu consentimento para tal tratamento. Desta forma, em não desejando ceder tais informações, será imediatamente informado sobre os impactos que tal negação possa incorrer, de forma clara e inequívoca.

- **Responsabilidade:**
  A escola se compromete e se responsabiliza por oferecer os melhores serviços disponíveis, cuidando para que a segurança da informação, a privacidade dos titulares e a liberdade destes de disporem de seus dados, com proteção, seja parte contínua a indissociável de suas operações.

  Contudo, a escola não se responsabiliza pelo mau uso deste conteúdo por outros sites, aplicativos e, ou redes sociais, bem como por qualquer outro tipo de prática maliciosa, falhas de segurança de dispositivos particulares ou atividades ilegais cometidas por terceiros ainda que tais delitos ocorram quando o dispositivo do titular estiver conectado junto a rede sem fio, *Wireless Fidelity* (Wi-Fi), da instituição.

- **Tecnologias de navegação:**
  Durante o uso dos aplicativos ou páginas, a escola poderá utilizar tecnologias de identificação de usuários e mapeamento de navegação, "Cookies", de forma a facilitar e otimizar a navegação do mesmo pelo conteúdo das páginas visitadas, fornecendo uma melhor experiência ao usuário. A escola sempre informará sobre tais operações, prestando ao usuário a opção de não aceitar que aquela faça uso de tais tecnologias:

  Cookies[16]: Cookies são pequenos arquivos que são gravados no computador do titular de dados quando acessa sites na Internet e que são reenviados a estes mesmos sites quando novamente visitados.
  São usados para manter informações sobre o titular, como carrinho de compras, lista de produtos e preferências de navegação, desta forma, melhorando a experiência do usuário (titular) com a(s) página(s) visitadas, tornando-as mais responsivas e dinâmicas.

  Cookies podem ser:

  1. Temporário (de sessão), quando é apagado no momento em que o navegador Web ou programa leitor de e-mail é fechado;
  2. Permanente (persistente), quando fica gravado no computador até expirar ou ser apagado;
  3. Primário (first-party), quando definido pelo domínio do site visitado;
  4. Terceiros (third-party), quando pertencente a outro domínio (geralmente relacionado a anúncios ou imagens incorporadas à página que está sendo visitada);
  5. Seguros: transmitidos apenas via HTTPS, normalmente observados em páginas de "check-out" dos sites de compras online;
  6. HTTPOnly: quando atribuídos definido, o navegador impede que qualquer script de cliente na página (como JavaScript) acesse o conteúdo do cookie.

  A escola utiliza os seguintes cookies:

Tipos	Razão	Cookies
Persistente e terceiro	Aprimorar a usabilidade, controles e experiência de navegação	csrftoken; mid
Sessão e primário		Phpsessid
Temporário e terceiros		rur; urlgen
Persistente e primário	Estatísticas para melhoria de serviços	_ga; _gat; _gid
Sessão e terceiro		collect

[16] Cookies: https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf e https://cookiepedia.co.uk/

Tipos	Razão	Cookies
Persistente e terceiro	Marketing próprio	gps; ide; ig_did; test_cookie; visitor_info1_live; ysc; yt-remote-cast-installed; yt-remote-connected-devices; yt-remote-device-id; yt-remote-fast-check-period; yt-remote-session-app; yt-remote-session-name

Os cookies utilizados pela escola são seguros, testados e pertinentes ao ideal uso das ferramentas e opções de navegação disponíveis, favorecendo primordialmente a navegabilidade e experiência do usuário, diante disto, caso sejam desativados o comportamento de algumas funcionalidades e acessos serão comprometidos, podendo não apresentar a resposta ideal e esperada, dado isto como claro, a instituição não se responsabiliza pela experiência negativa decorrente desta ação.

Em tempo, todos os dados coletados pelos cookies presentes em seu site não são, em momento algum, compartilhados por empresas terceiras de qualquer natureza sobre cunho comercial ou para exploração de marketing que não seja o próprio com vistas a oferta de serviços presentes e públicos em seu portfólio de produtos.

Desativar Cookies:

Comumente as opções para desativar ou limpar os cookies estão presentes nos navegadores de internet em “Opções” ou em “Preferências”, desta forma, para esclarecer melhor como proceder consulte as opções de ajuda e configuração do navegador utilizado:

Apple Safari Web:
https://support.apple.com/pt-br/guide/safari/sfri11471/mac
Chrome:
https://support.google.com/chrome/answer/95647?co=GENIE.Platform%3DDesktop&hl=pt-BR
Firefox:
https://support.mozilla.org/pt-BR/kb/desative-cookies-terceiros-impedir-rastreamento
Internet Explorer:
https://support.microsoft.com/pt-br/help/17442/windows-internet-explorer-delete-manage-cookies

- **Tratamento dos dados:**
  Todas as informações coletadas pela escola são, primordialmente, destinadas ao:

a) Exercício dos contratos de prestação de serviços educacionais;
b) Apoio a vida acadêmica e financeira do aluno dentro e fora da instituição;
c) Exercício dos contratos de trabalhos por professores e colaboradores;
d) Exercício dos contratos de prestação de serviço terceirizados;
e) Exercício de Marketing próprio dedico a promoção de cursos de seu portfólio;
f) Proteção a vida ou incolumidade;

g) Cumprimento obrigação legal ou regulatória.

Todo o qualquer dado coletado que não respeite as hipóteses acima será previamente informado, acrescido de seu respectivo uso e retenção em formato claro, simples e idôneo.

- **Armazenamento e Retenção de Dados:**
A escola adota processos de segurança da Informação pautados sobre a ISO 27001[17] (Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos) para seu parque tecnológico, de forma que os dados pessoais de seus titulares não possam ser identificados por pessoas ou equipamentos não autorizados, quando da coleta, tratamento, armazenamento e cópia de segurança (backup) sendo estes último mantido fisicamente em cofre e em formato ilegível a sistemas externos.

Quanto ao período de armazenamento a escola debruça-se sobre as retenções referentes a:

1. Cumprimento de contratos de prestação de serviços educacionais;
2. Cumprimento de contratos trabalhistas;
3. Cumprimento de obrigação legal ou regulatória, **ainda que revogado o consentimento do titular**;
4. Período de tratamento;
5. Tratamento pelo judiciário ou por órgão de pesquisa garantida, sempre que possível, a anonimização.

A temporalidade legal, normativa e prescricional acatada pela escola pode ser observada junto aos links abaixo:

- Ministério da Educação e Cultura – **MEC**:

http://www.siga.arquivonacional.gov.br/images/codigos_tabelas/portaria_n0922011_tabela_de_temporalidade_e_destinao.pdf

- Ministério da Fazenda – **MF**:

http://www.siga.arquivonacional.gov.br/images/codigos_tabelas/00_CodigoClassificacao_MF.pdf

- Secretaria da Receita Federal do Brasil – **RFB**:

http://www.siga.arquivonacional.gov.br/images/codigos_tabelas/RFB%20APRES%20C%C3%93DIGO%20AF%20REF%20LEGISL.pdf

- Ministério da Justiça e Segurança Pública – Gestão de Documentos e Arquivos**:** Classificação, Temporalidade e Destinação de documentos da União.

[17] https://www.abntcatalogo.com.br/norma.aspx?ID=306580
https://www.iso.org/isoiec-27001-information-security.html

http://www.siga.arquivonacional.gov.br/index.php/legislacao-e-normas/legislacao-portarias/31-gestao-de-documentos/resultado-das-atividades-de-gestao-documental/159-codigos-de-classificacao-e-tabelas-de-temporalidade-destinacao-de-documentos

- **Compartilhamento:**
  Os dados pessoais coletados pela escola respeitam as finalidades de uso previstas em lei e aqui descritas, isto dito, em momento algum são compartilhados com qualquer outra pessoa natural, física ou jurídica (de direito público ou privado) sob finalidade comercial e ou de marketing que não seja a própria.

  Caso dados precisem ser compartilhados em cumprimento de solicitação da autoridade pública, a mesma somente ocorrerá mediante ordem judicial, conforme definido em Lei.

  A tabela abaixo estratifica os dados coletados pela escola, clarificando a razão desta coleta, a hipótese de tratamento, prevista em Lei[18], e a retenção aplicada:

Index	Dado - Tipo	Razão	Hipótese	Retenção
1	Cadastral: nome, filiação, RG, CPF, endereço, etc.;	Execução de processo seleção vaga de emprego	Consentimento	06 meses
2	Cadastral: nome, filiação, RG, CPF, endereço, etc.;	Contratação colaborador para vaga de emprego	Consentimento e Obrigação Legal	05 anos após desligamento do colaborador
3	Sensível: dados biométricos, etnia e estado e histórico de saúde;			
4	Cadastral: nome, CPF, endereço, etc.;	Execução de processo seletivo Graduação	Consentimento	06 meses ou enquanto durar o tratamento dos dados coletados
5	Cadastral: nome, CPF, endereço, etc.;	Execução de serviços educacionais e apoio acadêmico, financeiro, profissional[19] e psicológico ao aluno.	Consentimento e Obrigação Legal	30 anos
6	Sensível: dados biométricos, etnia, nome social, etc.;			
7	Navegacional: IP, destino e conteúdo acessado, etc. ;	Segurança da Informação	Consentimento e Obrigação Legal	01 ano

[18] Lei 13.709 de 2018 – LGPD. Artigo 7º.
[19] Aconselhamento e Orientação de Carreira: Auxílio junto ao processo de recolocação profissional no mercado de trabalho.

Index	Dado - Tipo	Razão	Hipótese	Retenção
8	Navegacional: Dados de redes sociais, IP, destino e conteúdo acessado, etc.;	Marketing próprio	Consentimento	06 meses ou enquanto durar o tratamento dos dados coletados
9	Navegacional: Cookies.	Melhoria da experiência de navegação do titular e Marketing próprio	Consentimento	Enquanto durar o tratamento dos dados coletados.
10	Cadastral: nome, CPF, endereço, etc.; Sensível: dados biométricos.	Segurança patrimonial e pessoal.	Proteção à vida ou da incolumidade	01 ano

ATUALIZAÇÃO E FORO:

A escola reserva-se no direito de alterar e, ou atualizar esta política sempre que necessário objetivando a maior segurança ao titular de dados e acato a instância legal regulatória. Esta política está sujeita à Lei da República Federativa do Brasil e o Foro da Comarca de São Paulo é competente para dirimir qualquer controvérsia com relação à mesma.

Apêndice D5 - Ajustes contratuais e consentimentos: coleta e gestão (1_de_4)

DA PROTEÇÃO DOS DADOS: Termo de uso de dados pessoais para processo seletivo de **vaga empregatícia** (de trabalho)	Departamento de Recursos Humanos e Jurídico:
AUTORIZO, desde já, de forma expressa, consciente e inequívoca a coleta e tratamento dos dados pessoais ora informados, a título gratuito, à ESCOLA (IES Lócus), inscrita no CNPJ/MF sob o nº. (Informar número), com sede à (informar logradouro) sob a finalidade de participar de processo de seleção a vaga empregatícia (de trabalho) e, em tempo e igualmente, consinto a ESCOLA (IES Lócus) reter estes dados pelo período de (definir período junto ao DRH) para fins exclusivos de participação em futuros processos de seleção, casa haja, sendo estes informados por meio eletrônico em meu endereço de e-mail. Esta autorização poderá ser revogada a qualquer momento, mediante simples requerimento à ESCOLA em dpo@escola.br. **A NÃO ACEITAÇÃO** deste termo implicará na impossibilidade de participação do processo seletivo à vaga de emprego, neste momento ofertado. Todo tratamento de dados pessoais realizado pela ESCOLA (IES Lócus) cumpre conformidade com legislação pertinente: Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD) e Política Institucional de Privacidade e Proteção da Dados disponível em http://lgpd.escola.br.	
DA PROTEÇÃO DOS DADOS: Contratos que celebrarão avenças entre IES Lócus (ESCOLA) e Titulares de dados (**Colaboradores contratados**):	Departamento de Recursos Humanos e Jurídico:
Contrato de Trabalho Além de outras disposições incluir: ▪ ACESSO AOS DADOS PESSOAIS EM FUNÇÃO DA RELAÇÃO DE TRABALHO O EMPREGADO reconhece ser responsável pela guarda e proteção dos dados pessoais por ele acessados ou a ele confiados no âmbito das atividades prestadas para a EMPREGADORA, devendo utiliza-los somente segundo as finalidades legitimadas de uso e autorizadas pela EMPREGADORA e pelo titular dos dados, obrigando-se a tomar todas as medidas necessárias para impedir que sejam transferidos, revelados, divulgados ou utilizados sem autorização, a qualquer terceiro não autorizado pela EMPREGADORA, não podendo, em tempo algum, direta ou indiretamente, comentá-los em ambientes que não ofereçam a segurança necessária, mesmo dentro das instalações da EMPREGADORA, devendo a informação dos dados pessoais ficar restrita aos setores e pessoas autorizados. ▪ TRANSPARENCIA EM RELAÇÃO A COLETA E TRATAMENTO DE DADOS O EMPREGADO está ciente que o EMPREGADOR poderá realizar a coleta e captura de sua imagem, som da voz, bem como de quaisquer outros dados biométricos, como digital ou face, para autenticação de identidade e aplicação de controles de segurança dentro das instalações da EMPREGADORA, pelo tempo que perdurar a relação de trabalho, permanecendo a guarda por até 5 (cinco) anos após, podendo se estender por maior período para preservação de direitos ou cumprimento de disposição legal. Todo tratamento de dados pessoais realizado pela ESCOLA (IES Lócus) cumpre conformidade com legislação pertinente: Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD) e Política Institucional de Privacidade e Proteção da Dados disponível em http://lgpd.escola.br.	
X. DO MONITORAMENTO E AUDITORIAS: X.1. Tenho conhecimento, compreendi e aceito as determinações específicas da POLITICA INSTITUCIONAL DE PRIVACIDADE E PROTEÇÃO DA DADOS e da POLÍTICA DE SEGURANÇA DA INFORMAÇÃO [20] da ESCOLA. X.2. Concordo que será realizado o monitoramento e rastreio de todos acessos e comunicações através da infraestrutura tecnológica da ESCOLA, conforme previsto em lei e desta forma, renunciando a qualquer expectativa de privacidade enquanto utilizando o acesso agora concedido, enquanto colaborador contratado desta instituição, mesmo utilizando equipamento particular; X.3. O Departamento de Tecnologia e Informação da ESCOLA diante da responsabilidade de monitorar, rastrear e manter os registros de todos os acessos à Internet poderá bloquear automaticamente sites cujos conteúdos sejam contrários à lei, outros que sejam objeto de normas específicas e, ou violem valores institucionais; X.4. Declaro ciência e acordo que as informações de acesso correspondentes ao uso de recursos computacionais, dados ou métodos pertencentes à ESCOLA, que trafeguem nos dispositivos utilizados por mim, poderão ser fornecidos à autoridade competente, mediante a solicitação judicial, independentemente de minha ciência e anuência. X.5. Aceito minha responsabilidade administrativa, civil e penal por qualquer ato através do correspondente acesso à internet provido pela ESCOLA, que constitua violação a qualquer lei vigente no país ou mundo.	
DA PROTEÇÃO DOS DADOS: Termo de uso de dados pessoais para rede **WI-FI** da IES Lócus (ESCOLA)	Departamento de Tecnologia e Informação, Marketing e Jurídico:
ACEITAÇÃO DO TERMO DE USO WI-FI AUTORIZO, desde já, de forma expressa, consciente e inequívoca a coleta e o tratamento dos dados pessoais ora informados, a título gratuito, à ESCOLA (IES Lócus), inscrita no CNPJ/MF sob o nº. (Informar número), com sede à (informar logradouro) sob a finalidade de ingresso na rede sem fio (WI-FI) institucional e navegação de internet por meio desta rede, igualmente, permito a ESCOLA (IES Lócus) reter e usar estes dados pelo período de 01 (um) ano para fins de divulgação de serviços e cursos disponíveis e exclusivos da ESCOLA. Esta autorização poderá ser revogada, a qualquer momento, mediante simples requerimento à ESCOLA em dpo@escola.br. Oportunamente todo registro de navegação de internet será coletado e armazenado por igual período de 01 (um) ano para cumprimento de obrigação legal.	

[20] POLÍTICA DE SEGURANÇA DA INFORMAÇÃO não será abordada nesta intervenção;

A NÃO ACEITAÇÃO deste termo implicará na impossibilidade de ingresso e navegação de internet por meio da rede sem fio (Wi-Fi) da ESCOLA. Todo tratamento de dados pessoais realizado pela ESCOLA (IES Lócus) cumpre conformidade com legislação pertinente: Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD), Lei 12.965/2014 – Marco Cível da Internet (MCI) e Política Institucional de Privacidade e Proteção da Dados disponível em http://lgpd.escola.br.
DA PROTEÇÃO DOS DADOS: Termo de uso de dados pessoais (navegacionais) para **Cookies** de sítios eletrônicos da IES Lócus (ESCOLA) — Departamento de Tecnologia e Informação, Marketing e Jurídico:
Bem-vindo à www.ESCOLA.br! Este site utiliza COOKIES para aprimorar sua experiência de navegação, medir o desempenho do site, além de ajudar a entender seus interesses e desta forma propor relevante conteúdo promocional. Continue ou feche essa mensagem para permitir cookies. Para gerenciar seus cookies, clique aqui. Você pode retirar o seu consentimento para os cookies a qualquer momento. **A NÃO ACEITAÇÃO** de Cookies pode resultar em uma experiência de navegação inapropriada, neste site. Todo tratamento de dados pessoais realizado pela ESCOLA (IES Lócus) cumpre conformidade com legislação pertinente e demais informações sobre Cookies podem ser encontrados junto a Política Institucional de Privacidade e Proteção da Dados disponível em http://lgpd.escola.br.
DA PROTEÇÃO DOS DADOS: Termo de uso de dados pessoais para (pré) inscrição em vestibular da IES Lócus (ESCOLA) — Departamento de Tecnologia e Informação, Marketing e Jurídico:
AUTORIZO, desde já, de forma expressa, consciente e inequívoca a coleta e o tratamento dos dados pessoais ora informados, a título gratuito, à ESCOLA (IES Lócus), inscrita no CNPJ/MF sob o nº. (Informar número), com sede à (informar logradouro) sob a finalidade de inscrição em processo seletivo a curso de graduação aqui informado, de modo, permito a ESCOLA (IES Lócus) reter e usar estes dados pelo período de 01 (um) ano para fins de relacionamento e divulgação de serviços e cursos disponíveis e exclusivos da ESCOLA. Esta autorização poderá ser revogada, a qualquer momento, mediante simples requerimento à ESCOLA em dpo@escola.br. **A NÃO ACEITAÇÃO** deste termo implicará na impossibilidade de participação do processo seletivo da ESCOLA. Todo tratamento de dados pessoais realizado pela ESCOLA (IES Lócus) cumpre conformidade com legislação pertinente: Lei nº 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD) e Política Institucional de Privacidade e Proteção da Dados disponível em http://lgpd.escola.br.
DA PROTEÇÃO DOS DADOS: Contratos de prestação de serviços educacionais IES Lócus (ESCOLA) e Titulares de dados (ALUNO): — Departamento(s) de Matrícula (s), Secretaria Centro Universitário e Jurídico:
X.1. Proteção dos Dados Pessoais • A ESCOLA, por si e por seus colaboradores, obriga-se, sempre que aplicável, a atuar no presente Contrato em conformidade com a Legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial, a Lei 13.709/2018, além das demais normas e políticas de proteção de dados de cada país onde houver qualquer tipo de tratamento dos dados do ALUNO, o que inclui os dados dos clientes desta.
X.1.1. Caso exista modificação dos textos legais acima indicados ou de qualquer outro de forma que exija modificações na estrutura da prestação de serviços ao ALUNO ou na execução das atividades ligadas a este Contrato, a ESCOLA deverá adequar-se às condições vigentes.
X.2. A ESCOLA se compromete a **utilizar** ferramentas, processos e **tecnologias** necessárias para garantir a segurança dos dados e cumprir com suas obrigações, sempre considerando o estado da técnica disponível, incluindo, mas não se limitando, a antivírus, antimalware, detecção de intrusão e outros métodos adequados.
X.3. Autorização para uso de imagem do ALUNO • **Autorização de uso**. O RESPONSÁVEL LEGAL concede, expressa e gratuitamente, o direito de utilização de imagem e voz do ALUNO, bem como de sua obra, para fins de registro de acervo histórico, em campanhas institucionais, materiais impressos, audiovisuais e virtuais, incluindo mídias sociais e endereços eletrônicos da ESCOLA ou de quaisquer empresas do mesmo grupo econômico da ESCOLA. Caso o RESPONSÁVEL LEGAL não esteja de acordo com os usos aqui previsto, deverá manifestar sua discordância, por escrito, à secretaria da ESCOLA, sendo que qualquer situação que afete o ALUNO pela não autorização do uso de sua imagem nas atividades educacionais, que poderá impactar a sua regular participação em alguns casos, é de completa responsabilidade do RESPONSÁVEL LEGAL.
X.4. Autorização para uso publicitário • Uso publicitário. **O uso da imagem** para outros fins que tenham cunho publicitário e/ou promocional será feito sempre por prazo determinado e mediante assinatura prévia de Termo de Autorização específico por parte do RESPONSÁVEL LEGAL, regido por seus dispositivos e pela legislação nacional vigente.
X.5. Ciência e autorização de coleta de Dados Pessoais • Dados coletados. Durante a vigência da relação havida entre as Partes e para fins de cumprimento das atividades educacionais, atendimento de políticas públicas, proteção da vida e da saúde, bem como para aperfeiçoar seus serviços e promover um melhor desempenho na entrega dos serviços contratados, poderão ser coletados Dados Pessoais e Dados Pessoais Sensíveis, que, neste ato, autoriza expressamente, o ALUNO ou o(s) RESPONSÁVEL(IS), se aplicável, para utilização e tratamento pela ESCOLA e suas controladas para atender as finalidades aqui estabelecidas, em atenção à Lei Geral de Proteção de Dados Pessoais.

X.5.1. A Política de Privacidade e Proteção de Dados Institucional, bem como demais providências assumidas pela ESCOLA na direção de acato e *compliance* à Lei Geral de Proteção de Dados do Brasil, Lei 13.709/2018, e demais instrumentos legislativos pertinentes como Marco Civil da Internet, Lei 12.965/2014, podem ser observadas em http://lgpd.escola.br
X.6. Ciência e autorização de coleta de Dados Pessoais Sensíveis • Dados Pessoais Sensíveis. O ALUNO ou seu RESPONSÁVEL LEGAL, se aplicável, **autoriza neste ato o tratamento de Dados Pessoais Sensíveis** relacionados a saúde, coletados através de formulário específico preenchido pelo RESPONSÁVEL LEGAL, bem como, aqueles coletados em ambulatório, fornecidos pelo próprio ALUNO, para finalidade de atendimento emergencial, em atendimento aos artigos 11 e 14 da Lei Geral de Proteção de Dados Pessoais.
X.7. O Titular tem direito a obter da Controladora (ESCOLA), em relação aos dados por ele tratados, a qualquer momento e mediante requisição: I - confirmação da existência de tratamento; II - acesso aos dados; III - correção de dados incompletos, inexatos ou desatualizados; IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto na Lei nº 13.709; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador; V - portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa, de acordo com a regulamentação da autoridade nacional, observados os segredos comercial e industrial; VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 da Lei nº 13.709; VII - informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; VIII - informação sobre a possibilidade de não fornecer consentimento e sobre as consequências da negativa; IX - revogação do consentimento, nos termos do § 5º do art. 8º da Lei nº 13.709.

DA PROTEÇÃO DOS DADOS: Contratos que celebrarão avenças entre IES Lócus (Controlador - Contratante) e Parceiro Externo (Operador - Contratada):	Departamento de Compras, Jurídico e Departamento demandante:
X. A RESPONSABILIDADE É SOLIDÁRIA NO TRATAMENTO DE DADOS COMPARTILHADOS ENTRE CONTROLADOR E OPERADOR, LEI 13.709/2018 (LEI GERAL DE PROTEÇÃO DE DADOS – LGPD), ARTIGO 42, INCISOS I E II.	
X.1. Proteção dos Dados Pessoais. A CONTRATADA, por si e por seus colaboradores, obriga-se, sempre que aplicável, a atuar no presente Contrato em conformidade com a Legislação vigente sobre Proteção de Dados Pessoais e as determinações de órgãos reguladores/fiscalizadores sobre a matéria, em especial, a Lei 13.709/2018, além das demais normas e políticas de proteção de dados de cada país onde houver qualquer tipo de tratamento dos dados da CONTRATANTE, o que inclui os dados dos clientes desta.	
X.1.1. Caso exista modificação dos textos legais acima indicados ou de qualquer outro de forma que exija modificações na estrutura da prestação de serviços à CONTRATANTE ou na execução das atividades ligadas a este Contrato, a CONTRATADA (Operador) deverá adequar-se às condições vigentes. Se houver alguma disposição que impeça a continuidade do Contrato conforme as disposições acordadas, a CONTRATANTE poderá resolvê-lo sem qualquer penalidade, apurando-se os valores devidos até a data da rescisão.	
X.1.2. A CONTRATADA seguirá as instruções recebidas da CONTRATANTE em relação ao tratamento dos Dados Pessoais, além de observar e cumprir as normas legais vigentes aplicáveis, sob pena de arcar com as perdas e danos que eventualmente possa causar, sem prejuízo das demais sanções aplicáveis.	
X.1.3. A CONTRATADA, incluindo todos os seus colaboradores, compromete-se a tratar todos os Dados Pessoais como confidencial, exceto se já eram de conhecimento público sem qualquer contribuição da CONTRATADA, ainda que este Contrato venha a ser resolvido e independentemente dos motivos que derem causa ao seu término ou resolução.	
X.1.4. A CONTRATADA deverá garantir e cumprir com os requisitos das medidas de segurança técnicas e organizacionais para garantir a confidencialidade, pseudo-anonimização e a criptografia dos Dados Pessoais, inclusive no seu armazenamento e transmissão, especialmente nos compartilhamentos e comunicação de dados pessoais pela CONTRATADA à CONTRATANTE.	
X.1.6. A CONTRATADA deverá manter registro das operações de tratamento de dados pessoais que realizar, bem como implementar medidas técnicas e organizativas necessárias para proteger os dados contra a destruição, acidental ou ilícita, a perda, a alteração, a comunicação ou difusão ou o acesso não autorizado, além de garantir que o ambiente (seja ele físico ou lógico) utilizado por ela para o tratamento de dados pessoais são estruturados de forma a atender os requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos em Lei, e às demais normas regulamentares aplicáveis.	
X.1.7. A CONTRATADA deverá notificar a CONTRATANTE sobre as reclamações e solicitações dos titulares de dados (por exemplo, sobre a correção, exclusão, complementação e bloqueio de dados) e sobre as ordens de tribunais, autoridade pública e reguladores competentes e quaisquer outras exposições ou ameaças em relação à conformidade com a proteção de dados identificadas pelo mesmo.	
X.1.8. A CONTRATADA somente poderá subcontratar qualquer parte dos Serviços para um ou mais terceiros (suboperadores) mediante consentimento prévio e por escrito da CONTRATANTE. Neste caso, a CONTRATADA deverá celebrar um contrato escrito com o Suboperador para (i) obrigar o Suboperador às mesmas obrigações impostas por este Contrato em relação à CONTRATADA, no que for aplicável aos Serviços subcontratados, (ii) descrever os Serviços subcontratados e (iii) descrever as medidas técnicas e organizacionais que o Suboperador deverá implementar.	
X.1.9. A CONTRATADA deverá notificar a CONTRATANTE em 24 (vinte e quatro) horas de (i) qualquer não cumprimento (ainda que suspeito) das disposições legais relativas à proteção de Dados Pessoais; (ii) qualquer	

descumprimento das obrigações contratuais relativas ao processamento e tratamento dos dados pessoais; (iii) qualquer violação de segurança na CONTRATADA ou nos seus Suboperadores.
X.1.10. A CONTRATADA compromete-se a auxiliar a CONTRATANTE com a suas obrigações judiciais ou administrativas, de acordo com a Lei de Proteção de Dados Pessoais aplicável, fornecendo informações relevantes disponíveis e qualquer outra assistência para documentar e eliminar a causa e os riscos impostos por quaisquer violações de segurança.
X.1.11. A CONTRATANTE terá o direito de acompanhar, monitorar, auditar e fiscalizar a conformidade da CONTRATADA com as obrigações de Proteção de Dados Pessoais, sem que isso implique em qualquer diminuição de responsabilidade que a CONTRATADA possui perante a Lei e este Contrato.
X.2. Todo e qualquer tratamento de dados fora do Brasil, depende de autorização prévia pela CONTRATANTE à CONTRATADA.
X.3. A CONTRATADA se compromete a utilizar ferramentas e tecnologias necessárias para garantir a segurança dos dados e cumprir com suas obrigações, sempre considerando o estado da técnica disponível, incluindo, mas não se limitando, a antivírus, antimalware, detecção de intrusão e outros métodos adequados.
X.4. A CONTRATADA deverá realizar o registro de todas as atividades realizadas em seus sistemas/sistemas/ambientes, de modo a permitir a identificação de quem as realizou.
X.5. Propriedade dos dados em geral. O presente Contrato não transfere a propriedade dos dados da CONTRATANTE ou dos clientes desta para a CONTRATADA. Os dados gerados, obtidos ou coletados a partir da prestação dos serviços ora contratados são de propriedade da CONTRATANTE.
X.5.2. A CONTRATANTE não autoriza a CONTRATADA a usar, compartilhar ou comercializar quaisquer eventuais elementos de dados, produtos ou subprodutos que se originem ou sejam criados a partir do tratamento de dados estabelecido por este Contrato.
X.6. Banco de dados. A CONTRATADA restituirá à CONTRATANTE os dados contidos no banco de dados, nos casos de término, rescisão e resilição deste instrumento. Os dados deverão ser restituídos pela CONTRATADA, juntamente com o dicionário de dados que permita entender a organização do banco de dados, em até 10 (trinta) dias ou em eventual prazo acordado entre as Partes.
X.6.1. Todos os dados contidos no banco de dados são de propriedade da CONTRATANTE.
x.7. Fica assegurado à CONTRATANTE, nos termos da lei, o direito de regresso em face da CONTRATADA diante de eventuais danos causados por esta em decorrência do descumprimento das obrigações aqui assumidas em relação a Proteção dos Dados.”

Apêndice E1: Panorama da Pesquisa intervencionista – Visão teórica

Constructos	Literatura	Variáveis observáveis	INTERVENÇÃO: Aplicação *framework* intervencionista (Lima, 2019; Daniballe, 2017)					
			Análise ambiental			Coleta, Análise e EXECUÇÃO	Instrumentos Posteriores	Avaliação de Resultados
			Instrumentos Anteriores		Diagnóstico dos Problemas			
LGPD - Lei 13.709/18	Lei n. 13.709, (2018); SIEEESP, (2018); Mulholland, (2018); Tuttle, (2018); Global Risks Report, (2018); Privacy Governance Report, (2018); Privacy Rights Clearinghouse, (2014); Ariff, Zakuan, Tajudin, Ahmad, Ishak e Ismail, (2014); Machado Meyer, (2018); Pinheiro, (2018); Baffa, Poggio e Fachinetti, (2018); Maldonato, Blum e Borelli (2019); Feferbaum e Lima, (2019); Bioni, (2019);	Ciência	1) Entrevistas semi-estruturadas Stakeholders gestão administrativa, acadêmica e representantes discentes; 2) Questionários fechados (*Likert*) apliados aos times técnicos administrativosantes dos treinamentos sobre a LGPD	1	Autodeclara conhecimento;	INTERVENÇÃO Disposição de Framework Conseitual e Funcional de Uso e Proteção de Dados Pessoais, desenvolvido sobre a literatura de Bunge e Catelli, junto a IES lócus → Desenvolvimento e aplicação de Plano de Conformidade a LGPD	3) Entrevistas semi-estruturadas Stakeholders "chave" - Controladores; 2) Questionários fechados (*Likert*) apliados, times técnicos administrativosapós os treinamentos sobre a LGPD;	3 Melhora da percepção sobre a Lei
				2	Desconhece Lei e conceitos;			2 Melhora de 83% sobre conhecimento e impactos da Lei
		Importância		1	Não compreende prejuízos e benefícios			
				2				2 Ciência sobre a exposição da IES e plano de conformidade
		Conformidade		1	Afirma que IES manipula dados			
				1 2	Não conhece plano de compliance			2 3 Melhora sobre conscientização
Governança da Infomação (TI)	(Bianchi & Sousa, 2016; Wu, Straub, & Liang, 2015; Coen & Kelly, 2007)	Relevância		1	Reconhece importância de TI			3 Melhora sobre processo decisório, enquanto instrumento de apoio;
	(Global Risks Report, 2018; Privacy Governance Report, 2018; Ariff et al., 2014; ISO 27005, 2011)			1	Reconhece que TI vulnerabiliza			
	(Coffman, 2014; Privacy Rights Clearinghouse, 2018; Helsloot & Jong, 2006)			1	Reconhece ambiente institucional (IES) mais exposto			
	(Jairak & Praneetpolgrang, 2013; Hicks, Pervan, & Perrin, 2012 ; Tufano 2011; Sabherwal & Kirs, 1994)	Presença		1	Desconhece presença de Gov.TI			3 Melhora discreta da exposição da Governança de TI
				1	Afirma que IES não divulga Gov.TI			
				1	Não vê TI na estratégia			
	(Peleias, 2012; ISACA, 2010; COBIT, 2012, COSO-ERM, 2017; ISO31000, 2009; Kululanga & Kuotcha 2009)	Conformidade		1	Reconhece que Gov. TI apoia compliance			3 1) Identificação de melhorias; 2) Suporte a conformidade;

RESPONDENTES: **1**) Gestores administrativos (06), Gestores acadêmicos (07), Representantes discentes (04); **2**) Recursos Humanos (05), Relacionamento Institucional (05), Central do Aluno (05), Central de Carreiras (02), Financeiro (03), Segurança (02), Tecnologia (06); Compras (01); **3)** Reitor (Superintendente Geral) e Vice-Reitor (Superintendente Adjunto);