UNIVERSIDADE FEDERAL DE SANTA CATARINA
CENTRO DE CIÊNCIAS, TECNOLOGIAS E SAÚDE
PROGRAMA DE PÓS-GRADUAÇÃO
EM TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

FELIPE JOSÉ FERREIRA

# **CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS:** ESTUDO DE CASO EM INSTITUIÇÕES FINANCEIRAS COOPERATIVISTAS

ARARANGUÁ – SC
2021

Felipe José Ferreira

# **CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO, PRIVACIDADE E PROTEÇÃO DE DADOS:** ESTUDO DE CASO EM INSTITUIÇÕES FINANCEIRAS COOPERATIVISTAS

Dissertação submetida ao Programa de Pós-Graduação em Tecnologias da Informação e Comunicação da Universidade Federal de Santa Catarina para a obtenção do título de mestre em Tecnologias da Informação e Comunicação.
Orientadora: Prof.ª Dr.ª Andréa Cristina Trierweiller
Coorientador: Prof. Dr. Alexandre Moraes Ramos

Araranguá - SC
2021

Ficha de identificação da obra elaborada pelo autor,
através do Programa de Geração Automática da Biblioteca Universitária da UFSC.

Ferreira, Felipe José
Cultura organizacional de segurança da informação, privacidade e proteção de dados : estudo de caso em instituições financeiras cooperativistas / Felipe José Ferreira ; orientadora, Andréa Cristina Trierweiller, coorientador, Alexandre Moraes Ramos, 2021.
169 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Campus Araranguá, Programa de Pós-Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2021.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. Segurança da Informação. 3. Privacidade da Informação. 4. Proteção de Dados Pessoais. 5. Lei Geral de Proteção de Dados - LGPD. I. Trierweiller, Andréa Cristina. II. Ramos, Alexandre Moraes. III. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Tecnologias da Informação e Comunicação. IV. Título.

Felipe José Ferreira

**Cultura Organizacional de Segurança da Informação, Privacidade e Proteção de Dados:** Estudo de Caso em Instituições Financeiras Cooperativistas

O presente trabalho em nível de mestrado foi avaliado e aprovado por banca examinadora composta pelos seguintes membros:

Prof. Pedro Henrique de Moura Araujo, Dr.
Universidade Federal de Santa Catarina

Prof. João Bosco da Mota Alves, Dr.
Universidade Federal de Santa Catarina

Prof. Aires Jose Rover, Dr.
Universidade Federal de Santa Catarina

Certificamos que esta é a **versão original e final** do trabalho de conclusão que foi julgado adequado para obtenção do título de mestre em Tecnologias da Informação e Comunicação


Documento assinado digitalmente
Juarez Bento da Silva
Data: 23/08/2021 17:04:15-0300
CPF: 366.921.580-87
Verifique as assinaturas em https://v.ufsc.br

_____

Coordenação do Programa de Pós-Graduação


Documento assinado digitalmente
Andrea Cristina Trierweiller
Data: 23/08/2021 16:53:17-0300
CPF: 001.238.759-27
Verifique as assinaturas em https://v.ufsc.br

_____

Prof.ª Andréa Cristina Trierweiller, Dr.ª
Orientadora

Araranguá, 16 de julho de 2021

Mercedes Luiza Nascimento, onde estiveres, este trabalho é seu, minha mestre, professora e Madrinha. De todos os presentes que um afilhado poderia receber, ganhei o mais valioso: o exemplo e o incentivo pela leitura. Esta, é encanto e magia que apaixona e crava no espírito a insaciável sede pelo saber. Gratidão por conceder-me o desejo pelo cálice do conhecimento. És minha inspiração eterna para percorrer não só a vida acadêmica, mas toda esta trajetória que é apenas um sopro na imensidão.

## AGRADECIMENTOS

Ao amor da minha vida, Lígia Maciel, por nunca desistir e nunca me deixar desistir, por ser fonte infinita de apoio e amor, por ser a melhor mãe que minhas filhas poderiam ter, por acreditar em nossa família, meu maior presente. Você é meu sonho e é quem permite que eu seja feliz, ao realizar os meus.

Às minhas filhas, Helena e Luíza, a razão de cada segundo empenhado para este e outros trabalhos. Por me tornarem o pai e homem mais feliz do mundo, simplesmente ao sorrir todo dia para mim, mostrando porque devemos fazer a diferença para um mundo melhor.

Aos meus pais, Eliane e Clair, por terem me ensinado o que eu realmente preciso aprender e o que realmente importa nessa vida, por serem sempre meus exemplos.

Ao meu irmão André e cunhada Luciane, por serem amigos, irmãos e apoiadores.

Aos meus afilhados Thaís, Gabriel e Rafael, por compreenderem minha ausência e dedicação aos estudos.

À minha orientadora Prof. Dra. Andréa Cristina Trierweiller, a quem inspira um modo de vida de dedicação máxima, a fazer valer o verdadeiro significado de ensinar. Por toda paciência e tempo dedicado para a realização deste sonho.

Ao meu coorientador Prof. Dr. Alexandre Moraes, pelas contribuições de melhoria.

Ao amigo, colega e Prof. Dr. Maurício José Ribeiro Rotta, pela parceria e conhecimento como um dos grandes especialistas em LGPD no Brasil.

Ao Prof. Dr. Pedro Henrique de Moura Araujo, por disponibilizar tanto do seu tempo para a construção deste trabalho, carinhoso em cada consideração.

À Natália Martinello, pelo apoio profissional que me permitiu realizar este trabalho.

Aos amigos de pesquisa Adão Paulo Ronconi e Me. Yuri Borba Vefago, apoios no desespero. Obrigado por tornar esse caminho menos pedregoso.

Aos amigos, tantos que impossível nominá-los, mas que, de alguma forma ou outra, sempre estiveram do meu lado, torcendo por mim em cada segundo.

Ao sistema Sicoob, em especial à Eveline Dagostin, por permitir e transformar tantas horas de estudo em estratégias de fortalecimento para sua instituição.

Aos respondentes da pesquisa, pela sinceridade e tempo dedicado.

À Universidade Federal de Santa Catarina, por transformar a minha e a vida de milhões de pessoas no mundo através do conhecimento, da arte e da ciência.

***Explorar o desconhecido, avançar o óbvio, escrever, sentir, navegar e, mesmo com alguma incerteza, fazer com que a leitura nos torne melhores***.

Dra. Andréa Cristina Trierweiller

## RESUMO

O objetivo geral desta dissertação é analisar o nível de cultura organizacional de segurança da informação na percepção de gestores de instituições financeiras cooperativistas. Buscou-se, de forma complementar, avaliar a privacidade das informações e a proteção de dados, na perspectiva de alguns desses gestores, considerando a relevância do tema no contexto da LGPD e das sanções às empresas que não se adequarem à lei. Para isso, a pesquisa fundamenta-se em três eixos: o primeiro, baseado na busca exploratória e revisão de literatura, constituindo-se no levantamento de dado secundários; o segundo e terceiro eixos são referentes à pesquisa de campo, ou seja, dados primários, com levantamento junto a gestores de instituições financeiras cooperativistas sobre sua percepção da Segurança da Informação – SI, Privacidade da Informação – PI e Proteção de Dados – PD. Destaca-se, no eixo dois, a aplicação de instrumento validado por Araujo (2018), fundamentado na Teoria da Resposta ao Item – TRI e no eixo três, entrevistas utilizando questionário com perguntas abertas, elaboradas pelo autor. Dentre os resultados principais, as unidades estão no nível – de cultura organizacional de segurança da informação na percepção dos gestores – "encaminhado", ou seja, demonstram preocupação com a SI, mas o comportamento de alguns colaboradores pode comprometer os ativos da organização. E ainda, os gestores das unidades apontaram a tecnologia e os processos como instrumentos fortalecidos ao serem comparados com as pessoas, pois as unidades pesquisadas ainda precisam aculturar-se à SI, PI e PD, para que os comportamentos humanos garantam os princípios desses construtos e sua aplicação prática na gestão das organizações, além da preservação de direitos fundamentais. E ainda, como parte dos resultados, constatou-se a insipiência dos gestores quanto à importância que os colaboradores dão à temática da LGPD, talvez por não terem respaldo de sua liderança ou até mesmo, por não compreenderem os riscos. Sugere-se desenvolver uma escala de medida da cultura de privacidade da informação e proteção de dados, também com uso da TRI, que validada, possibilita a aplicação em organizações de qualquer segmento de mercado.



**Palavras-chave:** Segurança da Informação. Privacidade da Informação. Proteção de Dados Pessoais. Lei Geral de Proteção de Dados – LGPD. Teoria da Resposta ao Item – TRI.

## ABSTRACT

This dissertation aims to analyze the level of organizational culture of information security in the perception of managers of cooperative financial institutions. In addition, it was sought, in a complementary way, to assess the privacy of information and data protection, from the perspective of some of these managers, considering the relevance of the theme according to the context of the LGPD and sanctions for companies that do not comply with the law. In addition, we sought, in a complementary way, to understand the privacy of information and data protection, also from the perspective of some of these managers, considering the relevance of the theme in terms of the context of the LGPD and sanctions for companies that do not fit. For this, the research is based on three axes: a first, based on an exploratory search and literature review, constituting the survey of secondary data; the second and third axes refer to field research, that is, primary data, with a survey with managers of cooperative financial institutions about their perception of IS, IP, and PD. In axis two, the application of an instrument validated by Araujo (2018), based on the TRI, and in axis three, interviews using a questionnaire with open questions, prepared by the author, stand out. Among the main results, the units are at the level – of organizational culture of information security in the perception of managers – "referred", that is, they demonstrate concern with the IS, but the behavior of some employees can compromise the organization's assets. And yet, unit managers pointed out technology and processes as strengthened instruments when compared with people, as the units surveyed still need to acculturate to IS, PI, and PD, so that human behaviors guarantee the principles of these constructs and their practical application in the management of organizations, in addition to the preservation of fundamental rights. And yet, as part of the results, it was verified the incipiency of the managers regarding the importance that the collaborators give to the theme of the LGPD, perhaps because they do not have support from their leadership or even because they do not understand the risks. It is suggested to develop a scale for measuring the culture of information privacy and data protection, also using the TRI, which, when validated, enables its application in organizations in any market segment.



**Keywords:** Information Security. Information Privacy. Personal Data Protection. General Data Protection Law - GDPL. Item Response Theory – IRT

## LISTA DE FIGURAS

## LISTA DE QUADROS

## LISTA DE ABREVIATURAS E SIGLAS

ABNT – Associação Brasileira de Normas Técnicas

ANPD – Autoridade Nacional de Proteção de Dados

CC – Código Civil

CDC – Código de Defesa do Consumidor

CF – Constituição Federal

CID – Confidencialidade, Integridade e Disponibilidade

COVID-19 – *Coronavirus Disease 2019*

CP – Código Penal

CPC – Código de Processo Civil

CUn – Conselho Universitário

DP – Dado Pessoal

DPO – *Data Protection Officer*

DUDH – Declaração Universal dos Direitos Humanos

FGCoop – Fungo Garantidor do Cooperativismo

HFR – *Human Factor Report*

GDPR – *General Data Protection Regulation*

ICA – *International Cooperative Alliance*

ISO – *International Organization for Standardization*

LABeGIS – Laboratório de Gestão, Inovação e Sustentabilidade

LAI – Lei de Acesso à Informação

LCP – Lei do Cadastro Positivo

LGPD – Lei Geral de Proteção de Dados

OCB – Organização das Cooperativas do Brasil

OCDE – Organização para a Cooperação e Desenvolvimento Econômico

OECD – *Organisation for Economic Co-operation and Development*

*PbD – Privacy by Design*

PD – Proteção de Dados

PDCA – Plan Do Check Act

PEC – Proposta de Emenda à Constituição

PI – Privacidade da Informação

PMPEF – Programa de Mestrado Profissional em Ensino da Física

PNC – Plano Nacional do Cooperativismo

PPG – Programa de Pós-Graduação

PPGCR – Programa de Pós-Graduação em Ciências da Reabilitação

PPGES – Programa de Pós-Graduação em Energia e Sustentabilidade

PPGTIC – Programa de Pós-Graduação em Tecnologias da Informação e Comunicação

RE – Recurso Extraordinário

RGPD – Regulamento Geral de Proteção de Dados

RI UFSC – Repositório Institucional da Universidade Federal de Santa Catarina

SGSI – Sistema de Gestão de Segurança da Informação

SI – Segurança da Informação

STF – Supremo Tribunal Federal

TI – Tecnologia da Informação

TIC – Tecnologia da Informação e Comunicação

TRI – Teoria da Resposta ao Item

UFSC – Universidade Federal de Santa Catarina

**SUMÁRIO**

# 1 INTRODUÇÃO

No atual contexto de transformação digital, a informação se torna um importante ativo para o ambiente corporativo e a sua gestão passa a ser um desafio, pois a produção e o tratamento são necessários, não somente para a conformidade com as normativas e leis, mas para a conversão dos dados em valor.

Padrões inesperados nas atividades de negócio, novos tipos de previsões e análises de dados e novas fontes de valor são possíveis graças ao *big data*, esse dilúvio de dados que cerca a vida e os negócios, cada vez mais digitais, exige uma relação interativa, inovação e aprendizado contínuos (ROGERS, 2019).

Para acompanhar esta demanda de informações, conforme aponta Possolli (2012), as organizações precisam implementar métodos que reduzam custos e possibilitem a gestão da qualidade dos processos. Essas inovações navegam por um oceano de dados gerados em quantidades sem precedentes, o que torna o seu tratamento pelas instituições um grande desafio, pois é preciso transformá-los em informações valiosas (ROGERS, 2019).

Nesse universo digital, tem-se 4.54 (quatro ponto cinquenta e quatro) bilhões de usuários de internet no mundo, o que representa 59% (cinquenta e nove por cento) da população mundial. No Brasil, são 150.4 (cento e cinquenta ponto quatro) milhões de usuários, o que corresponde a 71% (setenta e um por cento) do total de 211.8 (duzentos e onze ponto oito) milhões (WE ARE SOCIAL, 2021).

Além disso, empresas de todos os tipos e tamanhos (tanto do setor público, quanto do privado), tratam dados (como por exemplo a coleta, o processamento, o armazenamento e a transmissão) em diferentes formatos, tanto eletrônico, quanto físico e até mesmo, verbal (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b). Essas informações são componentes fundamentais para o funcionamento, diferenciação de mercado e geração de valor das instituições (ROGERS, 2019). Esses ativos intangíveis requerem proteção, sendo objeto de ameaça, pois processos, sistemas, redes e pessoas têm vulnerabilidades, fazendo-se necessário o estabelecimento de protocolos, políticas, estrutura organizacional e funções de *software* e *hardware* para a segurança desse bem tão importante para a instituição: os dados (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b).

## 1.1 PROBLEMA DA PESQUISA

Diante da crescente importância do tratamento de dados, as informações profissionais e pessoais se tornam objeto de ameaças, com muitas vulnerabilidades, tanto em meio físico, quanto digital, o que inclusive, levou à aprovação da Lei Geral de Proteção de Dados - LGPD – Lei 13.709/18 no Brasil, com vigência durante a produção desta pesquisa, dispondo sobre tratamento de dados pessoais (BRASIL, 2018).

A condução dessa pesquisa, no contexto de segurança da informação – SI, privacidade da informação – PI e proteção de dados – PD, avaliada sob a ótica normativa e legal, é motivada pela carreira profissional deste pesquisador, bacharel em Direito e advogado, que também laborou no ramo corporativo, em uma instituição financeira cooperativista, o que estimulou a aplicação do estudo nesta conjectura.

Portanto, verifica-se a importância de responder a seguinte pergunta de pesquisa:

"Como analisar a cultura organizacional de segurança e privacidade da informação e proteção de dados na percepção de gestores de instituições financeiras cooperativistas?"

## 1.2 OBJETIVOS

Com a definição da problemática da pesquisa, o escopo do trabalho é desdobrado em um objetivo geral e seus objetivos específicos.

### 1.2.1 Objetivo Geral

Analisar o nível de cultura organizacional de segurança da informação na percepção de gestores de instituições financeiras cooperativistas. Buscou-se, de forma complementar, avaliar a privacidade das informações e a proteção de dados, na perspectiva de alguns desses gestores, considerando a relevância do tema no contexto da LGPD.

### 1.2.2 Objetivos Específicos

Para o alcance do objetivo geral, preservando os aspectos metodológicos da pesquisa, define-se os objetivos acessórios, que contribuem para o entendimento da matéria e do presente estudo, sendo eles:

- Realizar levantamento de literatura, em bases de dados que indexam publicações científicas, sobre segurança e privacidade da informação, proteção de dados, cultura organizacional e temas correlatos, com vistas a fundamentar tais construtos, bem como, fornecer subsídio para análise e discussão dos dados obtidos nas pesquisas de campo;
- Realizar levantamento de legislação e normativas sobre os temas estudados, em especial, sobre a Lei Geral de Proteção de Dados e seus princípios;
- Analisar a segurança da informação em instituições financeiras cooperativistas, com base na literatura e pesquisa de campo com os gestores de instituições financeiras, por meio da escala desenvolvida por Araujo (2018), que utilizou a Teoria da Resposta ao Item;
- Analisar a privacidade da informação e a proteção de dados em instituições financeiras cooperativistas, com base na literatura e depoimento de respondentes, obtido na pesquisa de campo com gestores, por meio de questionário construído com base nos princípios da Lei Geral de Proteção de Dados;
- Analisar as barreiras e benefícios do aculturamento da segurança e privacidade da informação em instituições financeiras cooperativistas;
- Contribuir com o avanço do conhecimento na área, inclusive, com a identificação de lacunas de pesquisa, apontando oportunidades futuras de estudo.

As pesquisas de campo, conduzidas nesta dissertação, ocorreram no período da pandemia da COVID-19, o que é explicitado adiante, no capítulo 3, referente aos Procedimentos Metodológicos.

## 1.3 ADERÊNCIA AO PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO E À LINHA DE PESQUISA

O *campus* da Universidade Federal de Santa Catarina – UFSC em Araranguá, foi fundado em 2008 com a criação de 04 (quatro) cursos de graduação: Tecnologias da Informação e Comunicação, Engenharia de Computação, Engenharia de Energia e Fisioterapia, a partir da Resolução 027/2008 do Conselho Universitário - CUn, com o objetivo de atender as demandas do mercado regional (UFSC, 2020). Em 2018 teve início o curso de graduação em Medicina. Já, a pós-graduação *stricto sensu,* se iniciou em junho de 2014, com o Mestrado em Tecnologias

da Informação e Comunicação - TIC, o primeiro programa de pós-graduação fora da sede da UFSC, em Florianópolis (UFSC, 2020).

Além do Programa de Pós-Graduação em Tecnologias da Informação e Comunicação – PPGTIC, em Araranguá ainda há mais três programas de mestrado, o Programa de Pós Graduação em Ciências da Reabilitação – PPGCR, o Programa de Pós-Graduação em Energia e Sustentabilidade – PPGES e o Programa de Mestrado Profissional em Ensino da Física – PMPEF (UFSC, 2020).

A necessidade de consumo de informação e da utilização de estratégias e ferramentas pelas organizações para atendimento de seus clientes e públicos de interesse, em um ambiente de negócios em constante transformação digital, demonstra que o presente trabalho é aderente à linha de pesquisa Tecnologia, Gestão e Inovação do PPGTIC, pois este trabalho busca utilizar as novas tecnologias da informação e comunicação para desenvolver novos métodos, técnicas e processos para a gestão de organizações (UFSC, 2020).

Nessa perspectiva, o trabalho se reveste de real importância tanto para o Programa, quanto para o mercado, pois a pesquisa contribui para a compreensão da segurança e da privacidade da informação no ambiente corporativo.

Ainda, a temática mantém ligação com o Laboratório de Gestão, Inovação e Sustentabilidade – LABeGIS, vinculado ao PPGTIC e à linha de pesquisa descrita, coordenado pela professora orientadora deste estudo.

Trata-se de um tema abordado somente em uma dissertação do PPGTIC. Os descritores “segurança da informação” e “privacidade da informação” obtiveram um resultado quando pesquisados no Repositório Institucional da UFSC – RI UFSC[1], utilizando-se como filtro Teses e Dissertações defendidas no PPGTIC (UFSC, 2021).

Entretanto, ao utilizar os mesmos descritores (de forma isolada) para toda a UFSC, mantendo o filtro “Teses e Dissertações” e incluindo “Título”, foram obtidos ao total, 08 (oito) trabalhos, apenas para “Segurança da Informação”, conforme Quadro 1:

Quadro 1 – Aderência desta pesquisa aos trabalhos do Repositório Institucional UFSC

| Título | Autor | Ano | Nível |
|---|---|---|---|
| Framework para identificar o nível de conformidade das empresas brasileiras do setor químico no processo de adequação à lei geral de proteção de dados pessoais | Silva, Rogério Hermínio da | 2021 | Dissertação do PPG em Tecnologias da Informação e Comunicação - Araranguá |

[1] Disponível em: https://repositorio.ufsc.br/

| | | | |
|---|---|---|---|
| Diretrizes para elaboração de uma política de segurança da informação (redes) em meio acadêmico | Casañas, Alex Delgado Gonçalves | 2001 | Dissertação do PPG em Engenharia de Produção - UFSC - Florianópolis |
| Construção da escala do nível da cultura organizacional de segurança da informação | Araujo, Pedro Henrique de Moura | 2018 | Tese do PPG em Engenharia de Produção – UFSC - Florianópolis |
| Segurança da informação: um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de instituições bancárias | Klettenberg, Josiane | 2016 | Dissertação do PPG em Ciência da Informação - UFSC - Florianópolis |
| Gestão da segurança da informação do acervo acadêmico: um estudo à luz das legislações e regulações | Pavanati, André | 2019 | Dissertação do PPG em Administração Universitária |
| Gerenciamento da segurança da informação em sistemas de teletrabalho | Machado, Cesar de Souza | 2002 | Dissertação do PPG em Engenharia de Produção - UFSC - Florianópolis |
| Políticas de segurança da informação nas organizações | Silva, Paulo Murilo | 2003 | Dissertação do PPG em Ciência da Informação - UFSC - Florianópolis |
| Disponibilidade, desempenho e segurança do ambiente de tecnologia da informação com acordo de nível de serviços utilizando ATM | Rezende, Ibraim de Sousa | 2002 | Dissertação do PPG em Ciência da Informação - UFSC - Florianópolis |
| Gerenciamento e uso da informação aplicada na área de Segurança Pública do Estado de Santa Catarina: um estudo de caso no CIASC | Barros, José Arilton Antunes | 2004 | Dissertação do PPG em Engenharia de Produção - UFSC - Florianópolis |

Fonte: UFSC (2021).

De toda busca realizada, constatou-se seis dissertações de mestrado e uma tese de doutorado, a de Araujo (2018), que tem estrita relação com esta pesquisa, abordando os temas segurança da informação e cultura organizacional.

O trabalho de Araujo (2018)teve como objetivo a construção de uma escala de medida da cultura de segurança da informação nas organizações, utilizando-se a Teoria da Resposta ao Item – TRI. Desta forma, o instrumento foi adaptado para esta pesquisa, modelando-o para aplicação sob a ótica dos gestores de segurança da informação de instituições financeiras e para as suas particularidades, bem como para o atual contexto tecnológico e do mercado. Inclusive, fez-se contato com Araujo para a utilização de seu questionário como base para esta dissertação, tendo o autor supracitado, autorizado e se colocado à disposição para ajustes ou ainda, sugestões.

Araujo (2018) conclui em seu trabalho que para a avaliação do nível de segurança da informação em uma organização é necessário avaliar o nível de cultura de segurança da informação, sugerindo inclusive o conceito de cultura organizacional aplicada à segurança da informação como a forma com que o grupo social compartilha, expressa ou manifesta seus conhecimentos, valores, crenças e acordos tácitos, de forma coletiva, sobre segurança da informação, com objetivo da sobrevivência da organização.

A principal contribuição do estudo de Araujo (2018), segundo o próprio autor, é a construção da escala, pois a utilização da TRI mostrou que a metodologia é capaz de avaliar características individuais e coletivas, considerando a inequidade, característica inerente à subjetividade. Níveis diferentes de proficiência em cultura de segurança da informação apresentarão *scores* diferentes.

Bortolotti (2010) destaca o princípio da invariância da TRI, que pressupõe que tanto indivíduos quanto itens são invariantes, desde que definido a escala para o traço latente, permitindo a utilização de outra amostra de indivíduos para determinar a resistência à mudança organizacional (traço latente estudado pela referida autora), sob o emprego da mesma escala estabelecida.

Para o caso em que os dados se ajustam ao modelo, a TRI pressupõe a propriedade de invariância dos parâmetros, a qual implica que as habilidades dos sujeitos são estimadas independentemente do teste utilizado. Assim como os parâmetros dos itens, independentemente da amostra de examinandos que os responderam (BAKER, 2001; HAMBLETON; SWAMINATHAN, 1984; ROGERS, 2019).

Dessa forma, a partir da escala construída por Araujo (2018), pode-se aplicar em diferentes tipos de organizações e outros sujeitos (o que foi realizado pelo pesquisador desta dissertação), permitindo a comparação entre as escalas, além de fornecer informações relevantes para auxiliar os gestores na tomada de decisões, garantindo maior adequação para a sobrevivência da instituição na atual sociedade da informação (ARAUJO, 2018).

# 2 FUNDAMENTAÇÃO TEÓRICA

Para uma melhor compreensão dos conteúdos e alcance dos objetivos propostos, é necessário adentrar em conceitos teóricos que dão suporte ao conhecimento deste trabalho, além de contribuírem com a compreensão dos resultados da pesquisa. Para tanto, temas como informação, segurança da informação, privacidade da informação, Lei Geral de Proteção de Dados, cultura e cultura organizacional são descritos a seguir.

## 2.1 INFORMAÇÃO

A informação participa na evolução e na revolução do homem na sua história como elemento organizador, que estabelece sua odisseia individual no espaço e no tempo, assumindo tamanha importância a ponto de levantar questionamentos sobre a sua natureza, conceito, benefícios e influência nos relacionamentos do indivíduo com o mundo (BARRETO, 1994).

Há inúmeras definições de informação que a condicionam à semântica de transferência, à mensagem entre interlocutor e receptor, à ação resultante de seu uso e ao começo e fim do processo de comunicação (WERSIG; NEVELING, 1975). Entretanto, há uma interpretação mais profunda de que a informação não é apenas a transmissão da mensagem, mas é substrato para o conhecimento, ultrapassando a semântica do termo, pois, conforme Barreto (1994) adjetivam a informação como modificador da consciência e da sociedade como um todo, como estrutura significante com a competência de gerar conhecimento para o indivíduo e para o grupo.

Para Castells e Cardoso (2006) o conhecimento e a informação sempre foram centrais em todas as sociedades historicamente conhecidas, mas a comunicação em rede transcendeu fronteiras, pois a sociedade em rede é global, integrando capital, bens, serviços, comunicação, informação, ciência e tecnologia.

Essa perspectiva pode ser observada sob o prisma corporativo que se consubstancia na “sociedade da informação”, expressão que passa a ser utilizada em substituição ao conceito de “sociedade pós-industrial” e como forma de transmitir o conteúdo específico do novo paradigma técnico-econômico, no qual as organizações não têm mais como fator-chave os insumos baratos de energia, como na sociedade industrial, mas os insumos da informação, propiciados pelos avanços tecnológicos (WERTHEIN, 2000).

As tecnologias digitais mudaram a maneira de conexão entre empresas e seus clientes, ofertando uma nova proposta de valor e o grande desafio é converter a enorme quantidade de dados em informações valiosas (ROGERS, 2019), pois informações são coletadas, processadas, armazenadas e transmitidas em diferentes formatos, físicos, digitais ou verbais por organizações de todos os tipos e tamanhos, tanto do setor privado quanto do público (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b)

A informação é um recurso essencial para toda organização e é com ela que processos organizacionais funcionam, a geração de conhecimento acontece e o compartilhamento desse conhecimento é realizado, impulsionada com a utilização de tecnologia da informação. (GALEGALE; FONTES; GALEGALE, 2017).

Como ativo, a informação ultrapassa barreiras, o que é perceptível ainda em décadas passadas, ao observar por exemplo o trabalho de Alan Turing, considerado amplamente como o pai da ciência da computação e da inteligência artificial. Seu legado com a máquina de Turing foi amplamente difundido com a obra cinematográfica O Jogo da Imitação (THE IMITATION GAME, 2014), no qual descreve a informação como um ativo importantíssimo durante a Segunda Guerra Mundial, no qual Turing teve uma contribuição expressiva.

Dessa forma, há uma mudança na estratégia da era analógica para a digital, pois agora os dados e a informação são gerados continuamente em todos os lugares, tornando-se ativos intangíveis importantes para a geração de valor nas organizações com necessidade da criação de condições de organizar o dilúvio de dados não estruturados, fenômeno conhecido por *big data*, possibilitando que empresas possam descobrir novas fontes de valor.

Esse valor ultrapassa as palavras escritas, números e imagens: marcas, conceitos, ideias e conhecimento são informações intangíveis valorosas. Redes, sistemas, processos relacionados e pessoas envolvidas nas operações são informações que, junto com outros ativos importantes, têm valor para o negócio da organização e por consequência, requerem proteção contra inúmeros riscos (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b).

Surge com essa demanda, a necessidade de uma estruturação no controle desses ativos com um Sistema de Gestão da Segurança da Informação – SGSI e conforme Araujo (2018), a necessidade de investimento em um processo crescente de aculturamento em segurança da informação.

## 2.2 SEGURANÇA DA INFORMAÇÃO

A segurança da informação é uma área complexa do conhecimento, envolvendo inúmeras subáreas, o que permite uma diversidade de definições sobre este tema (ARAUJO, 2018). Da mesma forma, Marciano (2006) destaca o caráter interdisciplinar do instituto, evitando o reducionismo tecnológico sob o qual geralmente é apresentado. Ambos os autores apontam a interação entre a segurança e o contexto organizacional, interação esta que se manifesta sob as nuances da cultura organizacional e do comportamento individual.

Como a SI é uma vasta área, que envolve outros construtos teóricos como a privacidade da informação e a proteção de dados, – em evidência no cenário nacional, devido a atual vigência da LGPD, o que exige adequação das empresas à essa legislação – este tópico abordará à SI e seus pilares, dentre eles a PI, que envolve a PD.

Para Sêmola (2014), a segurança da informação é uma área do conhecimento que se dedica à proteção dos ativos da informação contra alterações indevidas ou sua indisponibilidade e acessos não autorizados. Netto e Silveira (2007) ainda contribuem com o estudo afirmando que, a segurança da informação visa a proteção da informação das ameaças e sua Confidencialidade, Integridade e Disponibilidade – CID, garantindo a continuidade dos negócios e minimizando riscos.

Nessa mesma linha, Beal (2005) destaca a proteção à CID, aspectos que Torres (2015) aponta serem comuns em todas as descrições dos conceitos relatados por diversos autores. Tais elementos não se constituem de mera coincidência, mas são pilares da SI, conforme Figura 1.

Figura 1 – Pilares da Segurança da Informação


Fonte: Adaptado da Internation Organization for Standardization – ISO 27000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2014), Netto e Silveira (2007), Beal (2005), Lyra (2008) e Sêmola (2014).

A **confidencialidade** é a garantia que somente pessoas autorizadas terão acesso à informação, protegendo-a de acordo com seu grau de sigilo, a **integridade** visa garantir a exatidão da informação e a **disponibilidade** garante aos autorizados o acesso sempre que precisarem (NETTO; SILVEIRA, 2007). Estes mesmos atributos são elencados na ISO 27000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2014).

Somando à CID, Sêmola (2014) acrescenta ainda a **legalidade** e a **autenticidade**, a primeira refere-se à garantia da conformidade com a lei e a segunda, que no processo de comunicação os remetentes sejam o que dizem ser e que, a mensagem não tenha sido alterada após o envio ou validação.

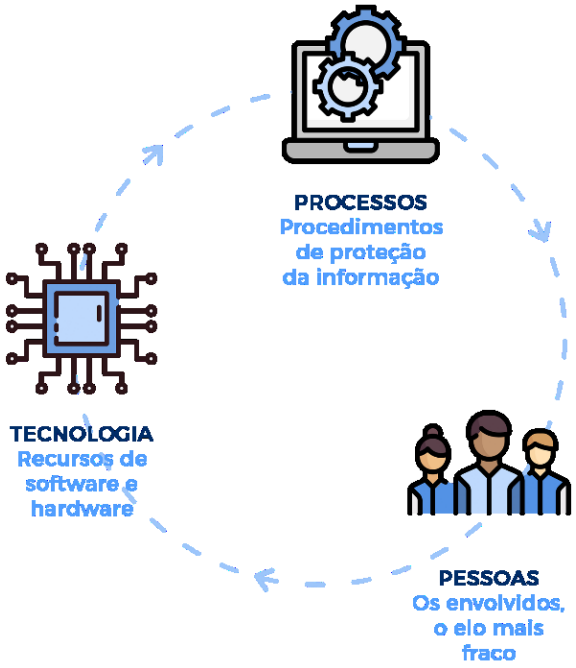
Torres (2015) contribui com mais três aspectos de garantia da Segurança da Informação, sendo eles: **não repúdio**, consistindo na capacidade que o sistema tem para provar que um usuário executou aquela ação; **privacidade**, que é a capacidade do sistema manter no anonimato o usuário; e **auditoria**, que é a capacidade do sistema auditar tudo que os usuários realizaram, detectando fraudes ou tentativas de ataques.

Como o objetivo deste trabalho envolve a cultura de segurança da informação, sob a ótica dos gestores da TI em instituições financeiras, é fundamental compreender a ligação da

Segurança da Informação com a Privacidade da Informação[2] em vários aspectos. Inicialmente, ao se buscar a conformidade da utilização da informação e sua legalidade, por consequência, surge a necessidade do estudo e adequação à LGPD[3], além da própria privacidade, aspecto que garante a SI e que é a essência da descrita lei, assegurando ao titular de um dado pessoal – DP[4] seu direito fundamental. Para Donda (2020), a SI e os seus pilares tem estrita ligação com a PI e a LGPD. Quando a organização tem controles de segurança e proteção em dia e um SGSI implementado facilita a adequação na LGPD.

Os princípios que fundamentam a Segurança da Informação abrangem três subdomínios (Figura 2), conforme descreve Araujo (2018): **tecnologia**, responsável pela implementação de recursos que envolvam *software* e *hardware*; **processos**, procedimentos aplicados à proteção da informação; e **pessoas**, pois o problema da Segurança da Informação não é simplesmente técnico-normativo e é preciso considerá-las em todos os processos. Principalmente, no âmbito dessa dissertação, em que o objetivo envolve a SI considerando nuances da cultura organizacional e do comportamento humano.

Figura 2 – Subdomínios da Segurança da Informação



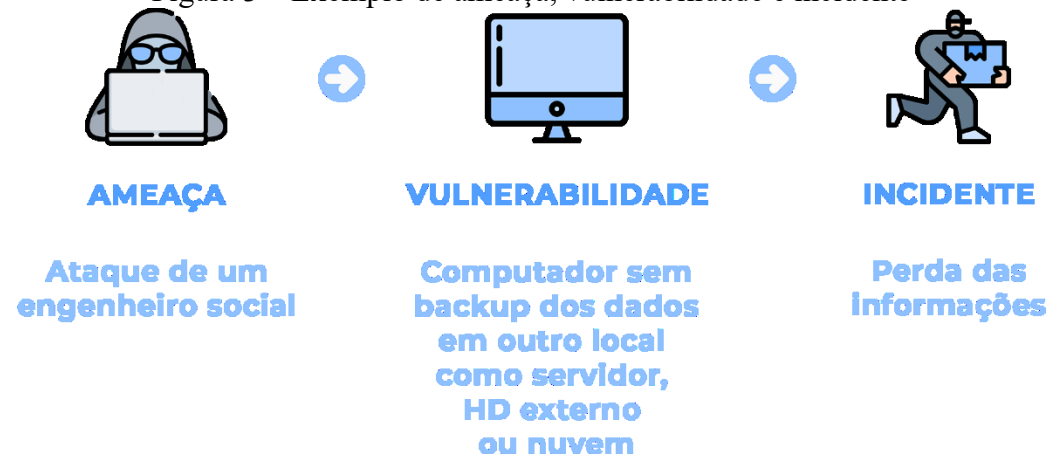

Fonte: Adaptado de Araujo (2018).

[2] Conceito que será abordado adiante.
[3] Legislação protetiva da privacidade de dados pessoais, conceitos que também serão abordados neste trabalho.
[4] Conforme a LGPD, titular de um dado pessoal é a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento (BRASIL, 2018).

Toda essa garantia visa assegurar um ativo importante para a instituição: as informações, que como outros ativos, estão sujeitas a diversos eventos e potencialidades nocivos a sua segurança (MARCIANO, 2006). Esses riscos, segundo a ISO 27000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2014) são efeitos da incerteza sobre os objetivos.

Schell (2001) afirma que não há como eliminar definitivamente os incidentes[5], restando apenas vigilância constante e verificação para trazer segurança contra esses ataques, que, segundo Marciano (2006), corresponde à concretização de uma ameaça[6], que pode ou não ser bem-sucedida (sob a ótica do atacante). Beal (2005) aponta que um ataque é um evento que decorre da exploração da vulnerabilidade[7] por uma ameaça e a ISO 27000 (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2014) conceitua ataque como uma tentativa de destruir, expor, alterar, desabilitar, roubar ou obter acesso não autorizado de um ativo.

Figura 3 – Exemplo de ameaça, vulnerabilidade e incidente




Fonte: Do autor

Na Figura 3, temos um indivíduo mal-intencionado que, utilizando de engenharia social[8], explorou uma vulnerabilidade e realizou um ataque no computador corporativo que não tinha backup das informações em outro dispositivo, tirando proveito dessa fragilidade. Dessa forma, o engenheiro obteve informações dos clientes da empresa, o que resultou em um

[5] Único ou uma série de eventos indesejados ou inesperados que tem significativa probabilidade de comprometer as operações (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2014).
[6] Causa potencial de um incidente indesejado que pode resultar em danos ao sistema ou à organização (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2014).
[7] Fraqueza de um ativo ou controle que pode ser explorado por uma ou mais ameaças (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2014).
[8] Conceito descrito nesse mesmo tópico, adiante.

incidente, pois não foi possível recuperar os dados, comprometendo as operações do usuário em sua empresa.

No caso, o risco é percebido na probabilidade de um engenheiro social furtar os dados dos computadores da instituição e nos efeitos da exploração das fragilidades e incertezas. Há várias formas de prevenir incidentes e minimizar vulnerabilidades, o que pode ser feito através do aperfeiçoamento de tecnologia, processos e pessoas.

O seriado britânico *Black Mirror,* disponível pelo *streaming* Netflix, ilustra inúmeras temáticas centradas nas imprevisibilidades das novas tecnologias, levando o observador a reflexões quanto às ameaças digitais e incidentes, como por exemplo, o que ocorre no episódio *Shut Up and Dance* (Manda Quem Pode) de 2016 (SHUT UP AND DANCE, 2016).

Nele, um garoto de dezenove anos tenta corrigir erros em seu computador infectado e acaba realizando o *download* de um *anti-malware*. Ocorre que o programa ativa a câmera do equipamento, gravando imagens de práticas obscenas. O material é coletado por *hackers* que passam a ameaçar e extorquir, prometendo divulgar as imagens caso o jovem não cumpra as exigências. O enredo demonstra que há outras vítimas dos engenheiros sociais que acabam participando da trama. Há uma desconforto ao assistir a obra que decorre da incapacidade de distinção realidade/ficção, onde o observador compreende claramente os riscos, as ameaças e as vulnerabilidades que está exposto no mundo digital, seja em seu ambiente pessoal ou profissional (SHUT UP AND DANCE, 2016).

Donda (2020), aponta que é necessário conhecer as ameaças para poder identificar os riscos e que a adoção de medidas certeiras decorre do conhecimento da existência de vulnerabilidades e ameaças. Inclusive, a adoção de medidas de segurança, técnicas e administrativas, para proteção de dados pessoais é matéria disciplinada pela LGPD, em seu artigo 46[9].

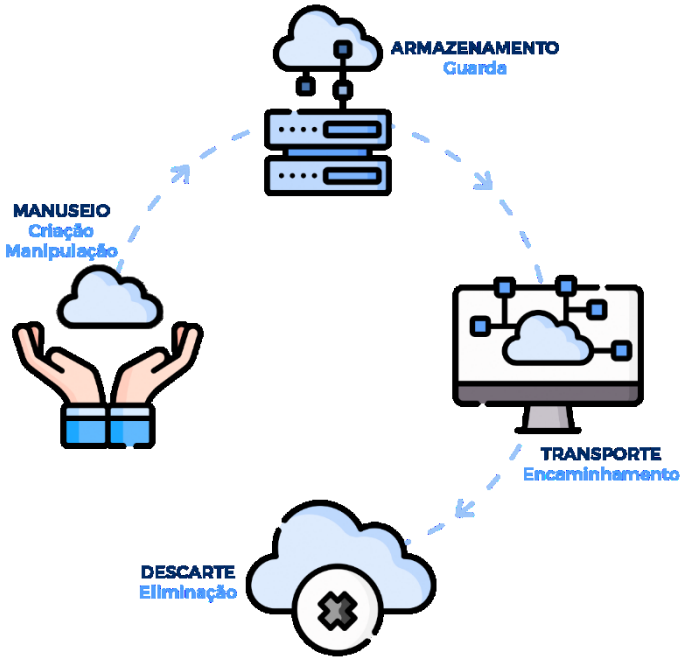
Nessa perspectiva, inserindo a frase "uma corrente é tão resistente quanto o seu elo mais fraco" no contexto da tríade supra descrita, os recursos computacionais chegaram em um nível de considerável acervo tecnológico, capaz de trazer proteção (MARCIANO, 2006), colocando as pessoas em um papel de destaque nessa fragilidade, inclusive no ambiente corporativo, em decorrência da cultura organizacional (o que abordaremos com maiores detalhes), claro, sem desconsiderar o risco em toda tríade.

---

[9] LGPD, artigo 46: Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

Nesse conjunto, Sêmola (2014) ensina que há momentos vividos pela informação que a colocam em risco, por isso estabelece um ciclo de vida quando ativos físicos, tecnológicos e humanos usam essa informação, o que sustenta processos e mantém a operação da empresa. O autor define etapas para o ciclo de vida da informação (Figura 4), sendo elas: **manuseio**, com a criação e manipulação; **armazenamento**, momento de guardar e armazenar; **transporte**, com o encaminhamento e transporte; e **descarte**, com eliminação e descarte.

Figura 4 – Ciclo de vida da informação




Fonte: Adaptado de Sêmola (2014).

Para Donda (2020), conhecer, entender e documentar o ciclo de vida dos dados na organização é vital para o desenvolvimento da adequação da empresa à LGPD, ressaltando que todo o processo envolve coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, processamento, distribuição, armazenamento, arquivamento, modificação e eliminação de dados.

Em todas essas etapas e sabendo que nelas há uma preocupação do risco quanto ao fator humano, muitos indivíduos agem de forma ilícita para obtenção de vantagens, utilizando na maioria das vezes da engenharia social, técnica que, segundo Asselstine (2018), é um mecanismo o qual agentes mal-intencionados utilizam para convencer um usuário a divulgar informações confidenciais.

Schneier (2004) aponta que a engenharia social não tem ênfase em criptografia, segurança do computador, segurança de rede e outros atributos tecnológicos, mas foca no que é o mais vulnerável e fraco: o ser humano. O mesmo autor descreve que para um invasor, informações em arquivos de papel são tão importantes quanto em arquivos digitais e que muitas vezes, o papel no lixo é mais valioso que os dados em computador. Dessa forma, uma organização que criptografa todos os dados digitais, mas não bloqueia seus arquivos físicos ou destrói seu lixo, está da mesma forma se expondo a ataques.

Esses ataques, muitas vezes, conseguem ser bem-sucedidos porque os agentes exploram comportamentos humanos e suas as vulnerabilidades (DAHBUR; BASHABSHEH; BASHABSHEH, 2017) e ocorrem porque um indivíduo respondeu de forma inadequada a um pedido de informações sigilosas (KOSTIC, 2020), afinal, os engenheiros sociais utilizam de sua sociabilidade para ganhar a confiança, fazendo com que o ataque não seja percebido como tal.

É como um estelionatário digital, um criminoso da quarta revolução industrial, em referência ao crime disposto no artigo 171[10] do Decreto-Lei Nº 2.848 de 1940 – Código Penal – CP, já que o engenheiro obtém vantagem ilícita induzindo ou mantendo a vítima em erro através de artifícios na *internet* (ou fora dela, às vezes usando-a como uma ferramenta em segundo plano).

De fácil propagação, difícil rastreio do invasor e geralmente de baixo custo, os ataques podem inclusive se dar na modalidade conhecida por engenharia social reversa, na qual o engenheiro insere uma isca que estimule a curiosidade da vítima e em uma segunda etapa, espera o contato, o que desperta maior atratividade e confiança por parte da vítima (IRANI *et al.*, 2005).

A engenharia social não é um termo predominantemente criado para a tecnologia, pois, segundo Hatfield (2018), a técnica já era utilizada para influências políticas desde os anos 1800, persuadindo a vítima com emoções e crenças, através do comportamento humano. A expansão do termo passou então a incluir elementos específicos da *internet* e dos dados (CONTEH; SCHMICK, 2016).

A mesma filosofia passou a contar com atributos técnicos da tecnologia para que o engenheiro social possa exercer sua influência através de toda rede mundial, aliando sociabilidade, confiança e comportamento humano a *internet, big data*, *nuvem*, *marktplace* e outras inúmeras plataformas digitais, como as redes sociais.

---

[10] CP, artigo 171: Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento (BRASIL, 1940).

Uma das formas de minimizar os riscos, inclusive os decorrentes de engenharia social, é implementando um SGSI, que é uma decisão estratégica para a organização e deve ser adequada às suas necessidades e objetivos, bem como pelos requisitos de segurança, pelos processos organizacionais, o tamanho e a estrutura, preservando a Confidencialidade, Integridade e Disponibilidade – CID das informações e fornecendo confiança para as partes interessadas de que os riscos são gerenciados (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a).

A promoção de uma cultura de SI também é preocupação da Organização para a Cooperação e Desenvolvimento Econômico - OCDE[11], que em 2002 adotou diretrizes com tópicos de preocupação e responsabilidade para todos os níveis de governo e negócio, envolvendo todos os integrantes, servindo como base para a participação e adoção de cultura de SI como forma de pensar, avaliar e atuar (OECD, 2002).

## 2.3 PRIVACIDADE DA INFORMAÇÃO

Enquanto a SI garante a CID das informações, protegendo um ativo importantíssimo para as instituições, a privacidade se ocupa em garantir proteção contra vigilâncias indesejáveis, ou seja, assegurar que terceiros não obtenham informações das quais o indivíduo quer manter apenas para si ou para destinatários escolhidos.

No contexto da sociedade da informação de Werthein (2000), ou da sociedade em rede de Castells (2000), em um intenso fluxo informacional, a privacidade ganha ainda mais relevância em uma base de dados total, como o *Big Brother* de George Orwell (ORWELL, 2021), o qual, através de tecnologias da informação, detém vigilância e controle sobre as pessoas. Tanto é que, conforme Matos, Torrado e Jachinto (2021), não é raro encontrar referências a Orwell e seu romance em estudos sobre a sociedade da informação, prova de que a literatura acompanha o pensamento sistemático da ciência.

Mas diferentemente do que ocorre em 1984[12], o Estado não pode ter um controle totalitário sobre os indivíduos de forma que a privacidade seja instrumento de poder e controle absoluto. É exatamente nesse bojo que reside a necessidade de um direito positivado, formal e que garanta a dignidade da pessoa humana.

---

[11] Os nove princípios estão destacados na discussão dos resultados, pois o instrumento de Araujo (2018) utilizado para a coleta de dados nas instituições financeiras é fundamentado nessas diretrizes.

[12] Título da obra de George Orwell, na qual é apresentado o personagem *Big Brother* (ORWELL, 2021).

Nesse contexto jurídico, a privacidade é um direito e garantia fundamental e está esculpida no artigo 5º da Constituição Federal da República Federativa do Brasil de 1989 – CF, no inciso X, assegurando ao indivíduo a inviolabilidade da sua intimidade e vida privada, além da honra e da imagem, permitindo a indenização pelos danos materiais ou morais decorrentes da sua violação (BRASIL, 1988), ou seja, conforme Franca e Farias (2017), há relação com os esses direitos e a privacidade, ainda que ela não seja taxativa na norma constitucional.

A Lei Nº 10.406 de 2002 – Código Civil – CC assegura em seu artigo 21[13] a vida privada como inviolável, permitindo a adoção de providências para impedir ou fazer cessar atos que atentem este direito (BRASIL, 2002).

Especificamente, o termo privacidade não é encontrado nesses dois diplomas legais, entretanto, Machado (2014) explica que a utilização pelo legislador constituinte dos termos "vida privada" e "intimidade" traz a problemática de valorar de forma distinta os dois temas.

Zanini (2020) aponta o estudo de Hubmann (1967) das esferas de proteção da vida (Figura 5), abrangendo os valores próprios da personalidade, reconhecendo a existência de três, a da vida individual (mais exterior e menos protegida), a da vida secreta (mais interior e tutelada) e um entre essas duas, a da vida privada, representadas da seguinte forma:

Figura 5 – Círculos Concêntricos de Hubmann (1967)


Fonte: Adaptado de Hubmann (1967) e Zanini (2020).

Doneda (2006) explica que o legislador pode ter optado por uma terminologia ampla, temendo por reduzir a aplicabilidade da norma, o que pode ter decorrido da ausência de determinações na doutrina e na jurisprudência. Independentemente, Machado (MACHADO,

[13] CC, artigo 21: A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

2014) esclarece que o objetivo de todas essas expressões são tutelar a pessoa humana da forma mais ampla possível.

Na esfera supralegal, a privacidade está assegurada pela Declaração Universal dos Direitos Humanos de 1948 – DUDH, através do artigo 12[14], assegurando ao indivíduo a não interferência em sua vida privada, da família, do lar e de sua correspondência, enquadrando-o na categoria de direitos humanos (ORGANIZAÇÃO DAS NAÇÕES UNIDAS, 1948).

A interpretação ampla da privacidade percorre um lapso temporal de extensão de direitos, até chegar a atual abrangência da privacidade para a tecnologia da informação. Exemplo disso é o que descrevem Warren e Brandeis (1890) em estudo que aponta a evolução de direitos fundamentais em termos de abrangência, inclusive para a proteção intelectual e não somente à vida, mas de aproveitar a vida, o que os levou formalizar o termo "ser deixado em paz" como um conceito de privacidade, ou seja, ter controle das informações ligadas à esfera íntima e pessoal, o que Doneda (2000) considera como a garantia de isolamento e solidão.

A ideia descrita pelos autores supracitados remete ao direito ao esquecimento, o qual, conforme apontam Lopes e Lopes (2015), estabelece o direito de ser esquecido eternamente por um fato pretérito ou por situações que possam trazer prejuízos.

É como se a privacidade percorresse a barreira temporal e estabelecesse limites a publicidade de fatos que poderiam trazer prejuízos ao indivíduo, tais como situações vexatórias, tanto na esfera cível, quanto criminal. Nesta, pode-se citar o direto de alguém, condenado ou não por determinado crime, ter seu passado escondido nas entranhas apenas do seu próprio consciente e não de toda a população, até mesmo porque a publicidade de tais fatos prejudica sua honra, imagem e privacidade e a pena tem uma extensão aquém do previsto na legislação penal.

Exemplo disso, o caso *The Red Kimono*, título da obra cinematográfica que retratou a vida pretérita de Melvin, inclusive, sem alterar o nome da personagem, o que estaria provocando danos ao discorrer sobre seu passado como prostitua e ao relatar sua acusação de homicídio, na qual foi inocentada em 1918. Dessa forma, em "novo estilo de vida", Melvin não desejava ser reconhecida dessa forma e buscou o Judiciário americano para ter reconhecido o direito ao esquecimento, sendo-lhe deferido o pedido, mas sob a fundamentação de garantia da felicidade. Quanto ao esquecimento, a Justiça limitou-se a declarar que os registros públicos de

[14] DUDH, artigo 12: Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques.

incidentes são suficientes negar a ideia de afronta à privacidade, e para isso, bastava que a produtora da obra não identificasse a autora da demanda (ESTADOS UNIDOS DA AMÉRICA, 1931).

Encontra-se nesse tema, um conflito de direitos, pois a população pode (e deve) estar informada pela mídia, direitos esculpidos na CF[15] (TEFFÉ; BARLETTA, 2016) o que sugere a problemática: qual o limite da publicidade dos fatos em termos temporais?

Franca e Farias (2017) apontam que conceitos iniciais sobre privacidade remontam à queda do sistema feudal, junto às transformações sociais, econômicas e políticas da Revolução Industrial do final do século XVIII na Europa. A privacidade, nessa seara, era um privilégio e não um direito, pois apenas as classes com alto poder econômico (senhores feudais e membros da Igreja) tinham condições de isolar-se em suas próprias casas.

Com o advento de ferramentas que facilitavam a publicidade, como o jornal impresso e a fotografia, bem como a ascensão da burguesia e o início das grandes concentrações urbanas, a privacidade ruma à direção de um valor existencial, como relatado por Warren e Brandeis (1890). O primeiro desses autores, conforme Franca e Farias (2017), foi motivado pela divulgação de fotos pessoais de sua família sem autorização, o que acabou por estimulá-lo a propor que a privacidade fosse tutelada pelo ordenamento jurídico norte-americano, à exemplo do que já acontecia com os direitos autorais.

O direito ao esquecimento foi inclusive matéria julgada com repercussão geral[16] reconhecida pelo Supremo Tribunal Federal – STF[17] durante a elaboração deste trabalho. A tese é no sentido de ser incompatível com a CF a ideia de um direito ao esquecimento entendido como o poder de obstar pela passagem do tempo a divulgação de fatos já publicados em meios de comunicação social, entretanto, excessos ou abusos na liberdade de expressão e de

[15] CF, artigo 5º, inciso IV: é livre a manifestação do pensamento, sendo vedado o anonimato; IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; XIV - é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional; XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (BRASIL, 1988).

[16] Em termos jurídicos, repercussão geral é ter relevância que ultrapasse interesses apenas das partes do processo, como está descrito no parágrafo primeiro do artigo 1.035 da Lei 13.105 de 2015 – Código de Processo Civil – CPC: artigo 1.035: O Supremo Tribunal Federal, em decisão irrecorrível, não conhecerá do recurso extraordinário quando a questão constitucional nele versada não tiver repercussão geral, nos termos deste artigo. § 1º Para efeito de repercussão geral, será considerada a existência ou não de questões relevantes do ponto de vista econômico, político, social ou jurídico que ultrapassem os interesses subjetivos do processo (BRASIL, 2015).

[17] Recurso Extraordinário – RE 1010606 do STF.

informação devem ser avaliados caso a caso, principalmente quando dizem respeito à proteção da honra, da imagem, da privacidade e da personalidade (BRASIL, 2021).

A ideia da privacidade, contudo, não pode ser encarada apenas como o direito de estar só, precisa estar alinhada ao contexto da sociedade da informação (ou em rede), descrito por Castells, ou seja, a transformação social do novo paradigma tecnológico iniciado nos anos de 1960, onde a tecnologia é a própria sociedade (CASTELLS; CARDOSO, 2006). Em consonância a este conceito, a privacidade precisa ser analisada sob a ótica de um direito à autodeterminação afirmativa (BAIÃO; GONÇALVES, 2014).

As organizações enfrentam, portanto, um grande desafio: preservar direitos de privacidade e liberdade civis no universo de *Big Data*. A incorporação de medidas e ações de boas práticas, conhecidas pelo que Cavoukian chamou de *Privacy by Design - PbD*, contribuem para aprimorar as proteções de privacidade, e ao mesmo tempo, preservar a funcionalidade de sistemas analíticos em *Big Data*. A privacidade do consumidor não se trata apenas de conformidade, mas de imperativo comercial e é por isso que a *PbD* e práticas de inovação responsáveis podem garantir que esse universo de informações mantenha um mercado no qual privacidade e liberdades civis prevaleçam (CAVOUKIAN; JONAS, 2012).

A privacidade deve ser construída no projeto e operação, não apenas na tecnologia, ou seja, processos de trabalho, estruturas de gerenciamento, espaços físicos e infraestrutura de rede. Para isso, a *PbD* deve ser introduzida em todas as etapas, durante o planejamento da arquitetura, no projeto do sistema, no procedimento operacional e deve estar enraizada no código com padrões que alinhem a privacidade e os imperativos do negócio. Reconhecida internacionalmente como um padrão para desenvolver sistemas de informação compatíveis com a privacidade, a *PbD* tem seu foco em processos ao invés de uma atenção singular direcionada a resultados tecnológicos (CAVOUKIAN; JONAS, 2012).

Há uma compreensão crescente de que a privacidade deve ser abordada através de uma perspectiva de *design-thinking*, ou seja, uma forma de ver o mundo e superar restrições que seja holística, interdisciplinar, integrativa, inovadora e inspiradora, devendo ser parte integrante das prioridades organizacionais, por isso, Cavoukian descreveu sete princípios básicos de *PbD* que devem ser implementados em padrões, protocolos e processos (CAVOUKIAN, 2010), conforme Quadro 2.

Quadro 2 – Princípios básicos de *Privacy by Design*

| |
|---|
| **Proativo não reativo; preventivo não corretivo** |
| Definição: antecipação de práticas para evitar eventos invasivos antes que aconteçam. Não aguardar os riscos se materializarem, evitando que ocorram, ou seja, vem antes do fato, não depois. |
| Boas Práticas: |
| Aplicação a tecnologias de *informação, práticas* organizacionais, design físico ou ecossistemas de informação em rede. |
| Reconhecimento explícito do valor e benefícios de boas práticas, de forma precoce e persistente. |
| Compromisso de definir e aplicar altos padrões de privacidade, superior aos estabelecidos pelas leis e regulamentos. |
| Compartilhamento comprovado com todas as partes envolvidas e pela comunidade de usuários, sempre em uma cultura de melhoria contínua. |
| Operar com métodos estabelecidos para reconhecer projetos de baixa privacidade. |
| **Privacidade como configuração padrão** |
| Definição: máximo grau de privacidade, garantindo que os dados pessoais sejam protegidos automaticamente em qualquer sistema de TI ou nas práticas do negócio. Mesmo com a inércia do indivíduo, a privacidade permanece intacta, ou seja, não é necessária nenhuma ação do titular para a proteção de seus dados, tudo isso integrado ao sistema, por padrão. |
| Boas Práticas: |
| As finalidades para as quais as informações pessoais são tratadas devem ser comunicadas ao titular dos dados antes ou no momento da coleta. Os objetivos especificados devem ser claros, limitados e relevantes às circunstâncias. |
| Coleta de informações pessoais justa, lícita e limitada ao necessário para o fim especificado. |
| A coleta de dados pessoais deve ser mantida em um mínimo estrito.<br>Sempre que possível, a identificação, a capacidade de observação e a vinculação das informações pessoais devem ser minimizadas. |
| Limitação de uso, retenção e divulgação de dados pessoais aos fins relevantes para o indivíduo, para os quais ele consentiu, devendo serem descartados após o cumprimento do objetivo declarado.<br>Na obscuridade da necessidade ou do uso de informações, deve existir uma presunção de privacidade, aplicando o princípio da precaução. |
| **Privacidade incorporada ao design** |
| Definição: está na essência do design, da arquitetura dos sistemas de TI e das práticas de negócio. É essencial e não um complemento. É parte integral do sistema, sem diminuir a funcionalidade. |
| Boas Práticas: |
| Incorporação às tecnologias, operações e arquiteturas de informação de maneira holística, integrativa e criativa. |
| Adoção de uma abordagem sistêmica e baseada em princípios para incorporação da privacidade. |
| Avaliação de impactos e riscos, com as devidas documentações. |
| Minimização de impactos de privacidade da tecnologia ou arquitetura de informação. |
| **Funcionalidade total** |
| Definição: acomodação de todos os interesses e objetivos legítimos para a construção de ganho coletivo, de soma "ganha-ganha", sem compensações desnecessárias, evitando a dicotômica privacidade x segurança, demonstrando a possibilidade de ter as duas. |
| Boas Práticas: |
| Satisfação de todos os objetivos da organização, não apenas o de privacidade, permitindo resultados reais, práticos e benéficos para todas as partes envolvidas. |
| A realização da funcionalidade total sem prejuízos na incorporação da privacidade na tecnologia, processo ou sistema. |
| Rejeição da abordagem soma zero e da competição com outros interesses legítimos, abraçando objetivos de maneira inovadora de soma positiva. |
| Documentação de interesses e objetivos, articulação de funções, métricas acordadas e aplicadas e a rejeição de trocas de problemas por outros problemas, encontrando a solução que permita a multifuncionalidade. |
| Criatividade e inovação na realização de todos os objetivos e funcionalidades de forma integrativa e de soma positiva e o alcance de liderança global de primeira classe em privacidade (padrão ouro). |
| **Segurança de ponta a ponta - Proteção total do ciclo de vida** |
| Definição: incorporação ao sistema da *PbD* que antecede a coleta do primeiro dado pessoal e extensão, com segurança, por todo o ciclo de vida, do início ao fim, permitindo o gerenciamento seguro do ciclo de vida, de ponta a ponta. |

| Boas Práticas: |
|---|
| Inexistência de lacunas na proteção ou na responsabilidade, sem segurança forte não há privacidade. |
| Autorresponsabilidade das instituições pela segurança das informações ao longo de todo o ciclo de vida. |
| Garantia da CID em todo o ciclo de vida, incluindo, métodos de destruição segura, criptografia apropriada, forte controle de acesso e métodos de registro. |
| **Visibilidade e transparência** |
| Definição: *PbD* visa garantir aos interessados que ela está operando de acordo com o prometido e os objetivos declarados, sujeita a verificação independente. Componentes e operações são visíveis e transparentes, tanto para usuários quanto para provedores. |
| Boas Práticas: |
| Responsabilidade – zelo pela proteção na coleta de informações pessoais, documentando e comunicando os procedimentos, conforme apropriado. Assegurar proteção aos dados equivalente à contratual (ou outros meios) quando compartilhado com terceiros. |
| Abertura – pronta disponibilização aos indivíduos das políticas e práticas relacionadas ao gerenciamento de informações pessoais. |
| Conformidade – adoção de medidas necessárias par monitorar, avaliar e verificar a conformidade com as políticas e procedimentos de privacidade. |
| **Respeito pela privacidade do usuário** |
| Definição: manutenção, pelos arquitetos e operadores, dos interesses do indivíduo em primeiro lugar, com o oferecimento de medidas e fortes padrões de privacidade, notificação apropriada e opções amigáveis ao usuário. |
| Boas Práticas: |
| Conceder aos titulares de dados um papel ativo na gestão de suas próprias informações, permitindo eficácia contra abusos da privacidade. |
| Necessidade de consentimento livre e específico para a coleta, uso ou divulgação de informações pessoais, com a possibilidade de revogação. |
| Informações claras e precisas, completas e atualizadas quanto ao cumprimento dos propósitos especificados. |
| Acesso pelos titulares de dados às suas informações, usos e divulgações, podendo contestar a exatidão e a integridade das informações, fazendo com que sejam corrigidas conforme apropriado. |
| Estabelecimento de mecanismos de reclamação e reparação, comunicando informações sobre eles ao público, inclusive como acessar o próximo nível de recurso. |
| Necessidade de interface homem-máquina centrada no homem, amigáveis ao usuário, assim como as operações de negócio e arquiteturas físicas demonstrando o mesmo grau de consideração pelo indivíduo. |

Fonte: Adaptado de Cavoukian (2010).

Métodos como *PbD* são fundamentais no contexto da sociedade da informação. Machado (2014) destaca que afrontas à privacidade passam a ser proporcionais aos avanços tecnológicos e ao desenvolvimento de tecnologias da informação e comunicação quando as informações pessoais são transmitidas a terceiros sem o conhecimento e a autorização do seu titular. O entrelace da privacidade no contexto da informação pode ser compreendido com a definição concebida por Rodotá (2008) como o direito de manter o controle sobre suas próprias informações, bem como determinar a maneira de construir sua própria esfera particular.

É possível extrair desse conceito a proteção da privacidade em face de terceiros, até mesmo do próprio Estado, o que, conforme Franca e Farias (2017), alcança toda a sociedade e auxilia e é auxiliado por outros direitos fundamentais, como a inviolabilidade de domicílio e correspondência, o sigilo das comunicações e a dignidade da pessoa humana, o que confere a sua identidade como direito da personalidade.

Baião e Gonçalves (2014) apontam que o direito à privacidade da informação é uma nova forma de liberdade pessoal que mergulha além da superficialidade da liberdade negativa de recusar ou proibir a utilização de dados pessoais, transformando-se em liberdade positiva de controlar os dados concernentes à própria pessoa.[18]

Retirar a privacidade inerente ao indivíduo mostra-se completamente dissociada de um Estado Democrático de Direito com garantias fundamentais, não podendo ela ser objeto de privação, ou o cacofônico "privar a privacidade", sem que haja regra legal.

As garantias historicamente conquistadas no tocante à temática até a sua evolução em uma norma legal, com o consequente regramento que minimiza, ou autoriza, a utilização de dados pessoais, seja pelo consentimento ou por outra razão, leva a compreensão do status de liberdade que o tema ganha. Para Doneda (2011) e Mañas (2005) a norma parecia estar apenas destinada a mudar determinado patamar tecnológico, mas veio formar bases como um direito fundamental à proteção de dados.

Tanto é que, o cinema muito bem retrata a pauta quando ilustra a hipotética situação da retirada da privacidade como mecanismo de aplicação penal, através do episódio *White Bear*, 2013 (Urso Branco), do seriado *Black Mirror*, disponível na Netflix (WHITE BEAR, 2013).

Ao acordar com amnésia, uma mulher percebe que as pessoas na rua a filmam incansavelmente e ao tentar contato, é ignorada. Essas pessoas estariam afetadas por um sinal que apareceu em suas telas e aqueles que não foram, tornaram-se caçadores que agem de maneira sádica, tentando matá-la. A única esperança é, junto com outro que ainda mantém total consciência, destruir um transmissor que cessaria o estado mental pelo qual passam a maioria das pessoas, que as faz simplesmente não responder e apenas filmar os acontecimentos desagradáveis pelos quais a personagem passa, vendo-a em extremo sofrimento psíquico ao lutar por sua vida, ignorando-a com indiferença quanto a possibilidade iminente de sua morte (WHITE BEAR, 2013).

Ao chegar nas instalações do transmissor, a personagem finalmente descobre que se trata de uma encenação recheada de atores. A verdade é que ela foi condenada pelo assassinato brutal de uma criança e sua pena consiste em diariamente sofrer abusos em sua privacidade, tornando-se um espetáculo do Parque *White Bear,* ao estilo *reality show,* onde os espectadores podem participar filmando e vendo-a diariamente passar por um procedimento extremamente

[18] Ideia ligada à autodeterminação afirmativa, na qual o sujeito tem pleno controle sobre seus dados, quanto a extensão, forma, tempo e consentimento na utilização deles por terceiros.

doloroso de apagar suas memórias e novamente, dia após dia, pagar sua pena (WHITE BEAR, 2013).

Este exemplo, ainda que em universo de ficção quanto a utilização da privacidade como mecanismo de cumprimento de pena na esfera criminal, mostra como a temática é relevante e necessita de regramentos, inclusive de informações do indivíduo consideradas sensíveis no mundo de transformação digital (que engloba a *big data*), o que culminou com a promulgação da LGPD, dispondo sobre o tratamento de dados pessoais, inclusive em meios digitais, por pessoas naturais[19] e jurídicas, protegendo os direitos fundamentais de liberdade e privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

## 2.4 PROTEÇÃO DE DADOS

Quase um século separa o início de uma legislação positivada para a proteção de dados, na Alemanha e as primeiras noções jurídicas sobre a necessidade de proteção de informações e privacidade de Warren e Brandeis (1890). Durante este período, várias nações evoluíram o debate e a consequente necessidade de se regulamentar o instituto. Passa-se atualmente à evolução normativa que culminou com a Lei Geral de Proteção de Dados no Brasil, em 2018.

Até a sua promulgação, o histórico da temática remonta ao estado germânico de Hesse, onde em 1970, entrava em vigor a mais antiga lei de proteção de dados do mundo, o Ato de Proteção de Dados para a administração pública. Em resumo, a legislação permitia o processamento de dados pelo ente público. Sete anos mais tarde, foi aprovada uma lei nacional sobre o tema, a *Bundesdatenschutzgesetz* (Lei Federal de Proteção de Dados), com forte embasamento no que já existia sobre sigilo médico, confessional e postal, posteriormente substituída pela Lei de Proteção de Dados Hessiana, em 1978, que incluiu a dependência do consentimento do titular de dados (LAMBOY, 2019).

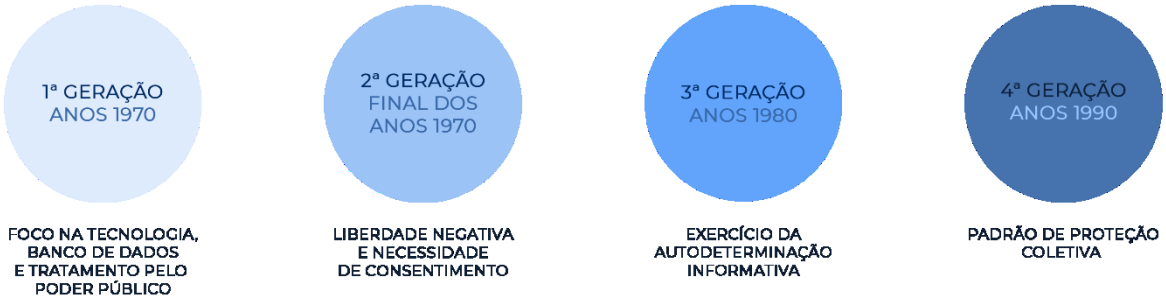
Em 1978 a lei de proteção de dados Hessiana substitui a antiga normativa de 1970 e estabelece que o processamento de dados pessoais também estaria sujeito à lei e seria necessário o consentimento da pessoa em questão. Já em 1987, depois de uma decisão do Tribunal Constitucional Federal da Alemanha, o estado de Hesse alterou a norma para garantir a autodeterminação informacional (LAMBOY, 2019).

[19] Popularmente conhecidas por pessoas físicas.

Doneda (2011) e Mayer-Scönberger (1997) apontam que as primeiras leis de proteção de dados não demoraram a ficar ultrapassadas, diante da multiplicação dos centros de processamento de dados e, no final da década de 1970, têm-se como primeiro grande exemplo de uma segunda geração a Lei Francesa de Proteção de Dados Pessoais de 1978 (Informatique et Libertées), além da *Bundesdatenschutzgesetz*, atualizada para comportar o consentimento como sendo fundamental. A diferenciação dessas duas primeiras gerações está que a estrutura passa a não mais estar fixadas em torno do fenômeno computacional, mas em considerar a liberdade negativa, exercida pelo próprio cidadão.

Uma terceira geração de leis surge então em 1980, garantindo além da liberdade de fornecer ou não os próprios dados pessoais, também a efetividade dessa liberdade, ou seja, decidir livremente, proporcionando o exercício da autodeterminação informativa. Entretanto, esta liberdade era um privilegia da minoria que decidia enfrentar os custos econômicos e sociais do exercício dessas prerrogativas, surgindo a quarta geração, com enfoque no problema integral da informação e instrumentos de padrão coletivo de proteção, reconhecendo o desiquilíbrio entre entidades que coletam e processam dados e os titulares (DONEDA, 2011; MAYER-SCHÖNBERGER, 1997). Essas gerações são apresentadas na Figura 6.

Figura 6 – Gerações da legislação de proteção e privacidade de dados




Fonte: Adaptado de Doneda (2011) e Mayer-Scönberger (1997).

Segundo Garcia et al. (2020), a autodeterminação informativa[20] é a possibilidade da pessoa natural determinar como suas informações podem ser e se serão utilizadas, é o direito de decidir o que será feito delas, quais dados a organização possui a respeito do titular, como são utilizados e se deseja manter ou não os dados com a instituição.

Rodotá (2008) aponta que a autodeterminação informativa engloba o poder de controle das próprias informações, e escolher o que será revelado e de esquecer o que não se quer mais

[20] O instituto foi incorporado pela LGPD no seu artigo 2º. A temática dos fundamentos da legislação é tratada a seguir, neste trabalho.

lembrar, determinando a maneira de construir a própria esfera particular, consistindo no mais expressivo direito fundamental da condição humana contemporânea e contribuindo para a constitucionalização da pessoa.

Em 1995 foi adotada uma diretiva europeia (Diretiva 95/46/CE) relativa à proteção de dados de pessoais, ainda sem força de lei para os Estados membros. Novas diretrizes sucederam o tema, como a Diretiva 02/58/CE de 2002, estabelecendo novos padrões para a proteção de dados no setor das comunicações, seguida pela Diretiva 09/136/CE, sobre *cookies*. Em 2014, o parlamento europeu apresentou uma proposta de regulamento geral relativo à proteção de dados, que entrou em vigor em 2016 e após dois anos transitórios, a *General Data Protection Regulation* – GDPR (Regulamento Geral de Proteção de Dados – RGPD) entra em vigor em 25 de maio de 2018 aos Estados-Membros da União Europeia (EUROPEAN UNION, 2016; LAMBOY, 2019).

A GDPR, considerando o contexto econômico, ocasionou um "efeito dominó", diante da sua exigência de que outros países possuíssem legislações de proteção de dados no mesmo nível, sob possibilidade de sofrerem barreiras econômicas e de mercado internacional, tornando-se o padrão mundial, quase que como uma norma ISO, no tocante a esta temática (PINHEIRO, 2020).

A proteção de dados e a privacidade, em termos de legislação do Brasil, podem ser encontrada também no artigo 5º, inciso X e XI da CF[21]; artigo 43 da Lei Nº 8.078 de 1990 – Código de Defesa do Consumidor – CDC[22]; artigo 3º da Lei 12.414 de 2011 – Lei do Cadastro Positivo – LCP[23]; artigo 4º e 31 da Lei 12.527 de 2011 – Lei de Acesso à Informação – LAI[24];

---

[21] CF, artigo 5º: Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XI - a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial (BRASIL, 1988).

[22] CDC, artigo 43: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes (BRASIL, 1990).

[23] LCP, artigo 3º: Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei (BRASIL, 2011a).

[24] LAI, artigo 4º: Para os efeitos desta Lei, considera-se: I - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato; II - documento: unidade de registro de informações, qualquer que seja o suporte ou formato; III - informação sigilosa: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado; IV - informação pessoal: aquela relacionada à pessoa natural identificada ou identificável; V - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação; VI - disponibilidade: qualidade

artigo 3º, incisos II e III e artigo 7º, incisos I, II e III, VII, VIII, IX e X da Lei 12.965 de 2014 – Marco Civil da Internet – MCI[25] (DONEDA, 2017).

Nesse contexto e sob influência da GDPR, mas sem prejuízo de outras referências internacionais e até mesmo do que já se aplicada no ordenamento pátrio, o Brasil promulgou a LGPD em 2018, com vigência para 2020[26] (MIRAGEM, 2019). Dessa forma, a regulamentação brasileira harmoniza um ecossistema de normas setoriais que já existiam de forma esparsa, apresentando-as e complementando-as de forma a conferir às pessoas, maior controle sobre seus dados pessoais e também fomentar um ambiente de desenvolvimento econômico e tecnológico (MONTEIRO, 2018).

Percebe-se que a proteção dos dados na LGDP é uma projeção de direitos fundamentais, relacionando-se com a proteção à vida privada e a intimidade (artigo 5º, inciso X da CF[27]), a dignidade da pessoa humana (artigo 1º, inciso III da CF[28]) e contra a discriminação, como expressões da liberdade e da igualdade (artigo 3º, inciso IV da CF[29])[30],

---

da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados; VII - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema; VIII - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino; IX - primariedade: qualidade da informação coletada na fonte, com o máximo de detalhamento possível, sem modificações; artigo 31: O tratamento das informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais (BRASIL, 2011b).

[25] MCI, artigo 3º: A disciplina do uso da internet no Brasil tem os seguintes princípios: II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; artigo 7º: O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei; VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que: a) justifiquem sua coleta; b) não sejam vedadas pela legislação; e c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet; IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei (BRASIL, 2014).

[26] Destaca-se as alterações dadas pela Lei 13.853 de 2019 e Lei nº 14.010 de 2020, que alteraram a vigência de itens específicos da LGPD, por conta do estado de calamidade pública e tempo hábil para adequação das empresas à normativa (BRASIL, 2018).

[27] CF, artigo 5º, inciso X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

[28] CF, artigo 1º: A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: III - a dignidade da pessoa humana (BRASIL, 1988).

[29] CF, artigo 3º Constituem objetivos fundamentais da República Federativa do Brasil: IV - promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação (BRASIL, 1988).

[30] A privacidade e os direitos fundamentais também foram abordados no tópico anterior.

além de ser uma recepção da autodeterminação informativa (uma evolução normativa da privacidade), inserida como um dos fundamentos da lei, já que o consentimento para coleta e uso de dados passa a ser a regra (MIRAGEM, 2019).

Durante a produção desta dissertação, havia uma Proposta de Emenda à Constituição - PEC em tramitação no legislativo federal, a PEC 17/2019, que objetiva incluir a proteção de dados pessoais entre os direitos e garantias fundamentais, além de fixar a competência legislativa privativa da União sobre o tema (BRASIL, 2018).

Esses direitos fundamentais estão expostos de forma taxativa no artigo 1º da LGPD[31], que de forma cristalina descreve a proteção da liberdade, da privacidade e do livre desenvolvimento da personalidade (BRASIL, 2018).

Para fundamentar a proteção de dados, a legislação elenca oito aspectos, em seu artigo 2º, exemplificados na Figura 7:

Figura 7 – Fundamentos da proteção de dados pessoais


Fonte: Adaptado de Brasil (2018).

[31] LGPD, artigo 1º: Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Para Garcia et al. (2020), esses fundamentos não podem ser “perdidos de vista” ao interpretar a legislação, dado seu cunho constitucional, já que todos os de caráter individual estão previstos na CF e os endereçados à sociedade e ao desenvolvimento nacional (desenvolvimento econômico e tecnológico e a inovação; a livre iniciativa, a livre concorrência e a defesa do consumidor) reconhecem a importância dos dados na sociedade da informação e do conhecimento, pois o dado é capaz de contribuir para a tomada de decisões sociais, políticas e econômicas.

A legislação conceitua o que é objeto de sua proteção: os dados pessoais, como informações relacionadas a pessoa natural identificada ou identificável. Além disso, ainda define que são sensíveis as informações sobre origem racial, convicção religiosa, opinião política, dados referentes à saúde e a vida sexual, entre outros (PINHEIRO, 2020).

Para tanto, é necessário observar o princípio norteador da norma, a boa-fé, juntamente com dez grandes princípios: finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas (BRASIL, 2018).

Esses princípios corroboram com as necessidades para a preservação do direito à privacidade, englobando os seus vários contextos e conceitos, desde o direito de estar isolado, só, sem interferências, até a autodeterminação informativa, resguardando a vontade de que ninguém obtenha dados dos quais o titular quer manter somente para si.

Em outro cenário, os princípios norteiam ações e práticas para que os dados pessoais sejam utilizados apenas para a finalidade que se propõem, resguardando sua privacidade, não podendo aquele que detém uma informação (para um determinado fim, ou até mesmo de forma ilícita), possa usá-la com fins mercantis sem consentimento do titular ou até mesmo de forma maliciosa, como fazem os engenheiros sociais.

Pinheiro (2020) aponta que a linha mestra para o tratamento de dados pessoais é o consentimento, que é a livre manifestação da concordância com o tratamento para aquela finalidade determinada, mas que há situações de exceção que não necessitam de consentimento expresso e, ao mesmo tempo, as empresas devem ter a liberdade de utilizar os dados de maneira transparente e ética, em troca de um serviço ou acesso, pois a legislação assegura o desenvolvimento econômico a esses sujeitos, utilizando os dados sempre de forma legítima.

Donda (2020) também destaca que o consentimento é provavelmente a base legal[32] que mais será utilizada e que as informações sobre o tratamento de dados devem ser claras e não podem deixar nenhuma dúvida, além de não permitir o vício de consentimento, pois qualquer tratamento sem uma das bases legais é ilícito e cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com a lei. Garcia et al. (2020) e Leite e Machado (2019) apontam que o consentimento não é a única hipótese, embora seja a regra.

Apesar de, segundo os autores acima, o consentimento ser a mais usual hipótese para o tratamento de dados, ele pode ser retirado a qualquer instante pelo titular de dados, conforme expressamente consta na LGPD[33] (BRASIL, 2018), de forma facilitada e gratuita. Kiss e Szőke (2015) apontam que o consentimento ter se tornado questão fundamental no tratamento de dados se deve ao fato do titular estar no controle do uso deles, ou seja, há estrita ligação com a autodeterminação informativa.

Todas as hipóteses de tratamento de dados pessoais estão descritas no artigo 7º da LGPD: consentimento; cumprimento de obrigação legal; tratamento e uso compartilhado de dados necessários à execução de políticas públicas, pela administração pública; realização de estudos por órgãos de pesquisa; execução de contrato ou procedimentos preliminares à ele; exercício regular de direitos em processos judicial, administrativo ou arbitral; proteção da vida ou incolumidade física; tutela da saúde em procedimentos realizados por profissionais da área; interesse legítimo do controlador; e proteção do crédito (BRASIL, 2018).

Para viabilizar a privacidade da informação, a legislação trata de aspectos ligados à governança, assim como as normas técnicas que versam sobre a segurança da informação (família da ISO 27000) definindo papeis, responsabilidades e boas práticas para os agentes que de alguma forma participam do tratamento dos dados pessoais.

A definição dos papeis principais consta no artigo 5º[34] da LGPD, conforme Figura 8:

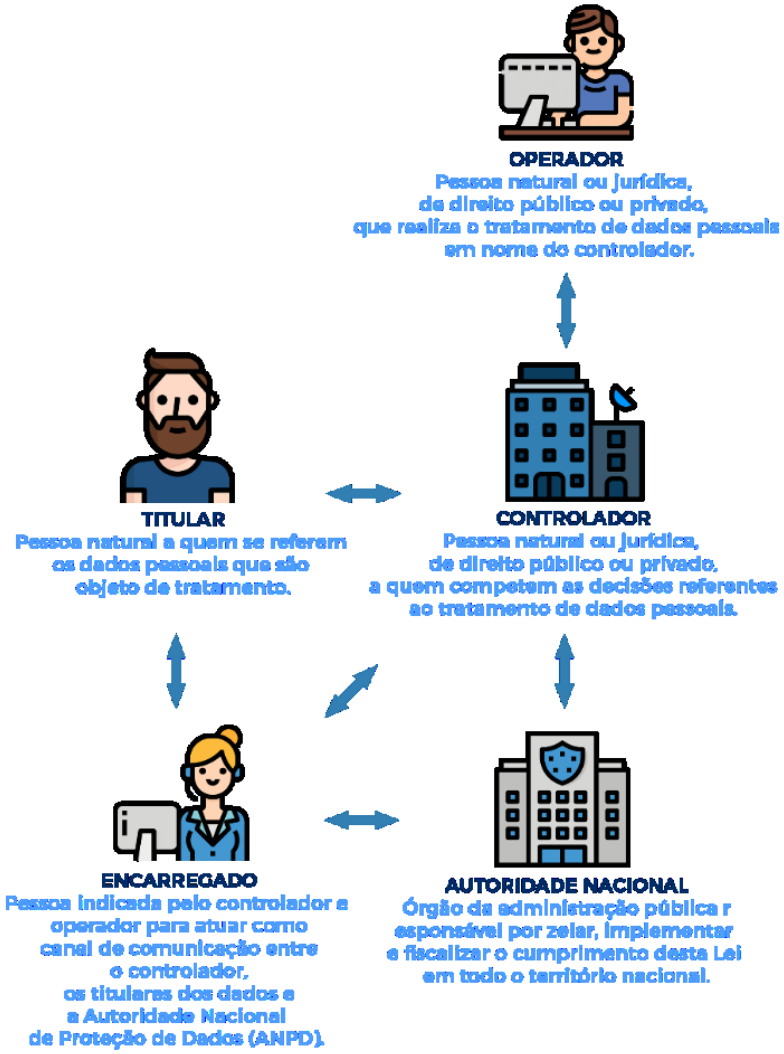
---

[32] Bases legais são as hipóteses que autorizam o tratamento de dados pessoais, ou seja, a fundamentação legal.

[33] Art. 8º, § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei.

[34] LGPD, artigo 5º: Para os fins desta Lei, considera-se: V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional (BRASIL, 2018).

Figura 8 – Papéis na LGPD




Fonte: Adaptado de Brasil (2018).

Ainda, há a figura do agente de tratamento, que segundo Pinheiro (2020), é tanto a o controlador, que recepciona os dados pessoais, quanto o operador, que realiza algum tipo de tratamento.

O controlador é o agente responsável pelas decisões referentes ao tratamento e pela definição das finalidades, como por exemplo, as instruções fornecidas a operadores. É ele que deve elaborar o relatório de impacto, comprovar o consentimento obtido do titular de dados, comunicar as intercorrências de incidentes de segurança, entre outras obrigações. O elemento que distingue das outras figuras é o poder de decisão (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2021).

O operador é o agente responsável por realizar o tratamento em nome do controlador, conforme a finalidade por este delimitada, podendo agir somente até o limite dela e definir elementos não essenciais, como medidas técnicas. É uma pessoa distinta do controlador e não atua coo profissional subordinado dela ou como membro de seus órgãos (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS, 2021).

Garcia et al. (2020) destaca que, com relação ao encarregado, não há pacificado na doutrina se este poderia ser pessoa natural e/ou jurídica e que poderia ser tanto interno quando externo à organização. Considerando a natureza multidisciplinar do cargo, é recomendado que o encarregado tenha conhecimento sobre direito, tecnologia, gestão e comunicação.

Pinheiro (2020) entende que termo encarregado, na legislação brasileira, ficou com uma interpretação abrangente de pessoa, podendo ser tanto natural quanto jurídica e até mesmo um comitê, dada a complexidade interdisciplinar do cargo.

A primeira redação da LGPD trazia em sua redação o encarregado como pessoa natural, o que foi suprimida pela Lei Nº 13.853 de 2019, levando a concluir que a o cargo pode, a partir disso, ser exercido por pessoa natural ou pessoa jurídica, nos moldes do que já estipulava a GDPR (BRASIL, 2018; EUROPEAN UNION, 2016). No mesmo sentido, Gomes (2020) destaca que após a alteração legal passou-se a admissão de empresas e pessoas naturais como Data Protection Officer – DPO, nomenclatura que no Brasil é utilizada como encarregado.

A Autoridade Nacional de Proteção de Dados – ANPD (2021) destaca que, considerando as boas práticas internacionais, o encarregado poderá ser tanto um colaborador quanto um agente externo, pessoa física ou jurídica. Definiu assim a figura como um indicado pelo controlador a tratar os dados pessoais, responsável por garantir a conformidade da organização, pública ou privada, à LGPD. Ele é o responsável por prestar esclarecimentos ao titular, receber comunicações da ANPD, orientar os colaboradores da entidade quanto às práticas de proteção de dados e executar as atribuições do controlador e das normas complementares.

A legislação ainda destaca aspectos para o tratamento de dados pessoais, inserindo as hipóteses que possibilitam essa prática, dá maior proteção a utilização de dados pessoais sensíveis e de crianças e adolescentes e estabelece um ciclo de vida para os dados. Como a hermenêutica jurídica procede à concepção de direitos e deveres, a LGPD também a faz, apontando direitos ao titular, estabelecendo regras do tratamento pelo Poder Público e inserindo responsabilizações pelas suas violações.

## 2.5 CULTURA

O tema é tão complexo quanto sua própria definição, mas é possível encontrar conceitos mais consolidados na antropologia, ciência que se dedicou, e vem o fazendo, ao estudo da matéria.

A etimologia remonta ao verbo latino *colere*, que significa cultivar (SANTOS, 2006), ligando noções de cultura de terra e de gado à agricultura (CARDOSO, 2003). A existência de costumes, crenças de diferentes povos, modos de vida e práticas já eram indagadas por pensadores da Grécia, China e Roma antiga, sendo que estes últimos ampliaram o significado ligado ao cultivo da terra para se referirem ao refinamento social, presente na expressão cultural da alma (SANTOS, 2006).

Séculos de reflexão traçaram o caminho para consolidar modernas preocupações com cultura, já existentes, entretanto, de forma sistemática, ganham destaque no século XVII, na Alemanha. Na falta de uma unidade política comum naquele país, era necessário uma forma de expressar uma unidade viva (SANTOS, 2006).

Em 1718 o Dicionário da Academia Francesa descreveu que cultura necessitava ser seguida de um objeto específico, como por exemplo, “cultura das artes” ou “cultura das letras”, conforme descrito por Cardoso (2003), aponta que talvez, o primeiro a empregar o termo cultura, integrando no campo semântico os inúmeros traços definíveis, sem a necessidade de um complemento posterior, tenha sido Gottfried Herder, em 1774.

Tão logo ocorreu, com esta nova acepção, a primeira grande bifurcação semântica à noção de cultura moderna, conforme Cardoso (2003): a primeira, como uma entidade complexa, holística e estruturada que fosse atributo de uma coletividade transindividual, com dimensões variáveis; a segunda, como a ideia vulgar utilizada para demonstrar a alta cultura intelectual, atributo de pessoas cultas, instruídas, entendida em um sentido normativo, genérico, repleta de juízo de valor, o que Bloom (1989) diz se referir a tudo que é elevado e edificante e que restaura a unidade da arte e da vida da antiga *polis*, apontado por Mintz (1982) como uma questão de privilégios.

Com a intensificação do poderia das nações europeias frente a outros povos do mundo, no século XIX, e com a industrialização e a formação de novos mercados, aumentando contatos entre as nações, a cultura se generaliza como questão científica, objeto de estudo das ciências humanas, que a tratam de forma sistematizada (SANTOS, 2006).

A antropologia passa, segundo Cardoso (2003), a ser considerada disciplina acadêmica, surgindo a partir disso, um conceito científico explicitamente formulado para a definição de cultura, ultrapassando a acepção holística para uma radicalmente reducionista. Para ele, a primeira definição retirou o caráter normativo e inseriu um enfoque descritivo e foi elaborada pelo antropólogo Edward Burnett Tylor, em 1871.

Tylor (1871) descreve cultura como sinônimo de civilização, e em seu sentido etnológico mais vasto, como um todo complexo que compreende conhecimento, crenças, artes, moral, leis, costumes e outros hábitos e capacidades adquiridas pelo homem enquanto membro da sociedade.

Mintz (1982) aponta que depois do emprego da definição de Tylor, os sentidos mais antigos e restritos foram perdendo terreno para essa nova referência de produtos comportamentais, espirituais e materiais da vida humana.

Esses estudos sistematizados de cultura se sobrepõem aqueles ainda do século XIX, que procuravam hierarquizá-la, como se a humanidade passasse por etapas sucessivas de evolução social, tendo como primeiro estágio a distinção da espécie humana da animal até o último grau, a civilização europeia ocidental, justificando o domínio das sociedades capitalistas centrais e racistas, de dominação e exploração de povos não europeus (SANTOS, 2006).

Laraia (2001) descreve que a discussão acerca do que é cultura não terminou e provavelmente nunca terminará, pois uma compreensão exata significa um entendimento da própria natureza humana, temática perene da incansável reflexão.

Há uma diversidade de culturas existentes que acompanha a variedade da história da civilização, expressando possibilidades de vida social organizada, graus e formas diferentes de domínio do homem sobre a natureza.

Culturas são dinâmicas e uma construção histórica, seja em sua concepção, seja como dimensão do processo social, é um produto coletivo do homem. Diz respeito à humanidade como um todo, ao mesmo tempo, a cada povo, nação, sociedade e grupo. É resultado de cada história particular e das relações com outras culturas. Compreendê-la significa fortalecer o respeito e a dignidade nas relações humanas e combater preconceitos (SANTOS, 2006).

Portanto, cada povo tem sua cultura e dentro do mesmo país (basta um olhar sobre o Brasil) há inúmeras outras, de diferentes modos, em diferentes dimensões, geográficas ou cronológicas, todas complexas, sem que seja possível subjugar uma por outra. Há uma infinita riqueza dessas multiplicidades, em tantas formas e histórias da existência humana.

## 2.6 CULTURA ORGANIZACIONAL

Como descrito por Araujo (2018) se a cultura é um processo em constante evolução e responsável por atitudes, crenças e valores do homem pertencente a um grupo social, é indispensável que a organização, dependente do comportamento de seus colaboradores, reconheça a importância do estabelecimento da cultura organizacional em consonância com seus valores e política.

Para a excelência organizacional, Schein (1984) descreve que a chave é a cultura organizacional e a definição desse conceito tão complexo, tanto para pesquisadores, quanto para quem vive e trabalha na organização.

Há ainda, conforme aponta Mascarenhas (2002), um enfoque mais pragmático na discussão do tema, visto que o assunto é abordado pelos teóricos da administração com certo distanciamento antropológico, mesmo que os conceitos básicos tenham sido preservados. Para ele, a antropologia interpretativa não considera a cultura apenas como um sistema fechado, formal, coerente e reconhecível como um padrão para o grupo.

Nesse ponto, Schein (1984) destaca que é necessário evitar modelos superficiais de cultura e deve-se construir sobre os modelos antropológicos mais profundos e complexos. Para ele, cultura como conceito será mais útil se ajudar a compreender melhor os aspectos ocultos e complexos da vida em grupos, organizações e ocupações e essa compreensão só será possível com reflexões profundas.

Esse fenômeno da cultura, conforme Fernandes e Zanelli (2006), já era estudado desde o início do século XX, a partir da experiência de Hawthorn, desenvolvida entre 1927 e 1932, na qual fora constatado grande influência do grupo sobre o indivíduo. Ostroff, Kinicki e Muhammad (2013) destacam que é considerado um dos primeiros estudos qualitativos do comportamento coletivo e individual.

Esta experiência também é relatada por Mascerenhas (2002), descrevendo que o estudo tinha estruturação a partir de conceitos e técnicas da antropologia, buscando compreender os grupos de trabalho como pequenas sociedades, ou seja, buscava entender a função da organização informal entre os trabalhadores e de suas relações com a disposição formal daquela instituição, o que demonstrou discrepâncias entre a realidade dos trabalhadores e o que os administradores adotavam como premissa, levando a conclusão de que estes teriam o papel de criar condições para a colaboração espontânea daqueles, garantindo o comprometimento com as realizações da organização.

Ostroff, Kinicki e Muhammad (2013) destacam que o tópico da cultura organizacional se tornou proeminente com os estudos contidos em três *best-sellers*[35] de Ouchi (1981), Deal e Kennedy (1982) e Peters e Walterman (1982), ambos sugerindo que a eficácia organizacional estava associada a fortes culturas organizacionais.

A complexidade da temática ainda é demonstrada em estudo de Verbeke, Volgering e Hessels (1998), ao identificar 54 definições diferentes na literatura entre 1960 e 1993, com expansões conceituais que pareciam restringidas racionalmente em torno de um conceito central, surgindo variações, e isso reflete indiretamente em um ambiente de pesquisa pluralista.

Dentre essas semelhanças, está o que Schein (1984) aponta ser um fenômeno socialmente construído e influenciado por fronteiras históricas e espaciais e que a compreensão da cultura organizacional está ligada a ideia de significado compartilhado.

Dessa forma, a conduta dos colabores está diretamente ligada à cultura organizacional, pois, como apontam Hofstede, Hofstede e Minkov (2010) a cultura como programação coletiva da mente influencia não só o comportamento, mas as explicações dadas a ele.

Importante destacar a categorização feita por Smircich (1983), em duas linhas: a primeira, na cultura como variável, algo que a organização possui; a segunda, como intrínseca à organização, ela própria.

Fleury (1987) destaca que no primeiro caso, é possível ainda distinguir a cultura como uma variável independente, ou seja, trazida da sociedade para a organização por seus membros; e como uma variável interna, produzida pela própria instituição. Em ambos os casos, a autora destaca que as linhas de pesquisa têm cunho claramente normativo.

A segunda linha descrita por Smircich (1983) adota a cultura como recurso epistemológico, o que, segundo Fleury (1987), deriva do conceito de cultura da antropologia, com enfoque no estudo como fenômeno social, sendo que Smircich (1983) teria diferenciado várias correntes antropológicas: cognitiva, simbólica e estruturalista.

Não há consenso na definição de cultura organizacional entre pesquisadores da temática (HOFSTEDE; HOFSTEDE; MINKOV, 2010; PARSONS, K. M. *et al.*, 2015; SCHEIN, 1984), assim como não há dúvidas da importância da compreensão da cultura antes de inseri-la no contexto laboral, inclusive quanto a sua acepção antropológica (MASCARENHAS, 2002; SMIRCICH, 1983). Esta confere uma visão da pesquisa qualitativa que usa a observação participante, entrevistas e exame de informações históricas para

[35] As obras correspondentes são: Teoria Z de Ouchi, Corporate Cultures: The Rites and Rituals of Corporate Life de Deal e Kennedy e In Search of Excellence de Peters e Walterman.

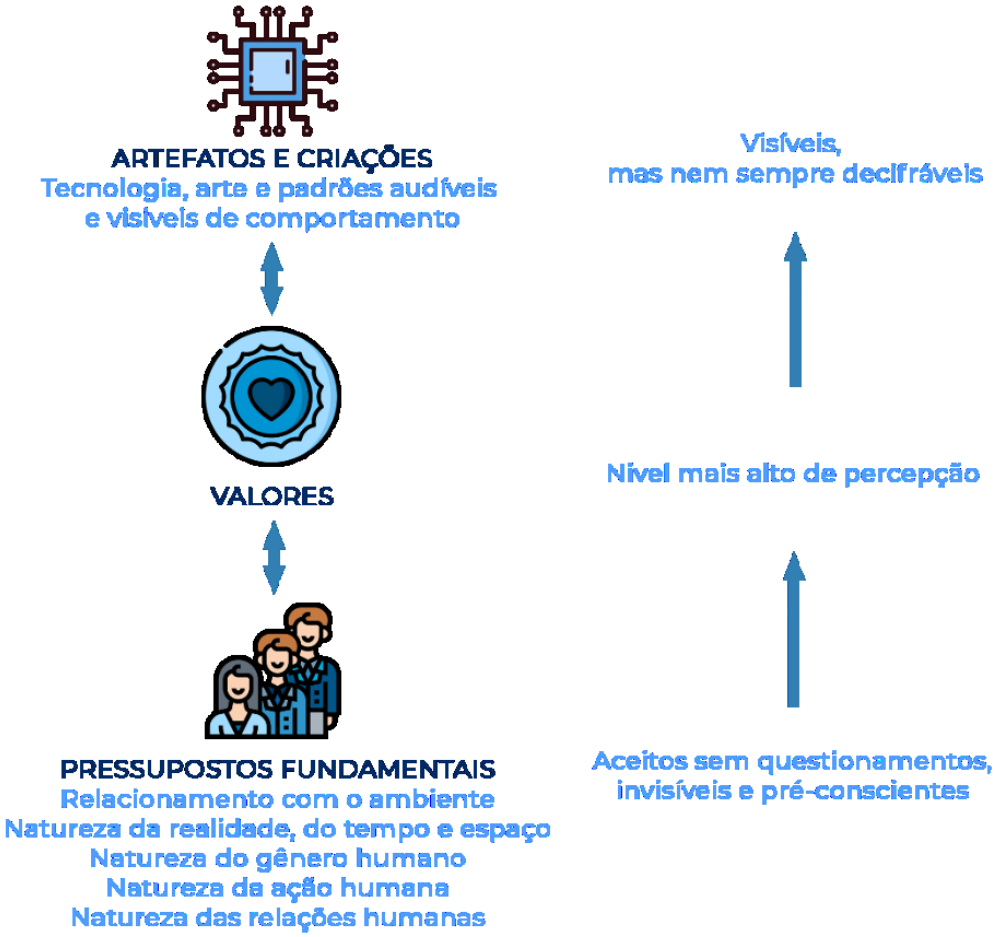
compreensão de como a cultura fornece um contexto para entender o comportamento do indivíduo, do grupo ou da sociedade (OSTROFF; KINICKI; MUHAMMAD, 2013).

O conceito descrito pelos gestores no trabalho de Deal e Kennedy (1982) como o jeito que sempre fizemos as coisas por aqui, o que Crozatti (1998) descreve como uma definição utilitarista e simplista, mas prático de entender a partir da observação de como as coisas são feitas, é contraposto pelo amplo conceito de cultura organizacional definido por Schein (1984).

Citado em inúmeros trabalhos (CROZATTI, 1998; DESHPANDE; WEBSTER JR., 1989; FERNANDES; ZANELLI, 2006; FLEURY, 1987; GOMES et al., 2017; MASCARENHAS, 2002; PEDRAZA-ÁLVAREZ et al., 2015; RAPOSO, 2020; SMIRCICH, 1983; VIEIRA; PEREIRA, 2020), muitos deles, referindo-o como o mais completo, o conceito de Schein (1984) é descrito como uma estrutura de pressupostos fundamentais estabelecida, descoberta ou desenvolvida por um grupo que resolveu os problemas de adaptação externa e integração interna, que tem funcionado bem o suficiente para ser admitido como válido e, portanto, ensinado a novos membros do grupo como a maneira correta de perceber, pensar e sentir aqueles problemas.

Schein (1984) propõe a análise da cultura organizacional em três níveis (Figura 9), que representam o grau de visibilidade do fenômeno cultural para o observador, afirma que parte da confusão, na definição da cultura, deriva da não diferenciação dos níveis de manifestação.

Figura 9 – Níveis de cultura




Fonte: Adaptado de Schein (1984).

Artefatos e criações são os ambientes construídos, arquitetura, tecnologia, vestimenta, produtos, artes, documentos, histórias e outros. Os dados são de fácil obtenção, mas de difícil interpretação. É possível descrever como um grupo se estrutura, quais os padrões de comportamento são discerníveis, mas com frequência não é possível entender a lógica subjacente, ou seja, por que o grupo se comporta de determinada maneira (SCHEIN, 1984). É perigoso interferir suposições profundas apenas a partir deste nível de cultura, porque as interpretações de uma pessoa são inevitavelmente projeções de seus sentimentos e reações (SCHEIN, 2004).

Os valores que regem o comportamento são essenciais para analisar o porquê do grupo de comportar do modo como faz, entretanto, é difícil identificar valores pela observação direta, tornando-se necessário entrevistar os membros da organização para obter e quando identificados, eles podem se restringir apenas àqueles expostos na cultura, aqueles que as pessoas dizem ser a razão do seu comportamento, mas as suposições básicas subjacentes podem

permanecer ocultas (SCHEIN, 1984). Nessa esfera, aqueles que podem influenciar o grupo na adoção de determinada abordagem para a resolução de um problema posteriormente serão identificados coo líderes ou fundadores, mas ainda não há base compartilhada para saber se o que o líder deseja será válido (SCHEIN, 2004).

Os pressupostos fundamentais são importantes para entender de fato uma cultura, sendo, para isso, necessário ir mais fundo, pois são tipicamente inconscientes e determinam o modo como os membros do grupo percebem, pensam e sentem. São respostas aprendidas que iniciaram como valores e que levaram ao comportamento, que, quando resolve o problema do estímulo início, se transforma gradualmente num pressuposto subjacente, explicando como as coisas são, então admitido como inquestionável, o que o faz desaparecer da percepção consciente (SCHEIN, 1984). São soluções para os problemas que funcionam repetidamente, passando a ser consideradas como um dado adquirido, ou seja, o que antes era uma hipótese torna-se uma realidade e o grupo passa a considerar que a natureza realmente funciona dessa maneira (SCHEIN, 2004).

O desenvolvimento da cultura da organização parte geralmente da liderança, enquanto a cultura também pode afetar o desenvolvimento dela. Líderes transacionais trabalham dentro de suas culturas organizacionais seguindo regras, procedimentos e normas existentes, já os transformacionais mudam sua cultura, entendendo-a e realinhando-a com uma nova visão e revisão dos pressupostos, valores e normas compartilhadas (BASS; AVOLIO, 1993), existe nesse contexto uma inter-relação entre cultura e liderança (BARRETO *et al.*, 2013).

Burns (1978) descreveu a manifestação da liderança nesses dois tipos: transacional e transformacional. A primeira é construtiva, mas limitada, em uma relação em que os líderes atendem os desejos e necessidades humanas, mas o relacionamento é superficial porque são dominados por cálculos rápidos de custos e benefícios; a segunda é o mais alto nível de liderança, quando os envolvidos elevam seus níveis de motivação e moralidade e seus propósitos se fundem e os líderes podem redefinir aspirações e gratificações para ajudar seus seguidores a ver seu interesse em novos movimentos.

Esper e Cunha (2015) apontam a liderança autêntica, não como uma teoria que busca descrever como é o líder, mas propões como ele deve ser e agir, com base nos princípios da Psicologia Positiva e no comportamento organizacional positivo, em uma transição da liderança transformacional para a autêntica, com base em princípios éticos.

Dessa forma, a cultura organizacional é moldada pelo comportamento da liderança, sua forma de agir, sua estratégia e visão, além de influenciar na formação do ambiente laboral e na

participação dos colaboradores na construção, definição e desenvolvimento da cultura. Se um líder promove e incentiva a participação, a sugestão de novas ideias e a inovação, há um ambiente propício a encontrar solução para os problemas e novas formas de gerar valor, em um processo de gestão horizontal no qual o colaborador sente-se participativo (cocriação).

Bass e Avolio (1993) destacam que organizações eficazes exigem pensamento tático e estratégico, além da construção de cultura por parte de seus líderes. O pensamento estratégico ajuda a construir a visão do futuro, a cultura é o ambiente no qual a visão se instala, e esta, pode determinar as características daquela.

Schein (2004) afirma que a liderança é originalmente a fonte das crenças e valores que fundamental as ações do grupo ao lidar com seus problemas internos e externos. Se a proposição do líder funciona, ela deixa de ser suposição vai gradualmente tornando-se suposição compartilhada. Um conjunto delas é formado por esse processo e pode funcionar como um mecanismo de defesa cognitivo tanto para o indivíduo quanto para o coletivo, pois eles buscam estabilidade e significado.

Como os líderes reagem aos problemas e os resolvem, recompensam e punem seguidores são relevantes para a cultura, bem como pela forma como a liderança é vista no ambiente interno e externo da organização, pois a cultura afeta a liderança tanto quanto a liderança afeta a cultura (BASS; AVOLIO, 1993).

Distorcer a cultura implementada é mais fácil pelo caminho da negação e de outros mecanismos de defesa do que pela alteração das suposições básicas enraizadas pela liderança, pois esta mudança é demorada e altamente provocadora de ansiedade (SCHEIN, 2004).

Há maior facilidade em deixar as coisas como estão (estado confortável) do que implementar qualquer alternativa de resolução de problemas que possa afetar a cultura, pois, para isso, é necessário esforço para compreensão dos pressupostos fundamentais que são invisíveis e pré-conscientes e muitas vezes, já bem consolidados pelo tempo. Esse é um dos grandes desafios para o líder que almeja implementar uma cultura, por exemplo, de segurança e de privacidade da informação.

Portanto, a liderança cria e muda a cultura, mas ela não é o único aspecto que influencia na mudança, pois a cultura é, como visto no tópico antecedente, complexa e mutável, mas o que pode se extrair é a importância do líder e o forte impacto dele na condução dela (BASS; AVOLIO, 1993; SCHEIN, 2004).

## 2.7 CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

A definição de cultura organizacional de SI é complexa por constituir-se em sua essência da própria cultura. Como apresentado no tópico 2.5, e por abranger inúmeros fatores e possibilidades, a temática não encontra consenso quanto ao conceito, mas, pela proximidade desta pesquisa com a de Araujo (2018), acolhe-se inicialmente o que ele sugere ser a forma que o grupo social coletivamente compartilha, expressa ou manifesta seus conhecimentos, crenças, valores e acordos tácitos quanto à SI, com o objetivo da sobrevivência da organização.

Sem distinção de importância ou assertividade com outras definições, Dhillon (1997) tem uma visão ampla do termo "cultura de segurança" como o comportamento da organização que contribui para a proteção de dados, informações e conhecimento. Veiga e Eloff (2010) definem cultura de SI como as atitudes, suposições, crenças, valores e conhecimentos que os envolvidos usam para interação com os sistemas e procedimentos da organização. Alhogail e Mirza (2014) descrevem a cultura de SI como o conjunto de percepções, atitudes, valores, premissas e conhecimentos que norteiam como as coisas são feitas na organização para o fim de ser consistente com os requisitos de SI, protegendo os ativos de informação e influenciando o comportamento de segurança dos colaboradores, tornando-se uma natureza.

Veiga e Eloff (2010) apontam que a cultura de segurança muda com o tempo. Nesse sentido, a própria SI se desenvolve, como bem aponta Von Solms (2000) ao descrever o ciclo de desenvolvimento dela em quatro ondas.

A primeira, a iniciar pelo começo dos anos oitenta, conhecida por sua abordagem técnica à segurança; a segunda, do início dos anos oitenta até meados dos anos noventa, compreendendo a gestão e o envolvimento com a importância da SI, complementando a primeira; a terceira, no final da década de noventa, chamada institucional, caracterizada pela implementação de códigos de práticas para gestão, certificações internacionais e cultura organizacional de SI. Em estudo posterior, Von Solms (2006) percebeu que uma quarta onda tornara-se clara e bem definida, relacionada ao desenvolvimento e ao papel crucial da governança.

Há uma estrita ligação entre governança corporativa e segurança da informação (SOLMS, B. Von, 2006), pois, como visto no tópico anterior, a construção da cultura perpassa por inúmeros fatores antropológicos, históricos e gerenciais, mas o ser humano é fundamental para sua construção e é de responsabilidade da gestão a implementação de programas para mitigação de riscos e impactos à SI,

A definição de papeis dentro da organização, com suas respectivas responsabilidades e atribuições é fundamental para a governança, além de aspecto legal para a proteção de dados, descrito na LGPD[36] (BRASIL, 2018). É a gestão que normalmente define as regras, os regulamentos e a visão da instituição e essas políticas fornecem orientação aos colaboradores e parceiros, mas idealmente, elas devem se manifestar em alguma cultura para garantir um comportamento adequado e isso só pode ser alcançado por meio de educação, integração de políticas e cultura (SOLMS, R. Von; SOLMS, 2004). A gestão precisa identificar o que motiva sua equipe e implementar estes impulsionadores para a adoção dessas práticas seguras (PARSONS, K. *et al.*, 2010).

Os colaboradores são vitais pra o sucesso da empresa, mas quando se trata de SI, são o elo mais fraco e é neles que deve se voltar os maiores investimento e fortalecimento para mitigar incidentes (ARAUJO, 2018; CONTEH; SCHMICK, 2016; D'ARCY; HOVAV; GALLETTA, 2009; KEMPER, 2019; METALIDOU *et al.*, 2014; NICHOL, 2000; PARSONS, K. *et al.*, 2010; RUSSELL, 2002; SCHNEIER, 2004; SCHULTZ, 2005; SOLMS, R. Von; SOLMS, 2004; VOSS, 2001; VROOM; SOLMS, 2004; WHITMAN; MATTORD, 2011).

Um estudo de Carlton, Levy e Ramim (2019) aponta que cerca de setenta e dois a noventa e cinco por cento das ameaças cibernéticas às organizações decorrem de erros dos usuários em virtude da falta de habilidade em segurança da informação.

Reforços em tecnologia e processos e a falta de uma cultura de SI é ilustrada por Whitman e Mattord (2011), ao descreverem o exemplo lendário da Grande Muralha da China, no qual, por volta de 200 antes de Cristo, o imperador chinês reforçou a segurança com a construção de uma muralha, defendendo a estabilidade do império contra os hunos, mas quase mil e quinhentos anos depois, ao tentarem escalar, cavar e quebrar a parede, foi preciso apenas subornar o porteiro[37]. Dessa forma, os autores que descrevem essa estória afirmam que a engenharia social se aproveita dos erros humanos, manipulando as pessoas.

As características de fraquezas nas instituições são exploradas por engenheiros sociais que percebem comportamentos inadequados e visam essas vulnerabilidades (METALIDOU *et al.*, 2014), até porque, para a SI, há abundância de tecnologia útil, gerenciada por pessoas e

[36] LGPD, artigo 50: Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

[37] O que se busca não é a realidade ou a ficção da analogia, apenas a reflexão que ela provoca.

isso não é um problema técnico, mas cultural e comportamental (SCHULTZ, 2005). Para diminuir a ameaça de engenheiros sociais os indivíduos precisam estar cientes de ataques em potencial, pois eles são uma ameaça real para todas as organizações (PARSONS, K. *et al.*, 2010).

A OCDE estabeleceu diretrizes para um ambiente de segurança e promoção de uma cultura da SI, com foco no desenvolvimento de sistemas e redes e na adoção de novas maneiras de pensar e se comportar ao usá-los, pois apenas uma abordagem que leve em conta os interesses de todos os envolvidos pode fornecer segurança eficaz, mas para isso, todos os participantes devem assumir responsabilidades e ter plena compreensão da necessidade de segurança, além é claro, de contarem com uma liderança que a promova, nesse sentido. Para tanto, formulou nove princípios e diretrizes[38], sendo eles: consciência, responsabilidade, resposta, ética, democracia, avaliação de risco, projeto de segurança e implementação, gestão de segurança e reavaliação (OECD, 2002).

Uma cultura utópica de SI seria aquela que o humano segue as diretrizes da organização de forma voluntária, como parte da sua natureza, por isso, é imperativo que a cultura reflita atitudes positivas, incorporada de comportamentos rotineiros e para a organização que assim não for, é necessário a implementação pela mudança (VROOM; SOLMS, 2004). Só assim comportamentos incorporados terão impacto direto na capacidade de mitigar o risco de ameaças à SI (KEMPER, 2019). A cultura organizacional pode dificultar a mudança e estabelecer o que deve mudar e o que não deve com base nos processos críticos de negócio, desempenhando um papel fundamental na SI (NOSWORTHY, 2000).

Outro ponto a ser destacado é que as organizações passam a dar ênfase e a preocupação que a segurança e a privacidade da informação merecem somente após a ocorrência de um incidente. Isso é muito bem ilustrado por Anderson (2003) ao usar a analogia de um cruzamento de trânsito mal feito, sem sinalização adequada, pertinho de casa e que faz refletir toda vez que é utilizado: “um dia alguém irá se machucar aí!”. Muitas vezes só são aplicadas as medidas corretas, como um semáforo ou placas indicativas, após a ocorrência de uma fatalidade, mesmo que diariamente muitos por ali passem e pensem a mesma coisa.

Portanto, é necessário realizar investimentos em tecnologia e processos, mas devem ser realizados esforços maiores para conscientização, educação e treinamento para o que muitos

[38] Foram estes princípios que constituíram o suporte referencial para elaboração do instrumento de avaliação da cultura organizacional de segurança da informação de Araujo (2018), utilizado neste trabalho. Mais informações no tópico 3.3.1 e Apêndice A.

autores, consideram o elo mais fraco da corrente: as pessoas, conforme supracitado. Elas são o foco deste estudo, através da pré-disposição de seu comportamento. Por isso, gestores devem, como líderes e peças fundamentais, incentivar o investimento em boas práticas, em governança e em políticas que contribuam para essa melhoria e formação da cultura em segurança da informação.

## 2.8 CULTURA ORGANIZACIONAL DE PRIVACIDADE DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Informação e dado pessoal, apesar de utilizados como sinônimos, possuem particularidades próprias, em que pese nosso ordenamento jurídico, inclusive a LGPD, não fazer clara distinção entre informação pessoal e dado pessoal, o que leva a utilização dos termos como sinônimos, para fins do contexto deste trabalho.

Nos tópicos anteriores, abordou-se inúmeros conceitos ligados à informação, aos dados e suas conexões, mas para o fim de incluí-los ao contexto da cultura organizacional, é necessário antes de tudo, sob a ótica holística, delinear alguns dos conceitos novamente, para somente então incluí-los na cultura de SI. Além disso, informação e dado são inseridos no âmbito da privacidade e do indivíduo (pessoal), contribuindo para a melhor compreensão da temática.

**"Dado"** apresenta uma conotação mais primitiva, uma informação em estado potencial ("pré-informação"), anterior à interpretação e ao processo de elaboração (DONEDA, 2011); **"informação"** tem o caráter de mensagem, transferência entre interlocutor e receptor (WERSIG; NEVELING, 1975), mas pode ser entendida com estrita ligação à comunicação e uma estrutura que gera conhecimento individual e coletivo Barreto (1994), ou ainda como a própria sociedade (CASTELLS, 2000); "**pessoal**" mantém um vínculo objetivo com uma pessoa, revelando informação sobre ela, como características, ações ou manifestações (DONEDA, 2011); e "**privacidade**" carrega em si um sentido muito amplo, desde o direito de estar só de Warren e Brandeis (1890), a vida particular, privada e secreta de Hubmann (1967) e até mesmo o direito à autodeterminação informativa contido na LGPD (2018) e esse conceito aberto, cujo escopo enfraquece a proteção, vai além da formulação jurídica e torna-se um meta-conceito (MONTI; WACKS, 2019).

A informação representa, além do contido no dado, chegando ao limiar da cognição[39], pressupondo um estado de depuração do conteúdo, levando consigo um sentido instrumental e de redução de incertezas (DONEDA, 2011). Talvez pelo liame semântico e pela trama espessa que amarra informação e dado e vice-versa, na qual é quase impossível desconstruí-los separadamente, a legislação e a literatura em geral usa ambos como sinônimos.

A inserção de todas essas definições ao contexto digital e à sociedade da informação de Castells (2000) leva ao entendimento que a privacidade da informação pessoal e a proteção de dados pessoais, preservando o caráter de direito fundamental e sem pretensão reducionista, refere-se à informações que identifiquem ou que possam identificar o indivíduo, seu comportamento, suas ações, suas feições e particularidades, incluindo, mas não se limitando a nome, dados sobre sua pessoa, geoposicionamento, biometria, informações de consumo, orientação sexual, opinião política, genética, reconhecimento facial, imagem, fatos da vida privada e outros. Catala (1983) destaca que é informação pessoal quando o objeto da informação é a própria pessoa.

Dessa forma, a informação pessoal está ligada à privacidade por uma equação simples e básica, quase como ato reflexo, que associa um maior grau de privacidade à menor difusão de informações pessoais e vice-versa, conforme descrito no artigo 6º, inciso III da LGPD, ao limitar o tratamento ao mínimo necessário. Isso não esgota a problemática complexa em torno da relação, mas dá suporte para compreensão da tutela do direito à privacidade e ao que gira em sua órbita, como os dados pessoais (BRASIL, 2018; DONEDA, 2011).

O que se observa é que informações e dados, seja no âmbito pessoal ou não, merecem proteção quanto à segurança e à privacidade, inclusive para as organizações. É nesse habitat que reside a importância da cultura organizacional para a garantia desses pressupostos.

Conforme apontado no tópico 2.6 deste trabalho, a liderança tem papel crucial na formação da cultura corporativa e esta, por sua vez, é responsável pela excelência organizacional, pois há forte ligação entre a cultura e o comportamento individual e coletivo.

Para que a privacidade seja estabelecida dentro dos níveis de cultura, descritos por Schein (2004), é necessário inseri-la por padrão em todos os processos da organização, além de compartilhar comportamentos que garantam e resguardem o direito à autodeterminação informativa, protegendo os dados dos titulares e colocando a instituição em conformidade com os fundamentos e princípios do que estabelece o ordenamento jurídico, sobretudo a LGPD.

[39] Conforme o conceito de informação de Barreto (1994), ligado a instrumento de construção de conhecimento.

Portanto, sugere-se o conceito de cultura organizacional de privacidade da informação e proteção de dados como a estrutura de pressupostos fundamentais, crenças, valores e conhecimentos compartilhados com o objetivo de garantir a privacidade por padrão nos processos e a autodeterminação informativa.

# 3 PROCEDIMENTOS METODOLÓGICOS

Este capítulo descreve os procedimentos metodológicos utilizados para o alcance dos objetivos propostos na pesquisa, destacando as atividades realizadas e demonstrando a caracterização da pesquisa, a coleta e o tratamento de dados. Além disso, descreve o sistema financeiro cooperativo, no qual foi realizado o estudo de caso, a delimitação do tema e a adaptação e composição dos questionários.

## 3.1 CARACTERIZAÇÃO DA PESQUISA

A pesquisa, conforme aponta Gil (2018, p. 1), é um "procedimento racional e sistemático que tem como objetivo fornecer respostas aos problemas propostos", desenvolvido com métodos e técnicas de investigação científica, envolvendo inúmeras fases.

Toda ciência utiliza dessas técnicas de investigação para obtenção de seus propósitos e esse levantamento de dados pode ser classificado em: primário, secundário ou terciário. Nesse estudo, utilizou-se de questionário online e questionário como roteiro da entrevista para levantamento de campo (dados primários) e análise documental de livros, artigos em periódicos científicos, revistas, leis, normativas, documentos e sites (dados secundários) (MARCONI; LAKATOS, 2017).

O conhecimento gerado com esse material-fonte (investigação com dados primários e secundários) torna possível a construção de um *background* sólido para o campo de interesse (MARCONI; LAKATOS, 2017). Classificar a pesquisa possibilita melhor organização dos fatos e por consequência, o seu entendimento, ou seja, rotulando o projeto de pesquisa de acordo com um sistema de classificação é possível conferir maior racionalidade às etapas da sua execução, o que pode significar a obtenção de resultados mais satisfatórios (GIL, 2018).

Quanto a sua natureza, esta pesquisa é aplicada, tendo como objetivo gerar conhecimentos para aplicação prática, destinados à solução de problemas específicos, envolvendo verdades e interesses locais (PROVDANOV; FREITAS, 2013).

A abordagem do problema pode ser classificada, segundo Prodanov e Freitas (2013), em dois tipos:

- Quantitativa: tudo que possa ser quantificável, traduzindo em números opiniões e informações para poder classificá-las e analisá-las, utilizando-se técnicas de

estatística, como percentagem, média, moda, mediana e outras. Formula-se e classifica-se a relação entre as variáveis, garantindo a precisão dos resultados;

- Qualitativa: há uma relação dinâmica entre o mundo real e o sujeito que não pode ser traduzida em número. Interpreta fenômenos e atribui significados. O ambiente é a fonte direta de dados, mantendo-se um contato direto com ele e com o objeto de estudo, não requerendo o uso de estatística, pois não tem a prioridade de numerar ou medir unidades.

Este estudo pode ser classificado como de natureza quantitativa, pois a utilização do instrumento de Araujo (2018) permite informar os resultados obtidos, acusando o nível de maturidade da segurança da informação na visão de gestores de tecnologia de instituições financeiras pertencentes a um sistema cooperativista. Ao mesmo passo, é de natureza qualitativa, pois o pesquisador mantém contato direto com o ambiente e o objeto de estudo, com trabalho intensivo de campo, coletando informações através de questionário com perguntas abertas e análise de conteúdo sobre a privacidade da informação. Assume, portanto, abordagem qualiquantitativa.

Como será demonstrado a seguir, no delineamento da pesquisa, este estudo utilizou o método misto, combinando elementos da natureza quantitativa e qualitativa (STRAUSS; CORBIN, 2008).

Quanto aos seus objetivos, a pesquisa é classificada em exploratória, descritiva e explicativa (GIL, 2018; PROVDANOV; FREITAS, 2013):

- Exploratória: proporciona maior familiaridade com o problema, tornando-o mais explícito. Facilita a delimitação do tema de pesquisa, possibilitando sua definição e delineamento. Possui um planejamento bem flexível, permitindo o estudo sob diversos prismas, considerando os mais variáveis aspectos relativos ao fato ou fenômeno estudado. A coleta de dados pode ocorrer de inúmeras formas, dentre elas, o levantamento bibliográfico, entrevistas com pessoas que tiveram experiências sobre o assunto e análise de exemplos que estimulem a compreensão do o assunto. A maioria das pesquisas acadêmicas, em pelo menos algum momento, geralmente o inicial, assume o caráter exploratório.
- Descritiva: objetiva descrever as características de determinada população ou fenômeno, podendo ter a finalidade de identificar relações entre variáveis. Utiliza técnicas para a coleta de dados como o questionário e a observação sistemática, geralmente assumindo a forma de levantamento. Nela, o pesquisador apenas

observa, registra, analisa, classifica, descreve e interpreta os fatos, sem interferir neles, ou seja, os fenômenos físicos e humanos são estudados, mas não manipulados.

- Explicativa: objetiva identificar fatores que determinam ou contribuem para a ocorrência de fenômenos, através do registro, da análise, da classificação e da interpretação. São as pesquisas mais profundas no conhecimento da realidade, pois explicam a razão, o porquê das coisas, constituindo-se no tipo mais complexo e delicado de pesquisa, com elevados riscos de erros. Os resultados dessa pesquisa são pilares para o conhecimento científico.

Diante disso, é possível classificar a presente dissertação como uma pesquisa exploratória em seu início, como forma de aproximação do problema e da temática, bem como para a definição dos construtos teóricos, tendo-se evoluído para pesquisa descritiva, que busca a relação entre os fenômenos.

Para o pesquisador deste estudo e sua professora orientadora, a tese de doutorado de Pedro Henrique de Moura Araujo, intitulada Construção da Escala do Nível da Cultura Organizacional de Segurança da Informação – UFSC, é inspiração e base para o trabalho. Destaca-se que, o instrumento construído por Araujo (2018), sofreu algumas adaptações para aplicação no segmento de instituições financeiras cooperativistas e outras, em decorrência do momento de pandemia da COVID-19.

Além da pesquisa exploratória, nos momentos iniciais da investigação, com o objetivo de obter maior familiaridade com a temática, explorou-se o RI UFSC, o *Google Scholar* e outros documentos e sites com informações sobre segurança da informação, privacidade da informação e cultura organizacional. Realizou-se levantamento nas bases *SciELO*, *Scopus e Web of Science*, com o objetivo de obter artigos científicos publicados em periódicos, além de dissertações, teses e livros, utilizando os construtos “segurança da informação”, “privacidade da informação”, “cultura organizacional”, “proteção de dados”, “Lei Geral de Proteção de Dados” e “LGPD”, com preferência para artigos publicados em 2018, 2019 e 2020 e em língua portuguesa, dada a relevância e vigência da LGPD (BRASIL, 2018).

A seleção das publicações se deu pela similaridade com a temática, através da leitura dos resumos, sem o objetivo de realizar uma revisão sistemática da literatura, mas uma busca exploratória com os descritores supracitados.

A busca exploratória contou com a pesquisa de normativas técnicas e legislações nacionais e internacionais sobre a segurança e a privacidade da informação, com livros que

versam sobre o cooperativismo financeiro e com documentos ligados à instituição financeira objeto de estudo.

A pesquisa se utiliza de técnicas para a coleta de dados, através de questionário com questões fechadas e abertas, objetivando estudar as características e o comportamento de uma população de um ambiente organizacional e a sua cultura quanto à segurança e a privacidade da informação.

As informações registradas são analisadas, descritas e interpretadas, observando em conjunto, a literatura científica sobre a temática e as informações obtidas na pesquisa de campo junto aos gestores de instituições financeiras cooperativistas.

No tocante ao delineamento, Gil (2018), Johnson, Onwuegbuzie e Turner (2007), Marconi e Lakatos (2017), Thiollent (1986) e Prodanov e Freitas (2013) apontam que a pesquisa leva em consideração o ambiente, a abordagem teórica e as técnicas de coleta e análise de dados, definindo um sistema com tipologias e definições. A partir desse sistema, esta dissertação se utilização dos seguintes tipos de pesquisa:

- Pesquisa bibliográfica: elaborada com base em materiais já publicados, como livros, revistas, teses, dissertações e outros, tanto impressos quanto virtuais. Praticamente toda pesquisa acadêmica requer pesquisa bibliográfica, elaborada com o propósito de fornecer fundamentação teórica ao estudo;
- Pesquisa documental: assim como a pesquisa bibliográfica, utiliza-se de dados já existentes, mas difere-se porque a fonte documental do material consultado é interna à organização, como documentos institucionais, documentos pessoais, documentos jurídicos, cartas, diários, certidões, fotografias e outros;
- Levantamento: solicita-se informações a um grupo de pessoas sobre o problema estudado e, mediante análise, obtém-se conclusões sobre os dados coletados. Quanto se tem informações de todos os integrantes do universo, tem-se um censo, quando se tem uma parcela do universo, tem-se uma amostra, que pode ser projetada para a totalidade.
- Estudo de caso: possibilita amplo e detalhado conhecimento de um ou poucos casos, permitindo compreender a distinção do fenômeno e seu contexto, inclusive com o propósito de explorar situações da vida real, possibilitando descrever o contexto em que está sendo feita a investigação;

- Pesquisa-ação: com base empírica, é desenvolvida com estreita associação com a ação ou com a resolução de um problema coletivo, onde pesquisadores e participantes se envolvem de modo participativo e cooperativo. Busca diagnosticar um problema específico numa situação específica, alcançando um resultado prático.
- Métodos mistos: a pesquisa qualitativa é reconhecida como importante para o estudo da experiência dos complexos processos de interação social, assim, é conveniente combinar elementos da pesquisa qualitativa com a quantitativa com o propósito de ampliar e aprofundar o entendimento e a corroboração dos resultados.

Foi utilizado o método de levantamento, ao adequar o questionário de Araujo (2018) para aplicação no sistema proposto, interrogando os gestores da segurança da informação quanto à cultura organizacional da sua instituição, para aferição do nível de maturidade em segurança da informação nessas organizações. Obteve-se um total de 25 (vinte e cinco) respondentes para as questões fechadas propostas.

Além disso, foi concebido um questionário específico para melhor compreensão da privacidade da informação e proteção de dados, com a coleta através de entrevista estruturada, contando com três respondentes que já participaram na primeira etapa com o instrumento de Araujo (2018).

Ambos os questionários, tanto o com questões fechadas, adaptado de Araujo (2018) quanto o com questões abertas, elaborado pelo autor, obedecem ao propósito de obter informações sobre conhecimentos, crenças, cultura, valores e comportamentos dos respondentes (GIL, 2018).

Foi utilizado o método de estudo de caso, já que a pretensão era compreender a cultura organizacional de um sistema de instituições financeiras cooperativistas, ou seja, coletar informações sobre a segurança e a privacidade da informação em um contexto real, descrevendo a sua situação.

Ainda, quanto ao delineamento da pesquisa, foi utilizado o método misto, pois se buscou produzir resultados com elementos quantitativos, os quais não seriam suficientes somente com os qualitativos.

Para tanto, a pesquisa se mostra qualitativa com a aplicação da análise de conteúdo para análise e interpretação dos dados das informações coletadas via questionário com perguntas abertas sobre privacidade da informação. Também é quantitativa, ao tratar os dados do questionário com perguntas fechadas sobre segurança da informação junto aos gestores de tecnologia da informação, via estatística descritiva e utilização de *software* desenvolvido por

Araujo (2018) para verificação do nível de maturidade em segurança da informação das instituições na percepção dos gestores respondentes.

Por fim, para melhor compreensão da caracterização da pesquisa, apresenta-se sua estrutura no Quadro 3:

Quadro 3 – Classificação da pesquisa[40]

| Fonte de dados | Natureza | Abordagem do problema | Objetivos | Métodos empregados |
|---|---|---|---|---|
| Primários | Básica | Qualitativa | Exploratória | Bibliográfico |
| Secundários | Aplicada | Quantitativa | Descritiva | Documental |
| | | Qualiquanti | Explicativa | Experimental |
| | | | | Ensaio clínico |
| | | | | Estudo de coorte |
| | | | | Caso-controle |
| | | | | Levantamento |
| | | | | Estudo de caso |
| | | | | Femenológico |
| | | | | Etnográfico |
| | | | | *Ground Theory* |
| | | | | Pesquisa-ação |
| | | | | Participante |
| | | | | Misto |

Fonte: Adaptado de Gil (2018); Johnson, Onwuegbuzie e Turner (2007); Marconi e Lakatos (2017), Thiollent (1986) e Prodanov e Freitas (2013).

## 3.2 ETAPAS DA PESQUISA

O delineamento da pesquisa pode ser apresentado em três eixos (Figura 10), um primeiro que versa sobre o levantamento de dados secundários via literatura através das pesquisas em bases de dados, sites, normativas, leis, livros e documentos, um segundo que versa sobre o levantamento de dados primários através da pesquisa de campo e um terceiro com levantamento de dados através de entrevistas.

O **Eixo 1** compreende o estudo preliminar e a busca exploratória no *Google Scholar*, RI UFSC, documentos e sites, visando a melhor compreensão e aproximação com o tema de pesquisa e sua problemática.

Nessa etapa foi possível a definição dos construtos teóricos e também a identificação do trabalho de Araujo (2018) como ferramenta basilar da pesquisa de campo, através de seu instrumento de pesquisa (questionário).

[40] Em destaque no quadro os que foram utilizados para esta pesquisa.

Ainda no levantamento de dados secundários, foi realizada a pesquisa nas bases, conforme descrito anteriormente.

Após a seleção das publicações, foi desenvolvido a fundamentação teórica ao mesmo tempo do desenvolvimento dos Eixos 2 e 3, o que inclusive possibilitou a compreensão do questionário de Araujo (2018) através do embasamento técnico que a leitura e a pesquisa trouxeram ao estudo, permitindo a realização das entrevistas com especialistas e grupo foco, além de contribuírem para a elaboração do roteiro (questionário) das entrevistas.

O **Eixo 2** apresenta a primeira etapa do levantamento de dados primário, através de pesquisa de campo nas instituições financeiras do sistema cooperativista.

Em um primeiro momento, antecedem à adaptação do instrumento de Araujo (2018) as etapas de entrevista com especialistas e as duas rodadas do grupo foco para posterior alterações no questionário, adaptando-o ao momento de pandemia (coincidindo com a aplicação) e ao ambiente pesquisado.

Com o instrumento adaptado, foi realizada a pesquisa com os gestores de tecnologia da informação das instituições, de forma remota, através de formulário no *Google Forms*, totalizando 25 respondentes.

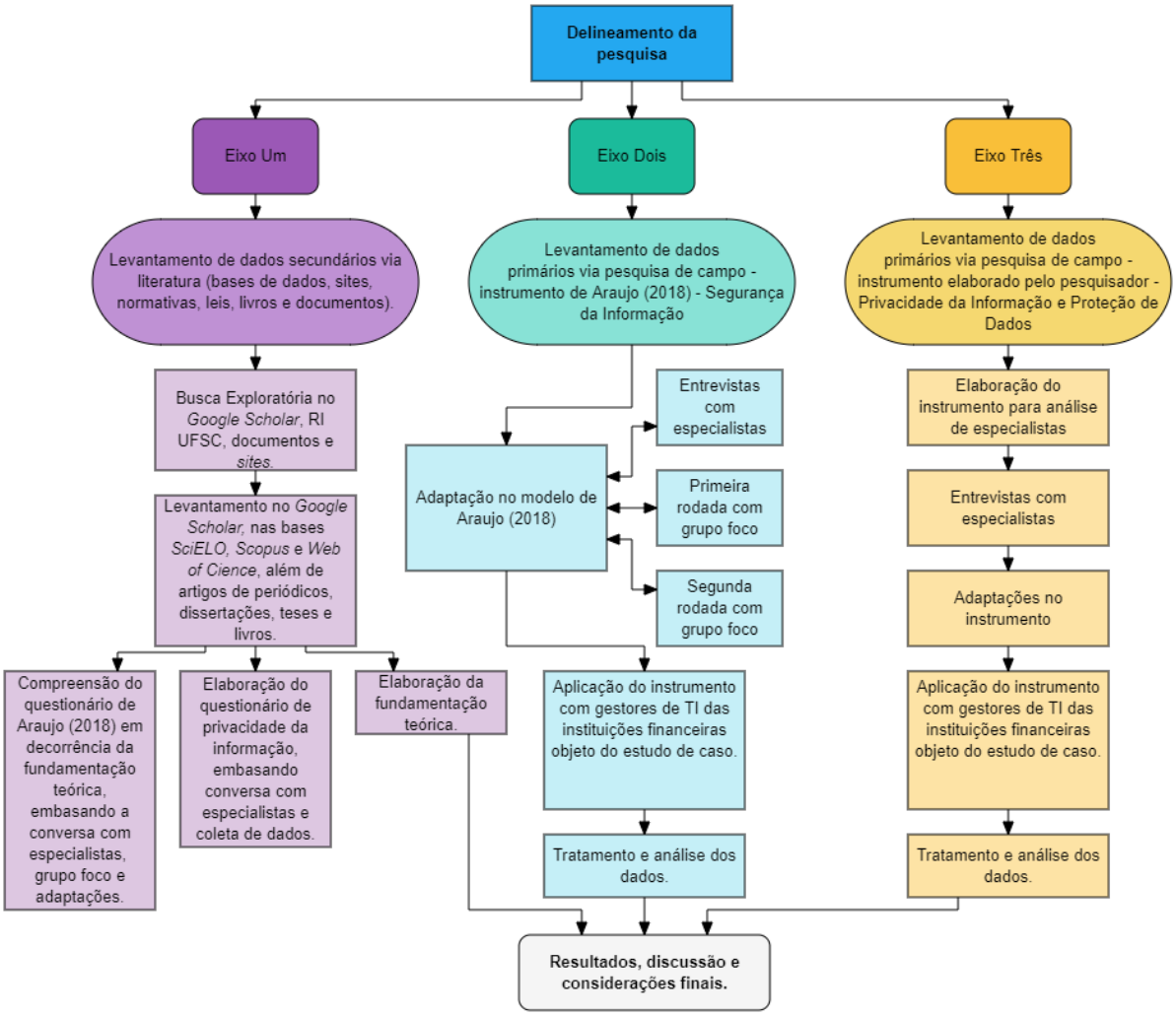
Com os dados coletados, o tratamento se deu através do *software* desenvolvido por Araujo (2018) e os resultados e discussões são apresentados no capítulo 4 à luz da revisão da literatura e embasam as considerações finais.

O **Eixo 3** apresenta a última etapa do levantamento de dados primários, também através de pesquisa de campo nas mesmas instituições, entretanto, junto a três respondentes, com objetivo de pesquisa exploratória para complementar a análise das respostas dos gestores quanto à percepção de SI em suas instituições. Destaca-se que, não se teve a pretensão de considerar este resultado como representativo dos gestores, mas inclusive, como oportunidade para maior profundidade e alcance em estudos futuros.

Para tanto, foi elaborado um instrumento específico, levando em consideração sugestões de uma equipe de especialistas que foram entrevistados, adaptando o instrumento para aplicação com gestores de TI.

O tratamento desses dados se deu através de análise de risco, o que é apresentado no capítulo 4 deste trabalho, através de discussões com base no levantamento teórico e os dados obtidos no Eixo 2.

Figura 10 – Delineamento da pesquisa




Fonte: Do autor.

## 3.3 PROCEDIMENTOS PARA COLETA DE DADOS: EIXO DOIS – SEGURANÇA DA INFORMAÇÃO

Para a realização da pesquisa, além da busca exploratória, procedeu-se ao estudo de caso através de questionário, originalmente desenvolvido por Araujo (2018). Dessa forma, o instrumento foi adaptado para o contexto deste estudo.

### 3.3.1 O instrumento de Araujo (2018) e suas adaptações

O pesquisador e sua professora orientadora realizaram contato com o autor do instrumento, Prof. Dr. Pedro Henrique de Moura Araujo e em 29 de abril de 2020 reuniram-se de forma online (por conta da distância geográfica entre os participantes e em decorrência do estado de calamidade pública provocado pelo novo coronavírus). Nessa reunião ficou autorizado a utilização do instrumento, bem como foi explanado pelo autor a metodologia aplicada na coleta de dados e em sua tese de doutorado. Participaram este pesquisador, sua orientadora, um dos especialistas que contribuíram com as adaptações e dois orientandos da professora, um em nível de mestrado e outro, de graduação, ambos com estudos e atividades profissionais na área.

O delineamento teórico de Araujo (2018) é focado nas definições de cultura organizacional e segurança da informação. A elaboração dos itens do instrumento de avaliação norteia-se em diretrizes e normas de segurança da informação para a mensuração de aspectos subjetivos da cultura com base em requisitos objetivos, adotando as diretrizes da OECD (2002) para uma cultura de SI nas organizações e as normas da família ISO 27000.

Além disso, o estudo de Araujo (2018) recorreu à psicometria e à TRI para respaldar a análise dos itens e a validação do instrumento de avaliação, garantindo a construção da escala do nível de cultura organizacional de SI. Dessa forma, a presente dissertação não tem objetivo de utilizar a TRI ou validar o instrumento, pois esta etapa foi superada por Araujo (2018) e maiores informações sobre estes procedimentos e todo o estudo metodológico podem ser consultadas em sua tese. Mesmo assim, a dissertação em tela buscou compreender a construção dos itens e o traço latente, para pequenas adequações do instrumento, conforme descrito no apêndice A.

A psicometria é um ramo da psicologia que tem interface com a estatística, conforme Pasquali (2009), oferecendo fundamentação epistemológica e teórica de medida para que seja possível representar numericamente fenômenos psicológicos, como por exemplo, a predisposição ao comportamento. Araujo utiliza a teoria psicométrica para a construção do seu instrumento, garantindo segurança no acesso às medidas desses fenômenos psicológicos, o que, conforme Cruz e Alchieri (2003), qualifica uma avaliação cientificamente respaldada.

Dessa forma, a teoria psicométrica contribui para o desenvolvimento do instrumento que mensura o nível de cultura organizacional de segurança da informação, o que é denominado na psicometria de traço latente ou construto (ARAUJO, 2018).

Um instrumento de medida deve ser válido e fidedigno com o objeto de estudo, nesse caso, a demonstração da validade é equivalência entre os processos empíricos e teóricos do traço latente e a fidedignidade é a confiabilidade (PASQUALI, 1997).

Segundo Trierweiller (2011) a TRI é um conjunto de modelos matemáticos que mensuram traços latentes, ou seja, características que não são medidas diretamente. Assim, a TRI utiliza um conjunto de itens para expressar a associação entre as variáveis latentes subjacentes, de uma escala de medição, e a resposta de um indivíduo a um item[41]. É uma ferramenta amplamente utilizada em diversas áreas, como educação e psicologia[42], medicina[43], marketing[44], serviços[45], gestão da qualidade[46], sistemas de informação[47], genética[48] e efetividade organizacional[49], dentre outras.

O instrumento deste trabalho, desenvolvido por Araujo (2018), utiliza o Modelo de Resposta Gradual – MRG de Samejima (1969), pois é o que melhor atende aos requisitos, extraindo muito mais informações do item do que apenas se a resposta está correta ou não (ANDRADE; TAVARES; VALLE, 2000). Samejima (1969) descreve que, nesse modelo, as respostas de um item são divididas em categorias politômicas e ordinais.

Araujo (2018) utilizou uma matriz de referência com as descrições e definições de cada faceta pesquisada, sendo elas: consciência, responsabilidade, resposta, ética, democracia, projeto de segurança e implementação, gestão de segurança, avaliação de risco e reavaliação, conforme a OECD (2002).

Nas descrições, o autor inseriu os itens, os quais foram compostos em duas etapas: a primeira com a redação atendendo a requisitos definidos na matriz de referência e a segunda com uma banca de especialistas. Os itens são politômicos e permitem obter dos respondentes o grau, a intensidade ou a frequência com que eles atendem ao questionamento.

Os parâmetros dos itens e as habilidades dos respondentes estão numa mesma métrica, uma vez que o modelo foi considerado ajustado, chegando portanto às condições necessárias e suficientes para a construção da escala do nível de cultura organizacional de segurança da informação (ARAUJO, 2018).

---

[41] Mellenbergh (1994), Hambleton (2000); Embretson e Reise (2000).
[42] De Ayala (2009).
[43] Ross e Allem-Meares (1998); Vidotto et al. (2006); Das e Hammer (2005); Lin e Yao (2009).
[44] Bayley (2001), Singh (2004).
[45] Costa (2001).
[46] Alexandre et al. (2002).
[47] Tezza, Bornia e Andrade (2011); Wu (1999).
[48] Tavares, Andrade e Pereira (2000).
[49] Trierweiller (2011).

A escala de verificação utilizada no instrumento é a Likert, na qual os entrevistados enunciam seu grau de concordância, através de um conjunto de afirmativas pertinentes à definição (SILVA JÚNIOR; COSTA, 2014).

A partir do entendimento dessas etapas desenvolvidas por Araujo (2018), iniciaram-se os primeiros ajustes para que o instrumento pudesse ser aplicado em um sistema financeiro cooperativista, objeto desta dissertação. O Apêndice A da tese de Araujo (2018) com suas primeiras adequações foi inserido em um formulário online (*Google Forms*) e submetido a análise de especialistas, primeiramente, professores doutores e, na sequência, profissionais do mercado (sistema financeiro).

Cada um dos especialistas apontou considerações, que julgava pertinente, para melhor compreensão dos termos, minimizando interpretações dúbias, bem como, sugestões de melhoria e adaptações para o sistema financeiro. As reuniões foram feitas através de plataformas digitais (on-line), sendo gravadas e arquivadas para consultas.

Após as considerações, o pesquisador e sua professora definiram, em reunião online, quais alterações seriam realmente aplicadas ao instrumento, sendo que nem todas as proposições feitas pelos especialistas foram acatadas, mas sim, as que sob a ótica daqueles, seriam pertinentes.

Do corpo de especialistas (Quadro 4) tem-se:

Quadro 4 – Corpo de especialista para considerações no instrumento de Araujo (2018) [50]

| **Especialista 01 – Encontro em 21/05/2020** |
|---|
| **Doutor (UFSC) em engenharia de produção, graduado em ciências da computação, professor universitário e gestor de projetos.** |
| Considerações: |
| Csc_04_1, Csc_04_2 e Csc_05_0 usar a palavra computador ou equipamento (mais amplo)? |
| Ao perguntar, deixar claro qual o equipamento (celular ou computador), caso seja usado a palavra equipamento; |
| Csc_06_1 e Rsp_03_0 manter a mesma lógica e ordem das respostas; |
| Rsp_02_0 na pergunta, colocar "com que frequência..."; |
| RsP_02_0 por que não cinco opções, padronizando com as demais? |
| Rpt_02_0 a pergunta é comissiva e a resposta é omissiva, usar um "aberta" na pergunta; |
| Rpt_03_0, Rpt_04_0, Etc_02_0 na pergunta, colocar "o que você faria"; |
| Etc_03_0 alterar a palavra confidencial para sigilosa, isso deixaria o impacto para responder menor; |
| Etc_04_0 na pergunta, colocar "o que você faz"; |
| Gts_02_2 acrescentar grupo gestor da segurança da informação; |
| Dmc_02_0, Rsc_13_0, Rsc_14_0, Rsc_15_0, Rsc_17_0 e Rvl_01_0 na pergunta, colocar "com que frequência..."; |
| Rsc_01_1 talvez colocar nuvem; |
| Rsc_02_0 e permissão? Tem instalar e tem autorizar, mas não tem permissão; |
| 8. começou a ficar cansativo; |

[50] Foi mantido a nomenclatura (codificação, exemplo: Csc_01_1) do item, a mesma utilizada por Araujo (2018) e que corresponde as dimensões teóricas que respaldaram a construção dos itens do questionário.

| |
|---|
| Rvl_02_2 não abreviar S.I.; |
| Questionário longo; |
| Possibilidade de dividir em duas etapas; |
| Reforçar confidencialidade; |
| Esclarecer objetivo do questionário e mostrar que não se busca punir ninguém; |
| Esclarecer que os dados serão gerais e não individuais, o que fará o respondente ser mais sincero; |
| **Especialista 02 – Encontro em 21/05/2020** |
| **Doutor (UFSC) em engenharia e gestão do conhecimento, graduado em ciências da computação e direito, professor universitário, empresário do ramo de *compliance* e consultor de segurança e privacidade da informação.** |
| Considerações: |
| Csc_03_6 o que seria a quebra do sigilo? Confunde com o Csc_03_4; |
| Csc_04_0, Csc_05_0, Dmc_01_0, Dmc_02_0, Dmc_03_0, Rsc_03_0, Rsc_04_0, Rsc_05_0 Rsc_06_0, Rsc_08_0, Rsc_09_0 e Rsc_11_0 não verifica necessidade de "nenhuma das alternativas"; |
| Rpt_02_0 melhorar a redação para não ser automática a resposta em "alertaria dependendo da situação"; |
| Gts_01_3 qual seria o planejamento? |
| Dmc_03_0 o que tem a ver com segurança da informação? |
| Dmc_05_0 exige conhecimento do respondente, talvez melhores explicações; |
| **Especialista 03 – Encontro em 04/06/2020** |
| **Mestre (UFSC) em engenharia e gestão do conhecimento, graduado em ciências da computação, professor universitário e empresário do segmento de educação corporativa.** |
| Considerações: |
| Extenso demais; |
| Exige muita atenção do respondente; |
| Formato difícil; |
| Verificar possibilidade de acompanhar o quanto já respondeu; |
| Cabeçalho muito extenso, o respondente esquece do início antes de finalizar; |
| **Especialista 04 – Encontro em 27/05/2020** |
| **Analista de tecnologia da informação de uma instituição financeira cooperativista.** |
| Considerações: |
| Csc_02_00 trocar o termo organização por cooperativa; |
| Csc_04_1 padronização; |
| Rsp_01_0 não tem uma unidade específica para a Segurança da Informação, está tudo na Tecnologia da Informação, quem sabe algo sobre isso; |
| Dmc_05_1 dados pessoais e corporativos? |
| Quando aplicar o questionário focar que o estudo é pela UFSC, o que facilitará a aceitação e a credibilidade; |
| Sentiu falta de algo sobre *home office*; |
| **Especialista 05 – Encontro em 05/06/2020** |
| **Diretora operacional e responsável pela segurança da informação de um sistema financeiro cooperativista.** |
| Considerações: |
| Verificar resolução Bacen 4.658; |
| Rsc_09_5 ajustar para “sua instituição financeira”; |
| Rlv_02_1 ficou em dúvida. |

Fonte: dados da pesquisa.

Após a etapa de entrevistas com os especialistas, foram realizados alguns ajustes no instrumento para então aplicá-lo em grupo foco. Dessa forma, foram realizadas duas rodadas, todas de forma virtual, em razão do estado de pandemia, que orientava o distanciamento social. Ressalta-se que neste momento o objetivo não era a aplicação para profissionais da área, nem

para especialistas, mas para estudantes e profissionais que contribuíssem para apontar melhorias na interpretação e na semântica do instrumento.

Ademais, a proposta dessa rodada também era registrar o tempo médio de resposta do instrumento para que o respondente tivesse uma estimativa de quanto tempo seria preciso dedicar para o preenchimento do questionário.

Na primeira rodada do grupo foco (Quadro 5), o questionário (*Google Forms)* foi enviado para 9 (nove) pessoas entre os meses de junho a julho de 2020, sendo que os participantes tinham a seguinte titulação: doutorado (1), mestre (2), mestrando (1), graduado (2), graduando (3). Foram apontadas considerações de forma individual, repassando-as a este pesquisador, resultando no seguinte:

Quadro 5 – Primeira rodada grupo foco para considerações instrumento Araujo (2018)

| **Participante 01 – UFSC/Doutor** |
|---|
| Considerações: |
| Respondeu em 37 minutos; |
| A partir da fase 7 já estava cansado; |
| Sugeriu no início (pode ser na introdução) do questionário um mapa indicando as 10 fases e o que será abordado em cada uma. Assim o respondente já se prepara. Sugeriu fazer um esqueleto (mapa ou fluxograma); |
| Não verifica necessidade do código inicial, sugere retirar; |
| Na questão Rsp-03-0 não tem a opção que reflete, “eu não saberia responder pela minha equipe”, o mesmo ocorre em outras como na Dmc-03-3; |
| Na fase 6, segurança da informação, sugere tirar a opção "nenhuma das alternativas"; |
| Na fase 7, Prj-01-0, por que o termo "convém"? Sugere tentar reescrever e também retirar a alternativa " nenhuma das alternativas"; |
| Na Prj-03-0; na RV1-01-1; na RV1-02-1; na RV1-02-2 por que a palavra frequente na pergunta e também nas opções? Sugere retirar e reestruturar a pergunta deixando só nas alternativas. |
| **Participante 02 – UFSC/Mestrando** |
| Considerações: |
| Respondeu em 28 minutos; |
| Etc_01_0 e Rsc_03_0 as perguntas estão fora de contexto comparado ao bloco todo; |
| Bloco 7, das Diretrizes, na descrição, o texto ficou confuso, teve que ler três vezes para entender o significado. |
| **Participante 03 – UFSC/Mestre** |
| Considerações: |
| Respondeu em 32 minutos; |
| Acredita que é um ótimo questionário e bem completo, não verifica necessidade de alterações; |
| Relata que o instrumento já possui uma chamada técnica para aplicação para a Lei Geral de Proteção de Dados. |
| **Participante 04 – UFSC/Graduando** |
| Considerações: |
| Respondeu em 15 minutos; |
| Poderia ser retirado aquelas nomenclaturas no início de cada pergunta? Acredita que deixará a leitura mais clara; |
| Tem uma pergunta sobre quem o respondente acha que é responsável pela segurança das informações, ou seja, ele gostaria de marcar mais de uma opção nessa pergunta, mas o formulário só permite uma; |
| Não entendeu muito bem aqueles textos iniciais de descrição e diretriz, qual seria o intuito deles no formulário; |
| Rvl_02_0 um tópico pergunta sobre a frequência em que um funcionário deveria reavaliar seus hábitos, contudo, as opções de resposta parecem abstratas (exemplo: o que seria frequentemente em dias? Um dia sim e outro não?). |
| **Participante 05 – UFSC/Mestre** |

| Considerações: |
|---|
| Respondeu em 29 minutos; |
| Não entendeu a codificação inicial, mas com o tempo se adaptou a ela; |
| Na questão Csc_03_0 entendeu que ficaria melhor: Severa (afeta a credibilidade) - Leve (não afeta a credibilidade); |
| Está bem longo, mas muito bom. |
| **Participante 06 – UniSATC/ Graduando** |
| Considerações: |
| Respondeu em 24 minutos; |
| Não entendeu o significado de “Csc_01_0”, “Rsp_01_0”, ou seja, da codificação; |
| Na pergunta “Com que frequência você trata de assuntos relacionados a sua organização nos seguintes ambientes?” algumas opções parecem muito especificas, como “em sala de embarque do aeroporto”, não entendeu o motivo; |
| Na pergunta 'Rsc_03_0 enquanto você está na sua posição de trabalho, com que frequência você costuma:' não fica claro se é na estação de trabalho (mesa) ou no local de trabalho (prédio). Por exemplo, o participante costuma se alimentar apenas no refeitório, não na sua mesa; |
| Na pergunta 'Rsc_04_0 quando você recebe um e-mail com arquivo anexo, com que frequência você costuma: ' poderia ter duas opções: 'abrir o anexo caso seja de um remetente conhecido' e 'abrir o anexo de um remetente desconhecido' ou algo assim. |
| **Participante 07 – UniSATC/ Graduando** |
| Considerações: |
| Respondeu em 40 minutos; |
| Csc_02_1 as informações da organização têm valor financeiro? Não compreendeu essa pergunta; |
| Acha importante identificar o significado de alguns termos, por exemplo, o que é o processo de “classificação das informações”, para que todos consigam compreender; |
| Na questão sobre a pessoa estranha dentro da organização, geralmente só avisaria se a pessoa parecesse suspeita, porque entra tanta gente em seu ambiente de trabalho que não sabe se está fazendo entrevista, se veio arrumar alguma coisa ou se vai falar com alguém; |
| Na pergunta: “ao receber um e-mail com conteúdo tipo SPAM (propagandas, anúncios, entre outros), com que frequência você” geralmente eu apago o e-mail, senti falta de uma opção nesse estilo; |
| Numeração das páginas (para ter uma ideia de começo, meio e fim); |
| Nomenclatura no começo de cada pergunta não fez muito sentido, seriam para dividir seções? |
| **Participante 08 – UniSATC/ Graduando** |
| Considerações: |
| Respondeu em 30 minutos; |
| Sentiu falta de informação de quantas páginas de perguntas teria para responder; |
| Não entendeu porque cada pergunta tinha um código no início. |
| **Participante 09 – UNISUL/Graduado** |
| Considerações: |
| Respondeu em 30 minutos; |
| Csc_03_0 e se a pessoa não trabalha em uma empresa? Respondeu levando em consideração onde trabalha; |
| Csc_05_1 sabe a marca mas não sabe o modelo; |
| Rsp_01_0 colocou sempre, pois acredita que todos devem participar e deve ter uma política para isso; |
| Rsp_02_3 verificaria sempre se soubesse como fazer o procedimento; |
| Rpt_04_1 olharia o que tem no *pendrive* para saber de quem é e tentaria devolver; |
| Etc_05 levou em consideração para responder locais onde já trabalhou; |
| Prj_02_0 nunca passou por tal situação para saber avaliar; |
| Gts_01_3, GTS_01_05 e GTS_01_06 não sabe avaliar |
| GTS_01_4 "Sempre" - caso exista uma orientação da empresa de como fazer. |

Fonte: Dados da pesquisa.

Ao finalizar a primeira rodada, foram realizadas as devidas alterações que o pesquisador e sua orientadora julgaram importantes para que o instrumento ficasse adequado ao ambiente organizacional da instituição financeira, bem como ao período pandêmico da

pesquisa e para que ficasse conciso e coerente, evitando interpretações dúbias, conforme apontado pelos respondentes.

A segunda rodada se consubstanciou em realizar uma reunião online através de plataforma digital de conferência com alunos da professora orientadora, acadêmicos da graduação da UFSC, todos membros do LABeGIS, em 08 de julho de 2020, totalizando 6 participantes. Nesta etapa, os envolvidos estavam de maneira síncrona visualizando o instrumento através do *Google Forms* e fazendo anotações e observações, que ao final, foram repassadas ao pesquisador.

Nesta etapa, resultaram as seguintes observações:

- Necessidade de um fluxograma;
- Inserir progresso do respondente durante o preenchimento;
- Retirar a codificação inicial.

As demais observações foram apenas dúvidas sem relevância para sugerir alterações, o que demonstrava que o instrumento estaria em um estágio satisfatório de leitura, tempo e interpretação para aplicação em uma escala maior.

Dessa forma, o pesquisador e sua orientadora debateram quais ainda seriam os itens que sofreriam alterações, o que foi realizado na data de 23 de julho de 2020. Ainda, foi definido que antes da disponibilização do questionário para resposta dos gestores da tecnologia da informação de unidades do sistema financeiro, o instrumento deveria ser avaliado pelo seu autor, o Dr. Pedro Henrique de Moura Araujo, em envio por e-mail em 30 de julho de 2020, tendo recebido parecer favorável em 03 de agosto de 2020, quanto a não verificação de irregularidades, possibilitando a aplicação e coleta dos dados.

### 3.3.2 Coleta dos dados

Com a etapa de adaptações concluída e apresentada ao autor do instrumento, passa-se a efetiva coleta das informações, através de ferramenta *on-line* do *Google Forms*.

A autorização para aplicação da pesquisa no sistema foi obtida com a apresentação do questionário para a diretora operacional responsável pela segurança da informação da central do sistema, objeto de pesquisa em Santa Catarina e Rio Grande do Sul, a qual inclusive participou como especialista na etapa da adaptação do instrumento.

Foi obtido parecer favorável quanto ao conteúdo em 05 de junho de 2020, com a observação que cada cooperativa singular teria competência para decidir sobre a participação de seus gestores de tecnologia da informação.

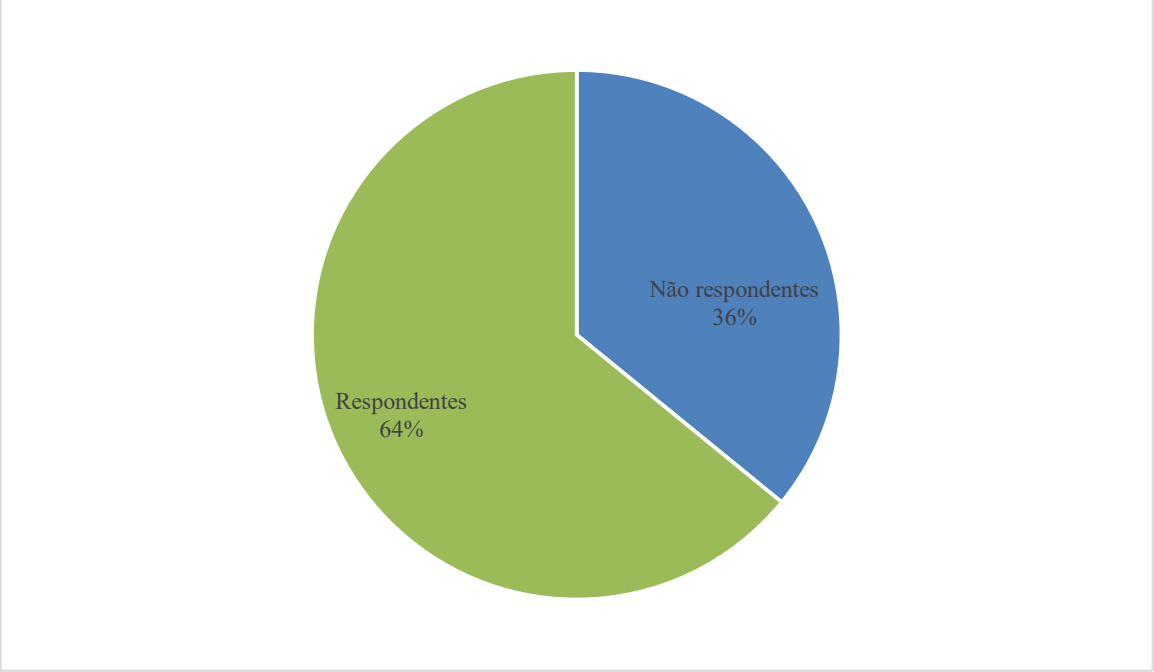
Dessa forma, foram colhidas informações de contato de todos esses gestores das cooperativas singulares, totalizando trinta e nove pertencentes ao sistema. Através de *chat* interno (este pesquisador teve acesso em decorrência de seu vínculo empregatício) e e-mail, foram agendados encontros *on-line*, objetivando explicar os procedimentos para coleta de dados.

Durante os dias 02, 03 e 04 de setembro de 2020 aconteceram três reuniões através da plataforma *Microsoft Teams* (o respondente tinha a opção de escolher o dia para participar), com objetivo de sensibilizar os gestores de TI quanto a importância da coleta de dados e da veracidade das informações por eles prestadas. O pesquisador esclareceu que todos os dados são anonimizados, sendo impossível identificar qualquer respondente ou sua instituição.

Por fim, ainda na reunião, foi informado que se trata de uma pesquisa acadêmica sob supervisão de uma professora doutora da UFSC e que os dados são utilizados, única e exclusivamente, para pesquisa, informações estas que constam no cabeçalho do instrumento no *Google Forms*.

Como apenas treze gestores da SI participaram das reuniões, optou-se também por ser disponibilizado um vídeo gravado com o mesmo conteúdo, o que foi feito, através de *link* do *Youtube,* no dia 07 de setembro de 2020, mesma data que foi habilitado a coleta das informações, também através de *link* enviado por e-mail e por *chat*, encerrando em 20 de setembro de 2020 com vinte e cinco respondentes (Figura 11).

Figura 11 – Número de convidados X respondentes da pesquisa




Fonte: Dados da pesquisa.

De forma complementar, decidiu-se por verificar a divulgação do estatuto social pelas singulares em seus sites, pois, as cooperativas têm como pressuposto a transparência administrativa e por conseguinte, o *disclosure* das informações, o que é estritamente ligado à temática deste trabalho.

Com os dados coletados e as informações necessárias, passa-se então ao tratamento, etapa na qual é possível chegar a novos resultados e suas discussões.

### 3.3.3 Tratamento dos dados

Com o término da aplicação do questionário, este pesquisador, sua orientadora e Araujo, autor do instrumento original, reuniram-se em 10 de dezembro de 2020 para repasse do banco de dados obtido junto aos gestores de TI das instituições financeiras cooperativistas, explicitando o contexto do segmento pesquisado, possibilitando que Araujo procedesse a inserção de dados no sistema desenvolvido para sua tese, o que forneceria diretamente os *scores* para mensurar o nível da cultura de segurança da informação em instituições financeiras de um sistema cooperativista.

O *output* do sistema de Araujo foi recebido em 07 de fevereiro de 2021 e em 18 de fevereiro de 2021, os três pesquisadores reuniram-se para alinhamento da análise dos dados.

Dessa forma, dos 149 itens no instrumento, o *software* considerou como necessários para o cálculo do *score* de cada respondente (representando cada uma das instituições financeiras pertencentes ao sistema) apenas os itens cujas categorias apresentavam frequência de resposta adequada, totalizando 55 itens.

De forma complementar, os resultados são apresentados na ótica da estatística descritiva, ilustrando os resultados em percentuais e gráficos.

## 3.4 PROCEDIMENTOS PARA COLETA DE DADOS: EIXO TRÊS – PRIVACIDADE DA INFORMAÇÃO E PROTEÇÃO DE DADOS

Objetivando uma melhor compreensão da unidade de estudo, inclusive quanto à cultura de privacidade da informação e em relação à LGPD, foi construído um instrumento específico para coleta de dados, o que se deu através de entrevistas com alguns dos gestores de TI, sendo que todos os que participaram desta etapa também foram respondentes do primeiro instrumento.

### 3.4.1 Entrevistas

O objetivo da entrevista é a obtenção de informações do entrevistado sobre determinado assunto, sendo que neste estudo, foi optado pela entrevista estruturada, que segundo Marconi e Lakatos (2017) segue um roteiro estabelecido, com pessoas selecionadas e as diferenças das respostas devem refletir diferenças dos respondentes e não, nas perguntas.

Quanto à classificação das perguntas do questionário elaborado para a entrevista, optou-se por perguntas abertas, o que, conforme Marconi e Lakatos (2017), permitem ao informante responder livremente, com sua linguagem própria e com a emissão de opiniões, conferindo ao pesquisador investigações mais profundas. Gil (2018) aponta que a definição da modalidade de entrevista aberta, com questões e sequência predeterminada, permite ampla liberdade para o respondente.

Dessa forma, o instrumento foi constituído de várias perguntas abertas, divididas em dimensões, as quais referem-se aos princípios[51] que norteiam a LGPD, descritos no artigo 6º da legislação, sendo eles: finalidade, adequação, necessidade, livre acesso, qualidade dos dados,

[51] Também abordados no item 2.4 deste trabalho. Para fins deste trabalho, princípios e dimensões foram tratados como sinônimos.

transparência, segurança, prevenção, não discriminação e responsabilização e prestação de contas.

Para tanto, verificou-se que analisar todos os setores e processos que tratam algum tipo de dado pessoal na instituição tornaria a pesquisa inexequível, motivo pelo qual optou-se por restringir as perguntas a três subdimensões (específicas ao tratamento de dados): associação ao sistema cooperativista, recrutamento de colaboradores e campanhas de marketing e comunicação.

Elaborado os itens com auxílio e contribuição do especialista 01, que inclusive concordou com o recorte nas subdimensões descritas anteriormente, o instrumento passou por análise de uma banca de outros três especialistas (ver Quadro 6), em reuniões online realizadas por *vídeo calls*, durante os dias 18 e 19 de maio de 2021, os quais apontaram sugestões de melhoria e possíveis interpretações destoantes do objetivo do instrumento, bem como considerações gerais.

Após este procedimento, o pesquisador e sua orientadora definiram quais alterações seriam realizadas, as que, sob a ótica deles, seriam importantes.

Do corpo de especialista tem-se (Quadro 6):

Quadro 6 – Corpo de especialista para considerações no instrumento do autor

| **Especialista 01 – Encontro em 17/04/2021** |
|---|
| **Doutor (UFSC) em engenharia e gestão do conhecimento, graduado em ciências da computação e direito, professor universitário, empresário do ramo de *compliance* e consultor de segurança e privacidade da informação.** |
| Considerações: |
| Transformar o artigo 9º da LGPD em perguntas específicas; |
| Perguntar se existe um aviso legal nas três subdimensões; |
| Usar algo com *leads*, voltado a marketing e propaganda; |
| Ade_02, Ade_04, Nec_02, Nec_03, Lia_03 muito amplas, dividir em mais questões; |
| Transformar em pergunta: A instituição permite o acesso dos dados pessoais pelo titular? |
| Dimensão da qualidade dos dados, deixar apenas a integridade; |
| Tra_01 alterar para colaboradores, não apenas agentes de tratamento; |
| Tra_02 retirar e colocar no final; |
| Tra_03 retirar na parte final e inserir na segurança; |
| Na dimensão da transparência, elaborar algo sobre acesso à informação clara e objetiva no aviso legal; |
| Na dimensão da segurança, perguntar se existe uma política de privacidade; |
| Pre_02 existe um procedimento de gestão de riscos formalizado na instituição para prevenir a ocorrência de incidentes a segurança da informação? |
| Nad_02 explicar melhor a pergunta; |
| Na dimensão da responsabilização e prestação de contas, verificar auditoria interna e externa e quais são elas. |
| **Especialista 02 – Encontro em 18/05/2021** |
| **Mestre (UFSC) em direito, professor universitário, empresário e consultor do ramo de proteção de dados.** |
| Considerações: |
| Fin_01_03, Fin_02_03 e Fin_03_03 mais ligadas ao princípio da necessidade; |
| Fin_01_04, Fin_02_04 e Fin_03_04 aviso legal está relacionado ao princípio da transparência; |

| |
|---|
| Na dimensão da necessidade, talvez um item sobre o tratamento de dados em base já existente; |
| Na dimensão da segurança, pensar na possibilidade de entrar mais em questões técnicas; |
| **Especialista 03 – Encontro em 19/05/2021** |
| **Mestre (UFSC) em direito, graduado em direito e ciências da computação** |
| Considerações: |
| Na dimensão da finalidade, o respondente talvez encontre alguma dificuldade na resposta, o pesquisador deve ficar atento ao perguntar para manter a qualidade da informação;<br>Sentiu falta de algo relacionado ao ciclo de vida do dado pessoa; |
| Na dimensão da adequação, acredita que o respondente não será sincero; |
| Nec_02_02 O termo justificativa seria o melhor? Ver a equivalência na LGPD; |
| Na dimensão da necessidade, perguntas como: o respondente estabelece critérios para definir a necessidade do tratamento? Quando um dado é necessário? Quando é adequado? Qual o critério utilizado? |
| Na dimensão do livre acesso, o que o respondente entende como imediatamente? Quais informações são prestadas na resposta sobre a consulta de dados? |
| Qua_02_01 incluir também a retificação; |
| Na dimensão da qualidade dos dados, incluir uma pergunta de como a cooperativa faz a validação dos dados; |
| Tra_03_01 informações claras sobre o que? |
| Seg_03_01 abordar melhor a política de privacidade, verificar a letra da lei; |
| Na dimensão da não discriminação, seria interessante abordar o direito de explicação em sistemas automatizados; |
| Na dimensão da responsabilização e prestação de contas, quais documentos a cooperativa gera como subsídio para a prestação de contas? Há contratos e acordos de tratamento de dados com terceiros? Explicar melhor também que as auditorias se tratam de SI; |
| **Especialista 04 – Encontro em 19/05/2021** |
| **Especialista em Gestão da Segurança da Informação e em direito digital e *compliance*, graduado em direito, advogado na área de tecnologia e *cybersegurança*.** |
| Considerações: |
| Analisar as respostas dos gestores de TI com respondentes colaboradores; |
| Talvez o gestor de TI não seja capaz de responder quanto ao setor de Gestão de Pessoas; |
| Na dimensão da finalidade, sentiu falta de coleta de dados através de *cookies;* |
| Na dimensão da adequação, acredita que o gestor de TI não tenha conhecimento para responder de forma suficiente quanto a divergência entre o aviso legal e o que acontece na prática; |
| Verificar a possibilidade do respondente ser o DPO; |
| Na dimensão da necessidade, acredita que o respondente não tenha plena noção das bases legais; |
| Lia_04_02 alterar para “como é feita”; |
| Verificar se onde a qualidade dos dados está no instrumento é o melhor momento e é a primeira vez que o especialista verifica questões direcionadas ao gestor de TI; |
| Incluir Tra_01_00 governança geral dos colaboradores, não somente quanto a LGPD; |
| A instituição tem um SGSI? Incluir isso na transparência; |
| Instituições financeiras obrigatoriamente já tem SGSI e Política de Privacidade da Informação; |
| Na dimensão da prevenção, rever se não está muito parecido com a dimensão da transparência; |
| Pre_02_01 já deve existir procedimento de gestão de risco formalizado, explorar melhor o item; |
| Rpc_02_01 com que frequência é realizada a auditoria, isso melhoraria a qualidade da resposta. |
| Rpc_03_02 talvez o respondente não saiba a metodologia; |
| Na dimensão da responsabilização e prestação de contas, acha interessante explorar o histórico das auditorias; |
| Na dimensão do livre acesso, segurança, não discriminação e responsabilização e prestação de contas: talvez as respostas sejam simplistas e limitem-se a sim ou não; |
| Acha importante ter questão aberta: o que deve melhorar em sua instituição? |

Fonte: Dados da Pesquisa.

Realizadas as alterações e estando adequado o instrumento[52] para aplicação com os gestores de TI, foi procedido as entrevistas nos dias 04, 11 e 14 de junho de 2021, com três gestores de TI que atuam como DPOs em suas respectivas cooperativas.

A primeira entrevista se deu pessoalmente, por se tratar de uma instituição mais próxima geograficamente. No momento da coleta, a instituição contava com uma sede administrativa, vinte e cinco agências e aproximadamente duzentos e cinquenta colaboradores; a segunda entrevista foi realizada de forma virtual e no momento da coleta, a cooperativa contava com uma sede administrativa, noventa e uma agências e mais de mil e duzentos colaboradores; a terceira entrevista foi virtual e a instituição era formada por uma sede administrativa, 11 agências e aproximadamente 50 colaboradores, conforme Quadro 7:

Quadro 7 – Estrutura das unidades pesquisadas no eixo três

| Instituição | Unidades | Colaboradores[53] |
|---|---|---|
| Alpha | Sede + 25 agências | 250 |
| Beta | Sede + 91 agências | 1200 |
| Gama | Sede + 11 agências | 50 |

Fonte: Dados da pesquisa.

A condução da entrevista se deu a partir da leitura do pesquisador do cabeçalho e dos itens e quando não compreendido, era refeita a leitura com as devidas explicações, de forma a evitar dúvidas. As anotações feitas pelo pesquisador das declarações não eram visíveis ao entrevistado, evitando influenciar suas respostas.

Realizada a coleta, os dados foram analisados através de avaliação de risco, possibilitando a compreensão, ainda que de forma inicial, de como algumas singulares da unidade de estudo estão se comportando em relação à SI, PI e PD quanto à implementação da LGPD.

Dessa forma, a análise das informações obtidas foi realizada de forma a permitir a visualização de não conformidades, as fundamentações legais e normativas dessas irregularidades e ainda o risco que a não adequação poderia gerar para a instituição. Ademais, foi possível compará-los e discuti-los com contribuições que a literatura científica dispõe nesse tocante.

Como os três gestores respondentes deste segundo questionário (eixo três) também participaram da primeira pesquisa (eixo dois), foi possível confirmar ou não, tópicos

[52] Material disponível no Apêndice B.
[53] O objetivo é dar noção da estrutura da instituição, por isso, o número é aproximado.

apresentados nos itens do primeiro questionário, relacionando as temáticas de SI, PI e PD, inclusive, quanto à pré-disposições de comportamento e cultura organizacional.

Por fim, os dados são apresentados no capítulo 4, sob a forma de resultados e discussões, tanto do eixo dois quanto do eixo três, conforme o delineamento da pesquisa definida para esta dissertação (conforme Figura 10).

## 3.5 ESTUDO DE CASO: O SISTEMA FINANCEIRO COOPERATIVISTA

O estudo foi realizado em um sistema financeiro cooperativista, objetivando mensurar o nível de cultura organizacional da segurança da informação daquele ambiente, sob a ótica de seus gestores. Este pesquisador foi colaborador de uma das instituições pertencente ao sistema, o que motivou a aplicação dos questionários nesse segmento, buscando um enfoque prático, que possa contribuir, de alguma maneira, para o desenvolvimento do mercado e da instituição.

### 3.5.1 O cooperativismo

Uma cooperativa é uma associação autônoma de pessoas, que buscam de forma voluntária atender aspirações comuns, econômicas, sociais e culturais, de forma democrática e por meio de empreendimento de propriedade comum (ORGANIZAÇÃO INTERNACIONAL DO TRABALHO, 2020).

Para a *International Co-operative Alliance* (ICA, 2021)cooperativa é uma empresa centrada nas pessoas e que pertence aos seus membros, os quais controlam e orientam para responder as ambições e necessidades econômicas, sociais e comuns. São instituições baseadas em valores, administradas democraticamente e que compartilham princípios internacionais para construir um mundo melhor por meio da cooperação.

Também pode ser definida como uma sociedade autônoma constituída por pessoas que voluntariamente se unem, buscando satisfazer necessidades e aspirações econômicas, sociais e culturais, por meio de uma empresa comum gerida de forma democrática (FARDINI, 2017).

Frantz (2012) destaca que o termo cooperativismo deriva do latim, composto por "*cum*", que significa "em companhia de", juntamente com "*operari*", que significa "trabalhar", trazendo em sua origem história a noção de trabalho em conjunto, expressando um movimento social. É baseado no mutualismo, ou seja, grupos sociais fornecem benefícios mútuos e

assistência entre si. Traz em seu conceito a ideia de altruísmo, cidadania e ideologia (SOARES; MELO SOBRINHO, 2015).

Para Frantz (2012), o movimento cooperativista deve ser interpretado como uma prática social com questões do mundo e da vida, que nasce de fenômenos sociais complexos de indivíduos com o mesmo propósito de fortalecer a instituição e alcançar resultados, predominantemente, de ordem econômica. É, em seu princípio constituinte, um acordo racional sobre economia, interesses e necessidades diante da produção e a distribuição de bens e riquezas. A operacionalização destes fins se dá nos espaços da empresa cooperativa, mediada pela comunicação.

Fardini (2017) aponta que George Jacob Holyoke defendeu, em seu livro Os 28 Tecelões de Rochdale, que uma cooperativa ajuda a distribuir riquezas e não prejudica a fortuna, não molesta o Estado e é transparente, não busca privilégios e honrarias e não teme a concorrência, mas a deseja de forma honesta, é contra o monopólio e sublima a responsabilidade e a participação de todos no progresso.

Rochdale, cidade na Inglaterra dos tecelões citados por Holyoke, torna-se o berço do moderno movimento do cooperativismo[54], em um cenário de Revolução Industrial, com vistas ao oferecimento de bens de consumo a preços mais acessíveis ao proletariado. Nesse contexto, surgiram doutrinadores que pregavam programas sociais, como John Bellers, Robert Owen, Willian Thompson e Willian King, muitos deles com participação no pensamento cooperativista. Rochdale inicia esse movimento, em 1844, com a primeira cooperativa de consumo com admirável capacidade de sobrevivência (SOUZA, A. S. de, 1990).

A Organização das Cooperativas do Brasil – OCB aponta que o movimento surgiu quando o mundo experimentava o início da doutrina econômica liberal, concepção sistematizada por Adam Smith (FARDINI, 2017).

Os vinte e oito tecelões pobres e necessitados fundavam a *Rochdale Society of Equitable Pioneers*, depois de uma fracassada greve desses trabalhadores do setor têxtil, com forte apelo por fundamentos sociais de cooperação, sobretudo de educação para membros e crianças e um programa de diretrizes para a abstinência, pois a miséria levava ao consumo de álcool. Em Rochdale também ocorre uma transformação com a introdução das mulheres como associadas, possibilitando sua independência civil, pois muitos homens eram desinteressados

[54] Termo utilizado para descrever o movimento pós pré-cooperativismo, ou seja, quando as cooperativas estavam organizadas de tal ponto a terem real capacidade de sobrevivência, com fundamentos descritos e formalizados. O cooperativismo moderno ocorre com diferenças cronológicas pelo mundo, a depender do contexto geográfico.

pela cooperativa. Essa reação prática ao individualismo liberalista, como meio de aprimoramento social, dá origem aos estatutos que normatizam princípios, cultivados até hoje no mundo todo (SOUZA, A. S. de, 1990).

O movimento cooperativo não iniciou apenas em Rochdale, mas foi lá que se transformou em um modelo de organização resultado de longas experiências e lutas sociais. Não foi criado pelo grupo de tecelões, o que eles fizeram foi sistematizar as experiências de cooperação realizadas ao longo de décadas para superar problemas sociais graves (FRANTZ, 2012).

Com o advento da Revolução Industrial, o Estado liberal se tornou cada vez mais poderoso, o que alavancou a economia, entretanto, levou a uma situação caótica de expressiva exclusão social, êxodo rural, altas taxas de desemprego, péssimas condições de trabalho, salários baixos e condições desumanas para crianças e mulheres. O liberalismo condicionou as pessoas a buscarem por conta própria soluções para os problemas sociais e transposição das barreiras para a sobrevivência. Como alternativa, o cooperativismo era uma possibilidade de acesso a bens, serviços e trabalho em tempos de desigualdade (FARDINI, 2017).

Charles Gide, responsável por sistematizar a doutrina cooperativista, enumerou virtudes que ficaram conhecidas no mundo todo: 1 – viver melhor; 2 – pagar a dinheiro; 3 – poupar sem sofrimento; 4 – suprimir os parasitas; 5 – combater o alcoolismo; 6 – interessar as mulheres nas questões sociais; 7 – educar economicamente o povo; 8 – facilitar a todos o acesso à propriedade; 9 – reconstruir uma propriedade coletiva; 10 – estabelecer o preço justo; 11 – eliminar o lucro capitalista, 12 – abolir os conflitos (FARDINI, 2017).

Quanto aos princípios e virtudes do cooperativismo, do texto original de 1845 da *Rochdale Society of Equitable Pioneers*, é possível extrair os enunciados: 1 – livre adesão; 2 – controle democrático; 3 – devolução de sobras e excedentes; 4 – juros limitados ao capital; 5 – neutralidade política, religiosa e racial; 6 – vendas a dinheiro e à vista; e 7 – fomento do ensino (FRANTZ, 2012; MEINEN; PORT, 2014).

Hoje, a Aliança Cooperativa Internacional, em três revisões realizadas em 1937, 1966 e 1995, com objetivo de alinhamento com a dinâmica social e os novos tipos cooperativos, definiram como diretrizes fundamentais: 1 – adesão livre e voluntária; 2 – gestão democrática; 3 – participação econômica; 4 – autonomia e independência; 5 – educação, formação e informação; 6 – intercooperação; 7 – interesse pela comunidade (FARDINI, 2017). Esses princípios é que diferem o sistema cooperativo de outras organizações, pois tem compromisso

com a comunidade e por um mundo sustentável, o que o coloca em destaque inclusive pela ONU como organização socioempreendedora em ações globais (MEINEN; PORT, 2014).

Esses princípios que regem todas as cooperativas no mundo criaram um modelo de negócio com visão de longo prazo e crescimento econômico sustentável, desenvolvimento social e responsabilidade ambiental, fazendo com que mais de 12% (doze por cento) da população mundial faça parte de uma das três milhões de cooperativas do planeta, gerando uma renda aproximada de 2.035.000.000 (dois bilhões e trinta e cinco milhões) de dólares (ICA, 2020).

No Brasil, a primeira cooperativa estabelecida, apesar de inúmeros registros de experiências pré-cooperativas, foi a Sociedade Cooperativa Econômica de Ouro Preto, em outubro de 1889. Em aspectos jurídicos, a Lei 5.764/71 disciplinou o regime jurídico dos empreendimentos cooperativistas, bem como a CF[55] assegura o cooperativismo como direito fundamental do cidadão (FARDINI, 2017).

O número de cooperativas no país em 2019 era de 5.314 (cinco mil, trezentas e quatorze), resultando em 15.539.376 (quinze milhões, quinhentos e trinta e nove mil e trezentos e setenta e seis) cooperados, distribuídos em 38% (trinta e oito por cento) mulheres e 62% (sessenta e dois por cento) homens. O sistema cooperativista emprega 427.576 (quatrocentos e vinte e sete mil, quinhentos e setenta e seis) colaboradores, destes, 65% (sessenta e cinco por cento) homens e 35% (trinta e cinco por cento) mulheres (OCB, 2020).

Dessa forma, 40% (quarenta por cento) da população brasileira conhece o cooperativismo, reconhecendo o sistema como competitivo, íntegro e capaz de gerar felicidade para as pessoas (OCB, 2019).

As cooperativas podem ser classificadas de acordo com seu ramo de atuação e são representadas pela OCB (BRASIL, 1971)[56]. Dentre as suas peculiaridades e diferenças com associações e empresas mercantis, podemos destacar, conforme Quadro 8:

[55] CF, artigo 5º, inciso XVIII: a criação de associações e, na forma da lei, a de cooperativas independem de autorização, sendo vedada a interferência estatal em seu funcionamento (BRASIL, 1988);

[56] PNC, artigo 105: A representação do sistema cooperativista nacional cabe à Organização das Cooperativas Brasileiras - OCB, sociedade civil, com sede na Capital Federal, órgão técnico-consultivo do Governo, estruturada nos termos desta Lei, sem finalidade lucrativa, competindo-lhe precipuamente: g) dispor de setores consultivos especializados, de acordo com os ramos de cooperativismo (BRASIL, 1971).

Quadro 8 – Diferenças entre cooperativas, associações e empresas mercantis

| Parâmetro de diferenciação | Cooperativa | Associação | Empresa mercantil |
|---|---|---|---|
| Finalidade | Com fins econômicos, mas sem objetivo de lucro | Sem fins lucrativos, podendo exercer atividade comercial | Com fins lucrativos |
| Membros mínimos para constituição | Vinte cooperados (podendo alterar de acordo com o ramo) | Dois associados | Um empresário |
| Objetivo | Prestar serviços ao cooperado | Representar os interesses dos associados | Lucrar |
| Voto | Cada cooperado tem direito a um voto | Cada associado tem direito a um voto | Maior o capital, maior o poder de voto |
| Capital social | Quotas-parte | Não possui | Ações dos proprietários |
| Cotas | Intransferíveis | Não possui | Transferíveis |

Fonte: Adaptado de Fardini (2017).

Quanto aos tipos de cooperativas existentes, até 2018, tinha-se 13 (treze) ramos, entretanto, em 2019, foi aprovada a reorganização em 7 (sete), conforme Figura 12. A Lei 5.764 de 1971, que define a PNC e institui o regime jurídico das sociedades cooperativas não exige a divisão em setores, portanto, cabe a OCB a divisão interna para melhor alcance de seus objetivos legais. Atualmente, temos os seguintes ramos (BRASIL, 1971; FARDINI, 2017; OCB, 2020):

Figura 12 – Ramos do cooperativismo


Fonte: Adaptado de Fardini (2017) e OCB (2020).

Assim, considerando os ramos atualmente existentes no cooperativismo brasileiro, a instituição financeira, objeto do estudo de caso, enquadra-se no cooperativismo de crédito.

### 3.5.2 O cooperativismo de crédito

A manifestação cooperativa de crédito se diferencia das demais pela prestação de serviços financeiros, com produtos e serviços inerentes à atividade de um banco convencional, mas com particularidades, que diferenciam tais organizações.

Dentre esses serviços, destacam-se promoção da poupança, financiamento de negócios, com taxas de juros, tarifas e prazos adequados às necessidades financeiras, utilizando os recursos de maneira sustentável (FARDINI, 2017).

Dessa forma, bancos e cooperativas financeiras são instituições distintas, conforme apontam Meinen e Port (2014), no Quadro 9:

Quadro 9 – Diferenças entre bancos e cooperativas financeiras

| Bancos | Cooperativas |
|---|---|
| Sociedades de capital. | Sociedades de pessoas. |
| Exercício de poder na proporção do número de ações. | Exercício de poder pelo voto (com igual peso, uma pessoa, um voto). |
| Deliberações concentradas. | Decisões compartilhadas entre muitos. |
| Administrado por terceiros (do mercado). | Administrado por associados. |
| Usuário dos serviços é o cliente. | Usuário dos serviços é o próprio dono (associado). |
| Pode existir distinção de usuários. | Vedada a distinção de associados (artigo 37 da Lei nº 5.764/71). |
| A remuneração das operações não tem parâmetro definido e limite. | A referência para preços das operações e serviços é o custo e as necessidades de reinvestimento. |
| Visam lucro por excelência. | Não objetivam lucro (artigo 3º da Lei nº 5.764/71). |
| Não há divisão de lucros com os clientes. | O excedente (sobras) é distribuído aos associados. |

Fonte: Adaptado de Meinen e Port (2014).

As operações de crédito não são os únicos serviços disponibilizados pelas cooperativas e com o passar do tempo, o portfólio operacional tem sido substancialmente ampliado, uma evolução da nomenclatura de cooperativa de crédito para cooperativa financeira, pois, aquele destoa da realidade e da necessidade do setor. O termo “financeiro” é gênero, abrangendo a espécie “crédito” (MEINEN; PORT, 2014). Dessa forma, ambos os termos podem ser usados como sinônimos. A OCB, mesmo depois da alteração dos ramos do cooperativismo em 2019, manteve a nomenclatura “crédito” para o ramo.

O movimento cooperativista de crédito inicia em 1849, na Alemanha, ganhando força no final do século XIX e início do XX, também na Itália e Canadá. Na Alemanha, diferentemente do que aconteceu na Inglaterra (Rochdale), o movimento não nasce da iniciativa popular, mas da visão e dos esforços de Herman Schulze e Friedrich W. Raiffeisen, ambos preocupados com as problemáticas de deficiência de crédito para trabalhadores rurais e urbanos (FARDINI, 2017; FRANTZ, 2012).

No Brasil, a primeira cooperativa desse ramo foi fundada em 28 de dezembro de 1902, a Caixa de Economia e Empréstimo Amstad, em Nova Petrópolis – Rio Grande do Sul, por estímulo do padre Thedor Amstad, atualmente pertencente ao sistema Sicredi. Theodor Amstad veio ao Brasil juntamente com certa de oitenta mil alemães que buscavam novas oportunidades diante do cenário de crise que se instalava na Europa (FARDINI, 2017; FRANTZ, 2012).

Atualmente, considerando mais de 118 anos de existência do ramo no Brasil, as instituições financeiras sob o regime cooperativista, submetem-se à Lei Complementar nº 130,

de 17 de abril de 2009 – LC 130/09. São 827 cooperativas, 10,7 milhões de cooperados, 71,7 mil empregados e 6.043 pontos de atendimento, sendo que são as únicas instituições financeiras presentes em 594 municípios no país, o que as qualifica como importante agente de desenvolvimento social e econômico (OCB, 2020).

### 3.5.3 O Sistema Cooperativista de Crédito

No início dos anos oitenta, diante de um cenário de dificuldades no sentido de diminuição de recursos de fomento rural e do recrudescimento inflacionário, surge a necessidade de organização sistêmica das cooperativas singulares, inclusive para sua sustentabilidade no mercado de grandes bancos, que já estavam organizados de forma sistêmica. Surge então, um movimento no Rio Grande do Sul, liderado por Mário Kruel Guimarães, de integração horizontal e vertical das cooperativas (MEINEN; PORT, 2014).

Esse rearranjo institucional permite a implementação de pilares já fixados e que sustentam os modelos europeu e canadense, como autogestão com ênfase em capacitação, autoregulação e autofiscalização. Esse amadurecimento no sistema e o cenário de abertura normativa permitiram o surgimento dos bancos cooperativos, sendo eles: o Banco Cooperativo Sicredi – Banco Sicredi[57], em 1995 e o Banco Cooperativo do Brasil – Bancoob, hoje chamado Banco Sicoob[58], em 1996. Surgem também, as confederações dos sistemas, a Unicred[59] do Brasil, em 1994; a Confederação Sicredi, em 2000; o Sicoob Confederação, em 2001; e a Confesol, em 2008, atualmente chamada de Cresol[60] Confederação. A organização de todos os sistemas permitiu a criação do Fundo Garantidor do Cooperativismo – FGCoop, em 2013, garantindo os depósitos do quadro social (MEINEN; PORT, 2014).

É justamente nesse arranjo institucional, que reside o sistema do estudo de caso, não denominado para preservar a confidencialidade da pesquisa. É organizado em três níveis, ou seja, um nível federativo, chamado confederação, um interestadual, que abrange cooperativas de Santa Catarina e Rio Grande do Sul, chamado de central e o nível das singulares, cooperativas que compõem todo o sistema. A pesquisa foi realizada especificamente, com a Central Santa Catarina e Rio Grande do Sul, composta por 39 (trinta e nove) singulares.

---

[57] Sicred: Sistema de Crédito Cooperativo.
[58] Sicoob: Sistema de Cooperativas de Crédito do Brasil.
[59] Unicred: Instituição Financeira Cooperativa.
[60] Cresol: Cooperativa de Crédito Rural com Interação Solidária.

Pertencente ao sistema, em nível de Confederação, ainda há um banco, uma gestora de recursos de terceiros, uma provedora de soluções de previdência privada, uma administradora de consórcios e uma "bandeira de cartões", além de outras empresas que diretamente e indiretamente proporcionam o desenvolvimento de produtos e serviços, que trazem soluções financeiras para os cooperados.

## 3.6 DELIMITAÇÕES DO TEMA DE PESQUISA

A pesquisa, conforme Marconi e Lakatos (2017), pode ser delimitada quanto ao assunto, à extensão e outros fatores humanos, econômicos e de exiguidade, impedindo que se torne muito extensa ou complexa, abranja o que é possível no âmbito que se desenrola e fique restrita ao campo de atuação.

Nesse sentido, esta pesquisa foi definida com base em sua problemática, consistindo em responder o nível da cultura de segurança e privacidade da informação em instituições financeiras de um sistema cooperativista, sob a ótica dos gestores da Tecnologia da Informação.

Este pesquisador e sua orientadora definiram que, para o alcance da resposta ao problema de pesquisa e seu objetivo, seria necessário compreender a Segurança da Informação, a Privacidade da Informação e a Cultura Organizacional, através de métodos, procedimentos e técnicas para coleta e tratamento dos dados, que não são os únicos, tampouco melhores ou piores, mas que representam a escolha dos pesquisadores (o autor e sua orientadora) considerando a exequibilidade e a possibilidade de pesquisa no ambiente do sistema cooperativista.

Contando com um questionário já calibrado por Araujo (2018) e adaptado para o cenário da unidade de estudo de caso, considerando também o estado de calamidade pública causado pelo novo coronavírus, e o instrumento do eixo três, desenvolvido pelo pesquisador, os resultados obtidos não têm a pretensão de generalizá-los para o universo de todas as cooperativas ou instituições financeiras do Brasil, mas o de contribuir para a compreensão da temática e do cenário, além de apresentar oportunidades de melhoria para o segmento, fazendo com que o conhecimento científico ultrapasse barreiras acadêmicas e possa contribuir com o mercado.

# 4 RESULTADOS E DISCUSSÕES

Primeiramente, serão apresentados os resultados da aplicação da escala desenvolvida por Araujo (2018), que neste trabalho ocorreu com os gestores de um sistema financeiro cooperativista. Na sequência, constarão os resultados obtidos, através de entrevistas, quanto à privacidade da informação e proteção de dados, na visão de alguns dos gestores das unidades de estudo.

## 4.1 NÍVEL DE CULTURA DE SI DO SISTEMA PESQUISADO – EIXO DOIS

Aplicado o questionário com os representantes de cada instituição, partiu-se para o tratamento dos dados obtidos para a obtenção do *score*, iniciando a análise e discussão dos resultados.

A escala desenvolvida por Araujo (2018), utilizada neste trabalho, é composta de cinco níveis. Para tanto, tais níveis serão explicitados a seguir, tendo sido adaptados do original, p. 111-123, conforme Quadro10:

O **Nível 0 (Caos)** é o das organizações que não atingiram o nível mínimo de 65 pontos de segurança da informação e estão expostas a todos os tipos de riscos, inexistindo um padrão de comportamento estabelecido e há total desconhecimento sobre o tema. As iniciativas são isoladas, pessoais e sem fundamentação técnica, ou seja, meramente intuitivas. É impossível identificar as facetas e não há uma cultura de segurança da informação formalizada.

O **Nível 1 (Elementar)** é o das organizações acima de 65 até 75 pontos e que contemplam requisitos mínimos de comportamento de segurança da informação. Não é possível observar ainda uma relação entre colaborador e tecnologia da informação. Os comportamentos são ocasionais, não frequentes e só às vezes são observados. A preocupação com a segurança da informação por parte dos colaboradores é demonstrada de forma empírica e não sistemática.

O **Nível 2 (Em evolução)** corresponde às organizações acima de 75 até 90 pontos que possuem colaboradores que apresentam conhecimentos iniciais e superficiais sobre as temáticas de segurança e tecnologia da informação. Não há uma cultura de SI consolidada, mas há indícios de um preparo para atingir essa consolidação.

O **Nível 3 (Encaminhado)** refere-se às organizações acima de 90 até 120 pontos e que demonstram preocupação com a segurança da informação. O comportamento dos colaboradores

ainda aponta a condição “às vezes”, mas há incutido o comportamento “sempre”. Há condições que encaminham a organização em direção a uma cultura de SI plena.

O **Nível 4 (Otimizado)** é o das organizações acima de 120 pontos. Elas já estão posicionadas em uma cultura de segurança da informação estabelecida e os colaboradores entendem que a SI é vital para sua instituição. A preocupação se fundamenta em encontrar formas e procedimentos eficazes.

Para que a organização corresponda a um determinado nível, ela precisa necessariamente apresentar as características do nível anterior, acrescidas das características do nível inerente a sua pontuação. O Nível 3 (Encaminhado), por exemplo, pode ser considerado o de estabilidade cultural, pois os colaboradores já apresentam uma consciência e atitudes favoráveis à SI.

Quadro 10 – Níveis da escala de cultura da segurança da informação

| Nível | Regra |
|---|---|
| 0 – Caos | A quantidade de respondentes nesse nível é maior ou igual a 10%, independente dos níveis mais elevados. |
| 1 – Elementar | Menos do que 10% do nível anterior e a soma dos níveis 0 e 1 é maior ou igual a 10%. |
| 2 – Em evolução | A soma dos níveis anteriores deve ser menor que 10% e a totalização dos níveis 0, 1 e 2 é maior ou igual a 20%. |
| 3 – Encaminhado | Os níveis 0, 1 e 2 devem totalizar menos que 20% e deve ter menos de 30% no nível 3. |
| 4 – Otimizado | Mais de 70% dos respondentes devem estar no nível 4. |

Fonte: Adaptado de Araujo (2018).

Em relação a esta dissertação, foram 25 instituições participantes, representadas por seus gestores de TI, ou seja, cada respondente corresponde a uma instituição. Para fins acadêmicos, os dados foram anonimizados e optou-se pela descrição numérica para cada uma delas, nomeando-as de 1 (um) a 25 (vinte e cinto).

As organizações que estão na média atingiram *score* 100 (cem), portanto, são 14 (quatorze) instituições financeiras acima da média e 11 (onze) unidades abaixo da média (conforme Quadros 11 e 12). Contudo, todas elas estão no nível 3 “encaminhado”, acima de 90 e abaixo de 120:

Quadro 11 – *Score* das instituições pesquisadas

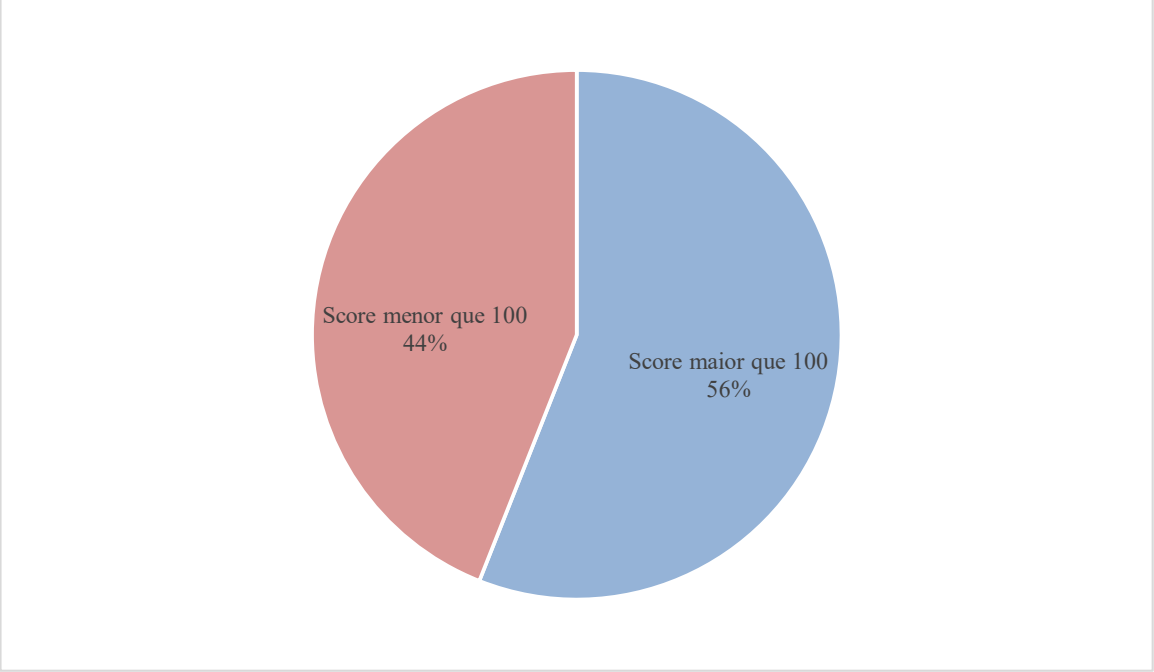
| Cooperativa | Abaixo de 100 (cem) | Acima de 100 (cem) |
|---|---|---|
| 1 | | 100,9511025 |
| 2 | | 101,1502722 |
| 3 | | 101,6664827 |
| 4 | 98,19730682 | |

| | | |
|---|---|---|
| 5 | | 101,4230912 |
| 6 | 99,63116863 | |
| 7 | 99,62031119 | |
| 8 | 98,88442735 | |
| 9 | 99,26526808 | |
| 10 | 99,00054958 | |
| 11 | | 100,7143173 |
| 12 | | 101,2674003 |
| 13 | 99,8286774 | |
| 14 | | 101,5024799 |
| 15 | 99,63831459 | |
| 16 | | 101,9763215 |
| 17 | 98,13713822 | |
| 18 | 99,26647993 | |
| 19 | | 102,1095315 |
| 20 | | 101,1373894 |
| 21 | | 101,8208196 |
| 22 | | 100,3391111 |
| 23 | 99,46216137 | |
| 24 | | 101,6373631 |
| 25 | | 100,0265016 |

Fonte: Dados da pesquisa.

Ao comparar esses *scores* com a escala de Araujo (2018), 44% (quarenta e quatro por cento) das instituições, ou seja, 14 (quatorze) estão no nível acima de 100 (cem) e 56% (cinquenta e seis por cento), ou seja, 11 (onze) estão abaixo de 100 (cem). Entretanto, todas elas estão no Nível 3 (Encaminhado), o que demonstra que todo o sistema encontra-se na condição de encaminhamento à uma cultura de segurança da informação plena, apresentando um *score* na escala 100, 10 (média 100, desvio padrão 10).

Figura 13 - Instituições com *Score* menor e maior que 100

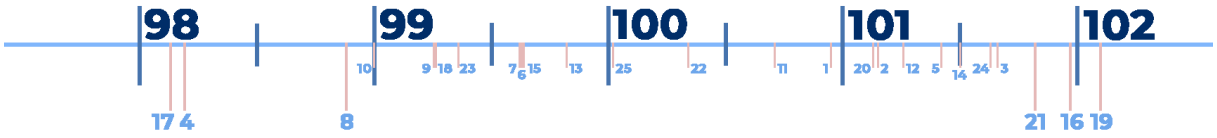



Fonte: Dados da pesquisa.

**Destacando as organizações que obtiveram menor *score***, tem-se em ordem crescente a 17 (dezessete), com 98,13 (noventa e oito vírgula treze); a 4 (quatro), com 98,19 (noventa e oito vírgula dezenove); e a 8 (oito), com 98,88 (noventa e oito vírgula oitenta e oito).

Estas três são apresentadas em destaque na Figura 14, juntamente com as três com maior *score* (que também serão analisadas adiante).

Figura 14 – Régua ilustrativa com destaque para as organizações com maior e menor *score*




Fonte: Dados da pesquisa.

O reflexo da cultura organizacional da liderança se expande por todo o ambiente corporativo. Se o líder (gestor de TI) não compreende aspectos fundamentais e necessários da SI, nem apresenta comportamentos compatíveis com as boas práticas, não é exigível que seus colaboradores tenham condutas diferentes, o que apresenta certa preocupação, pois a instituição não compreende a importância de tais comportamentos, como por exemplo, ao analisar a

diretriz da consciência, as cooperativas 4 e 17 declararam que a perda dos dados e informações teria um impacto leve em sua organização, o que não afetaria a credibilidade.

Levando em consideração o ramo da atividade que detém inúmeras informações e dados pessoais (instituição financeira), nos termos do que preceitua a LGPD (BRASIL, 2018), o impacto da perda[61] de dados pessoais, como o histórico financeiro, patrimônio, salários, aposentadorias, documentos de identidade e inúmeros outros, pressupõe naturalmente um dano que poderia ser inclusive irreparável.

Não é desejável que um colaborador da instituição não tenha a mínima compreensão da importância da proteção das informações, muito menos é aceitável que um gestor da tecnologia da informação mantenha comportamentos que sejam incoerentes com as boas práticas de uma política de SI, pois, suas atitudes enquanto liderança tem reflexo direto na cultura da segurança da informação e da privacidade da informação, ideais descritos por Schein (2004), Bass e Avolio (1993) e Barreto et. al (2013).

Em outras palavras, se nem o gestor (que deveria ser a figura de liderança) apresenta comportamentos adequados, quiçá apesentarão seus subordinados, o que certamente reflete em uma cultura que não se importa com a segurança e a privacidade.

É possível dessa forma verificar o que Araujo (2018) ensina quando descreve que o *subdomínio das pessoas* na SI tem relevância porque o problema não é apenas técnico-normativo, tornando-as realmente o *elo mais fraco*, conforme apontam inúmeros autores[62].

Outras questões que envolvem diretamente o comportamento também refletem à atitudes que podem se tornar vulnerabilidades, como por exemplo, na diretriz da resposta, a percepção de um desconhecido sem identificação no ambiente de trabalho; a não comunicação ao setor responsável; a não solicitação para que essa pessoa se retire; e a não comunicação à chefia, exatamente como declararam as instituições 4 e 8.

Nesses e em outros casos, a percepção de risco e as diferenças individuais são afetadas pelo ambiente, dessa forma, a cultura tem impacto significativo nos valores, atitudes e comportamentos, por isso que compreender a cultura pode fornecer *insights* sobre por que alguns comportamentos ocorrem e outros não (PARSONS et al., 2010).

---

[61] Nesse sentido, a perda deve ser interpretada não somente como a indisponibilidade da informação, mas também quanto a confidencialidade, como por exemplo, o furto ou roubo de dados que a instituição possui *backup*, não comprometendo a confidencialidade, mas sujeitos a divulgação não autorizada (violação da confidencialidade).

[62] Araujo (2018), Conteh e Schmick (2016), D'Arcy, Hovav e Gallerra (2009), Kemper (2019), Metalidou et. al (2014), Nichol (2000), Parsons et. al (2010), Russel (2002); Schneier (2004); Schultz (2005); Solms e Solms (2004), Voss (2001), Vroom e Solms (2004), Whitman e Mattord (2011).

Na diretriz da **resposta**, os gestores das cooperativas 4 e 17 declaram que, ao tomarem conhecimento de um novo tipo de ataque a computadores, “nunca” ou “raramente” comunicam os colegas de equipe, o setor responsável ou ainda verificam se o computador está vulnerável a esse ataque.

As instituições 8 e 17 apontam que a equipe de trabalho dos respondentes “não” conhece as suas respectivas responsabilidades e atribuições relacionadas à SI, o que demonstra uma problema de governança, pois, conforme a ISO 27001 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a), é necessário que a instituição assegure a distribuição e a comunicação das responsabilidades e autoridades dos papéis para a segurança da SI.

Nesse sentido, a LGPD (BRASIL, 2018) descreve a adoção de boas práticas e de governança[63] que estabeleçam competências, papeis, responsabilidades e procedimentos relacionados ao tratamento de dados. Pinheiro (2020) destaca que a adoção de medidas e regras de boas práticas e de governança à proteção de dados pessoais é essencial para a efetividade da proteção de dados.

Na diretriz da **ética**, a cooperativa 4 declarou comportamento de “raramente” alertar os seus colegas sobre a necessidade de desligar o computador quando não estiver em uso (o que também foi declarado como “nunca” pela 8); “raramente” bloquear o computador quando não estiver em sua estação de trabalho; “nunca” manter a mesa organizada e limpa (o mesmo foi declarado pela 8 e 17); e “raramente” proteger os documentos de trabalho de acesso não autorizado (o que também ocorreu com a 17).

Na democracia, a cooperativa 4 não consegue visualizar seu chefe como um líder, bem como declara que o chefe não motiva ou incentiva um comportamento a favor da SI e o respondente não se sente seguro com a liderança em relação à SI.

Líderes que não buscam transformar a cultura da sua organização, mas apenas seguem os padrões já existentes estão mais próximos do que Burns (1978) descreve como líderes transacionais. Entretanto, para que exista uma mudança de comportamentos, é necessário que existam pressupostos de segurança da informação enraizados na cultura e essa transformação, segundo Schein (2004) é mais difícil de acontecer e demanda maiores esforços, por isso a

[63] LGPD, artigo 50: Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

importância de líderes que Burns (1978) descreve como transformacionais, que motivam e elevam os níveis de moralidade de seus propósitos, os quais deveriam ser alinhados com a SI.

Outro ponto de destaque é que o sistema cooperativista de crédito tem em suas singulares um histórico de pouca alternância de lideranças (no mais alto nível), ou seja, muitas delas tem como presidente a mesma pessoa por vários mandatos e algumas delas nunca tiveram outro senão o mesmo desde a fundação, o que inclusive enfraquece o processo democrático que, segundo Meinen e Port (2014) é um dos valores e alicerces da modalidade de negócio.

Em contraponto ao conceito de cultura organizacional descrito pelos gestores na pesquisa de Deal e Kennedy (1982) como "é assim que as coisas são feitas por aqui", a cultura descrita por Schein (1984) encontra estágios organizacionais, ou seja, o principal impulso cultural vem dos fundadores e se eles permanecem há demasiado tempo, há grande possibilidade de manutenção dos pressupostos já bem inseridos no contexto e muitos elementos da cultura que foram aprendidos são utilizados como defesas. É provável que propostas para mudanças sejam ignoradas ou fortemente resistidas e os membros dominantes tentarão preservar a aprimorar a cultura já existente.

Ademais, cabe destacar o que Hersey, Blanchard e Natemeyer (1979) descrevem como a liderança situacional, quando a maturidade do seguidor não apenas dita o estilo de liderança que terá maior probabilidade de sucesso, mas também a base de poder que o líder deve usar para influenciar. Dessa forma, o líder deve avaliar com precisão o nível de maturidade do seguidor e modelar o comportamento de forma adequada, ajudando-o a amadurecer.

O respondente 4, ainda avalia como precária a sua comunicação com a chefia e entre seus colegas.

Quanto à percepção da segurança da informação na organização, o representante da instituição 8 afirma que "não" se sente seguro quanto à proteção de seus dados pessoais na organização e "não" se sente seguro com relação à confidencialidade das informações da organização, este último item é visto da mesma forma pela cooperativa 17.

Na diretriz da **avaliação de risco**, a cooperativa 4 declara que "raramente" faz cópia de segurança em mídias externas ou nuvem e "raramente" verifica se as cópias estão atualizadas, o que pode comprometer a segurança, tornando-se facilmente uma vulnerabilidade. O mesmo ocorre quando indagado a frequência de passar um antivírus ao abrir um anexo do e-mail, declarando que "nunca" o faz (o mesmo ocorre com a 8 e com a 17).

As cooperativas 8 e 17 declararam que, ao receber uma mídia "raramente" passam o antivírus antes de abrir ou executar programas dessa mídia. Isso demonstra uma vulnerabilidade

que, conforme Torres (2015) pode ser uma falha de um agente e uma fragilidade, um ponto fraco que Marciano (2006) destaca ser passível de ser explorado por uma ameaça. No caso em tela, essa ameaça poderia ser um *malware* dentro da mídia, inserido propositalmente por um engenheiro social, o que poderia ocasionar um incidente que comprometeria as informações (e um dos ativos da instituição).

Nesse mesmo sentido, a cooperativa 17 declara, por seu representante, que independentemente do equipamento ser pessoal ou profissional, "frequentemente" tem o hábito de acessar redes sem fio abertas em locais públicos. Os respondentes da 4, 8 e 17 "raramente" ou "nunca" trocam a senha de acesso ou criptografam os dados importantes.

Ainda na diretriz da avaliação de risco, as cooperativas 8 e 17 declaram que, ao acessar uma página na internet, "raramente" verificam se o site é seguro, da mesma forma "raramente" verificam se a rede é segura.

O acesso às redes sociais pessoais através do computador profissional é "frequentemente" realizado pelo representante da instituição 4, bem como contas externas de e-mail pessoal e sites de compras.

A adoção de medidas de segurança, técnicas e administrativas para proteção de dados é também descrita[64] pela LGPD (BRASIL, 2018), legislação inclusive, que aponta as responsabilizações e o ressarcimento de danos causados pelo não cumprimento das medidas necessárias. Essas medidas não devem ser apenas de responsabilidade dos agentes de tratamento, pois, a segurança e a privacidade da informação é dever de todos os colaboradores (DONDA, 2020; OECD, 2002) e deve estar presente na cultura da organização.

Já na diretriz do **projeto de segurança e implementação**, as cooperativas 8 e 17 declararam que "raramente" a segurança da informação é considerada nas fases de execução e de gerenciamento de projetos. Aliás, a 17 ainda apontou a mesma frequência de comportamento para a fase de definição e elaboração do projeto.

Na mesma diretriz, a instituição 17 destacou que durante o ciclo de um projeto ou trabalho "nunca" faz um levantamento dos riscos de possíveis incidentes que possam prejudicar o andamento ou a organização (a 4 e 8 declararam "raramente"); o comportamento "nunca" para a reavaliação dos procedimentos em busca de falhas ou possíveis incidentes no decorrer das atividades é apontado pela instituição 8 (a 17 declarou "raramente"). Quanto a formalizar

[64] LGPD, artigo 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

por meio de documentos as intercorrências, a frequência “nunca” é a opção da cooperativa 8 (a 4 e a 17 declararam “frequentemente”). Quanto a verificar se o trabalho ou projeto está em conformidade no tocante às recomendações, o comportamento “nunca” é a opção da instituição 8 (a 4 e a 17 declararam “raramente”).

Na diretriz da **gestão de segurança**, durante o processo de manuseio dos dados da organização, a cooperativa 4 declarou o comportamento “nunca” para todos os itens, sendo eles: avaliação dos riscos de danos ou incidentes (a 8 também declarou “nunca” e a 17 “raramente”); planejamento do local e da forma como os dados serão armazenados (a 8 e a 17 declararam “frequentemente”); levar em consideração as diretrizes da organização; execução dos processos conforme planejado (a 17 declarou “raramente”); avaliação dos procedimentos adotados atendendo às necessidades de segurança (a 8 e a 17 declararam “raramente”); e por fim, a execução das modificações necessárias para adequação às novas necessidades (a 8 e a 17 declararam “raramente”).

**Destacando as organizações que obtiveram maior *score***, tem-se a 19, com 102,10 (cento e dois e um décimo), seguido pela 16, com 101,97 (cento e um vírgula noventa e sete) e pela 21, com 101,82 (cento e um vírgula oitenta e dois).

Essas três cooperativas, mesmo obtendo índices acima das demais, ainda apresentam comportamentos que necessitam de melhoria contínua, ou seja, através da análise desses resultados é possível extrair oportunidades de melhoria, pois, conforme aponta Araujo (2018), ainda que a média no *score* da instituição seja mais elevado, ações de baixa proficiência dos colaboradores colocam a organização em alto risco de segurança.

Em sua definição dos níveis, Araujo (2018) considera a quantidade de colaboradores (ou neste estudo, de cooperativas do sistema) nos níveis de alto risco para a SI e não somente a média ou o *score* geral. Os resultados, portanto, podem fornecer informações para o autoconhecimento da organização e auxiliar os gestores para a tomada das decisões.

Dessa maneira, pode-se observar estes comportamentos de risco, por exemplo, ao questionar o impacto na organização caso ocorresse a interrupção ou indisponibilidade dos serviços (internet, acessos remotos, banco de dados e outros). A cooperativa 21 acredita que não afetaria a credibilidade e o impacto seria leve.

Por se tratar de uma instituição financeira, que oferta serviços essenciais e que não pode interrompê-los, considerar sua indisponibilidade como leve não é condizente com a CID, tampouco faz consonância com uma gestão de risco em termos jurídicos, pois, a má prestação

do serviço ocasiona lesão de direito ao consumidor, sendo que a atividade de natureza financeira é considerada como serviço, nos moldes do CDC[65].

Através da Resolução Nº 4.658 de 2018 o Banco Central do Brasil dispôs sobre a política de segurança cibernética e sobre os requisitos para contratação de processamento e armazenamento de dados pelas instituições financeiras, com diretrizes que devem ser seguidas por todas estas instituições (BANCO CENTRAL DO BRASIL, 2018).

Pagamentos, crédito, saque e aporte financeiro por cooperativas de crédito são considerados serviços essenciais e não podem ser suprimidos ou interrompidos, conforme aponta o Decreto 10.282 de 2020[66] que regulamenta e define as atividades essenciais, inclusive para o momento da pesquisa, de calamidade pública em decorrência da COVID-19. A previsão de atividades essenciais inclusive encontra respaldo constitucional[67].

Além disso, com a Resolução Nº 2.554 de 1998, o Bacen definiu que as instituições financeiras devem ter implantado e implementado controles internos voltados para as atividades que desenvolve, seus sistemas de informação financeira, operacionais e gerenciais (BANCO CENTRAL DO BRASIL, 1998).

Outro ponto de destaque é quanto ao questionamento da responsabilidade por garantir a SI na organização. A cooperativa 16 declara que o responsável é o setor de SI, enquanto espera-se que toda a organização esteja comprometida com a CID. A OECD (2002), ao tratar da diretriz da responsabilidade, destaca claramente que todos os participantes são responsáveis pela SI, corrente também defendida por Donda (2020) quando descreve que a proteção da informação é abrangente a todos os setores e recursos da empresa.

Desenvolver um ambiente ético e de respeito aos interesses legítimos do próximo perpassa pelo reconhecimento do quanto as ações e omissões podem prejudicar os outros. Tratar de assuntos relacionados à organização em ambientes externos (tanto no mundo físico quanto digital) pode prejudicar a CID das informações, ainda que esse comportamento ocorra "raramente", pois a informação pode percorrer caminhos intangíveis, ainda mais em pleno universo digital.

---

[65] CDC, artigo 3º, § 2°: Serviço é qualquer atividade fornecida no mercado de consumo, mediante remuneração, inclusive as de natureza bancária, financeira, de crédito e securitária, salvo as decorrentes das relações de caráter trabalhista (BRASIL, 1990).

[66] Decreto 10.282/20, artigo 3º, § 3º, inciso XX: serviços de pagamento, de crédito e de saque e aporte prestados pelas instituições supervisionadas pelo Banco Central do Brasil (BRASIL, 2020).

[67] CF, artigo 9º, § 1º: A lei definirá os serviços ou atividades essenciais e disporá sobre o atendimento das necessidades inadiáveis da comunidade (BRASIL, 1988).

Dessa forma, ao questionar a frequência de tratar desses assuntos em ambientes externos à organização, a singular 16 apresentou comportamento de "raramente" falar de assuntos em 5 de 8 ambientes exemplificados, mesmo que o desejável seja "nunca".

Quando questionado se o respondente espera na sala do colega pacientemente enquanto ele está no telefone, a instituição 21 declarou que "sempre" o faz, o que sugere que pode ouvir informações que não deveria.

Considerando que a Confidencialidade garante o acesso da informação somente às pessoas autorizadas, a Integridade garante a exatidão dela e a Disponibilidade permite que esteja sempre disponível aos autorizados (INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, 2014; NETTO; SILVEIRA, 2007), um ambiente sem uma cultura de respeito aos interesses legítimos da segurança e da privacidade da informação é dissonante daqueles pilares (CID), pois há risco de pessoas não autorizadas terem acesso a determinada informação que não deveria (Confidencialidade) e que a informação seja repassada sem a devida exatidão, pois pode existir máculas subjetivos inseridas pelo interlocutor e receptor em uma cadeia de repasse de informações de maneira "informal" (Integridade).

Além disso, a utilização de dados pessoais sem o consentimento do titular ou sem uma das bases legais que assim a autorizam, conforme disposto no artigo 7º[68] da LGPD, causando lesão patrimonial, moral, individual ou coletivo, é obrigado a reparar o dano, conforme o artigo 42[69] da LGPD (BRASIL, 2018), ou seja, tratar assuntos da interesses corporativos fora do ambiente laboral coloca em risco a segurança e a privacidade da informação e pode ocasionar alguma das lesões acima citadas. Mas antes mesmo da esfera legal, comportamentos como esse

[68] LGPD, artigo 7º: O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: I - mediante o fornecimento de consentimento pelo titular; II - para o cumprimento de obrigação legal ou regulatória pelo controlador; III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados; VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro; VIII - para a tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente (BRASIL, 2018).

[69] LGPD, artigo 42: O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2018).

ainda refletem na ética (ou a falta dela) e como o indivíduo demonstra respeito ao ambiente e aos demais colaboradores.

Na diretriz da **democracia**, a singular 21 apresentou que seu chefe não é um líder, ou seja, não é capaz de comandar pessoas, atrair seguidores, influenciar ou motivar positivamente o comportamento do grupo. Diante dessa informação, mesmo sendo uma das instituições com *score* mais elevado, percebe-se que a falta da figura de liderança pode comprometer a formação de uma cultura em benefício da segurança da informação, bem como pode afetar a transparência entre os envolvidos[70].

Da mesma forma, esta instituição declara que seu chefe tem comportamentos autoritários e uma gestão não participativa, pois "sempre" impõe as suas decisões sem ouvir a opinião dos colegas, "raramente" estimula os colegas a emitirem opiniões e "nunca" dá total liberdade aos colegas para decidirem.

A não percepção dos membros da equipe da sua voz, enquanto prática de construção gestão e de resolução de problemas, em decorrência da comportamentos não democráticos da sua liderança, é fator que não estimula as partes envolvidos a exporem suas ideias, comprometendo inclusive um ambiente de inovação e novas práticas que possam gerar valor.

Na diretriz da **avaliação de risco**, alguns comportamentos podem ser aperfeiçoados para minimizar riscos, mesmo que apontem algum grau satisfatório para estes quesitos, conforme Quadro 12:

Quadro 12 – Pré-disposição do comportamento diretriz da avaliação de risco com oportunidades de melhoria para as 3 instituições (16, 19, 21) com maior *score*

| Item | Nunca | Raramente | Frequentemente | Sempre |
|---|---|---|---|---|
| Realiza cópia de segurança dos arquivos profissionais em mídias externas (CD, DVD, storage, pendrive) ou nuvem. | 21 | | | |
| Realiza cópia de segurança dos arquivos profissionais no mesmo computador de trabalho | | 16 | | 19 |
| Pede autorização para instalar software ou aplicativos de seu interesse no seu equipamento de trabalho. | 16 | 21 | | |
| Beber na estação de trabalho. | | | 21 | |
| Alimentar-se na estação de trabalho. | | | 21 | |
| Passar o antivírus antes de abrir o anexo quando recebe um e-mail. | | | 16 e 21 | |
| Acessa o link recebido em um e-mail, independente de quem enviou | | 16 | | |
| Acessa o link recebido em um e-mail, se vier de remetente conhecido | | 19 | 16 | |

[70] A correlação entre liderança e transparência administrativa é apresenta a seguir, neste mesmo capítulo.

| | | | | |
|---|---|---|---|---|
| Acessa redes sociais pessoais utilizando computador da instituição. | | 19 e 21 | | |
| Acessa contas externas de e-mail pessoal utilizando computador da instituição. | | | 21 | |
| Acessa sites de compra utilizando computador da instituição. | | 21 | | |
| Acessa a conta pessoal da instituição financeira utilizando computador da instituição. | | 21 | | 19 |
| Passa a sua senha de acesso para um colega quando não está presente no local de trabalho. | | 21 | | |
| Comunica a sua senha ao seu chefe para que ele se responsabilize pelo acesso quando não está presente no local de trabalho. | | 19 e 21 | | |
| Usa nomes e apelidos para composição da senha de acesso | | 16 | | |
| Usa datas ou parte de datas para composição da senha de acesso | | 16 e 21 | | |
| Usa uma senha padrão para composição da senha de acesso | | 19 | | |
| Tem por hábito criptografar os dados importantes | | | 19 | |
| Tem por hábito acessar redes sem fio aberta | | 16 e 19 | | |
| Têm por hábito guardar ou fixar a senha de acesso no próprio equipamento (computador, celular, entre outros). | | 16 e 21 | | |
| Tem por hábito limpar e higienizar o seu equipamento de trabalho | | | 16 | |
| Ao utilizar sua senha, verifica se está sendo filmado | | 19 | | |
| Lê a licença de um aplicativo durante o processo de instalação | | 19 | | |
| Ao descartar uma mídia, registra o descarte ou a baixa dela | | | 19 | |
| Utiliza o seu crachá de identificação em local visível? | | 21 | | |
| Verifica se as pessoas que possam por você estão utilizando crachá de identificação | 21 | 16 | | |

Fonte: Dados da pesquisa.

É desejável que os participantes das instituições analisem e reavaliem a segurança dos sistemas e redes de informação, no intuito de realizar as modificações necessárias para a evolução da segurança.

O respondente da 19 declarou que “frequentemente”, ele ou a equipe, revisam as políticas de SI da sua organização. Os respondentes das singulares 16 e 19 declararam que “frequentemente” reavaliam as suas atitudes com respeito a segurança da informação e os da 19 e 21 também descreveram que “frequentemente” a organização promove uma reavaliação dos procedimentos de segurança da informação.

Considerando que a diretriz da **reavaliação** está diretamente ligada à melhoria contínua e que, sem ela, a melhora dos índices de cultura e do *score* tornam-se muito difíceis

ou impossíveis, é uma dimensão que merece atenção por parte das instituições e que, mesmo com colaboradores que apontem comportamentos favoráveis, é desejável que essas frequências sejam sempre no mais alto nível, por isso, o estudo dessa diretriz apresenta oportunidades de evolução no *score* e no ambiente da cultura da organização para promoção da SI.

A reavaliação dos processos para a atuação corretiva é parte essencial do ciclo PDCA (*Plan, Do, Check, Action*), descrito por Juran e Godfrey (1998) e que é um instrumento valioso de controle e melhoria dos processos. É nesse padrão de comportamento visando a qualidade que reside a importância da reavaliação e da documentação para a gestão do capital intelectual[71] da organização e também, como descrevem Souza e Abiko (1997), identificar não-conformidades, reparar falhas e evitar repetições.

A ISO 27001 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013a), destaca que a organização deve continuamente melhorar a pertinência, adequação e eficácia do sistema de gestão de segurança da informação e que a alta direção deve demonstrar sua liderança e comprometimento, promovendo a melhoria contínua.

Com alguns recortes das três instituições com menor e com maior *score*, passa-se também a análise de alguns pontos que merecem destaque, por item. Quando perguntado aos representantes se as informações integram o patrimônio da organização, temos que um representante considera que não, da instituição 18.

Conforme Galegale, Fontes e Galegale (2017), a ISO 27002 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013b) e Rogers (2019), as informações são ativos importantes para as instituições. A não compreensão da relevância desse ativo pode acarretar em manifestações comportamentais que não sejam de boas práticas, afinal, se o colaborador não vislumbra a informação como ativo, a tendência é que descarte a necessidade de sua preservação e da sua CID. O quadro é ainda mais preocupante quando se trabalha com o gestores da SI, afinal, são também lideranças.

A responsabilidade por garantir a segurança da informação é de todos os colaboradores, cada indivíduo tem seu papel dentro da cadeia organizacional e não é possível transmitir responsabilidades e isentar-se delas de forma completa.

O sistema contempla 18 singulares que compreendem dessa forma, ou seja, 72% (setenta e dois por cento), entretanto, 5 singulares creem que a responsabilidade pela SI é do

[71] O registro do conhecimento na organização é fundamental para a gestão do capital intelectual, conforme descrito por Nonaka (2007), o que será apresentado a seguir, neste estudo.

setor próprio, 20% (vinte por cento) e 2 (duas) singulares declararam que os responsáveis são os encarregados da manutenção dos dados, 8% (oito por cento), conforme Figura 15.

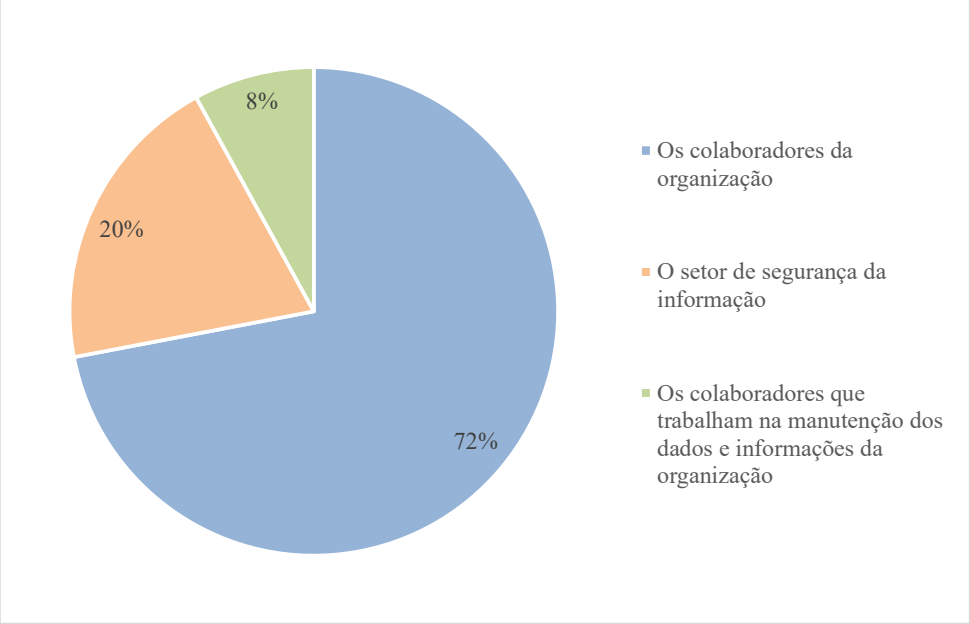
Araujo (2018) destaca a importância da conscientização das pessoas para a cultura de segurança da informação, pois a SI é um movimento internacional, de todos os países, todas as organizações e todas as pessoas.

Há uma responsabilidade coletiva intrínseca. Mesmo as instituições com alto nível de maturidade de SI podem ter elevados riscos de incidentes. Uma vulnerabilidade pode ser constituída de apenas um único colaborador que não apresenta comportamentos que assegurem a CID das informações.

Segundo o *Human Factor Report* – HFR da Proofpoint (2019), relatório com as conclusões de pesquisas de 18 meses entre 2018 e 2019, com coleta de dados na base de dados de clientes globais e análise de bilhões de mensagem diárias e centenas de milhões de domínios que apontam as maneiras como os atores estão explorando o elo mais fraco: o comportamento humano.

Invasores concentram suas ameaças cada vez mais nas pessoas, em vez de infraestrutura, por isso é de extrema importância identificar quais usuários em uma organização representam as maiores fontes de risco. O HRF (PROOFPOINT, 2019) ainda destaca que pessoas muito atacadas não são necessariamente perfis de executivos e que as áreas mais atacadas são educação, publicidade/marketing e finanças. Esta última corresponde exatamente ao setor pesquisado.

Figura 15 – Quem é responsável por garantir segurança da informação na sua organização?

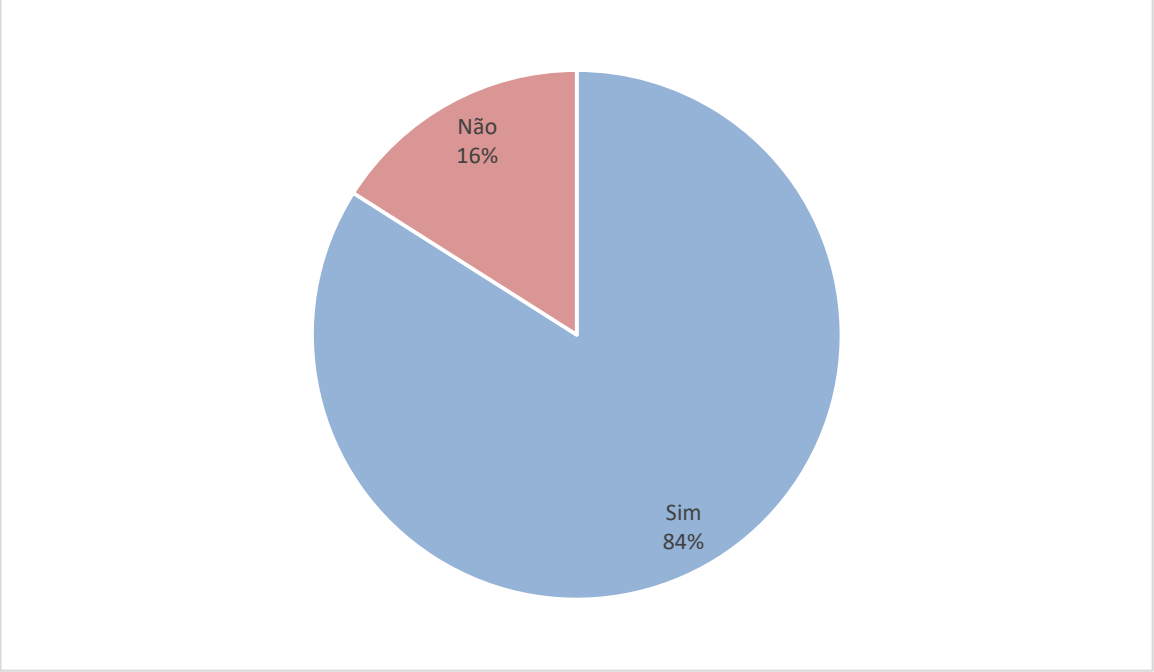



Fonte: dados da pesquisa.

Na diretriz da democracia, vale ressaltar a compreensão das cooperativas quanto a sua liderança, pois 21 (vinte e uma) delas considera a chefia um líder, 84% (oitenta e quatro por cento), mas 4 (quatro) assim não o fazem, 16% (dezesseis por cento), conforme Figura 16.

Há uma ligação implícita e explícita da liderança na cultura organizacional (OGBONNA; HARRIS, 2000), como demonstrado no item 2.6 deste trabalho. Se 16% (dezesseis por cento) dos gestores de TI não conseguem visualizar seu chefe como um líder, deve existir uma preocupação da cultura de segurança e privacidade da informação nesses ambientes, pois, a liderança é fundamental para a formação daquela.

Figura 16 – Na sua opinião, o seu chefe é um líder?




Fonte: Dados da pesquisa.

Ainda no tocante a liderança, 20 (vinte) cooperativas declararam que a chefia motiva ou incentiva um comportamento a favor da segurança da informação, 80% (oitenta por cento) e 5 (cinco) declararam que não, 20% (vinte por cento). Quando questionado o gestor da SI quanto a sentir-se seguro com a liderança do seu chefe em relação à SI, 18 (dezoito) declararam sentir-se seguros, ou seja, 72% (setenta e dois por cento) e 7 (sete) relataram não se sentir seguros, o que perfaz 28% (vinte e oito por cento).

Destaca-se a avaliação quanto à transparência administrativa, pois 11 (onze) singulares declararam ser ela boa, ou seja, 44% (quarenta e quatro por cento), 12 consideram suficiente, o que corresponde a 48% (quarenta e oito por cento), 1 (uma) considera precário e 1 (uma) considera não existente, sendo que estas duas últimas correspondem a 4% (quatro por cento) cada.

O comportamento do chefe que não é visto como líder pela sua equipe, tampouco apresenta comportamentos de liderança reflete na transparência administrativa, pois, conforme Avolio e Gardner (2005), a liderança autêntica tem foco em produzir relações humanas e desenvolver líderes conforme seu próprio eu, com transparência na forma de se relacionar com os outros.

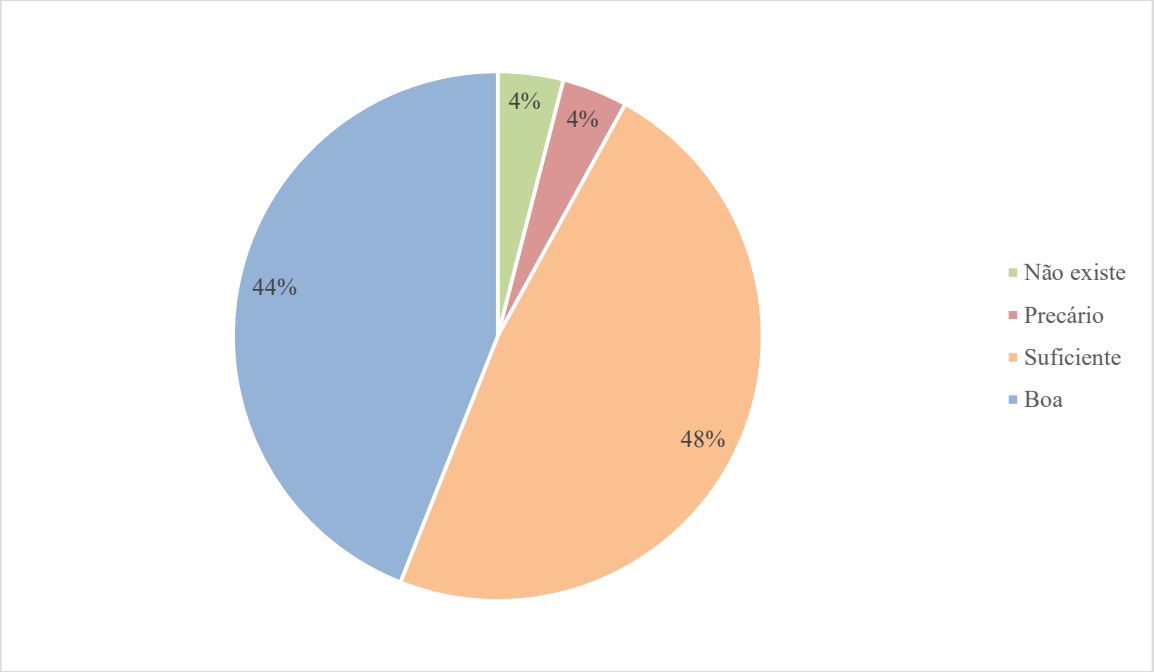
Isso é notável quando correlacionamos a transparência administrativa com instituições que chefes não são líderes (ou assim não são vistos pela equipe). O respondente da singular 21

declarou que a transparência administrativa é precária e que seu chefe não é um líder, não incentiva um comportamento favorável a SI e não se sente seguro com a liderança do chefe em relação à SI.

O respondente da 18 declarou que seu chefe não incentiva um comportamento favorável a SI e que não se sente seguro com a liderança do chefe em relação à SI, manifestando também que a transparência administrativa sequer existe.

As instituições 3, 4, 18, 21, 22, 23, 24 e 25 declaram que seu chefe não é um líder ou não incentiva um comportamento favorável à SI ou não se sente seguro quanto a liderança do chefe em relação à SI. Dessa forma, pode-se dizer que 8 instituições precisam melhorar sua liderança para que a cultura de segurança da informação possa ter níveis mais maduros, ou seja, 32% (trinta e dois por cento).

Figura 17 – Como você avalia a sua organização no seguinte aspecto: transparência administrativa?




Fonte: Dados da pesquisa.

Nesse quesito, também há uma divergência institucional, pois, 8% (oito por cento) apontam que há precariedade na transparência (Figura17). Meinem e Port (2014) apontam que este alicerce faz parte dos valores do cooperativismo e traz clareza, não deixa ambiguidades e segredos, pois todos tem o direito de conhecer as regras, a gestão e os números, entretanto,

percebe-se que pelo menos em duas instituições o discurso teórico se distancia da prática, na visão dos gestores da SI.

A transparência administrativa é uma forte aliada no combate a irregularidades e ilegalidades, proporcionando conhecimento de direitos e deveres a cada um dos envolvidos. A adequada transparência resulta em confiança e não deve se restringir ao desempenho econômico-financeiro. Essa prática de governança qualifica o relacionamento entre instituição e cooperados, reduz riscos e harmoniza conflitos entre todos os envolvidos (IBGC, 2015).

O *disclosure* (evidenciação das informações) ganha destaque, inclusive no mercado de capitais e financeiro, em decorrência de inúmeros problemas de governança e pela obrigatoriedade legal e normativa (LANZANA, 2004). Souza (1995) destaca que, como condição fundamental para credibilidade das instituições com seus membros e com o público geral, deve existir igualdade de condições de acesso às informações.

A governança cooperativa estabelece práticas éticas que tem por finalidade ampliar a transparência da administração da sociedade cooperativa e aprimorar a participação do cooperado no processo decisório. Essa transparência é um dos princípios da governança que facilita de forma voluntária o acesso às informações, inclusive aquelas que vão além das determinações de dispositivos legais (OCB, 2016).

Uma prática básica da transparência é a disponibilização do estatuto social para os associados, de forma prática e objetiva, pois ele é o instrumento que contém as diretrizes, direitos e deveres de cada sócio, bem como descreve o sistema de eleição e prestação de contas.

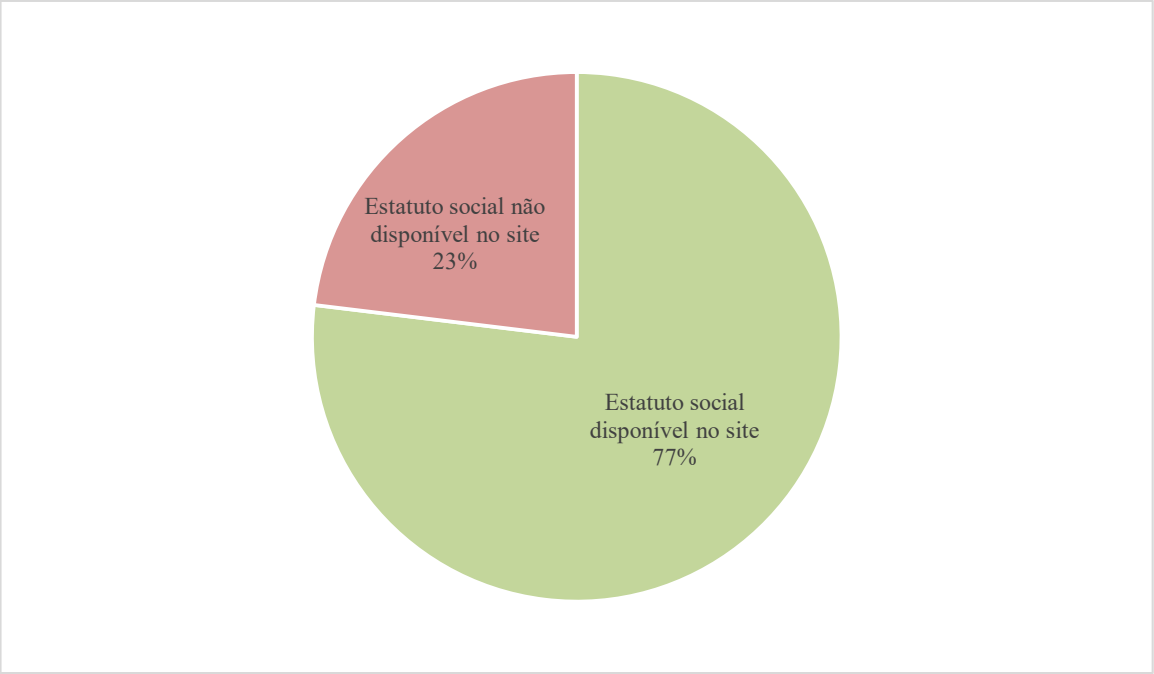
O executivo principal da organização deve garantir que as partes interessadas tenham acesso às informações de seu interesse, além daquelas obrigatórias (por lei ou regulamento), inclusive garantindo que pessoas com níveis de conhecimento diferentes tenham condições de compreender as informações. (IBGC, 2015).

A PNC estabelece, em seu artigo 21, inciso II[72], que o estatuto social da cooperativa deve dispor dos direitos e deveres dos associados, garantindo a sua participação efetiva na tomada de decisão, o que corrobora com a gestão democrática. Mas para isso, cada sócio deve ter noções mínimas de suas atribuições, do seu papel e também do sistema de escolha dos gestores (BRASIL, 1971).

[72] Art. 21. O estatuto da cooperativa, além de atender ao disposto no artigo 4º, deverá indicar: I - os direitos e deveres dos associados, natureza de suas responsabilidades e as condições de admissão, demissão, eliminação e exclusão e as normas para sua representação nas assembléias gerais (BRASIL, 1971).

Para compreender a transparência administrativa e a gestão democrática, foi realizada a pesquisa nos sites de cada singular do sistema (trinta e nove instituições), as mesmas que foram convidadas a responder o questionário, verificando quais delas disponibilizavam o estatuto para consulta pública (Figura 18).

Figura 18 – Cooperativas que disponibilizam o estatuto social em seu site




Fonte: Dados da pesquisa.

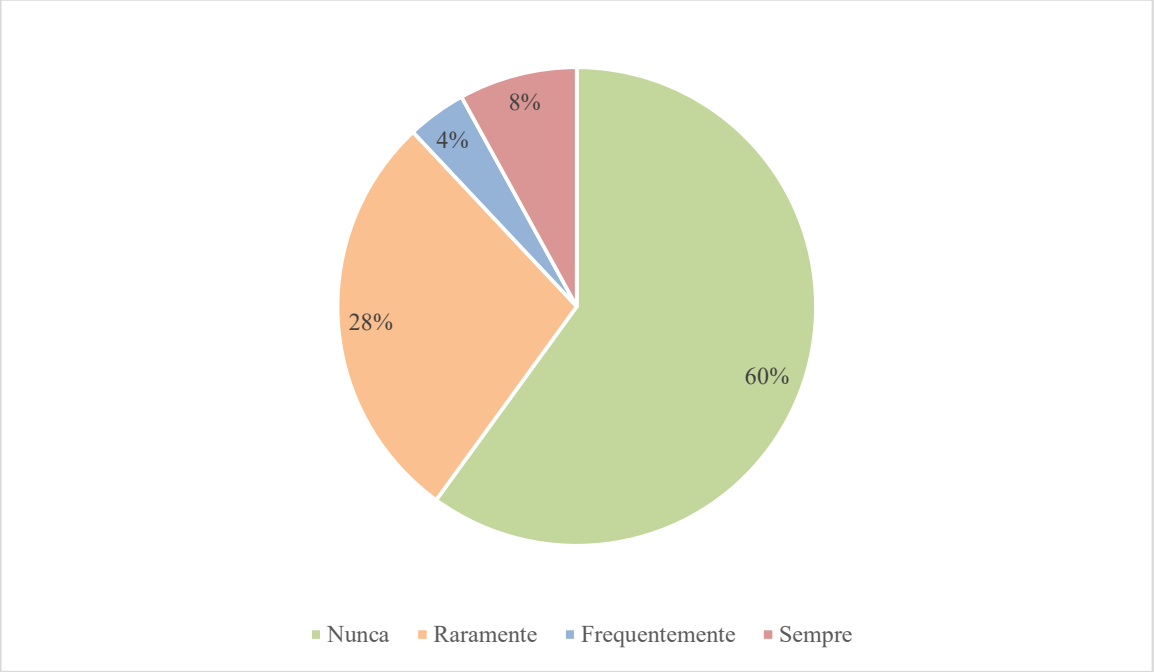
Dessa forma, é perceptível como uma prática simples de gestão democrática e transparência, ambos critérios basilares do cooperativismo, não são implementados por 23% (vinte e três por cento) das instituições, através da disponibilização de um documento de direito do associado.

Como oportunidade de melhoria, sugere-se ao sistema que compartilhe informações como o Estatuto Social, facilitando a gestão e melhorando a transparência, pois, de fato, disponibilizar um documento no site é simples e praticamente não oneroso. O Manual de Boas Práticas de Governança Cooperativa do IBGC (2015) orienta, nesse sentido, que a internet e outras tecnologias devem ser exploradas para a rápida e ampla divulgação das informações.

Com respeito à diretriz da avaliação de risco, destaca-se comportamentos cotidianos que são fundamentais para preservação da CID, mas que ainda apresentam gestores que demonstram “nunca” ou “raramente” para essas ações, vejamos:

Quanto à cópia de segurança dos arquivos profissionais ser feita no mesmo computador de trabalho, o que não garante a segurança de um *backup* em mídia externa, tem-se que 2 (dois) respondentes sempre assim o fazem e 1 (um) "frequentemente", o que corresponde a 8% (oito por cento) e 4% (quatro por cento) respectivamente (Figura 19).

Figura 19 – Você realiza cópia de segurança dos arquivos profissionais no mesmo computador?



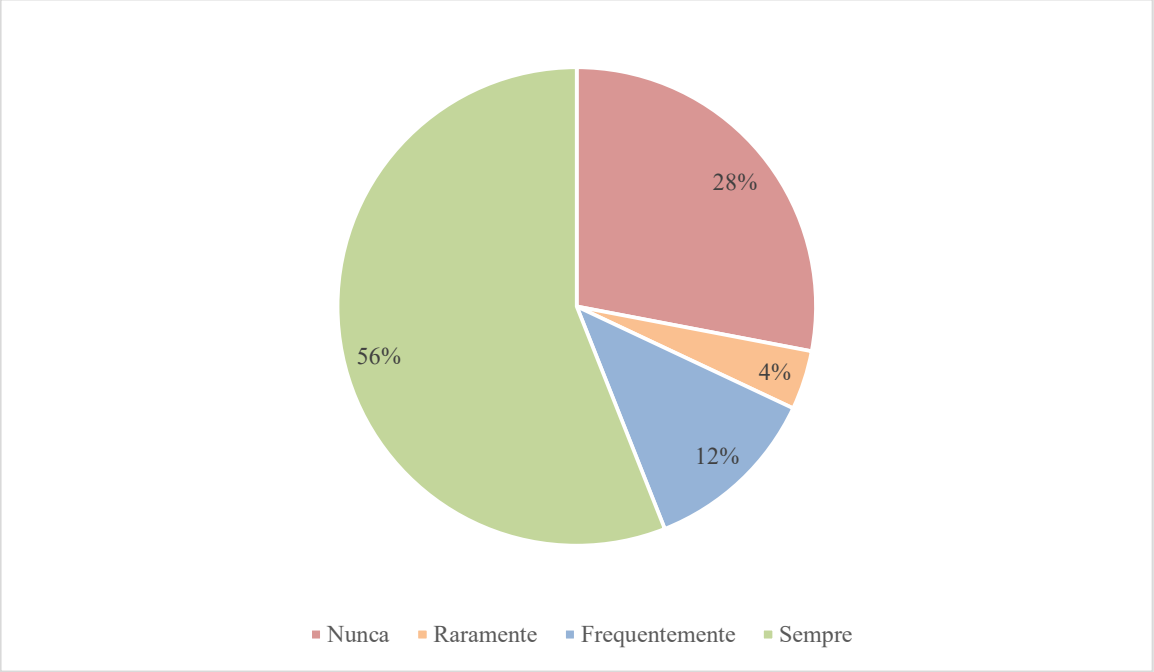

Fonte: Dados da pesquisa.

Considerando a importância das informações para a instituição e que 100% (cem por cento) dos respondentes acredita que as informações têm valor financeiro, não realizar *backup* dos arquivos de trabalho de forma adequada é uma vulnerabilidade que pode ocasionar um incidente com danos irreparáveis.

Uma adequação a este comportamento, em termos de tecnologia é simples, basta a realização de cópia de segurança em uma mídia externa, como por exemplo um HD ou até mesmo na nuvem. O hábito de realizar o *backup* com determinada frequência, também é um processo que diminui riscos, mas sem uma alteração comportamental de compreender a importância disso, processos e tecnologia não são suficientes, porque as pessoas são o elo mais fraco.

Especificamente a este comportamento de realizar a cópia de segurança em mídia externa, 7 (sete) instituições “nunca” o fazem, 28% (vinte e oito por cento) e 1 (uma) “raramente, 4% (quatro por cento), conforme demonstra a Figura 20.

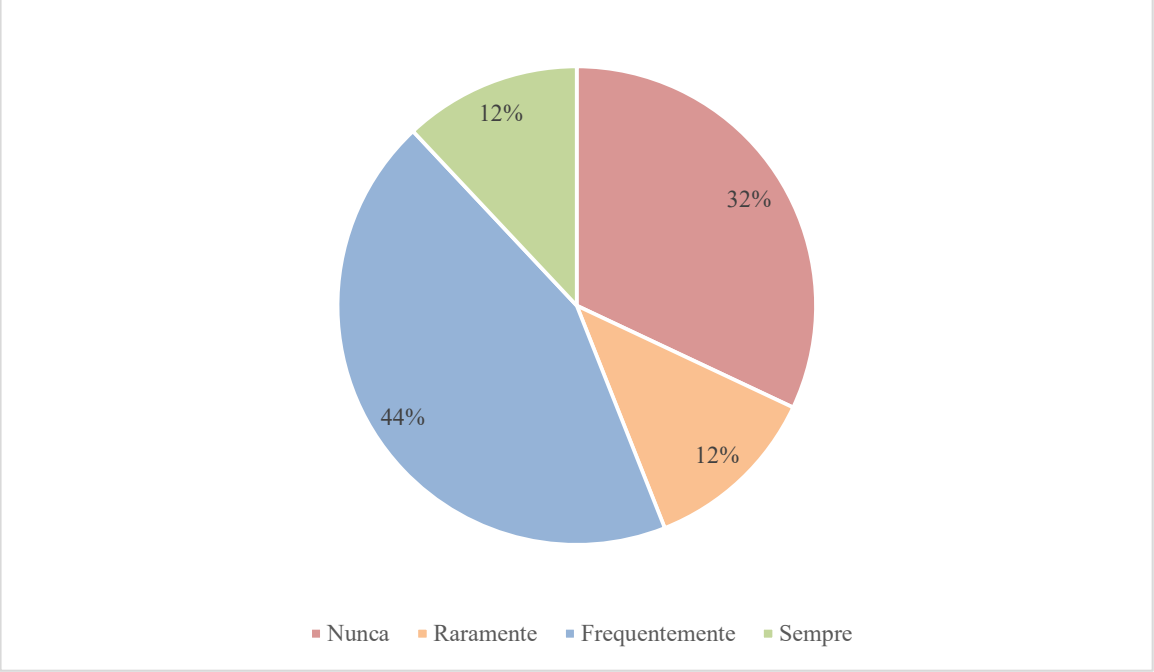
Figura 20 – Você realiza cópia de segurança dos arquivos profissionais em mídia externa?




Fonte: Dados da pesquisa.

Outro comportamento que auxilia a compreensão do risco à CID é apontado quando questionado a frequência de passar o antivírus em um anexo recebido por e-mail, antes de abri-lo. Dessa forma, 3 (três) instituições “raramente” assim o fazem, 12% (doze por cento) e 8 (oito) “nunca”, 32% (trinta e dois) por cento, como mostra a Figura 21.

Figura 21 – Ao receber um e-mail com anexo, você passa o antivírus antes de abri-lo?




Fonte: dados da pesquisa.

Quando indagado se os gestores verificam se as pessoas que passam por ele estão utilizando crachá de identificação, 11 (onze) declararam “raramente”, 44% (quarenta e quatro por cento) e 3 (três) “nunca”, 12% (doze por cento). Comportamentos como esse podem facilitar a ação de engenheiros sociais e de ameaças que utilizam o espaço físico para ações mal-intencionadas (Figura 22).

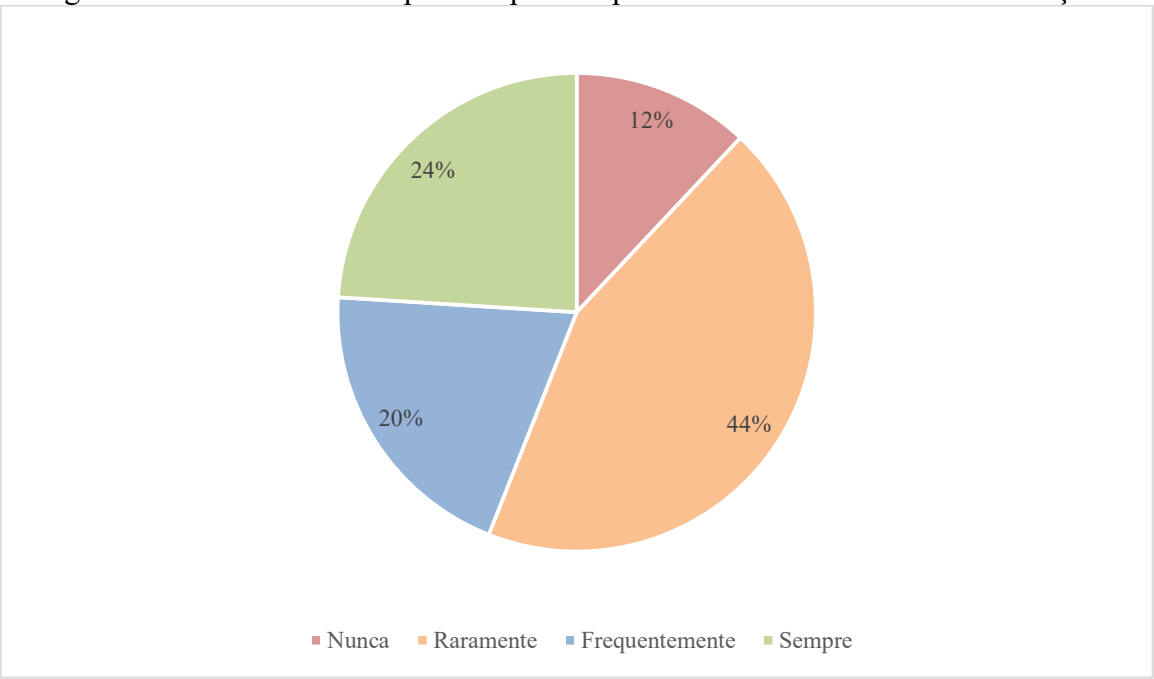
Segundo o HRF (PROOFPOINT, 2019), invasores estão melhorando técnicas de engenharia social e cada vez mais focados na obtenção de credenciais para novos ataques. Eles estabelecem uma posição silenciosa nas organizações e roubam dados e credenciais, em vez de simplesmente focar na utilização de *malwares,* sendo que através destes, segundo o Kaspersky Security Bulletin, 10,18% (dez vírgula dezoito por centro) dos computadores usuários de internet em todo o mundo, no ano de 2020, sofreram pelo menos um ataque (KASPERSKY, 2020).

Klettenberg (2016) destaca que a Federação Brasileira dos Bancos orienta a realizar o controle de acesso de terceiros mediante registros e conferência de documento de identificação durante o ingresso nas dependências da instituição.

Dessa forma, o uso de crachá é uma prática que dificulta o acesso indevido de terceiros, mas muito além disso, a construção do item é representativa, pois o uso do crachá é um nível

básico de identificação; o que se busca conhecer do respondente é se ele está atento ao seu redor.

Figura 22 - Você verifica se pessoas passam por você utilizam crachá identificação?




Fonte: Dados da pesquisa.

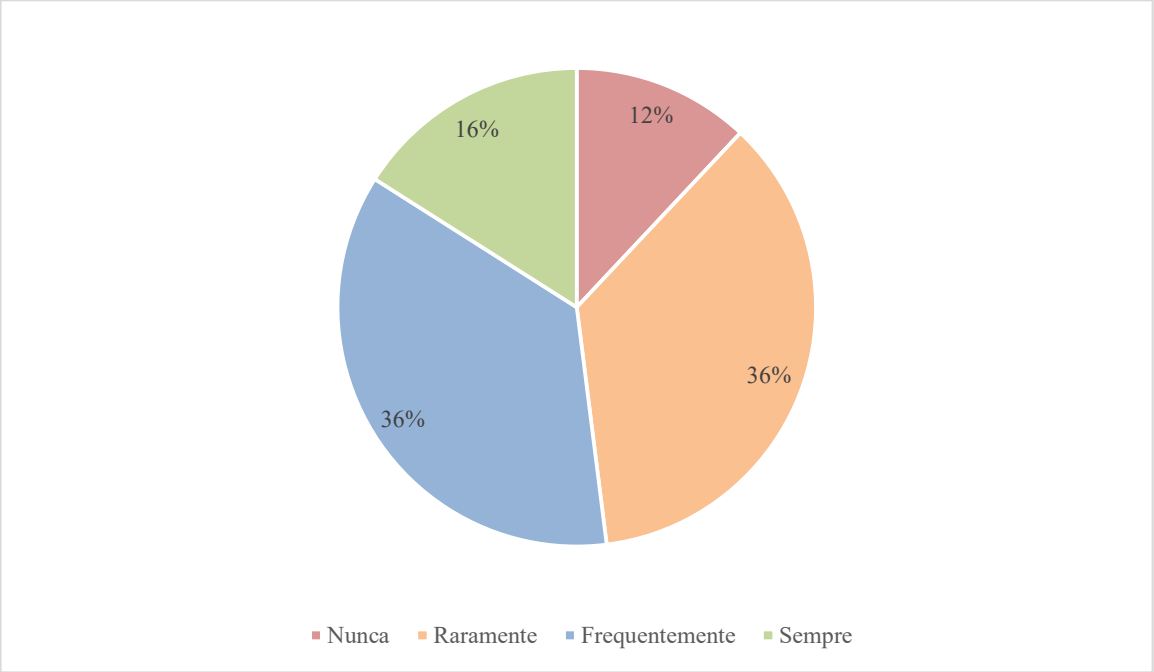
Na diretriz do projeto de segurança e implementação, também há assuntos que merecem destaque e que apontam a necessidade de melhorias, como por exemplo a periodicidade que o gestor e sua equipe, após a conclusão da atividade, trabalho ou projeto, formalizam por meio de documentos as intercorrências para uso futuro, sendo que 9 (nove) gestores declararam “raramente”, 36% (trinta e seis por cento) e 3 (três) “nunca”, 12% (doze por cento), conforme Figura 23.

A falta de formalização das intercorrências certamente faz com que as experiências pessoais e até mesmo coletivas, que não forem sistematizadas, sejam esquecidas ou não compartilhadas, enquanto poderiam ser uma importante ferramenta para fortalecimento do capital intelectual da organização e para a gestão do conhecimento, com melhores resultados, menor incidência de erros (e recorrência deles) e melhoria contínua dos processos, inclusive os ligados à SI.

Nonaka (2007) corrobora com o tema, pois a exploração de *insights*, intuições e palpites tácitos, disponibilizados para uso e teste de toda a empresa, cria novos conhecimentos e oportunidades de negócios e inovações. A experiência pessoal deve ser transformada em

conhecimento organizacional, tornando-se valiosa para a organização. Nesse processo, o conhecimento tácito (subjetivo) deve ser formalizado e sistematizado, tornando-se explícito, o que o faz ser facilmente comunicado e compartilhado.

Figura 23 - Após a conclusão da atividade, trabalho ou projeto, você e sua equipe formalizam por meio de documento as intercorrências para uso futuro?

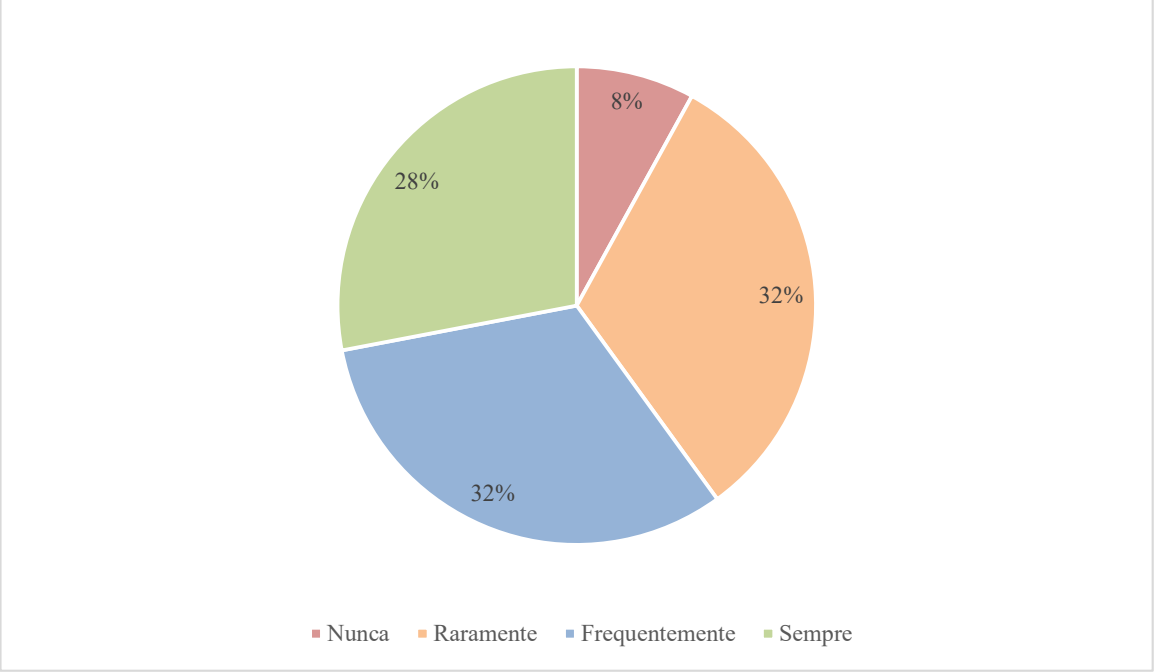



Fonte: Dados da pesquisa.

Na diretriz da gestão da segurança, quando indagado aos participantes quanto a avaliação dos riscos de danos ou incidentes durante o processo de manuseio dos dados da organização, 2 (duas) instituições declararam nunca fazerem, 8% (oito por cento) e 8 (oito) raramente, 32% (trinta e dois por cento), como mostra a Figura 24.

Este item demonstra a cultura da gestão de SI na prática da cooperativa, pois, a avaliação dos riscos está diretamente ligada ao entendimento do colaborador quanto à informação ser um ativo importante para a instituição, consequentemente, a sua adequada gestão para minimizar incidentes.

Figura 24 – No processo de manuseio dos dados, você avalia riscos de danos ou incidentes?



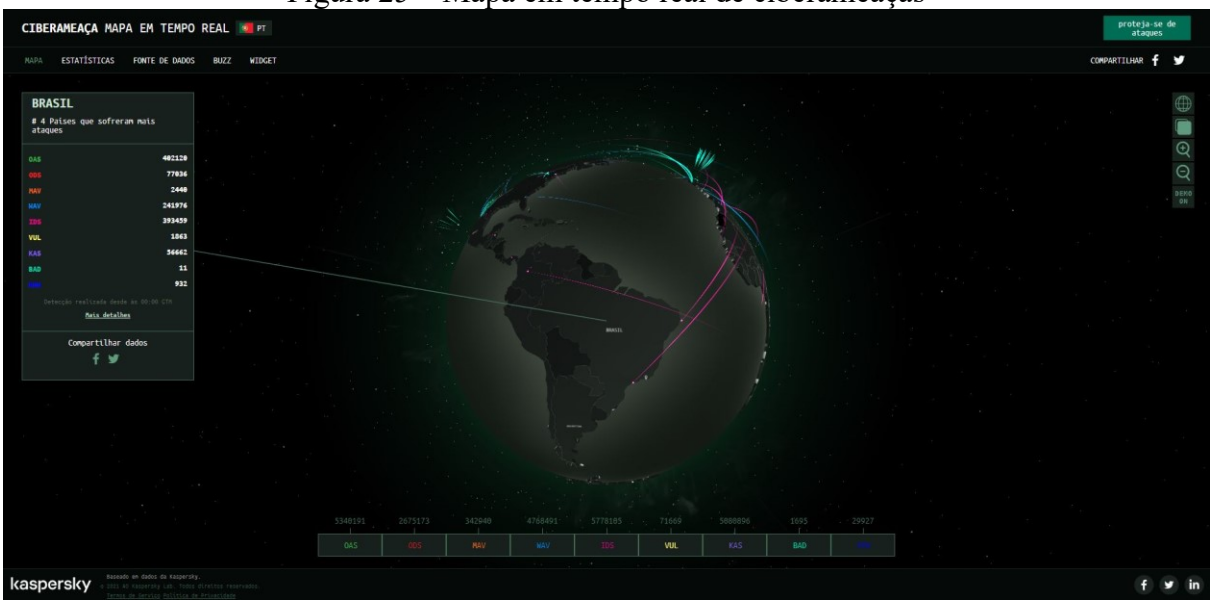

Fonte: Dados da pesquisa.

Quando questionado sobre a organização possuir um grupo gestor da segurança da informação, todos os 25 (vinte e cinco) respondentes confirmaram a existência, entretanto, 1 (uma) cooperativa declarou não acha-lo necessário, 4% (quatro por cento). Este respondente claramente não tem a mínima percepção, nem aponta comportamentos adequados à CID, o que pode colocar em risco a SI da sua organização, quiçá compreende a importância de um grupo gestor para minimizar riscos e gerir adequadamente os processos. Não é por acaso que este respondente é o 17, ou seja, a instituição com o menor *score*, 98,13 (noventa e oito vírgula treze).

Incidentes com dados são cada vez mais frequentes no mundo. Segundo a Kaspersky, empresa privada de cibersegurança, o Brasil é o quarto país que mais sofre ataques no mundo[73], perdendo apenas para Rússia e Alemanha. A empresa disponibiliza um mapa em tempo real com informações de ciberameaças (KASPERSKY, 2021) conforme Figura 25.

[73] Informações obtidas em 22 de abril de 2021, através do link: https://cybermap.kaspersky.com/pt

Figura 25 – Mapa em tempo real de ciberameaças




Fonte: Kaspersky (2021).

Não é por menos que em janeiro de 2021 importantes portais de notícia do país comunicaram dois megavazamentos de mais de 223 milhões de pessoas, número maior do que a população nacional, estimada em 212 milhões. Dentre as informações expostas estão nome, endereço, sexo, data de nascimento, fotos de rosto, imposto de renda de pessoa física, *score* de crédito, renda, cheques sem fundo, informações financeiras, cadastro de serviços de telefonia, escolaridade, benefícios do Instituto Nacional do Seguro Social – INSS, Cadastro de Pessoas Física – CPF e Cadastro de Nacional de Pessoa Jurídica – CNPJ, além de informações sobre veículos, servidores públicos e informações da rede social LinkedIn (CNN, 2021; G1, 2021).

Segundo o Institute Business Education, conveniado à Fundação Getúlio Vargas – FGV, criminosos podem usar os dados pessoais para aplicar golpes dos mais variados tipos, usando de engenharia social para obterem vantagens ilícitas. Para a instituição, não havia nada que o cidadão pudesse fazer para proteger seus dados e que a falta de um regramento até então, incentivava que órgãos do governo mantivessem dados pessoais desnecessários (INSTITUTE OF BUSINESS EDUCATION, 2021).

A PSafe, empresa especializada em cibersegurança e que descobriu o megavazamento de dados afirma que essa divulgação torna a atividade de engenheiros sociais muito mais fácil e que informações valiosas estão sendo comercializadas na internet, inclusive de grandes autoridades do país (PSAFE, 2021).

O impacto do vazamento de dados é resultado da falta de uma cultura de proteção de dados, conforme aponta O Globo (2021), e isso traz impactos no cotidiano dos titulares de dados, ao lhe ser negado um empréstimo ou uma promoção, na preservação da sua saúde e também da sua segurança.

A LGPD traz sanções administrativas[74], responsabilizações e a obrigação de reparação de danos em decorrência da violação à legislação de proteção de dados[75], inclusive quanto ao acesso não autorizado, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer outras formas de tratamento ilícito ou inadequado (BRASIL, 2018).

Assim como um desastre natural que muitas vezes é impossível de restaurar o dano, o vazamento de informações dificilmente poderá restabelecer o estado anterior, o que comprova a importância da cultura de segurança e privacidade de dados e informações não só em nosso país, mas em todo o mundo.

A LGPD estipula (artigo 5º, inciso XVII[76] e artigo 38[77]) a necessidade do controlador elaborar relatório de impacto e para isso, é necessário sobretudo, a análise dos riscos à privacidade da informação nas instituições, medida que visa mitigar por exemplo, vazamentos de dados e prejuízos aos titulares (BRASIL, 2018).

## 4.2 ENTREVISTAS SOBRE PI E PD – EIXO TRÊS

São apresentados resultados do eixo três que, segundo a ótica do pesquisador e sua orientadora, demonstram aspectos importantes para compreensão da temática, pontos críticos e também oportunidades de melhoria, sendo que, por questões de exequibilidade, são descritos a seguir apenas alguns tópicos de toda a coleta realizada.

---

[74] O artigo 50 da LGPD (já descrito neste tópico) destaca que os agentes de tratamento de dados, em razão das infrações cometidas às normas prevista naquela legislação, ficam sujeitos à sanções administrativas aplicáveis pela autoridade nacional, desde advertências, multas, suspensões e até proibições de tratamento de dados.

[75] LGPD, artigo 42: O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo (BRASIL, 2018).

[76] LGPD, artigo 5º: Para os fins desta Lei, considera-se: XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco (BRASIL, 2018);

[77] LGPD, artigo 38: A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (BRASIL, 2018).

Por motivos de não identificação do sistema objeto de estudo, as instituições foram nomeadas como Alpha, Beta e Gama, sem alteração no sentido e contexto dos dados obtidos, correspondendo, e em conformidade, ao declarado pelos respondentes.

Na dimensão da **finalidade**, quando questionado aos gestores de TI/DPOs das instituições pesquisadas, se há armazenamento de DP mesmo de não associados ao sistema, a instituição Alpha respondeu que sim, usam DP de avalistas em operações de crédito, segurados, e de operadores de sistemas internos; o gestor da Beta declarou não ter conhecimento suficiente para poder responder, pois não sabe se há coleta ou não de DP; a Gama relatou coletar e armazenar dados de avalistas em contratos de crédito, DP de referência para contatos e cadastros e ainda, outras possíveis informações como o nome dos pais.

Nota-se dessa forma, que as instituições não têm definido o propósito para o tratamento, tampouco identificaram as bases legais que autorizam o armazenamento dessas informações, violando o princípio da finalidade e consequentemente, colocando em risco o atendimento à esse fundamento, conforme demonstrado no Quadro 13:

Quadro 13 - Há armazenamento de informações pessoais mesmo de não associados?

| Dimensão/princípio | Finalidade |
|---|---|
| Item do questionário | Há armazenamento de informações pessoais mesmo de não associados? |
| Instituição | Alpha e Gama |
| Não conformidade | Há coleta de dados pessoais de terceiros que não participam diretamente do contrato, ausente a base legal para o tratamento. |
| Fundamentação legal | LGPD – artigo 6º, incisos I e III; |
| Fundamentação normativa | ISO 27701 – 7.2.1 Identificação e documentação do propósito; |
| Risco | Não atendimento do princípio da finalidade e da necessidade. |
| Instituição | Beta |
| Não conformidade | A organização não tem conhecimento de quais dados pessoais são coletadas e se existe a coleta ou não de dados pessoais de terceiros. |
| Fundamentação legal | LGPD – artigo 6º, incisos I e III; artigo 37. |
| Fundamentação normativa | ISO 27701 – 7.2.1 Identificação e documentação do propósito; |
| Risco | Não atendimento do princípio da finalidade e da necessidade. |

Fonte: Dados da pesquisa, Brasil (2018) e ISO 27701 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020).

O artigo 6º da LGPD dispõe claramente no inciso I que o tratamento deve ser utilizado para propósitos legítimos, específicos e informados ao titular; no inciso III que o tratamento deve se limitar apenas ao necessário para a finalidade descrita; e no artigo 37 que o controlador e o operador devem manter o registro das operações, o que sequer é feito pela Beta, pois esta nem iniciou o mapeamento do fluxo e do ciclo de vida dos dados e a Alpha e Gama estão nesta etapa, realizando o levantamento (BRASIL, 2018).

Quanto ao princípio da **adequação**, ao serem questionadas sobre o destino de dados pessoais coletados, mas não utilizados para a finalidade descrita, as três instituições responderam no mesmo sentido, "guardam as informações para utilização futura", conforme Quadro 14.

Entretanto, o armazenamento dessas informações não se sustenta em uma das bases legais, tampouco é amparado por consentimento e há um viés que merece atenção, pois se trata de informações descritas através de currículos, ou seja, são informações autodeclaradas, podendo conter dados pessoas sensíveis, notadamente, merecem resguardo proporcional ao que a lei lhe confere, nos termos do artigo 11 da LGPD.

Inclusive, conforme determinação do art. 16[78] da LGPD, os dados pessoais devem ser eliminados, após o término do seu tratamento. Não é o que ocorre, pois as três instituições retêm dados pessoais por tempo indeterminado, em desatenção ao comando legal. O ideal neste caso, seria a definição de políticas, procedimentos e/ou mecanismos documentados para a eliminação e/ou descarte seguro dos dados pessoais.

Quadro 14 – O que a instituição faz com os dados pessoais coletados para o fim de candidatar-se à vaga de emprego, mas não utilizados para a finalidade descrita na coleta?

| Dimensão/princípio | Adequação |
|---|---|
| Item do questionário | O que a instituição faz com os dados pessoais coletados para o fim de candidatar-se à vaga de emprego, mas não utilizados para a finalidade descrita na coleta? |
| Instituição | Alfa, Beta e Gama. |
| Não conformidade | Armazenamento de dados pessoais sem consentimento ou base legal para composição de banco de currículos (incluindo possíveis dados pessoais sensíveis). |
| Fundamentação legal | LGPD – artigo 7, inciso I; artigo 11, inciso I. |
| Fundamentação normativa | ISO 27701 – 7.2.2 Identificação de bases legais; 7.2.3 Determinando quando e como o consentimento deve ser obtido; 7.2.4 Obtendo e registrando o consentimento |
| Risco | Não atendimento do princípio adequação |

Fonte: Dados da pesquisa, Brasil (2018) e ISO 27701 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020).

A instituição Alfa relata que não são mais recebidos currículos de forma física e estão em processo de digitalização para converter tudo em formato digital, o que facilita a identificação e o processo de acompanhamento do dado pessoal. A utilização de processos e

[78] LGPD, artigo 16: Os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades: I - cumprimento de obrigação legal ou regulatória pelo controlador; II - estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; III - transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou IV - uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados (BRASIL, 2018)

tecnologia[79] para auxiliar nas boas práticas de privacidade é fundamental, pois, *softwares* e procedimentos de gestão contribuem para a organização desses dados pessoais, entretanto, ainda assim é preciso o fortalecimento do elo mais fraco, o humano[80], como bem apontam Araujo (2018), Vroom e Somls (2004), Kemper (2019) e outros[81].

Esse banco de currículos inicialmente precisa estar em conformidade com a legislação, ou seja, é necessário que, caso o candidato não seja escolhido e o tratamento não esteja respaldado pelo artigo 7º, inciso V[82] da LGPD, exista o consentimento para o armazenamento dos DP, descrito no inciso I[83] do mesmo artigo.

A partir disso, a SI faz seu papel, ao traçar ferramentas para garantia da CID dessas informações, por isso, tanto PI quando SI andam lado a lado na jornada da proteção de dados pessoais.

Como há necessidade da implementação de uma cultura de privacidade e proteção de dados, impõe-se às lideranças que tenham comportamentos favoráveis e de boas práticas nesse sentido, fomentando essas atitudes com seus liderados. É tarefa da alta administração e também do gestor de pessoas implementar boas práticas para o recrutamento e para a seleção de novos colaboradores e quando selecionados, desde o início, terem pleno conhecimento das políticas da empresa nesse sentido.

Para tanto, a privacidade e a proteção de dados devem ser pressupostos fundamentais na cultura organizacional, consideradas pelo grupo como parte da natureza e que realmente funciona dessa maneira, tão intrínseco ao grupo que desaparece da percepção consciente (SCHEIN, 1984, 2004).

Como oportunidade de melhoria, sugere-se ao sistema que, para melhores práticas de privacidade, os currículos sejam recebidos sempre de forma digital ou sejam digitalizados de forma a facilitar a busca dos DP, sua alteração e atualização e seja colhido consentimento para que o documento possa ser armazenado em uma base de dados para eventual consulta posterior, limitando e especificando ao titular de dados o lapso temporal disso, sendo que *softwares* podem emitir avisos e fazer a exclusão automática no decurso do prazo. Em suma, sugere-se

---

[79] Ver Figura 2.
[80] Para mais informações, ver tópicos 2.7 e 2.8 deste trabalho.
[81] Contech e Schmick (2016); D'Arcy, Hovav e Galletta (2009), Metalidou et at. ( 2014), Nichol ( 2000), Parsons et al. (2010), Russel (2002), Schneier (2004), Schultz (2005), Solms e Solms (2004), Voss (2001), Vroom e Solms (2004), Whitman e Mattord (2011).
[82] LGPD, artigo 7º, inciso V: quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados (BRASIL, 2018).
[83] LGPD, artigo 7º, inciso I: mediante o fornecimento de consentimento pelo titular (BRASIL, 2018);

que as organizações façam o uso ostensivo de avisos legais, comunicando aos titulares de dados, de forma transparente, clara e objetiva, os propósitos do tratamento de dados pessoais, em conformidade com o art. 9º[84] da LGPD.

Além disso, ao coletar essas informações, as instituições podem prescrever ao titular que não declare nenhum dado pessoal sensível, não permitindo que assim o faça, pois, além de não adequado e necessário, há um risco jurídico em manter esses dados, ou seja, a instituição pode muito bem fazer essa gestão e minimizar estes riscos.

Para a adequação da instituição na LGPD é necessário, antes de tudo, conhecer todo o processo e o ciclo de vida do dado pessoal[85], o que pode ser feito através do mapeamento de dados, portanto, esta etapa é primordial para a conformidade.

Para ter pleno conhecimento do porquê da coleta do DP, é necessário saber seu fim, portanto, na dimensão da **necessidade,** é imperativo que se tenha definido todo o mapeamento e partir disso, a dispensa ou não do tratamento.

Dessa forma, quando questionado às instituições a existência desse *data mapping*, Beta e Gama não possuem nada concretizando, conforme Quadro 15, descrevendo ambas que iniciaram o processo, mas que ainda faltam inúmeras etapas para finalização, desatendendo ao princípio da transparência**.** A Alpha descreveu que já realizou este procedimento, através de consulta com o gestor de cada setor da instituição e que este documento está disponível aos interessados internos para acompanhamento.

Quadro 15 – Há um mapeamento do fluxo dos dados tratados na instituição?

| Dimensão/princípio | Necessidade |
|---|---|
| Item do questionário | Há um mapeamento do fluxo dos dados tratados na instituição? |
| Instituição | Beta e Gama. |
| Não conformidade | Inexistência de registro das operações de tratamento de dados pessoais realizados. |
| Fundamentação legal | LGPD – artigo 6, inciso VI; artigo 37. |
| Fundamentação normativa | ISO 27701 – 7.2.8 Registros relativos ao tratamento de DP. |
| Risco | Não atendimento do princípio da transparência. |

Fonte: Dados da pesquisa, Brasil (2018) e ISO 27701 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020).

[84] LGPD, artigo 9º: O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei (BRASIL, 2018).

[85] Ver Figura 4.

O mapeamento permite a conformidade com os princípios, pois ele é um instrumento facilitador, como por exemplo, na dimensão do **livre acesso**, a consulta dos dados pessoais pode ser realizada através da busca no mapa, ou seja, quando um titular requer acesso e informações sobre seus dados[86], a instituição consegue respondê-lo com facilidade e no tempo adequado[87], conforme Quadro 16.

O livre acesso ainda compõe a disponibilização de informações sobre a forma e a duração do tratamento dos seus dados, por isso, fora questionado aos respondentes se o titular de dados tem acesso fácil à essas informações na internet, rede social ou aplicativo, o que resultou na mesma resposta de ambos: acesso apenas mediante requerimento.

A LGPD dispõe que a consulta a essas informações devem ser facilitada e gratuita[88], por isso, o indicado é apresentar ao titular de dados um aviso legal contendo de forma clara como e por quanto tempo seus dados são tratados, além de dispor de um canal de comunicação para requisição de informações, ao encontro do princípio da transparência[89], e também, ao art. 18 da LGPD, o qual determina que o titular dos dados pessoais tem direito de requisitar ao controlador, em relação aos dados do titular por ele tratados, a qualquer momento, informações e ações pertinentes aos seus dados pessoais.

Assim sendo, nota-se que, em que pese as instituições disponibilizarem um canal para tanto (e-mail), ainda não há descrito de forma facilitada a forma e a duração dos dados pessoais e isso pode ser adequado com um aviso legal nas plataformas físicas e digitais, através de comunicação fácil, transparente e acessível para todos os públicos, o que se sugere ao sistema.

Alpha descreve que teria acesso aos dados pessoais de forma simplificada, pois já realizaram o mapeamento, Beta relata que não teria estas informações para disponibilizar e Gama diz que o e-mail disponibilizado para esta consulta pelo titular é do DPO da confederação, ou seja, outra instituição do sistema, em nível nacional, o que poderia inclusive atrasar e dificultar ainda mais esse processo.

---

[86] LGPD, artigo 18: O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição (BRASIL, 2018).

[87] Atendendo o que dispõe o artigo 19 da LGPD: A confirmação de existência ou o acesso a dados pessoais serão providenciados, mediante requisição do titular: I - em formato simplificado, imediatamente; ou II - por meio de declaração clara e completa, que indique a origem dos dados, a inexistência de registro, os critérios utilizados e a finalidade do tratamento, observados os segredos comercial e industrial, fornecida no prazo de até 15 (quinze) dias, contado da data do requerimento do titular (BRASIL, 2018).

[88] LGPD, artigo 6º, inciso IV: livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais (BRASIL, 2018);

[89] LGPD: artigo 6º, inciso VII: transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial (BRASIL, 2018);

Quadro 16 – A instituição permite o acesso de todos os dados pessoais do titular?

| Dimensão/princípio | Livre Acesso |
|---|---|
| Item do questionário | A instituição permite o acesso de todos os dados pessoais do titular? |
| Instituição | Alpha, Beta e Gama. |
| Não conformidade | Disponibilização das informações sobre os dados pessoais somente mediante requerimento solicitado por e-mail. |
| Fundamentação legal | LGPD – artigo 6º, inciso IV e VI, artigo 18; artigo 19, I e II; CDC – artigo 43. |
| Fundamentação normativa | ISO 27701 – 7.3.1 Determinando e cumprindo as obrigações para os titulares de DP; 7.3.2 Determinando as informações para os titulares de DP; 7.3.3 Fornecendo informações aos titulares de DP. |
| Risco | Não atendimento do princípio do livre acesso e da transparência. |

Fonte: Dados da pesquisa, Brasil (2018) e ISO 27701 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020).

Além disso, o princípio do livre acesso já é garantido ao consumidor desde a vigência do CDC[90], que institui o acesso à informações de dados pessoais do titular e suas respectivas fontes, ou seja, consolidado desde o início dos anos noventa.

Não basta somente que seja concedido ao titular livre acesso aos dados, mas que estes dados sejam exatos, claros e passíveis de atualização. É nessa ótica que na dimensão da **qualidade dos dados** buscou-se conhecer quais as ferramentas disponibilizadas ao titular de dados para que ele possa alterar ou atualizar seus dados pessoais.

Alpha, Beta e Gama declaram que essa atualização pode ser feita através das agências, principal meio de contato físico entre associado e cooperativa e através do aplicativo da instituição (*mobile bank*), em uma aba de atualização cadastral.

Percebe-se a conformidade das instituições nesse tocante e como sugestão de melhoria, indica-se que seja permitido ao titular a atualização em outras plataformas, como por exemplo o site institucional, através de uma aba ou opção “atualize seus dados pessoais”, pois nem todos os associados utilizam o aplicativo pelo celular.

Na dimensão da **transparência**, dentre outros itens, verificou-se a existência de informações sobre a utilização de dados pessoais em ações de marketing e propaganda, conforme Quadro 17, sendo que apenas a Alpha tem um aviso legal, de forma genérica, no preenchimento de formulários, relatando a finalidade do tratamento e solicitando o consentimento para tal.

[90] CDC, artigo 43: O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes (BRASIL, 1990).

Beta e Gama não possuem aviso legal, sendo que esta última recebe *leads*[91] através da central, ou seja, os dados pessoais são compartilhados entre as instituições e o respondente não soube dizer se há algum documento que formalize essa transferência, tampouco se a central disponibiliza um aviso legal na coleta, nem se há consentimento do titular.

Quadro 17 – Em campanhas de marketing/propaganda, o associado/titular de dados tem acesso a informações claras no aviso legal?

| Dimensão/princípio | Transparência |
|---|---|
| Item do questionário | Em campanhas de marketing/propaganda, o associado/titular de dados tem acesso à informações claras no aviso legal? |
| Instituição | Alpha |
| Não conformidade | Insuficiência de informações prestadas sobre o tratamento dos dados coletados. |
| Fundamentação legal | LGPD – artigo 6º, inciso IV; artigo 9º. |
| Fundamentação normativa | ISO 27701 – 7.3.1 Determinando e cumprindo as obrigações para os titulares de DP; 7.3.2 Determinando as informações para os titulares de DP; 7.3.3 Fornecendo informações aos titulares de DP. |
| Risco | Não atendimento do princípio da transparência. |
| Instituição | Beta |
| Não conformidade | Ausência de aviso legal e de informação sobre o tratamento dos dados coletados. |
| Fundamentação legal | LGPD – artigo 6º, inciso IV; artigo 9º. |
| Fundamentação normativa | ISO 27701 – 7.3.1 Determinando e cumprindo as obrigações para os titulares de DP; 7.3.2 Determinando as informações para os titulares de DP; 7.3.3 Fornecendo informações aos titulares de DP. |
| Risco | Não atendimento do princípio da transparência. |
| Instituição | Gama |
| Não conformidade | Ausência de aviso legal e de informação sobre o tratamento dos dados coletados; transferência de dados com outro controlador. |
| Fundamentação legal | LGPD – artigo 6º, inciso IV; artigo 9º. |
| Fundamentação normativa | ISO 27701 – 7.3.1 Determinando e cumprindo as obrigações para os titulares de DP; 7.3.2 Determinando as informações para os titulares de DP; 7.3.3 Fornecendo informações aos titulares de DP. |
| Risco | Não atendimento do princípio da transparência. |

Fonte: Dados da pesquisa, Brasil (2018) e ISO 27701 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020).

Com o mapeamento dos dados, o aviso legal torna-se ferramenta importante para a adequação ao princípio da transparência, lembrando que, não somente para ações de comunicação nas plataformas digitais, mas também físicas, como por exemplo, nas agências.

Na dimensão da **segurança**, ao serem questionados sobre a realização de treinamentos com os colaboradores da instituição sobre a privacidade da informação, as três instituições relataram que anualmente realizam este procedimento, tanto para SI, quanto para a PI.

[91] Nomenclatura utilizada para descrever um contato comercial, uma possível prospecção.

Ações educativas devem ser realizadas pelo controlador e pelo operador de dados, conforme disciplina a LGPD[92], mas muito além da realização de um treinamento por ano, como fazem as instituições pesquisadas, devem ser aplicadas medidas que fortaleçam boas práticas, fazendo com que a cultura da empresa reflita a PI e a PD.

Não é por acaso que a literatura, em muitos momentos[93], reflete e descreve que a implementação de uma cultura no âmbito organizacional perpassa por uma forte influência da liderança e de ações pedagógicas, bem como pela concretização do conhecimento da instituição de forma explícita, podendo ser repassado com facilidade para novos colaboradores, conforme destaca Nonaka (2007), sendo compartilhado e transmitido, transcendendo do individual para o coletivo.

O fato é que as três instituições, mesmo realizando uma vez por ano um treinamento de SI (os quais incluem PI), estão no Nível 3 (Encaminhado) da escala de Araujo (2018) no tocante à cultura de segurança da informação, o que demonstra que possuem preocupação com a SI, mas ainda há comportamentos de risco e, por se tratar de respondentes gestores de TI e DPOs, espera-se ações e conhecimentos técnicos mais elevados do que demais colaboradores.

O comportamento de um único membro pode colocar em risco toda a estrutura de ativos no tocante à informação, basta lembrar do exemplo da Muralha da China[94], no qual não foi preciso destruí-la, apenas subornar um único porteiro. (WHITMAN; MATTORD, 2011).

Não se discute a importância do treinamento, mas sim, do quanto está sendo absorvido em termos de conhecimento e de importância que os colaboradores dão à temática, talvez por não terem respaldo de sua liderança ou até mesmo por não compreenderem os riscos, por isso, muitas vezes, a frequência de estudos e debates, bem como o método de ensino podem ser discutidos pela instituição, pois, é necessário que haja esse aculturamento, e ações afirmativas e pedagógicas são fundamentais para tanto.

Essa temática pode ser melhor compreendida quando analisado a resposta da Gama ao questionamento de barreiras e dificuldade quanto à proteção de dados e à LGPD, sendo declarado que a maior barreira são as pessoas, tanto da ponta (referindo-se aos colaboradores

---

[92] LGPD, artigo 50: Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

[93] Ver tópicos 2.6, 2.7 e 2.8 deste trabalho.

[94] Ver tópico 2.7 deste trabalho.

das agências) quanto da administração, pois a preocupação desses agentes é menor do quanto deveria ser.

Ainda no item das barreiras, o respondente da Beta declara que é necessário uma mudança de cultura e que a proteção de dados não é uma prioridade para a instituição hoje, ficando praticamente tudo a cargo do seu setor, que já está sobrecarregado de demandas. Essa falta de tempo e pessoas é relata pela Alpha, no mesmo item do questionário.

Líderes precisam colocar a SI e a PI como prioridades, pois são eles que originalmente estipulam crenças e valores (SCHEIN, 2004) e como eles reagem aos problemas e os resolvem tem forte ligação com a construção da cultura (BASS; AVOLIO, 1993). Não é recomendável deixar que um incidente ocorra para só depois tomar as medidas adequadas, nem esperar acontecer uma fatalidade no trânsito, fazendo analogia ao exemplo de Anderson (2003), descrito no tópico 2.7. No contexto da PD, a fatalidade pode ser desde a aplicação de sanções administrativas, como multa pela ANPD[95], até o vazamento de dados, atingindo ativos da instituição, tanto materiais quanto incorpóreos, como por exemplo, a imagem e a marca.

Portanto, ações de melhoria contínua, proativas[96] e educacionais devem ser propostas com recorrência por parte das instituições, envolvendo diretamente todos os colaboradores, visando mitigar riscos e implementar a SI, a PI e a PD na cultura da organização.

Na dimensão da prevenção, ao serem questionadas sobre a existência de um procedimento de gestão de riscos formalizado para prevenção de incidentes à SI, conforme Quadro 18, Alpha declarou que é realizada (pelo próprio setor de TI) uma vez por ano, uma análise de risco, fundamentada nos padrões da Associação Brasileira de Normas Técnicas – ABNT e da Política de Segurança da Informação do sistema cooperativo; Gama declarou que realiza análise de risco anualmente e em consequência dela elabora um plano de ação, destacando também que usa informações do *software* utilizado na auditoria promovida pela

[95] LGPD, artigo 52: Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: 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 - publicização 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; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

[96] Como por exemplo, as boas-práticas de *PbD* de Cavoukian (2010).

central do sistema cooperativo para formulação do plano; Beta declarou não existir nada nesse sentido, manifestando o desejo de criação, após finalizar a implementação e adequação da LGPD.

Quadro 18 – Existe um procedimento de gestão de riscos formalizado na instituição para prevenir a ocorrência de incidentes a segurança da informação?

| Dimensão/princípio | Prevenção |
|---|---|
| Item do questionário | Existe um procedimento de gestão de riscos formalizado na instituição para prevenir a ocorrência de incidentes a segurança da informação? |
| Instituição | Beta |
| Não conformidade | Inexistência de procedimentos para gestão de riscos. |
| Fundamentação legal | LGPD – artigo 6º, inciso VIII; artigo 50, parágrafo 1º. |
| Fundamentação normativa | ISO 27701 – 6.2 Políticas de segurança da informação |
| Risco | Não atendimento do princípio da prevenção. |

Fonte: Dados da pesquisa, Brasil (2018) e ISO 27701 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020).

A análise de risco torna-se fundamental para que a organização conheça as ameaças, as vulnerabilidades e os possíveis incidentes[97], como por exemplo, o vazamento de dados pessoais. Nesse caso, a própria LGPD estabelece a possibilidade da ANPD solicitar relatório de impacto à proteção de DP[98].

Além disso, a LGPD descreve que os agentes de tratamento de dados pessoais devem adotar as medidas técnicas e administrativas para proteção de DP de acessos não autorizados e de situações de incidentes[99]. A garantia da SI em relação a DP também é objeto da lei, ao obrigar que assim a faça os agentes supracitados ou ainda outras pessoas que intervenham em alguma fase do tratamento[100].

As três instituições declararam que utilizam como medidas técnicas e administrativas várias tecnologias, como *firewall*, *data loss prevention*, criptografia, redundância de *links*, servidores, *backups*, testes de *phishing*, treinamentos e conscientização.

A gestão de risco inclusive contribui para a implementação da cultura de SI, PI e PD na organização, pois, os colaboradores, ao tomarem conhecimento dos riscos, podem adotar

[97] Mais informações no tópico 2.2 e figura 3 deste trabalho.

[98] LGPD, artigo 38: A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial (BRASIL, 2018).

[99] LGPD, artigo 46: Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito (BRASIL, 2018).

[100] LGPD, artigo 47: Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término (BRASIL, 2018).

medidas e comportamentos favoráveis, ao invés de simplesmente aguardarem a ocorrência de um incidente.

Em caso de vazamento de dados, a LGPD estabelece que o controlador é obrigado a comunicar a ANPD com uma série de descrições a respeito dos dados, do tratamento, dos riscos e das medidas adotadas[101]. Neste capítulo, abordamos este tema e alguns vazamentos ocorridos no Brasil, inclusive com o possível impacto causado por eles.

Aliás, a LGPD aponta que a ANPD poderá dispor sobre padrões técnicos mínimos sobre o tratamento, principalmente sobre dados pessoais sensíveis, os quais, por sua própria natureza, estão diretamente ligados à não discriminação, pois se tratam de informações que muitas vezes estão no mais central dos círculos de Hubmann (1967), o da vida secreta, apontado por Zanini (2020) como aquele que é o mais protegido.

Dessa forma, na dimensão da **não discriminação** foi questionado aos respondentes se a organização realiza a coleta de algum tipo de dado pessoal sensível, sendo que todas declararam assim o fazerem (Quadro 19).

Alpha citou como exemplo dados de menores, saúde (contratos e simulações de seguro) e de colaboradores, como exame admissional. Disse ainda, que há compartilhamento dessas informações com terceiros, por cumprimento de questões contratuais. Beta apontou que há coleta de dados pessoais sensíveis também, mas que desconhece qualquer utilização para fins discriminatórios[102]. Gama relatou que trata esses dados, por exemplo, em contratação de colaboradores e para contratos de seguros.

Quadro 19 – A instituição coleta algum tipo de dado pessoal sensível?

| Dimensão/princípio | Não discriminação |
|---|---|
| Item do questionário | A instituição coleta algum tipo de dado pessoal sensível? |
| Instituição | Alpha, Beta e Gama. |
| Não conformidade | Coleta de dados pessoas sensíveis sem base legal e sem consentimento. |
| Fundamentação legal | LGPD – artigo 6º, inciso IX; artigo 11, inciso I e II. |
| Fundamentação normativa | ISO 27701 – 7.2.1 Identificação e documentação do propósito; 7.2.2 Identificação de bases legais; 7.2.3 Determinando quando e como o consentimento deve ser obtido; 7.2.4 Obtendo e registrando o consentimento; 7.4.1 Limite de coleta; 7.4.2 Limite de tratamento. |
| Risco | Não atendimento do princípio da não discriminação. |

Fonte: Dados da pesquisa, Brasil (2018) e ISO 27701 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2020).

[101] LGPD, artigo 48: O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares (BRASIL, 2018).
[102] Em seu sentido de injusto, desigual.

A LGPD somente autoriza, de forma expressa e restrita, o tratamento desse tipo de dado mediante consentimento[103] ou sem, nas hipóteses do artigo 11, inciso II[104]. Dessa forma, percebe-se um maior rigor por parte do legislador em conferir um elevado grau de proteção relativo a esses dados, o que se justifica no objetivo de diminuir a possibilidade de usos discriminatórios, em respeito aos fundamentos da lei, como por exemplo a inviolabilidade da intimidade, da honra, os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e cidadania da pessoa[105].

Um exemplo disso é a escolha – de um candidato à vaga de emprego – que não deve se pautar por exemplo na orientação sexual, na opinião política, na saúde, na religião ou em outras características que a LGPD considera como dado pessoal sensível[106], seguindo a ótica geral do direito, da ética e diversos dispositivos legais[107] (BRASIL, 2018). Exceto, no caso de discriminação (categorização) de minorias que possam ser beneficiadas em programas de inclusão e de ações afirmativas nas empresas.

Portanto, o armazenamento desses DP sem justificativa ou uma ação afirmativa embasada na lei, só dificulta a gestão de riscos e se mostra totalmente desnecessária, inclusive porque, ao exemplo da orientação sexual, uma pesquisa da rede social LinkedIn (2019) aponta que 37% (trinta e sete por cento) de respondentes autodeclarados LGBT+[108] não compartilha com seus colegas de trabalho a sua orientação sexual devido a medo de represálias.

---

[103] LGPD, artigo 11: O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses: inciso I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas (BRASIL, 2018);

[104] LGPD, artigo 11, inciso II: sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para: a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, em procedimento realizado por profissionais da área da saúde ou por entidades sanitárias; ou f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018).

[105] Para mais informações sobre todos os fundamentos da LGPD, ver tópico 2.4 e figura 7 deste trabalho.

[106] Nos moldes do artigo 5º, inciso II: dado pessoal sensível: 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.

[107] Cita-se por exemplo, o artigo 7º, inciso III, XXX, XXXI, XLI e XLII da CF; artigo 5º e 461 da Consolidação das Leis do Trabalho – CLT; Lei 9.029 de 1995 (BRASIL, 1943, 1988, 1995);

[108] Sigla utilizada para identificar a comunidade de lésbicas, gays, bissexuais, transgêneros e outras identidades de gênero e orientação sexual.

Entretanto, situações que exijam a coleta desses dados devem estar legalmente fundamentadas e o tratamento deve sempre se pautar na mínima intervenção e na necessidade, resguardando a autodeterminação informativa.

Isso demonstra a importância de ações inclusivas e afirmativas por parte das empresas e confirma a desnecessidade de coletar esse tipo de informação se não for para esse fim, moldando um ambiente de respeito e pluralidade.

No caso das instituições pesquisadas, percebe-se que a utilização de dados pessoais sensíveis para o fim de cumprimento de obrigação contratual (seguros) encontra respaldo no artigo 11, inciso II, alíneas a, d[109], mas, à título de sugestão e conformidade legal, indica-se que sejam estabelecidas normas e cláusulas contratuais com os terceiros (internos ao sistema ou não), que tratam conjuntamente estes dados, como por exemplo o *Data Processing Agreement – DPA*[110]*,* restando ambos adequados. Sugere-se também que, no caso de discriminação (categorização), os dados não sejam utilizados para fins que atentem aos direitos fundamentais (BRASIL, 2018).

Na dimensão da **responsabilização e prestação de contas**, quando indagado às instituições se as ações relativas à privacidade da informação são documentadas, Alpha relata que há o mapeamento dos dados, registros de treinamentos e documentos das auditorias de SI, tanto externa, quanto interna; Beta aponta que as ações de conscientização de colaboradores estão documentadas e que apresenta relatórios para diretoria e auditoria, além de ter registro de testes de *phishing* e das reuniões do comitê de proteção de dados; Gama destaca que os treinamentos são documentados, há registros em ata das reuniões do comitê de PD e possuem informações de análise de risco, entretanto, esta última informação pode se mostrar equivocada, pois a mesma instituição afirmou que sequer iniciou o mapeamento dos dados, ou seja, seguindo padrões da ISO 27701, que determina as práticas de conformidade, e da LGPD, o mapeamento é uma etapa importante para análise de risco, pois só assim é possível compreender onde há não conformidades e avaliar os riscos.

Quanto às auditorias, as três instituições relataram que realizam auditoria interna, pelo próprio setor de TI e externa, pela central do sistema, através de empresa terceirizada, nos padrões da família da ISO 27000. Entretanto, não há nenhuma metodologia específica para

[109] LGPD, artigo 11, inciso II: a) cumprimento de obrigação legal ou regulatória pelo controlador; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) (BRASIL, 2018).

[110] O DPA é um acordo de tratamento de dados, um documento formal que pode ser inclusive um aditivo aos contratos já existentes.

avaliar conformidades de proteção de dados, apesar de todos os respondentes terem confirmado que, em 2020 a auditoria externa abordou alguns aspectos específicos da LGPD e acreditam que, nas próximas o tema será melhor explorado.

No tocante à SI, os respondentes declararam que, por se tratar de instituições financeiras, existe uma dedicação mais antiga para a sua proteção, em decorrência das normativas do órgão fiscalizador, o BACEN, como por exemplo a Resolução Nº 4.658 de 2018 (BANCO CENTRAL DO BRASIL, 2018).

A LGPD estabelece sanções administrativas[111] pela ANPD no caso de descumprimento da legislação, sem prejuízo de outras sanções, inclusive judiciais, inclusive com multas que podem chegar até dois por cento do faturamento, limitando a cinquenta milhões de reais. Além disso, estabelece que se pode tornar público a infração, ou seja, existe também a possibilidade de prejuízos à reputação e imagem da empresa. Ainda como medida de sanção, a ANPD poderá suspender e proibir o exercício do tratamento de dados (BRASIL, 2018).

Nota-se que, a divisão em dimensões dos princípios elencados na LGPD para a utilização neste instrumento de pesquisa (eixo três) faz sentido na aplicação acadêmica, pois, na prática, há uma rede onde todos se comunicam, uns mais que outros, mas é impossível dissociá-los, bem como, não faz sentido estudá-los ou aplicá-los de forma isolada dos fundamentos[112], que norteiam a legislação.

Foi possível verificar que as instituições pesquisadas detém aparato tecnológico mínimo para conformidade legal, inclusive porque há algum tempo já são reguladas por órgãos fiscalizadores quanto à SI, mas como apresentado na fundamentação teórica deste trabalho, a tecnologia é utilizada por pessoas e essas, são muito mais vulneráveis, por isso, recomenda-se um trabalho de aculturamento dos colaboradores quanto à SI, PI e PD, principalmente para que a liderança tenha, em vários níveis, plena consciência da importância que a temática toma no

---

[111] LGPD. Artigo 52: Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: 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 - publicização 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; X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador; XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período; XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados (BRASIL, 2018).

[112] Ver artigo 2º da LGPD (BRASIL, 2018), tópico 2.4 e figura 7 deste trabalho.

contexto atual, dito como a Quarta Revolução Industrial, onde, no conceito de Castells (2000), a informação é tão importante para a sociedade que esta pode ser considerada como aquela.

Portanto, informações e dados são para empresa um ativo de grande proporção e consequentemente, motivo de ameaças e devem ser protegidos por inúmeras razões, sejam por adequação à legislação, por geração de valor na própria organização ou ainda, por preservação de direitos fundamentais dos envolvidos.

# 5 CONSIDERAÇÕES FINAIS

A sociedade baseada em dados e informações carrega em sua própria essência uma rede de infinitas conexões que, no contexto digital, ganham dimensões sem barreiras geográficas e muitas vezes, sem limitações temporais. Nesse oceano de dados há infinitas formas de identificar o indivíduo, colocando-o, muitas vezes sem seu consentimento, em situações que prejudicam a sua privacidade, nas quais ele não desejava ser reconhecido.

Portanto, quem navega por essas águas deve ter consciência da necessidade e importância da preservação da confidencialidade, integridade e disponibilidade, princípios fundamentais da segurança da informação, o que incluí também a privacidade de dados pessoais.

Dentro dessa esfera global, pode-se inserir, por exemplo, as organizações, cada uma com sua cultura específica e nela, tecnologias, processos e pessoas devem estar preparadas para garantir a proteção de dados pessoais.

Entretanto, como importante ativo dentro das instituições, as informações e os dados pessoais tornam-se, muitas vezes, vulneráveis, pois o comportamento humano enfraquece fortalezas tecnológicas e processuais, sendo o homem considerado o elo mais fraco, então, motivo de ataques de engenheiros sociais.

Como forma de garantir padrões e boas práticas, adentra no cenário nacional uma legislação específica para tratamento de dados (LGPD), que é analisada sob o prisma hermenêutico em um contexto real, através do estudo em um sistema financeiro cooperativista.

Assim, buscou-se responder à pergunta da pesquisa: “Como analisar a cultura organizacional de segurança e privacidade da informação e proteção de dados na percepção de gestores de instituições financeiras cooperativistas?”

Compreendendo a importância da cultura organizacional e o papel fundamental da liderança na formação de pressupostos fundamentais, que devem estar enraizados no ambiente corporativo, verificou-se que o sistema se encontra no nível da escala, desenvolvida por Araujo (2018), descrito como “Encaminhado”, ou seja, tem em si a prática de ações para a SI, mas alguns de seus colaboradores, por vezes, ainda apontam pré-disposições comportamentais que podem colocar em risco os ativos da informação.

De forma complementar, avaliou-se a privacidade da informação e proteção de dados na percepção de alguns desses gestores e, dentre os resultados, observou-se a baixa liderança para questões de PI e PD.

Considerando que os respondentes eram gestores de tecnologia e consequentemente, devem deter conhecimentos relevantes sobre esse assunto, comparando-os com os demais colaboradores da instituição, o quadro pode ser analisado sob uma ótica que exige maior preocupação, pois, espera-se que os demais colaboradores apresentem comportamentos ainda menos favoráveis. Por isso, como **oportunidade de trabalho futuro**, sugere-se que a aplicação dos instrumentos deste trabalho também seja feita com todos os setores e colaboradores das instituições.

Como **sugestão de novos estudos,** pode-se desenvolver uma escala de medida da cultura de privacidade da informação e proteção de dados, permitindo mensurar o nível dessas e de outras instituições, como por exemplo, órgãos públicos e de ensino, além de outros segmentos do mercado.

Com a construção teórica e a discussão dos resultados da pesquisa de campo, foram alcançados os objetivos específicos "realizar levantamento de literatura, em bases de dados que indexam publicações científicas, sobre segurança e privacidade da informação, proteção de dados, cultura organizacional e temas correlatos, com vistas a fundamentar tais construtos, bem como, fornecer subsídio para análise e discussão dos dados obtidos nas pesquisas de campo" e "realizar levantamento de legislação e normativas sobre os temas estudados, em especial, sobre a LGPD e seus princípios".

Da mesma forma, a compreensão e análise de barreiras e benefícios permitiu o alcance do objetivo específico "analisar as barreiras e benefícios do aculturamento da segurança e privacidade da informação em instituições financeiras cooperativistas", inclusive pelas discussões dos resultados, através do levantamento de dados primários e secundários, alcançando, dessa maneira, os objetivos específicos "analisar a segurança da informação em instituições financeiras cooperativistas, com base na literatura e pesquisa de campo com os gestores dessas instituições por meio da escala desenvolvida por Araujo (2018), via TRI" e "analisar a privacidade da informação e a proteção de dados em instituições financeiras cooperativistas, com base na literatura e depoimento dos respondentes, obtido na pesquisa de campo com gestores, por meio de questionário construído com base nos princípios da LGPD".

Além disso, com a sugestão de trabalhos futuros, o objetivo específico "contribuir com o avanço do conhecimento na área, inclusive, com a identificação de lacunas de pesquisa, apontando oportunidades futuras de estudo" foi alcançado, sendo possível declarar oportunidades de melhoria para o sistema pesquisado, como por exemplo, a adequação de várias não conformidades no tocante à implementação da LGPD, ao desenvolvimento de atividades

de conscientização sobre a temática e principalmente, o comportamento de promoção de segurança e privacidade da informação por parte da gestão e da liderança, pois, elas têm papel fundamental e de destaque na cultura do ambiente.

A literatura aponta que, na tríade "tecnologia, processos e pessoas", o elo mais fragilizado da corrente é este último, pois os dois primeiros estão em constante evolução e dificultam a ação de agentes maliciosos à informações protegidas. Entretanto, basta um único colaborador que, sem comportamentos adequados, facilite (muitas vezes sem intenção) o acesso ilícito de terceiros.

Implementar uma consciência e uma cultura de segurança e privacidade da informação na instituição significa não somente proteger os ativos corporativos e os objetivos do cooperativismo (no caso do sistema pesquisado), mas principalmente, respeitar o cidadão enquanto indivíduo que merece e tem proteção constitucional e legal de seus direitos ligados à PD.

Dessa forma, implementando a privacidade como padrão nos projetos e processos, há maior garantia de adequação legal e de proteção ao titular de dados e sua autodeterminação informativa, além de respeitá-lo em seus direitos fundamentais, esculpidos na CF e porque não, contribuir para o cumprimento inclusive dos princípios cooperativistas, que em sua essência, desde o nascimento desse modelo de negócio, têm o mutualismo e o crescimento coletivo como objetos de construção de uma sociedade mais próspera.

Considerando a relevância da LGPD e recente início da sua vigência, as organizações precisam estar adequadas as orientações descritas, inclusive para não incorrer nas sanções previstas nesse ordenamento, pois, além de responsabilizações administrativas, com multas que podem chegar ao patamar milionário, há possibilidade de condenações judiciais, o que pode afetar a imagem, a reputação e a própria sobrevivência da instituição.

Nota-se que a legislação não se restringe apenas à adequação por parte das organizações, mas é um paralelo entre elas e a sociedade, como ferramenta de construção e garantia de princípios fundamentais, visando garantir um convívio social pacífico no contexto digital, onde todos podem desfrutar dos benefícios derivados da adequação.

Não se pode negar a importância da informação e dos dados para a inovação e o desenvolvimento tecnológico e econômico, mas sobretudo, para concretizar estes objetivos, as corporações devem garantir os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania e para isso, precisam compreender seu papel e suas responsabilidades.

Portanto, mesmo que a instituição tenha sido construída e solidificada em recursos tecnológicos, exaltando a magnificência de sua fortaleza digital e tenha os processos e políticas alinhados e bem definidos, não é necessário mais do que apenas um agente para que um exército todo desfile diante da imensidão de proteção, que intacta, será invadida e poderá causar prejuízos incalculáveis e com efeito à coletividade, muitas vezes, irreparáveis. Entretanto, uma estratégia que se mostra poderosa para minimizar riscos é fazer com que cada colaborador compreenda a SI e PI, seu papel na organização e suas responsabilidades, ficando incutido na cultura organizacional a proteção de dados.

# REFERÊNCIAS

ALEXANDRE, João Welliandre Carneiro; ANDRADE, Dalton Francisco de; VASCONCELOS, Alan Pereira de; ARAUJO, Ana Maria Souza de. Uma proposta de análise de um construto para a medição dos fatores críticos da gestão pela qualidade através da teoria da resposta ao item. **Gestão & Produção**, vol. 9, n. 2, p. 129–141, 2002.

ALHOGAIL, Areej; ABDULRAHMAN, Mirza. A Framework of Information Security Culture Change. **Journal of Theoretical and Applied Information Technology**, vol. 64, n. 2, p. 540–549, 2014.

ANDERSON, James M. Why we need a new definition of information security. **Computers and Security**, vol. 22, n. 4, p. 308–313, 2003. Disponível em: https://doi.org/10.1016/S0167-4048(03)00407-3

ANDRADE, Dalton Francisco de; TAVARES, Heliton Ribeiro; VALLE, Raquel da Cunha. **Teoria da Resposta ao Item:** Conceitos e Aplicações. São Paulo: ABE - Associação Brasileira de Estatística, 2000.

ARAUJO, Pedro Henrique de Moura. **Construção da Escala do Nível da Cultura Organizacional de Segurança da Informação**. 205 f. 2018. Tese (Doutorado em Engenharia de Produção) - Universidade Federal de Santa Catarina, 2018.

ASSELSTINE, D. Cyber-risk : a breach may be inevitable. **Plans and Trusts**, vol. 36, n. 2, p. 18–23, 2018.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:** Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro: ABNT, 2013a.

_____. **ABNT NBR ISO/IEC 27002 :** Tecnologia da informação — Técnicas de segurança — Código de prática para controles de segurança da informação. Rio de Janeiro: ABNT, 2013b.

_____. **ABNT NBR ISO/IEC 27701:** Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes. Rio de Janeiro: ABNT, 2020.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. **Guia Orientativo para Definições dos Agentes de Tratamento de Dados Pessoais e do Encarregado**. Brasília: ANPD, 2021.

AVOLIO, Bruce J.; GARDNER, William L. Authentic leadership development: Getting to the root of positive forms of leadership. **The Leadership Quarterly**, vol. 16, n. 3, p. 315–338, 2005. Disponível em: https://doi.org/10.1016/j.leaqua.2005.03.001

BAIÃO, Kelly C Sampaio; GONÇALVES, Kalline Carvalho. A garantia da privacidade na sociedade tecnológica : um imperativo à concretização do princípio da dignidade da pessoa

humana construção de uma sociedade de vigilância . **Civilistica Com**, vol. 3, n. 2, p. 1–24, 2014.

BAKER, Frank B. **The basics of Item Response Theory**: ERIC Clearinghouse on Assessment and Evaluation, 2001.

BANCO CENTRAL DO BRASIL. **Resolução N 2.554, de 24 de setembro de 1998.** Dispõe sobre a implantação e implemenação de sistema de controles internos. 1998.

_____. **Resolução N 4.658, de 26 de abril de 2018.** Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições financeiras, 2018.

BARRETO, Aldo de Albuquerque. A Questão da Informação. **São Paulo em Perspectiva**, vol. 8, n. 4, p. 3–8, 1994.

BARRETO, Leilianne Michele Trindade da Silva; KISHORE, Angeli; REIS, Germano Glufke; BAPTISTA, Luciene Lopes; MEDEIROS, Carlos Alberto Freire. Cultura organizacional e liderança: uma relação possível? **Revista de Administração**, vol. 48, n. 1, p. 34–52, 2013. Disponível em: https://doi.org/10.5700/rausp1072

BASS, Bernard M.; AVOLIO, Bruce J. Transformational Leadership and Organizational Culture. **Public Administration Quarterly**, vol. 17, n. 1, p. 112–121, 1993.

BAYLEY, Scoot. Measuring customer satisfaction. **Evaluation Journal of Australasia**, vol. 1, n. 1, 2001.

BEAL, Adriana. **Segurança da Informação:** Princípios e Melhores Práticas para a Proteção dos Ativos de Informação nas Organizações. São Paulo: Atlas, 2005.

BLOOM, Allan. **O declínio da cultura ocidental: da crise da universidade à crise da sociedade**. São Paulo: Editora Best Seller, 1989.

BORTOLOTTI, Silvana Ligia Vincenzi. **Resistência à mudança organizacional: medida de avaliação por meio da Teoria da Resposta ao Item**. 291 f. 2010. - Universidade Federal de Santa Catarina, 2010.

BRASIL. **Constituição da República Federativa do Brasil de 1988**, 1988.

_____. **Decreto-Lei Nº 5.452, de 1 de maio de 1943.** Aprova a Consolidação das Leis do Trabalho, 1943.

_____. **Decreto Lei Nº 2.848, de 7 de dezembro de 1940.** Código Penal, 1940.

_____. **Decreto Nº 10.282, de 20 de março de 2020.** Regulamenta a Lei nº 13.979, de 6 de fevereiro de 2020, para definir os serviços públicos e as atividades essenciais, 2020.

_____. **Lei Nº 10.406, de 10 de janeiro de 2002.** Institui o Código Civil, 2002.

_____. **Lei Nº 12.414, de 9 de junho de 2011.** Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito, 2011a.

_____. **Lei Nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências, 2011b.

_____. **Lei Nº 12.965, de 23 de abril de 2014.** Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil, 2014.

_____. **Lei Nº 13.105, de 16 de março de 2015.** Código de Processo Civil, 2015.

_____. **Lei Nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados - LGPD, 2018.

_____. **Lei Nº 5.764, de 16 de dezembro de 1971.** Define a Política Nacional de Cooperativismo, institui o regime jurídico das sociedades cooperativas, e dá outras providências, 1971.

_____. **Lei Nº 8.078, de 11 de setembro de 1990.** Dispõe sobre a proteção do consumidor e dá outras providências, 1990.

_____. **Lei Nº 9.029, de 13 de abril de 1995.** Proíbe a exigência de atestados de gravidez e esterilização, e outras práticas discriminatórias, para efeitos admissionais ou de permanência da relação jurídica de trabalho, e dá outras providências, 1995.

_____. **Recurso Extraordinário 1010606.** Supremo Tribunal Federal, 2021.

BURNS, James MacGregor. **Leadership**. New York: Harper and Row, 1978.

CARDOSO, Ciro Flamarion. Sociedade e cultura: comparação e confronto. **Estudos Ibero-Americanos - PUCRS**, vol. 29, n. 2, p. 23–29, 2003.

CARLTON, Melissa; LEVY, Yair; RAMIM, Michelle. Mitigating cyber attacks through the measurement of non-IT professionals' cybersecurity skills. **Information and Computer Security**, [*s. l.*], vol. 27, n. 1, p. 101–121, 2019. Disponível em: https://doi.org/10.1108/ICS-11-2016-0088

CASTELLS, Manuel. **A sociedade em rede**. 8. ed. São Paulo: Paz e Terra, 2000.

CASTELLS, Manuel; CARDOSO, Gustavo. **A Sociedade em Rede:** do Conhecimento à Acção Política. Lisboa: Imprensa Nacional - Casa da Moeda, 2006.

CATALA, Pierre. Ébauche d'une théorie juridique de l'information. **Informatica e diritto**, vol. 9, n. 1, p. 15–31, 1983.

CAVOUKIAN, Ann. **Privacy by Design:** The 7 Foundational Principles. Toronto: Information and Privacy Commissioner, 2010.

CAVOUKIAN, Ann; JONAS, Jeff. **Privacy by Design in the Age of Big Data**. Toronto: Information and Privacy Commissioner, 2012. Disponível em: https://jeffjonas.typepad.com/Privacy-by-Design-in-the-Era-of-Big-Data.pdf

CNN. **Mega vazamento de dados pode ter mais de uma origem; investigação continua,** 2021. Disponível em: https://www.cnnbrasil.com.br/business/2021/01/29/mega-vazamento-de-dados-pode-ter-mais-de-uma-origem-investigacao-continua. Acesso em: 22 Abr. 2021.

CONTEH, Nabie Y; SCHMICK, Paul J. Cybersecurity: risks , vulnerabilities and countermeasures to prevent social engineering attacks. **International Journal of Advanced Computer Research**, vol. 6, n. 23, p. 31–38, 2016. Disponível em: https://doi.org/10.19101/IJACR.2016.623006

COSTA, M. B. F. T. **Técnica derivada da Teoria de Resposta ao Item (TRI) aplicada ao setor de serviços**. Universidade Federal do Paraná, 2001.

CROZATTI, Jaime. Modelo de gestão e cultura organizacional : conceitos e interações. **Caderno de Estudos - FIPECAFI**, vol. 10, n. 18, p. 01–20, 1998. Disponível em: https://doi.org/10.1590/s1413-92511998000200004

CRUZ, Roberto Moraes; ALCHIERI, João Carlos. **Avaliação psicológica: Conceito, métodos e instrumentos**. São Paulo: Casa do Psicólogo, 2003.

D'ARCY, John; HOVAV, Anat; GALLETTA, Dennis. User Awareness of Security Countermeasures and Its Impact on Information Systems Misuse: A Deterrence Approach. **Information Systems Research**, vol. 20, n. 1, 2009. Disponível em: https://doi.org/10.1287/isre.1070.0160

DAHBUR, Kamal; BASHABSHEH, Ziad; BASHABSHEH, Deema. Assessment of Security Awareness : a Qualitative and Quantitative Study. **International Management Review**, vol. 13, n. 1, p. 2017, 2017.

DAS, Jishnu; HAMMER, Jeffrey. Which doctor? Combining vignettes and item response to measure clinical competence. **Journal of Development Economics**, vol. 78, p. 348–383, 2005.

DE AYALA, Rafael Jaime. **The theory and practice of Item Response Theory**. New York: The Guilford Press - New York Wiley, 2009.

DEAL, Terrence E.; KENNEDY, Allan .A. **Corporate Cultures: The Rites and Rituals of Corporate Life**. Reading: Addison Wesley Publishing Company, 1982.

DESHPANDE, Rohit; WEBSTER JR., Frederick E. Organizational Culture and Marketing : defining the research agenda. **Journal of Marketing**, vol. 53, n. 1, p. 3–15, 1989.

DHILLON, Gurpreet. **Managing Information System Security**. London: MacMillan Press, 1997.

DONDA, Daniel. **Guia Prático de Implementação da LGPD**. São Paulo: Labrador, 2020.

DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, vol. 12, n. 2, p. 91–108, 2011. Disponível em: http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315

_____. Considerações iniciais sobre os bancos de dados informatizados e o direito à privacidade. *Em*: Gustavo Tepedino (ed.). **Temas de Direito Civil**. Rio de Janeiro: Renovar, 2000. p. 37–54.

_____. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006.

_____. **Privacidade e Proteção de Dados Pessoais**: Ministério da Transparência, Fiscalização e Controladoria-Geral da União, 2017.

EMBRETSON, Susan E.; REISE, Steven Paul. **Item Response Theory for psychologists**. New Jersey: Lawrence Erlbaum Associates, 2000.

ESPER, Aulina Judith Folle; CUNHA, Cristiano José Castro de Almeida. Liderança autêntica: uma revisão integrativa. **Navus - Revista de Gestão e Tecnologia**, vol. 5, n. 2, p. 60–72, 2015. Disponível em: https://doi.org/10.22279/navus.2015.v5n2.p60-72.254

ESTADOS UNIDOS DA AMÉRICA. **Corte de Apelação do Quarto Distrito do Estado da Califórnia.** Apelante Gabrielle Darley Melvin e Apelada Dorothy Davenport Reid. Relator John Bernard Marks, 1931.

EUROPEAN UNION. **Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016**: on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016.

FARDINI, Giulianna. **Fundamentos do cooperativismo**. Brasília: SESCOOP, 2017.

FERNANDES, Karina Ribeiro; ZANELLI, José Carlos. O processo de construção e reconstrução das identidades dos indivíduos nas organizações. **Revista de Administração Contemporânea**, vol. 10, n. 1, p. 55–72, 2006. Disponível em: https://doi.org/10.1590/s1415-65552006000100004

FLEURY, Maria Tereza Leme. Estórias, mitos, heróis - cultura organizacional e relações do trabalho. **Revista da Administração de Empresas**, vol. 27, n. 4, p. 7–18, 1987.

FRANCA, Rafael Penna; FARIAS, Rodrigo Vieira. A Tutela Material e Processual da Privacidade no Meio Ambiente Digital. **R. Emerj**, vol. 19, n. 4, p. 291–311, 2017.

FRANTZ, Walter. **Associativismo, cooperativismo e economia solidária**. Ijuí: Unijuí, 2012.

G.OUCHI, William. Organizational paradigms: A commentary on Japanese management and theory Z organizations. **Organizational Dynamics**, vol. 9, n. 4, p. 36–43, 1981.

G1. **Megavazamento de dados de 223 milhões de brasileiros:** o que se sabe e o que falta saber, 2021. Disponível em: https://g1.globo.com/economia/tecnologia/noticia/2021/01/28/vazamento-de-dados-de-223-milhoes-de-brasileiros-o-que-se-sabe-e-o-que-falta-saber.ghtml. Acesso em: 22 Abr. 2021.

GALEGALE, Napoleão Verardi; FONTES, Edison Luiz Gonçalves; GALEGALE, Bernardo Perri. Uma contribuição para a segurança da informação : um estudo de casos múltiplos com organizações brasileiras. **Perspectivas em Ciências da Informação**, vol. 22, n. 3, p. 75–97, 2017. Disponível em: https://doi.org/10.1590/1981-5344/

GARCIA, Lara Rocha; AGUILERA-FERNANDES, Edson; GONÇALVES, Rafael Augusto Moreno; PEREIRA-BARRETO, Marcos Ribeiro. **Lei Geral de Proteção de Dados Pessoais (LGPD):** guia da implementação. São Paulo: Blucher, 2020.

GIL, Antonio Carlos. **Como Elaborar Projetos de Pesquisa**. 6. ed. São Paulo: Atlas, 2018.

GOMES, Giancarlo; TORRENS, Edson Wilson; SCHONS, Manuir; SORGETZ, Bárbarah. Cultura Organizacional e Inovação : uma perspectiva a partir do modelo de Schein. **Revista de Administração da Unimep**, vol. 15, n. 1, p. 51–72, 2017. Disponível em: https://doi.org/10.15600/rau.v15i1.965

GOMES, Rodrigo Dias de Pinho. Considerações sobre a figura do encarregado pelo trarament de dados pessoais na Lei Geral de Proteção de Dados. **OAB Norte a Sul**, vol. 1, 2020.

HAMBLETON, Ronald K. Emergence of Item Response Modeling in instrument development and data analysis. **Medical Care**, [*s. l.*], vol. 38, n. 9, p. 60–65, 2000.

HAMBLETON, Ronald K.; SWAMINATHAN, Hariharan. **Item response theory: Principles and applications**. Hingham: MA: Kluwer, Nijhoff, 1984.

HATFIELD, Joseph M. Social engineering in cybersecurity : the evolution of a concept. **Computers and Security**, vol. 73, p. 102–113, 2018. Disponível em: https://doi.org/10.1016/j.cose.2017.10.008

HERSEY, Paul; BLANCHARD, Kenneth H.; NATEMEYER, Walter E. Situational leadership, perception, and the impact of power. **Group & Organization Studies**, vol. 4, n. 4, p. 418–428, 1979.

HOFSTEDE, Geert; HOFSTEDE, Gert Jan; MINKOV, Michael. **Culture and Organizations**. New York: McGraw-Hill, 2010.

HUBMANN, Heinrich. **Das Persönlichkeitsrecht**. 2. ed. Köln: Böhlau, 1967.

IBGC. **Guia das Melhores Práticas de Governança para Cooperativas**. São Paulo: Instituto Brasileiro de Governança Corporativa, 2015.

ICA. **Exploring the Cooperative Economy**. World Cooperative Monitor, 2020.

ICA. **International Cooperative Alliance**, 2021. Disponível em: https://www.ica.coop/en. Acesso em: 10 Fev. 2021.

INSTITUTE OF BUSINESS EDUCATION. **Magavazamento de dados: o que se sabe e o que falta saber**. IBE, 2021. Disponível em: https://ibe.edu.br/megavazamento-de-dados-o-que-se-sabe-e-o-que-falta-saber/. Acesso em: 22 Abr. 2021.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. **ISO/IEC 27000:** Information technology — Security techniques — Information security management systems — Overview and vocabulary. Genebra: ISO, 2014.

IRANI, Danesh; BALDUZZI, Marco; BALZAROTTI, Davide; KIRDA, Engin; PU, Calton. Reverse Social Engineering Attacks in Online Social Networks. *Em*: HOLZ, Thorsten (ed.). **Detection of Intrusions and Malware, and Vulnerability Assessment**. Amsterdam: Springer, 2005.

JOHNSON, R. Burke; ONWUEGBUZIE, Anthony J.; TURNER, Lisa A. Toward a Definition of Mixed Methods Research. **Journal of mixed methods research**, vol. 1, n. 2, p. 112–133, 2007.

JURAN, Joseph M.; GODFREY, A. Blanton. **Juran's Quality Handbook**. 5. ed. New York: McGraw-Hill, 1998.

KASPERSKY. **Cybermap**, 2021. Disponível em: https://cybermap.kaspersky.com/pt . Acesso em: 22 Abr. 2021.

KASPERSKY. **Kaspersky Security Bulletin 2020. Statistics**, 2020. Disponível em: https://securelist.com/kaspersky-security-bulletin-2020-statistics/99804/

KEMPER, Grayson. Improving employees ' cyber security awareness. **Computer Fraud e Security Bulletin**, vol. 2019, n. 8, p. 11–14, 2019. Disponível em: https://doi.org/10.1016/S1361-3723(19)30085-5

KISS, Attila; SZŐKE, Gergely László. Evolution or Revolution? Steps Forward to a New Generation of Data Protection. *Em*: GUTWIRTH, Serge; LEENES, Ronald; HERT, Paul de (eds.). **Reforming European Data Protection Law**. Pécs: Springer Science, 2015. p. 311–331. Disponível em: https://doi.org/10.1093/idpl/ipq003.

KLETTENBERG, Josiane. **SEGURANÇA DA INFORMAÇÃO : Um estudo sobre o uso da engenharia social para obter informações sigilosas de usuários de Instituições Bancárias**. Dissertação (Mestrado em Ciências da Informação). 2016. - Universidade Federal de Santa Catarina - UFSC, 2016.

KOSTIC, Linda C. **Information Security Awareness Techniques That Reduce Data Breaches Causaed By Social Engineering Attacks**, 2020.

LAMBOY, Chtistian Karls de. Proteção de Dados uma introdução geral. *Em*: LEITE, Luciano

Vasconcelos; LAMBOY, Christian Karl de; ANDRADE, Marcelo Henrique Lapolla Aguiar (eds.). **Manual de Implementação da Lei Geral de Proteção de Dados**. São Paulo: Via Ética, 2019.

LANZANA, Ana Paula. **Relação entre disclosure e governança corporativa das empresas brasileiras**. Dissertação (Mestrado em Administração). 165 f. 2004. - Universidade de São Paulo - USP, 2004.

LARAIA, Roque de Barros. **Cultura : um conceito antropológico**. 14. ed. Rio de Janeiro: Jorge Zahar Editor, 2001. Disponível em: https://doi.org/10.31496/rpd.v1i2.36

LEITE, Luciano Vasconcelos; MACHADO, Gabriela de Ávila. Introdução na Lei Geral de Proteção de Dados no Brasil. *Em*: LEITE, Luciano Vasconcelos; LAMBOY, Christian Karl de; ANDRADE, Marcelo Henrique Lapolla Aguiar (eds.). **Manual de implementação da Lei Geral de Proteção de Dados**. São Paulo: Via Ética, 2019.

LIN, Ting Hsiang; YAO, Grace. Evaluating Item Discrimination Power of WHOQOLBREF from an Item Response Model Perspectives. **Soc. Indic. Res**, vol. 91, p. 141–153, 2009.

LINKEDIN. **Assumido, com orgulho**. Proud At Work, 2019. Disponível em: https://business.linkedin.com/content/dam/me/business/pt-br/talent-solutions-lodestone/body/pdf/ProudAtWork_eBook_VF_LinkedIn.pdf

LOPES, Lucas Guglielmelli; LOPES, Matheus Guglielmelli. Direito ao Esquecimento. **Jornal Eletrônico Faculdades INtegradas Vianna Júnior**, vol. 7, n. 1, p. 94–104, 2015.

LYRA, Maurício Rocha. **Segurança e Auditoria em Sistemas de Informação**. Rio de Janeiro: Ciência Moderna, 2008.

MACHADO, Joana de Moraes Souza. A expansão do conceito de privacidade e a evolução na tecnologia de informação com o surgimento dos bancos de dados. **Revista da AJURIS**, vol. 41, n. 134, 2014. Disponível em: http://www.ajuris.org.br/OJS2/index.php/REVAJURIS/article/view/206

MAÑAS, José Luis Piñar. El derecho fundamental a la protección de datos personales. Algunos retos de presente y futuro. **Revista Parlamentaria de la Asamblea de Madrid**, vol. 13, n. 1, p. 21–46, 2005. Disponível em: https://doi.org/10.2307/j.ctv14t46sm.8

MARCIANO, Luiz Pereira. **Segurança da Informação:** uma abordagem social. Tese (Doutorado em Ciência da Informação) 212 f. - Unviersidade de Brasília, 2006. Disponível em: http://repositorio.unb.br/handle/10482/1943

MARCONI, Marina de Andrade; LAKATOS, Eva Maria. **Fundamentos de Metodologia Científica**. 8. ed. São Paulo: Atlas, 2017.

MASCARENHAS, André Ofenhejm. Etnografia e cultura organizacional : uma contribuição da antropologia à administração de empresas. **Revista de Administração de Empresas**, vol. 42, n. 2, p. 88–94, 2002. Disponível em: https://doi.org/10.1590/s0034-75902002000200008

MATOS, José Claudio; MURIEL TORRADO, Enrique; JACINTHO, Eliana Maria Bahia. Literatura distópica e sociedade da informação : uma análise das menções ao romance 1984 de George Orwell no livro Modernidade Líquida de Bauman. **Revista Ibero-americana de Ciência da Informaçao**, vol. 14, n. 1, p. 194–214, 2021. Disponível em: https://doi.org/10.26512/rici.v14.n1.2021.31534

MAYER-SCHÖNBERGER, Viktor. General development of data protection in Europe. *Em*: AGRE, Phillip; MARC, Rotenberg (eds.). **New, Technology and privacy : The Landscape**. Cambridge: MIT Press, 1997.

MEINEN, Ênio; PORT, Márcio. **Cooperativismo financeiro: p**ercurso histórico, perspectivas e desafios. Brasília: Confebras, 2014.

MELLENBERGH, Gideon J. Generalized linear item response theory. **Psychol Bull Journal**, vol. 115, n. 2, p. 300–307, 1994.

METALIDOU, Efthymia; MARINAGI, Catherine; TRIVELLAS, Panagiotis; EBERHAGEN, Niclas; SKOURLAS, Christos; GIANNAKOPOULOS, Georgios. The Human Factor of Information Security : Unintentional Damage Perspective. **Procedia - Social and Behavioral Sciences**, vol. 147, p. 424–428, 2014. Disponível em: https://doi.org/10.1016/j.sbspro.2014.07.133

MINTZ, Sidney W. Culture : an anthropological view. **The Yale Review**, vol. 17, n. 4, p. 499–512, 1982.

MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. **Revista dos Tribunais**, vol. 1009, p. 1–35, 2019.

MONTEIRO, Renato Leite. **Existe um direito à explicação na Lei Geral de Proteção de Dados do Brasil?** Instituto Igarapé, 2018.

MONTI, Andrea; WACKS, Raymond. **Protecting Personal Information:** The Right to Privacy Reconsidered. Oxford: Hart Publishing, 2019.

NETTO, Abner da Silva; SILVEIRA, Marco Antonio Pinheiro da. Gestão da Seguranã da Informação: fatores que influenciam sua adoção em pequenas e médias empresas. **Revista de Gestão da Tecnologia e Sistemas de Informação**, vol. 4, n. 3, p. 375–397, 2007. Disponível em: https://doi.org/10.1590/S1807-17752007000300007

NICHOL, Kelly. **Implementing a Security Awareness Training Program in Your Environment for Every Day Computer Users**. SANS Institute, 2000.

NONAKA, Ikujiro. A Empresa Criadora de Conhecimento. **Harvard Business Review**, 2007.

NOSWORTHY, Julie D. Implementing Information Security in the 21st Century — Do You Have the Balancing Factors? **Computers and Security**, vol. 19, n. 4, p. 337–347, 2000.

O GLOBO. **Sabe como proteger seus dados pessoais? Confira as orientações para reduzir riscos**, 2021. Disponível em: https://oglobo.globo.com/economia/defesa-do-

consumidor/sabe-como-proteger-seus-dados-pessoais-confira-as-orientacoes-para-reduzir-riscos-24923351. Acesso em: 22 Abr. 2021.

OCB. **Anuário do Cooperativismo Brasileiro.** OCB, 2019.

_____. **Anuário do Cooperativismo Brasileiro**. OCB, 2020.

_____. **Manual de Boas Práticas de Governança Cooperativa**: OCB, 2016.

OECD. **OECD Guidelines for the Security of Information Systems and Networks:** towards a culture of security. Paris: Organisation for Economic Co-operation and Development, 2002. Disponível em: https://doi.org/10.1787/9789264059177-en-fr

OGBONNA, Emmanuel; HARRIS, Lloyd C. Leadership style, organizational culture and performance: Empirical evidence from UK companies. **International Journal of Human Resource Management**, vol. 11, n. 4, p. 766–788, 2000. Disponível em: https://doi.org/10.1080/09585190050075114

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**, 1948.

ORGANIZAÇÃO INTERNACIONAL DO TRABALHO. **Cooperativas**, 2020. Disponível em: https://www.ilo.org/lisbon/temas/WCMS_650798/lang--pt/index.htm. Acesso em: 22 Ago. 2020.

ORWELL, George. **1984**. Jandira: Principis, 2021.

OSTROFF, Cheri; KINICKI, Angelo J.; MUHAMMAD, Rabiah S. Organizational Culture and Climate. *Em*: WEINER, Irving B. (ed.). **Handbook of Psychology**. Hoboken: John Wiley e Sons, 2013. Disponível em: https://doi.org/10.1093/oxfordhb/9780199928309.013.0020

PARSONS, Kathryn Marie; YOUNG, Elise; BUTAVICIUS, Marcus Antanas; MCCORMAC, Agata; PATTINSON, Malcolm Robert; JERRAM, Cate. **Human Factors and Information Security:** Individual, Culture and Security Environment. Edinburgh: Defence Science and Technology Organisation, 2010.

PARSONS, Kathryn; MCCORMAC, Agata; BUTAVICIUS, Marcus; FERGUSON, Lael. The influence of organizational information security culture on information security decision making. **Journal of Cognitive Engineering and Decision Making**, vol. 9, n. 2, p. 117–129, 2015. Disponível em: https://doi.org/10.1177/1555343415575152

PASQUALI, Luiz. **Psicometria: Teoria e Aplicações**. Brasília: UnB, 1997.

_____. Psicometria Psicometría Psychometrics. **Revista da Escola de Enfermagem da USP**, vol. 43, p. 992, 2009.

PEDRAZA-ÁLVAREZ, Lilibeth; OBISPO-SALAZAR, Kelly; VÁSQUEZ-GONZÁLEZ, Lina; GÓMEZ-GÓMEZ, Leonardo. Cultura organizacional desde la teoría de Edgar Schein : estudio fenomenológico. **Clío América**, vol. 9, n. 17, p. 17–25, 2015. Disponível em:

https://doi.org/10.21676/23897848.1462

PETERS, Thomas J.; WATERMAN, Robert H. **In Search of Excellence: In Search of Excellence: Lessons from America's Best-Run Companies.** New York: Harper & Row, 1982.

PINHEIRO, Patricia Peck. **Proteção de Dados Pessoais:** Comentários à Lei N. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

POSSOLLI, Gabriela Eyng. **Gestão da inovação e do conhecimento**. Curitiba: InterSaberes, 2012.

PROOFPOINT. **Human Factor Report**: Proofpoint, 2019.

PROVDANOV, Cleber Cristiano; FREITAS, Ernani Cesar De. **Metodologia do trabalho científico:** métodos e técnicas da pesquisa e do trabalho acadêmico. Novo Hamburgo: Freevale, 2013. ISSN 1098-6596. Disponível em: https://doi.org/10.1017/CBO9781107415324.004

PSAFE. **Vazamento em massa expõe número de CPF de milhões de brasileiros, alerta PSafe**. 2021. Disponível em: https://www.psafe.com/blog/vazamento-expoe-numero-de-cpf-de-milhoes-de-brasileiros-alerta-psafe/. Acesso em: 22 Abr. 2021.

RAPOSO, Ruben José de Almeida Martins. Modelos operativos da cultura organizacional. **Lusíadas. Economia e Empresa**, vol. 28, 2020. Disponível em: https://doi.org/doi.org/10.34628/79mc-wn49

RODOTÁ, Stefano. **A vida na sociedade da vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROGERS, David L. **Transformação Digital:** Repensando o seu negócio para a era digital. 1. ed. São Paulo: Autêntica Business, 2019.

ROOS, Yosikazu de; ALLEN-MEARES, Paula. Aplication of Rasch analysis: Exploring differences in depression between African-American and White children. **Journal of Social Service Research**, vol. 23, n. 3/4, p. 93–107, 1998.

RUSSELL, Chelsa. **Security Awareness:** Implementing an Effective Strategy: SANS Institute, 2002.

SAMEJIMA, Fumiko. Estimation of latent ability using a response pattern of graded scores. **Psychometrika**, vol. 17, 1969.

SANTOS, José Luiz dos. **O que é cultura**. 16. ed. São Paulo: Brasiliense, 2006.

SCHEIN, Edgar H. Coming to a New Awareness of Organizational Culture. **Sloan Management Review**, vol. 25, n. 2, p. 3–16, 1984.

_____. **Organizational Culture and Leadership**. 3. ed. San Francisco: Jossey-Bass, 2004.

SCHELL, Roger R. Information Security: Science, Pseudoscience, and Flying Pigs. **Conference, Seventeenth Annual Computer Security Applications**. New Orleans: IEEE, 2001. p. 205–216. Disponível em: https://doi.org/10.1109/ACSAC.2001.991537

SCHNEIER, Bruce. **Secrets and lies:** digital security in a networked world. New York: John Wiley e Sons, 2004.

SCHULTZ, Eugene. The human factor in security. **Computers and Security**, vol. 24, p. 425–426, 2005. Disponível em: https://doi.org/10.1016/j.cose.2005.07.002

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva**. 2. ed. Rio de Janeiro: Elsevier, 2014.

SHUT UP AND DANCE (TEMPORADA 3, EP. 3). BLACK MIRROR (SERIADO). Director: James Watkins. Reino Unido: Endemol UK - Netflix, 2016.

SILVA JÚNIOR, Severino Domingos da; COSTA, Francisco José. Mensuração e Escalas de Verificação: uma Análise Comparativa das Escalas de Likert e Phrase Completion. *Em*: , 2014. **XVII Semead**. [*S. l.: s. n.*], 2014.

SINGH, J. Tackling measurement problems with Item Response Theory: principles, characteristics, and assessment, with an illustrative example. **Journal of Business Research**, vol. 57, p. 184–208, 2004.

SMIRCICH, Linda. Concepts of culture and organizational analysis. **Administrative Science Quarterly**, vol. 28, n. 3, p. 339–358, 1983. Disponível em: https://doi.org/10.4324/9781315241371-20

SOARES, Marden Marques; MELO SOBRINHO, Abelardo Duarte de. **Microfinanças:** O Papel do Banco Central do Brasil e a Importância do Cooperativismo de Crédito. Brasília: Biblioteca do Banco Central do Brasil, 2015.

SOLMS, Basie von. Information Security - the four wave. **Computers and Security**, vol. 25, p. 165–168, 2006.

SOLMS, Rossouw Von; SOLMS, Basie Von. From policies to culture. **Computers and Security**, vol. 23, p. 275–279, 2004. Disponível em: https://doi.org/10.1016/j.cose.2004.01.013

SOUZA, Alzira Silva de. **Cooperativismo:** uma alternativa econômica. Rio de Janeiro: CECRERJ, 1990.

SOUZA, Roberto de; ABIKO, Alex. **Metodologia para Desenvolvimento e Implantação de Sistemas de Gestão da Qualidade em Empresas Construtoras de Pequeno e Médio Porte**. São Paulo: EPUSPI, 1997.

SOUZA, Paulo Roberto de Barros. **Análise do atual estágio de disclosure das companhias abertas no mercado de capitais brasileiro e contribuições para o seu aprimoramento**. 1995. - Faculdade de Economia, Administração e Contabilidade da Universidade de São

Paulo, 1995.

STRAUSS, Anselm; CORBIN, Juliet. **Pesquisa Qualitativa:** técnicas e procedimentos para o desenvolvimento de teoria fundamentada. Porto Alegre: Artmed, 2008.

TAVARES, H. R.; ANDRADE, D. F.; PEREIRA, C. A. Detection of determinant genes and diagnostic via item response theory. **Genetics and Molecular Biology**, vol. 27, n. 4, p. 679–685, 2004.

TEFFÉ, Chiara Spadaccini de; BARLETTA, Fabiana Rodrigues. O Direito ao esquecimento : uma expressão possível do direito à privacidade. **Revista Direito do Consumidor**, vol. 105, 2016.

TEZZA, Rafael; BORNIA, Antonio Cezar; ANDRADE, Dalton Francisco de. Measuring web usability using item response theory: Principles, features and opportunities. Interacting with Computers. **Interacting with Computers**, vol. 23, p. 167–175, 2011.

THE IMITATION GAME. Director: Morten Tyldum. Reino Unido: The Weinstein Company, 2014.

THIOLLENT, Michel. **Metodologia da pesquisa-ação**. São Paulo: Cortez, 1986.

TORRES, Fábio Cabral. Conceitos e Princípios da Segurança da Informação. *Em*: LYRA, Maurício Rocha (ed.). **Governança da segurança da informação**. Brasília: Edição do autor, 2015. p. 161.

TRIERWEILLER, Andréa Cristina; PEIXE, Blênio César Severo; BORNIA, Antonio Cezar TEZZA, Rafael; PEREIRA, Vera Lúcia Duarte do Valle; PACHECO Junior, Waldemar. Avaliação da Efetividade Organizacional com o Uso da Teoria de Reposta ao Item: Estudo no Setor de Tecnologia da Informação e Comunicação, 2011, Rio de Janeiro. **XXXV Encontro da ANPAD**. Rio de Janeiro: 2011. p. 1–17.

TYLOR, Edward Burnett. **Primitive Culture:** researches into the development of mythology, philosophy, religion language, art and custom. London: John Murray, 1871.

UFSC. **Campus Araranguá**, 2020. Disponível em: https://ararangua.ufsc.br/. Acesso em: 16 Set. 2020.

_____. **Repositório Institucional**, 2021. Disponível em: https://repositorio.ufsc.br/. Acesso em: 15 Jun. 2021.

VEIGA, Adele; ELOFF, Jan H. P. A framework and assessment instrument for information security culture. **Computers and Security**, vol. 29, n. 2, p. 196–207, 2010. Disponível em: https://doi.org/10.1016/j.cose.2009.09.002

VERBEKE, Willem; VOLGERING, Marco; HESSELS, Marco. Exploring the Conceptual Expansion Within the Field of. **Journal of Management Studies**, vol. 35, n. 3, p. 303–329, 1998.

VIDOTTO, Giulio; BERTOLOTTI, Giorgio; CARONE, Mauro; ARPINELLI, Fabio BELLIA, Vincenzo; JONES, Paul Wyatt; DONNER, Claudio Ferdinando. A new questionnaire specifically designed for patients affected by chronic obstructive pulmonary disease: The Italian Health Status Questionnaire. **Respiratory Medicine**, vol. 100, n. 5, p. 862–870, 2006.

VIEIRA, Ubiratan Negrão; PEREIRA, Bruno Gomes. Cultura brasileira e cultura organizacional : uma relação existente. **Revista São Luís Orione**, vol. 1, n. 15, p. 84–94, 2020.

VON SOLMS, Basie. Information security -The third wave? **Computers Security**, vol. 19, n. 7, p. 615–620, 2000. Disponível em: https://doi.org/10.1016/S0167-4048(00)07021-8

VOSS, Brian. **The Ultimate Defense of Depth:** Security Awareness in Your Company.: SANS Institute, 2001.

VROOM, Cheryl; SOLMS, Rossouw von. Towards information security behavioural compliance. **Computers and Security**, vol. 23, p. 191–198, 2004.

WARREN, Samuel; BRANDEIS, Loius D. The Right to Privacy. **Harvard Law Review**, vol. 4, n. 5, p. 193–220, 1890.

WE ARE SOCIAL. **DIGITAL 2020 : Global Digital Overview**: Hootsuite, 2021. Disponível em: https://wearesocial.com/digital-2020

WERSIG, Gernot; NEVELING, Ulrich. The phenomena of interest to Information Science. **Information Science**, vol. 9, n. 4, p. 127–140, 1975.

WERTHEIN, Jorge. A sociedade da informação e seus desafios. **Ciência da Informação**, vol. 29, n. 2, p. 71–77, 2000.

WHITE BEAR (TEMPORADA 2, EP. 2). BLACK MIRROR (SERIADO). Director: Carl Tibbetts. Reino Unido: Endemo UK - Netflix, 2013.

WHITMAN, Michael E.; MATTORD, Herbert J. **Principles of Information Security Fourth Edition**. 4. ed. Boston: Cengage Learning, 2011.

WU, I. Model Management system for IRT: based test construction decision support system. **Decision Support Systems**, vol. 27, p. 443–458, 1999.

ZANINI, Leonardo Estevam de Assis. A Proteção dos Direitos da Personalidade na Alemanha. **Revista Jurídica Luso-Brasileira**, vol. 6, n. 2, p. 731–759, 2020.

# APÊNDICE A – O instrumento de Araujo (2018) e suas adaptações

**Legenda:**

- Título da diretriz
- Título dos itens da diretriz
- Item da diretriz
- Original no instrument de Araújo (2018) que sofreu alteração
- Alteração realizada no instrumento de Araújo (2018)
- Original no instrument de Araújo (2018) que não sofreu alteração
- Nota explicativa da alteração
- Indicação à referência da alteração

| Diretriz | Consciência | | | | | | |
|---|---|---|---|---|---|---|---|
| Definição | As partes interessadas devem estar cientes da necessidade de garantir a segurança dos sistemas de informação e de redes e do que elas podem fazer para melhorar a segurança. | | | | | | |
| Descrição | - Os participantes devem entender que as falhas na segurança podem prejudicar significativamente os sistemas e redes sob seu controle, bem como os dos outros.<br>- Os participantes devem, também, ter conhecimento da configuração e das atualizações disponíveis para seus sistemas, do lugar que ocupam nas redes e das boas práticas que possam implementar para melhorar a segurança.<br>- Os participantes devem considerar as necessidades dos outros participantes. | | | | | | |
| | Os participantes devem:<br>- Entender que as falhas na segurança podem prejudicar significativamente os sistemas e redes sob seu controle, bem como os sistemas e redes de outras pessoas;<br>- Ter conhecimento da configuração e das atualizações disponíveis para seus sistemas, do lugar que ocupam nas redes e das boas práticas que possam implementar para melhorar a segurança;<br>- Considerar as necessidades dos outros participantes. | | | | | | |
| Código | Item | Categorias | | | | | |
| Csc_01_0 | Os "*malwares*" são programas que causam danos aos sistemas computadorizados, como destruição e/ou roubo de dados. | Nunca | Raramente | Frequentemente | Sempre | N.A. | |
| Csc_01_1 | Com que frequência você verifica se o antivírus está atualizado? | 0 | 1 | 2 | 3 | 9 | |
| Csc_01_2 | Com que frequência você verifica o histórico (relatório) do antivírus? | 0 | 1 | 2 | 3 | 9 | |
| Csc_02_0 | O patrimônio de uma organização é o conjunto de seus bens e direitos. Em sua opinião: | Não | | | Sim | | |
| Csc_02_1 | As informações da organização têm valor financeiro? | 0 | | | 1 | | |
| Csc_02_2 | As informações integram o patrimônio da organização | 0 | | | 1 | | |
| Csc_02_3 | As informações da sua organização necessitam de segurança? | 0 | | | 1 | | |
| Csc_03_0 | Em sua opinião, qual seria o impacto na sua organização caso ocorressem os incidentes a seguir? | Nenhum | Leve (não afeta a credibilidade) | | Severa (afeta a credibilidade) | | |
| Csc_03_1 | A perda dos dados e informações. | 0 | 1 | | 2 | | |
| Csc_03_2 | Acesso indevido aos dados e informações. | 0 | 1 | | 2 | | |
| Csc_03_3 | Adulteração dos dados. | 0 | 1 | | 2 | | |
| Csc_03_4 | Divulgação não autorizada das informações | 0 | 1 | | 2 | | |
| Csc_03_5 | Interrupção ou indisponibilidade dos serviços (*internet*, acessos remotos, banco de dados, etc) | 0 | 1 | | 2 | | |
| Csc_03_6 | Quebra do sigilo da informação. | 0 | 1 | | 2 | | |
| Csc_03_7 | Furto dos dados e informações. | 0 | 1 | | 2 | | |
| Csc_04_0 | Sobre o sistema operacional do seu computador que utiliza para trabalhar, você: | Não | Sim | | N.A. | | |

Redigido para deixar a leitura mais fácil e objetiva.

Retirado para que o respondente se posicione.

Alterado a ordem para manutenção da mesma lógica sequencial.

Inclusão da nota explicativa entre parênteses na descrição da categoria.

Alterado a ordem para manutenção da mesma lógica sequencial.

Retirado para que o respondente se posicione.

| | | | | |
|---|---|---|---|---|
| | Sobre o sistema operacional do equipamento que utiliza para trabalhar, você: | | | |
| Csc_04_1 | **Sabe qual é o sistema operacional do seu equipamento?** | 0 | 1 | 9 |
| | Sabe qual é o sistema operacional? | | | |
| Csc_04_2 | **Sabe qual a versão do sistema operacional do seu computador?** | 0 | 1 | 9 |
| | Sabe qual é a versão do sistema operacional? | | | |
| Csc_04_3 | Sabe se o seu sistema operacional está atualizado? | 0 | 1 | 9 |
| Csc_05_0 | Sobre o equipamento que utiliza, você: | Não | Sim | N.A. |
| | Sobre o equipamento que utiliza para trabalhar, você: | | | |
| Csc_05_1 | Sabe qual é o tipo de processador (marca, modelo, etc) ? | 0 | 1 | 9 |
| | Sabe qual é o seu processador? | | | |
| Csc_05_2 | Sabe qual é a quantidade de memória RAM? | 0 | 1 | 9 |
| Csc_05_3 | Sabe qual a capacidade de armazenamento do disco? | 0 | 1 | 9 |
| Csc_05_4 | Sabe o tipo de conexão do seu computador com a rede? | 0 | 1 | 9 |
| Csc_06_0 | A classificação da informação é uma etapa muito importante para a segurança da informação. Sobre a classificação da informação na sua organização. | Não sei informar | Não implementado | Sim implementado |
| Csc_06_1 | Você sabe se sua organização tem os procedimentos e diretrizes para classificação da informação implementados? | 0 | 1 | 2 |

Adequação à modalidade de trabalho *home officce.*

Retirado para que o respondente se posicione.

Adequação à modalidade de trabalho *home officce.*

Redigido para deixar a leitura mais fácil e objetiva.

Alterado a ordem para manutenção da mesma lógica sequencial.

| Diretriz | Responsabilidade | | |
|---|---|---|---|
| Definição | Todos os participantes são responsáveis pela segurança dos sistemas de informação e de redes | | |
| **Descrição** | - Eles devem compreender a sua responsabilidade pela segurança desses sistemas e redes.<br>- Devem prestar contas, na razão de suas funções individuais.<br>- Os participantes devem, regularmente, rever e avaliar suas próprias políticas, práticas, medidas e procedimentos para se assegurarem que estão adequados ao seu ambiente.<br>- Os participantes devem considerar a segurança dos sistemas e redes e divulgar as informações ade- quadas, incluindo atualizações em tempo hábil | | |
| | Os participantes devem:<br>- Compreender a sua responsabilidade;<br>- Rever e avaliar regularmente suas próprias políticas, práticas, medidas e procedimentos para se assegurarem que estão adequados ao seu ambiente;<br>- Considerar a segurança dos sistemas e redes e divulgar as informações adequadas, incluindo atualizações em tempo hábil. | | |
| Código | Item | Gabarito | Categorias |
| Rsp_01_1 | Em sua opinião, quem é o responsável por garantir a segurança da informação na sua organização? | | |
| Rsp_01_1 | Ninguém. | 0 | 0 |
| | A sua chefia. | 0 | 1 |
| | O setor de segurança da informação | 0 | 2 |
| | Os colaboradores da organização. | 1 | 5 |
| | Os colaboradores que trabalham na manutenção dos dados e informações da organização. | 0 | 3 |
| | Os técnicos de rede. | 0 | 4 |
| Código | Item | Categorias | |

Redigido para deixar a leitura mais fácil e objetiva.

| | | | | | |
|---|---|---|---|---|---|
| Rsp_02_0 | Você soube de um novo tipo de ataque a computadores. Você: | Nunca | Raramente | Frequentemente | Sempre |
| **Rsp_02_1** | **Alerta os colegas de equipe** | **0** | **1** | **2** | **2** |
| **Rsp_02_2** | **Comunica o setor responsável.** | **0** | **1** | **2** | **3** |
| **Rsp_02_3** | **Verifica se o seu computador está vulnerável a esse ataque.** | **0** | **1** | **2** | **3** |
| Rsp_03_0 | Para que a organização seja segura, convém que todas as responsabilidades e as respectivas atribuições sejam definidas. | Não sei informar | Não | Sim | |
| **Rsp_03_1** | Você conhece suas responsabilidades e atribuições relacionadas à segurança da informação? | | **0** | **1** | |
| **Rsp_03_2** | **A sua equipe conhece as suas respectivas responsabilidades e atribuições relacionadas à segurança da informação?** | **0** | **1** | **2** | |

Retirado para que o respondente se posicione.

Alterado a ordem para manutenção da mesma lógica sequencial.

| Diretriz | Resposta (reação) | | | | |
|---|---|---|---|---|---|
| Definição | Os participantes devem agir em tempo hábil e de maneira cooperativa para prevenir, detectar e responder a incidentes de segurança. | | | | |
| **Descrição** | - Os participantes devem reagir prontamente e com um espírito de cooperação aos incidentes de segurança<br>- Devem compartilhar suas informações sobre ameaças e vulnerabilidades<br>- Devem implementar procedimentos para a rápida e efetiva cooperação a fim de prevenir, detectar e responder a incidentes de segurança | | | | |
| | Os participantes devem:<br>- Reagir prontamente e com um espírito de cooperação aos incidentes de segurança;<br>- Compartilhar suas informações sobre ameaças e vulnerabilidades;<br>- Implementar procedimentos para a rápida e efetiva cooperação a fim de prevenir, detectar e responder a incidentes de segurança. | | | | |
| Código | Item | Categorias | | | |
| Rpt_02_0 | Suponha que ocorreu um incidente que afeta a segurança da informação, como vírus, interrupção do serviço, perda de dados, invasão.<br>Qual seria a sua atitude em relação a cada uma das partes envolvidas a seguir? | Não Alertaria | Alertaria dependendo da situação | Alertaria imediatamente | |
| **Rpt_02_1** | **Sua chefia.** | **0** | **1** | **2** | |
| Rpt_02_2 | Os parceiros internos à organição (outros departamentos). | 0 | 1 | 2 | |
| Rpt_02_3 | Os parceiros externos à organização (organizações parceiras). | 0 | 1 | 2 | |
| Rpt_02_4 | O gestor responsável pela segurança da informação. | 0 | 1 | 2 | |
| Rpt_03_0 | Você está no seu local de trabalho e percebe a presença de uma pessoa desconhecida e também que não está utilizando uma identificação.<br>Você: | Não | Raramente | Frequentemente | Sempre | N.A. |
| Rpt_03_1 | Comunica ao setor responsável pela segurança? | 0 | 1 | 2 | 3 | 9 |
| Rpt_03_2 | Solicita que ela se retire? | 0 | 1 | 2 | 3 | 9 |
| Rpt_03_3 | Comunica a sua chefia? | 0 | 1 | 2 | 3 | 9 |
| Rpt_04_0 | Supondo que você encontrou um *Pendrive* no estacionamento nas proximidades da empresa. Você: | Não | | Sim | | |

Redigido para deixar a leitura mais fácil e objetiva.

Alterado a ordem para manutenção da mesma lógica sequencial.

Alterado a ordem para manutenção da mesma lógica sequencial.

| | | | |
|---|---|---|---|
| Rpt_04_1 | Utiliza o dispositivo em seu equipamento para saber o que contém? | 1 | 0 |
| Rpt_04_2 | Pede à equipe de segurança que avalie o dispositivo? | 0 | 1 |

| Diretriz | Ética | | | | | |
|---|---|---|---|---|---|---|
| Definição | Os participantes devem respeitar os interesses legítimos de outros participantes. | | | | | |
| Descrição | - Os participantes devem reconhecer o quanto suas ações ou omissões podem prejudicar os outros.<br>- Devem ter atitudes que promovam comportamentos que reconheçam a necessidade de segurança da informação.<br>- Devem respeitar os interesses legítimos dos outros participantes. | | | | | |
| | Os participantes devem:<br>- Reconhecer o quanto suas ações ou omissões podem prejudicar os outros;<br>- Ter atitudes que promovam comportamentos que reconheçam a necessidade de segurança da informação;<br>- Respeitar os interesses legítimos dos outros participantes. | | | | | |
| Código | Item | Categorias | | | | |
| Etc_01_0 | Com que frequência você trata de assuntos relacionados a sua organização nos seguintes ambientes? | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Etc_01_1 | Dentro de aviões, ônibus, taxi ou elevador. | 3 | 2 | 1 | 0 | 9 |
| Etc_01_2 | Em bares ou restaurantes. | 3 | 2 | 1 | 0 | 9 |
| Etc_01_3 | Em reuniões sociais. | 3 | 2 | 1 | 0 | 9 |
| Etc_01_4 | Na sala de embarque do aeroporto. | 3 | 2 | 1 | 0 | 9 |
| Etc_01_5 | No cafezinho. | 3 | 2 | 1 | 0 | 9 |
| Etc_01_6 | Em redes sociais. (Facebook, Linkedin, WhatsApp, *chat*, ...) | 3 | 2 | 1 | 0 | 9 |
| **Etc_01_7** | **Em cabeleireiros, barbeiros ou salão de beleza.** | **3** | **2** | **1** | **0** | **9** |
| Etc_01_8 | Por telefone fora do ambiente de trabalho. | 3 | 2 | 1 | 0 | 9 |
| Etc_02_0 | Você entra na sala de um colega para tratar de um assunto e verifica que ele está ao telefone. Você: | Nunca | Raramente | Frequentemente | Sempre | |
| **Etc_02_1** | Espera na sala pacientemente enquanto ele está ao telefone? | **3** | **2** | **1** | **0** | |
| | Espera na sala do colega pacientemente enquanto ele está ao telefone? | | | | | |
| **Etc_02_2** | **Retira-se e aguarda o final do telefonema?** | **0** | **1** | **2** | **3** | |
| Etc_03_0 | Suas atividades permitem a você ter acesso a informações confidenciais. Sobre essas informações você costuma: | Nunca | Raramente | Frequentemente | Sempre | |
| Etc_03_1 | Conversar com seus colegas? | 3 | 2 | 1 | 0 | |
| Etc_03_2 | Comenta com sua equipe? | 3 | 2 | 1 | 0 | |
| Etc_03_3 | Conversar com seus amigos mais próximos? | 3 | 2 | 1 | 0 | |
| Etc_03_4 | Conversar com seus familiares? | 3 | 2 | 1 | 0 | |

Redigido para deixar a leitura mais fácil e objetiva.

Retirado para que o respondente se posicione.

Redigido para deixar a leitura mais fácil e objetiva.

| | | | | | |
|---|---|---|---|---|---|
| Etc_04_0 | O seu colega está trabalhando no computador. Você: | Nunca | Raramente | Frequentemente | Sempre |
| | O seu colega está trabalhando no computador. O que você faz? | | | | |
| Etc_04_1 | Verifica o que ele está fazendo? | 3 | 2 | 1 | 0 |
| Etc_04_2 | Desvia o olhar enquanto ele digita a senha? | 0 | 1 | 2 | 3 |
| Etc_05_0 | Com que frequência você costuma: | Nunca | Raramente | Frequentemente | Sempre |
| Etc_05_1 | Emprestar a sua senha para um colega? | 3 | 2 | 1 | 0 |
| Etc_05_2 | Solicitar a senha de um colega? | 3 | 2 | 1 | 0 |
| Etc_05_3 | Participar de conversas informais sobre outros colegas? | 3 | 2 | 1 | 0 |
| Etc_05_4 | Comentar sobre falhas/erros de colegas? | 3 | 2 | 1 | 0 |
| Etc_06_0 | Com que frequência você costuma alertar os seus colegas sobre a necessidade de: | Nunca | Raramente | Frequentemente | Sempre |
| Etc_06_1 | Desligar o computador quando não estiver em uso? | 0 | 1 | 2 | 3 |
| Etc_06_2 | Bloquear o computador quando não estiver em sua estação de trabalho? | 0 | 1 | 2 | 3 |
| Etc_06_3 | Manter a mesa limpa/organizada? | 0 | 1 | 2 | 3 |
| Etc_06_4 | Proteger os documentos de trabalho de acesso não autorizado? | 0 | 1 | 2 | 3 |

Redigido para deixar a leitura mais fácil e objetiva.

| Diretriz | Democracia | | | |
|---|---|---|---|---|
| Definição | A segurança dos sistemas e redes de informação deve ser compatível com os valores essenciais de uma sociedade democrática. | | | |
| **Descrição** | - Os participantes devem respeitar os valores, a liberdade de troca de ideias, pensamentos, o livre fluxo de informações, a confidencialidade da informação e da comunicação, a proteção adequada dos dados pessoais, a abertura e a transparência.<br>- Os participantes devem respeitar e reconhecer a liderança. | | | |
| | Os participantes devem:<br>- Respeitar os valores, a liberdade de troca de ideias, pensamentos, o livre fluxo de informações, a confidencialidade da informação e da comunicação, a proteção adequada dos dados pessoais, a abertura e a transparência;<br>- Respeitar e reconhecer a liderança. | | | |
| Código | Item | Categorias | | |
| Dmc_01_0 | O líder de uma equipe ou organização deve ser capaz de comandar pessoas, atrair seguidores, influenciar e motivar positivamente o comportamento do grupo. | Não | Sim | N.A ou não tenho chefe |
| **Dmc_01_1** | **Na sua opinião, o seu chefe é um líder?** | **0** | **1** | **9** |
| Dmc_01_2 | O seu chefe motiva ou incentiva um comportamento a favor da segurança da informação? | 0 | 1 | 9 |
| **Dmc_01_3** | **Você se sente seguro(a) com a liderança do seu chefe em relação à segurança da informação?** | **0** | **1** | **9** |

Redigido para deixar a leitura mais fácil e objetiva.

Alterado a ordem para manutenção da mesma lógica sequencial.

Mantido apenas o "não tenho chefe" para que o respondente se posicione.

| | | | | | | |
|---|---|---|---|---|---|---|
| Dmc_02_0 | Durante um processo de tomada de decisão que tem como consequência mudanças de hábitos e comportamentos da sua equipe ou grupo de trabalho, o seu chefe: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Dmc_02_1 | Impõe as suas decisões sem ouvir a opinião dos colegas? | 3 | 2 | 1 | 0 | 9 |
| Dmc_02_2 | Estimula os colegas a emitirem opiniões, promove um ambiente participativo? | 0 | 1 | 2 | 3 | 9 |
| Dmc_02_3 | Dá total liberdade aos colegas para decidirem e simplesmente homologa o que foi decidido? | 3 | 2 | 1 | 0 | 9 |
| Dmc_03_0 | Sobre o seu ambiente de trabalho. | Nunca | Raramente | Frequentemente | Sempre | |
| Dmc_03_1 | Você se sente confortável em emitir suas opiniões? | 0 | 1 | 2 | 3 | |
| Dmc_03_2 | Você aceita a opinião dos seus colegas mesmo que elas entrem em conflito com as suas? | 0 | 1 | 2 | 3 | |
| Dmc_03_3 | A sua equipe aceita a divergências de posicionamentos? | 0 | 1 | 2 | 3 | |
| Dmc_04_0 | O setor responsável pelo controle de acesso aos sistemas da organização resolve modificar as regras de criação e a periodicidade das senhas. | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Dmc_04_1 | Você aceita as regras sem questionamentos? | 3 | 2 | 1 | 0 | 9 |
| Dmc_04_2 | A sua equipe aceita as regras sem questionamentos? | 3 | 2 | 1 | 0 | 9 |
| Dmc_05_0 | Quanto a sua percepção da segurança da informação na sua organização: | Não | | Sim | | |
| Dmc_05_1 | Você se sente seguro(a) quanto a proteção dos seus dados pessoais na organização? | 0 | | 1 | | |
| Dmc_05_2 | Você se sente seguro(a) com relação à confidencialidade das informações da organização? | 0 | | 1 | | |
| Dmc_06_0 | Como você avalia a sua organização no seguinte aspecto: | Não existe | Precária | Suficiente | Boa | |
| Dmc_06_1 | Comunicação da chefia? | 0 | 1 | 2 | 3 | |
| Dmc_06_2 | Comunicação entre colegas? | 0 | 1 | 2 | 3 | |
| Dmc_06_3 | Transparência administrativa? | 0 | 1 | 2 | 3 | |

Mantido apenas o "não tenho chefe" para que o respondente se posicione.

Alterado a ordem para manutenção da mesma lógica sequencial.

| Diretriz | Avaliação de Risco | |
|---|---|---|
| Definição | Os participantes devem realizar avaliações de risco. | |
| Descrição | - As avaliações devem ser suficientemente amplas para abranger o conjunto dos principais fatores internos e externos, tais como tecnologia, fatores físicos e humanos, políticas e serviços de terceiros que influenciam na segurança da informação. | |
| | A avaliação de risco deve:<br>- Ser suficientemente ampla para abranger o conjunto dos principais fatores internos e externos, tais como tecnologia, fatores físicos e humanos e políticas e serviços de terceiros que influenciam na segurança da informação. | |
| Código | Item | Categorias |

Redigido para deixar a leitura mais fácil e objetiva.

| | | | | | | |
|---|---|---|---|---|---|---|
| Rsc_01_0 | Com respeito a cópia de segurança dos seus arquivos profissionais, com que frequência você realiza as seguintes atividades? | Nunca | Raramente | Frequentemente | Sempre | |
| Rsc_01_1 | Cópia de segurança em mídias externas. (CD, DVD, *storage*, *pendrive*,...) | 0 | 1 | 2 | 3 | |
| | Cópia de segurança em mídias externas (CD, DVD, *storage*, *pendrive*) ou nuvem. | | | | | Incluído a tecnologia da nuvem. |
| Rsc_01_2 | Cópia de segurança no mesmo computador de trabalho. | 3 | 2 | 1 | 0 | |
| Rsc_01_3 | Verifica se as copias de segurança estão atualizadas. | 0 | 1 | 2 | 3 | |
| Rsc_02_0 | Instalação de *software* (aplicativos): | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| | Em relação à instalação de *software* (aplicativos), o que você costuma fazer: | | | | | |
| Rsc_02_1 | Você costuma instalar software ou aplicativos de seu interesse no seu computador de trabalho? | 3 | 2 | 1 | 0 | 9 |
| | Instalar software ou aplicativos de seu interesse no equipamento que você usa para trabalhar? | | | | | Redigido para deixar a leitura mais fácil e objetiva. |
| **Rsc_02_2** | Você pede autorização para instalar software ou aplicativos de seu interesse no seu computador de trabalho? | **0** | **1** | **2** | **3** | **9** |
| | Pede autorização para instalar software ou aplicativos de seu interesse no seu equipamento de trabalho? | | | | | |
| Rsc_03_0 | Enquanto você está na sua posição de trabalho, com que frequência você costuma: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| | Enquanto você está na sua estação de trabalho, com que frequência você costuma: | | | | | Redigido para deixar a leitura mais fácil e objetiva. |
| **Rsc_03_1** | **Fumar?** | **3** | **2** | **1** | **0** | 9 |
| Rsc_03_2 | Beber (água, sucos ou outros?) | 3 | 2 | 1 | 0 | 9 |
| **Rsc_03_3** | **Alimentar-se?** | **3** | **2** | **1** | **0** | 9 |
| Rsc_04_0 | Quando você recebe um e-mail com arquivo anexo, com que frequência você costuma: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| **Rsc_04_1** | **Abrir o anexo?** | **3** | **2** | **1** | **0** | |
| Rsc_04_2 | Passar o antivírus antes de abrir o anexo? | 0 | 1 | 2 | 3 | |
| **Rsc_04_3** | **Verificar a procedência do e-mail antes de abrir o anexo?** | **0** | **1** | **2** | **3** | |
| Rsc_05_0 | Quando você recebe um endereço de site da internet (*link*), com que frequência você: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| **Rsc_05_1** | Acessa o *link* independente de quem enviou? | **3** | **2** | **1** | **0** | 9 |
| Rsc_05_2 | Acessa o *link* se vier de remetente conhecido? | 3 | 2 | 1 | 0 | 9 |
| **Rsc_05_3** | Verifica se o *link* é seguro? | **0** | **1** | **2** | **3** | 9 |

Retirado para que o respondente se posicione.

Retirado para que o respondente se posicione.

Retirado para que o respondente se posicione.

| | | | | | | |
|---|---|---|---|---|---|---|
| Rsc_06_0 | Ao receber uma mídia (CD, DVD, *pendrive*, entre outros), com que frequência você: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| **Rsc_06_1** | **Abre a mídia, independente de quem a enviou?** | **3** | **2** | **1** | **0** | 9 |
| Rsc_06_2 | Executa os programas contidos na mídia? | 3 | 2 | 1 | 0 | 9 |
| **Rsc_06_3** | **Passa o antivírus antes de abrir ou executar programas da mídia?** | **0** | **1** | **2** | **3** | 9 |
| Rsc_07_0 | Uso do e-mail corporativo. | Não | | Sim | | N.A. |
| **Rsc_07_1** | **Você utiliza o e-mail da organização para receber mensagens pessoais?** | **1** | | **0** | | **9** |
| Rsc_07_2 | Você utiliza o e-mail da organização para enviar mensagens pessoais? | 1 | | 0 | | 9 |
| **Rsc_07_3** | **Você divulga o e-mail da organização para os seus contatos pessoais?** | **1** | | **0** | | **9** |
| Rsc_08_0 | Ao receber um e-mail com conteúdos tipo *spam* (propagandas, anúncios, entre outros), com que frequência você: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| **Rsc_08_1** | **Abre o e-mail para ver se o conteúdo interessa?** | **3** | **2** | **1** | **0** | 9 |
| Rsc_08_2 | Denuncia como *spam* e/ou bloqueia o remetente? | 0 | 1 | 2 | 3 | 9 |
| **Rsc_08_3** | **Repassa ou reencaminha o e-mail?** | **3** | **2** | **1** | **0** | 9 |
| Rsc_09_0 | Com que frequência você costuma utilizar o computador da organização para acessar: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| **Rsc_09_1** | Suas Redes sociais (Facebook, linkedin, ...)? | **3** | **2** | **1** | **0** | 9 |
| | Suas redes sociais (Facebook, Linkedin, Instagram, entre outros)? | | | | | |
| Rsc_09_2 | Contas externas de e-mail pessoais? | 3 | 2 | 1 | 0 | 9 |
| Rsc_09_3 | Sites de compras? | 3 | 2 | 1 | 0 | 9 |
| Rsc_09_4 | Jogos? | 3 | 2 | 1 | 0 | 9 |
| Rsc_09_5 | Seu Banco (Caixa, Banco do Brasil, ...)? | 3 | 2 | 1 | 0 | 9 |
| | Sua conta pessoal da instituição financeira (banco, cooperativa de crédito, entre outras)? | | | | | |
| Rsc_10_0 | Supondo que você não está presente no seu local de trabalho e o seu colega necessita de um arquivo que está no seu computador, você: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| **Rsc_10_1** | **Passa a sua senha de acesso para que ele possa pegar o arquivo?** | **3** | **2** | **1** | **0** | **9** |
| Rsc_10_2 | Comunica a sua senha ao seu chefe para que ele se responsabilize pelo acesso? | 0 | 1 | 2 | 3 | 9 |
| Rsc_11_0 | No momento da composição da sua senha de acesso, quais dos elementos a seguir você costuma utilizar? | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Rsc_11_1 | Nomes ou apelidos. | 3 | 2 | 1 | 0 | 9 |

Retirado para que o respondente se posicione.

Alterado a ordem para manutenção da mesma lógica sequencial.

Retirado para que o respondente se posicione.

Retirado para que o respondente se posicione.

Inserido uma rede social popularmente utilizada.

Adaptado para o público respondente.

Retirado para que o respondente se posicione.

Retirado para que o respondente se posicione.

| | | | | | | |
|---|---|---|---|---|---|---|
| Rsc_11_2 | Datas ou parte de datas. | 3 | 2 | 1 | 0 | 9 |
| Rsc_11_3 | Números, letras e caracteres especiais misturados. | 0 | 1 | 2 | 3 | 9 |
| Rsc_11_4 | Uma senha padrão. | 3 | 2 | 1 | 0 | 9 |
| Rsc_12_0 | Independentemente do equipamento ser pessoal ou profissional, você tem por hábito: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Rsc_12_1 | Trocar a sua senha de acesso? | 0 | 1 | 2 | 3 | |
| Rsc_12_2 | Criptografar os dados importantes? | 0 | 1 | 2 | 3 | 9 |
| Rsc_12_3 | Acessar redes sem fio abertas (*wifi* sem senha) em locais públicos, tais como aeroportos e restaurantes? | 3 | 2 | 1 | 0 | 9 |
| Rsc_12_4 | Guardar ou fixar a senha de acesso no próprio equipamento (computador, cellular, entre outros)? | 3 | 2 | 1 | 0 | |
| Rsc_12_5 | Bloquear o computador ao se afastar dele por algum motivo? | 0 | 1 | 2 | 3 | |
| Rsc_12_6 | Limpar, higienizar o seu equipamento de trabalho? | 0 | 1 | 2 | 3 | |
| Rsc_13_0 | Ao acessar uma página na internet você: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Rsc_13_1 | Verifica se o site é seguro? | 0 | 1 | 2 | 3 | 9 |
| Rsc_13_2 | Verifica se a rede é segura? | 0 | 1 | 2 | 3 | 9 |
| Rsc_14_0 | Independentemente da atividade que está fazendo, ao utilizar a sua senha você: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Rsc_14_1 | Verifica se alguém está te observando? | 0 | 1 | 2 | 3 | 9 |
| Rsc_14_2 | Verifica se está sendo filmado? | 0 | 1 | 2 | 3 | 9 |
| Rsc_14_3 | Verifica se o dispositivo que está utilizando está em bom estado de conservação? | 0 | 1 | 2 | 3 | 9 |
| Rsc_15_0 | Durante o processo de instalação de um aplicativo você: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Rsc_15_1 | Lê a licença de uso do aplicativo? | 0 | 1 | 2 | 3 | 9 |
| Rsc_15_2 | Procura saber a procedência do aplicativo? | 0 | 1 | 2 | 3 | 9 |
| Rsc_16_0 | Uma questão importante no processo da segurança da informação é o descarte de mídias (CD, DVD, disquete, fita magnética, papel, entre outros). Ao descartar uma mídia, com que frequência você realiza os procedimentos a seguir? | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Rsc_16_1 | Confirma o conteúdo da mídia antes de descartar. | 0 | 1 | 2 | 3 | 9 |
| Rsc_16_2 | Destroi a mídia. | 0 | 1 | 2 | 3 | 9 |
| Rsc_16_3 | Registra o descarte ou a baixa da mídia. | 0 | 1 | 2 | 3 | 9 |
| Rsc_16_4 | Verifica se a mídia está em conformidade com os requisitos para o seu descarte. | 0 | 1 | 2 | 3 | 9 |

Retirado para que o respondente se posicione.

Retirado para que o respondente se posicione.

Retirado para que o respondente se posicione.

Retirado para que o respondente se posicione.

| | | | | | | |
|---|---|---|---|---|---|---|
| Rsc_17_0 | Com respeito ao uso do crachá | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| **Rsc_17_1** | **Utiliza o seu crachá de identificação em local visível?** | **0** | **1** | **2** | **3** | **9** |
| Rsc_17_2 | Verifica se as pessoas que passam por você estão utilizando o crachá de identificação? | 0 | 1 | 2 | 3 | 9 |

Retirado para que o respondente se posicione.

| Diretriz | Projeto de Segurança e Implementação |
|---|---|
| Definição | Os participantes devem integrar a segurança como um elemento essencial dos sistemas e redes de informação. |
| **Descrição** | - Os participantes devem preocupar-se com a criação e adoção de salvaguardas e soluções para evitar ou limitar o dano potencial de ameaças e vulnerabilidades identificadas. |
| | - Os participantes devem preocupar-se com a criação e adoção de salvaguardas e soluções para evitar ou limitar o dano potencial de ameaças e vulnerabilidades identificadas. |

Redigido para deixar a leitura mais fácil e objetiva.

| | | | |
|---|---|---|---|
| Prj_01_0 | É adequado que um conjunto de políticas de segurança da informação seja definido, aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes. | Não sei informar ou não implementada | Parcialmente ou totalmente implementada |
| Prj_01_1 | A política de segurança da informação na sua organização está em que estágio? | 0 | 1 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Prj_02_0 | Convém que a segurança da informação seja considerada em todas as fases do projeto, independentemente do tipo do projeto. Com que frequência a segurança da informação é considerada na fase de: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Prj_02_1 | Definição e elaboração do projeto. | 0 | 1 | 2 | 3 | 9 |
| Prj_02_2 | Execução do projeto. | 0 | 1 | 2 | 3 | 9 |
| Prj_02_3 | Gerenciamento do projeto. | 0 | 1 | 2 | 3 | 9 |

Retirado para que o respondente se posicione.

| | | | | | | |
|---|---|---|---|---|---|---|
| Prj_03_0 | Durante o ciclo de um projeto ou trabalho, com que frequência você e suaequipe realizam as atividades a seguir? | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| | Durante o ciclo de um projeto ou trabalho, com que periodicidade você e sua equipe realizam as atividades a seguir? | | | | | |
| **Prj_03_1** | **Antes de iniciarem um novo trabalho ou projeto, fazem um levantamento dos riscos de possíveis incidentes que possam prejudicar o andamento ou a organização.** | **0** | **1** | **2** | **3** | **9** |
| Prj_03_2 | Durante o decorrer das atividades, reavaliam os procedimentos em busca de falhas ou possíveis incidentes. | 0 | 1 | 2 | 3 | 9 |
| Prj_03_3 | Após a conclusão da atividade, projeto ou trabalho, formalizam por meio de documento as intercorrências para uso futuro. | 0 | 1 | 2 | 3 | 9 |
| Prj_03_4 | Verificam se o trabalho ou projeto está em conformidade no tocante às recomendações. | 0 | 1 | 2 | 3 | 9 |

Retirado para que o respondente se posicione.

Redigido para deixar a leitura mais fácil e objetiva.

| Diretriz | Gestão da Segurança |
|---|---|
| Definição | Os participantes devem adotar uma abordagem abrangente para a gestão da segurança. |
| **Descrição** | - Deve ser baseada na avaliação dos riscos. |

Alterado a ordem da diretriz para conformidade com a OECD (2002)

| | | | | | | |
|---|---|---|---|---|---|---|
| | - Deve ser dinâmica e global, de modo a abranger todos os níveis de atividades dos participantes e todos os aspectos de suas operações.<br>- Deve incluir, respostas antecipadas às ameaças emergentes e a prevenção, detecção e resolução dos incidentes, a recuperação dos sistemas, a manutenção contínua, o controle e a auditoria.<br>- As políticas de segurança dos sistemas e redes de informações, as práticas, medidas e procedimentos em matéria de segurança devem ser coordenados e integrados para criar um sistema coerente de segu- rança.<br>- Os requisitos da gestão de segurança dependem do nível de envolvimento, do papel do participante, dos riscos envolvidos e das características do sistema. | | | | | |
| | A gestão da segurança deve:<br>- Ser baseada na avaliação dos riscos;<br>- Ser dinâmica e global, de modo a abranger todos os níveis de atividades dos participantes e todos os aspectos de suas operações;<br>- Incluir respostas antecipadas às ameaças emergentes e a prevenção, detecção e resolução dos incidentes, a recuperação dos sistemas, a manutenção contínua, o controle e a auditoria;<br>- Ter políticas de segurança dos sistemas e redes de informações, práticas, medidas e procedimentos coordenadas e integradas para criar um sistema coerente de segurança;<br>- - Ter requisitos da gestão de segurança que dependam do nível de envolvimento, do papel do participante, dos riscos envolvidos e das características do sistema. | | | | | |
| Gts_01_0 | Durante o processo de manuseio dos dados da organização (agenda, cadastros, dados de pessoas, etc.) você executa uma ou mais das seguintes etapas: armazenamento, recuperação ou atualização dos dados.<br>Com que frequência você: | Nunca | Raramente | Frequentemente | Sempre | N.A. |
| Gts_01_1 | Avalia os riscos de danos ou incidentes como perda, roubo, adulteração e acesso indevido aos dados? | 0 | 1 | 2 | 3 | 9 |
| Gts_01_2 | Planeja o local e a forma como os dados serão armazenados e acessados, levando-se em consideração a avaliação dos riscos? | 0 | 1 | 2 | 3 | 9 |
| Gts_01_3 | Leva em consideração as diretrizes estabelecidas pela sua organização no planejamento? | 0 | 1 | 2 | 3 | 9 |
| | Leva em consideração as diretrizes estabelecidas pela sua organização? | | | | | |
| Gts_01_4 | Executa os processos conforme planejado? | 0 | 1 | 2 | 3 | 9 |
| Gts_01_5 | Avalia se os procedimentos adotados estão atendendo às necessidades de segurança? | 0 | 1 | 2 | 3 | 9 |
| Gts_01_6 | Executa as modificações necessárias para adequar às novas necessidades? | 0 | 1 | 2 | 3 | 9 |
| Gts_02_0 | Para a melhor gestão da segurança da informação é recomendado que a organização tenha um comitê ou grupo gestor da segurança da informação.<br>Com respeito a essa afirmação | Não sei informar | | Não | | Sim |
| Gts_02_1 | A sua organização possui um grupo gestor da segurança da informação? | 0 | | 1 | | 2 |
| Gts_02_2 | Você acha necessário ter um grupo gestor na sua organização? | 0 | | 1 | | 2 |
| | Você acha necessário ter um grupo gestor da segurança da informação na sua organização? | 0 | | 1 | | 2 |

| Diretriz | Reavaliação |
|---|---|
| Definição | Os participantes devem analisar e reavaliar a segurança dos sistemas e redes de informação, e fazer as modificações necessárias nas políticas, práticas, medidas e procedimentos de segurança. |
| Descrição | - Todos os participantes devem continuamente rever, reavaliar e modificar todos os aspectos da segurança para lidar com esses riscos que estão em evolução. |
| | Os participantes devem:<br>- Rever, reavaliar e modificar frequentemente todos os aspectos da segurança para lidar com riscos que estão em evolução. |

Redigido para deixar a leitura mais fácil e objetiva.

Retirado para que o respondente se posicione.

Retirado o "planejamento" para evitar equívocos na interpretação.

Retirado para que o respondente se posicione.

Alterado a ordem para manutenção da mesma lógica sequencial.

Redigido para deixar a leitura mais fácil e objetiva.

Redigido para deixar a leitura mais fácil e objetiva.

| | | | | | | |
|---|---|---|---|---|---|---|
| Rvl_01_0 | Convém que as políticas de segurança da informação sejam analisadas criticamente em intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia. | Nunca | Raramente | Frequentemente | Sempre | N.A. ou desconheço |
| Rvl_01_1 | Com que frequência você ou sua equipe revisa as políticas de segurança da informação da sua organização? | 0 | 1 | 2 | 3 | 9 |
| Rvl_01_2 | Você é convidado(a) a participar da reavaliação das politicas de segurança da informação? | 0 | 1 | 2 | 3 | 9 |
| Rvl_02_0 | A segurança da informação é uma área que requer uma reavaliação constante. | Nunca | Raramente | Frequentemente | Sempre | Desconheço |
| Rvl_02_1 | Com que frequência você reavalia as suas atitudes com respeito a segurança da informação? | 0 | 1 | 2 | 3 | |
| Rvl_02_2 | Na sua opinião, qual seria a frequência adequada para um funcionário reavaliar os seus hábitos com respeito a segurança da informação? | 0 | 1 | 2 | 3 | |
| Rvl_02_3 | Com que frequência a sua organização promove uma reavaliação dos procedimentos de segurança da informação? | 0 | 1 | 2 | 3 | 9 |

Mantido apenas o "deconheço" para que o respondente se posicione.

## APÊNDICE B – Roteiro/questionário das entrevistas

*Olá!*

*Você está sendo convidado a participar de uma pesquisa para o mestrado de Felipe José Ferreira (UFSC), sob orientação da Prof. Dra. Andrea Cristina Trierweiller (UFSC) e tem como objetivo analisar o nível da cultura da segurança e privacidade da informação em instituições financeiras cooperativistas.*

*Trata-se da segunda etapa de coleta de dados, exclusivamente para fins acadêmicos, na qual os dados serão tratados sempre de forma a impossibilitar a identificação do respondente e sua instituição.*

*Destaca-se que esta pesquisa jamais terá algum objetivo discriminatório, repreensivo ou que possa trazer qualquer prejuízo (ônus) para o respondente.*

*A sinceridade e a veracidade da informação prestada durante as respostas é de fundamental importância para compreensão dos dados.*

*Dessa forma, aceitando participar desta pesquisa, você consente em ceder as informações prestadas exclusivamente para os fins aqui descritos.*

*Sua ajuda é fundamental, muito obrigado.*

*Boa experiência!*

**Diante da publicação da Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD e sua atual vigência, em especial o artigo 6º, que define dez princípios para o tratamento de dados pessoais, quais são as ações e procedimentos adotados em sua instituição:**

### Princípio da Finalidade

*Realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.*

**Fin_01_01.** O cadastro de associados ou candidato a sócio é utilizado para quais finalidades?
**Fin_01_02.** É informado ao titular de dados a finalidade específica, forma e duração do tratamento, e os seus direitos, ao se tornar associado ou fornecer informações para este fim?

**Fin_01_03.** Há armazenamento de informações pessoais mesmo de não associados?

**Fin_01_04.** É fornecido algum aviso legal sobre o tratamento de dados pessoais nas plataformas de comunicação da instituição (físicas e digitais) para associação ao sistema?

**Fin_02_01.** O cadastro de candidatos à vaga de empregos é utilizado para quais finalidades?

**Fin_02_02**. É informado ao titular de dados a finalidade específica, forma e duração do tratamento, e os seus direitos, ao se candidatar a uma vaga de emprego?

**Fin_02_03.** Há armazenamento de informações pessoais de candidatos à vaga de emprego não selecionados?

**Fin_02_04.** É fornecido algum aviso legal sobre o tratamento de dados pessoais nas plataformas de comunicação da instituição (físicas e digitais) na hora do recrutamento?

**Fin_03_01.** Há coleta de informações pessoais através de campanhas de marketing/publicidade?

**Fin_03_02.** É informado ao titular de dados a finalidade específica, forma e duração do tratamento, e os seus direitos, ao preencher informações em campanhas de marketing/publicidade?

**Fin_03_03.** Há armazenamento de informações pessoais de interessados em produtos/serviços que não os adquiriram?

**Fin_03_04.** É fornecido algum aviso legal sobre o tratamento de dados pessoais nas plataformas de comunicação da instituição (físicas e digitais) nas campanhas de marketing e publicidade?

**Fin_04_01**. Em quais situações o titular de dados fornece consentimento para utilização de seus dados pessoais?

**Princípio da Adequação**

*Compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento.*

**Ade_01_01.** Há transferência de dados pessoais entre setores da singular, entre o sistema cooperativista da singular ou outras instituições financeiras?

**Ade_02_01.** No caso de fornecimento de dados pessoais para o fim de associar-se ao sistema cooperativista, quais os procedimentos adotados pela instituição para garantir a compatibilidade do tratamento com a finalidade?

**Ade_02_02.** O que a instituição faz com os dados pessoais coletados para o fim de associar-se ao sistema cooperativista, mas não utilizados para a finalidade descrita na coleta?

**Ade_02_03.** No caso de dados pessoais coletados para o fim de associar-se ao sistema cooperativista, há algum tipo de divergência entre o que está descrito no aviso legal daquilo que acontece na prática do tratamento?

**Ade_03_01.** No caso de fornecimento de dados pessoais para o fim de candidatar-se à vaga de emprego, quais os procedimentos adotados pela instituição para garantir a compatibilidade do tratamento com a finalidade?

**Ade_03_02.** O que a instituição faz com os dados pessoais coletados para o fim de candidatar-se à vaga de emprego, mas não utilizados para a finalidade descrita na coleta?

**Ade_03_03.** No caso de dados pessoais coletados para o fim de candidatar-se à vaga de emprego, há algum tipo de divergência entre o que está descrito no aviso legal daquilo que acontece na prática do tratamento?

**Ade_04_01.** No caso de fornecimento de dados pessoais em campanhas de marketing/publicidade, quais os procedimentos adotados pela instituição para garantir a compatibilidade do tratamento com a finalidade?

**Ade_04_02.** O que a instituição faz com os dados pessoais coletados em campanhas de marketing/publicidade, mas não utilizados para a finalidade descrita na coleta?

**Ade_04_03.** No caso de dados pessoais coletados em campanhas de marketing, há algum tipo de divergência entre o que está descrito no aviso legal daquilo que acontece na prática do tratamento?

**Princípio da Necessidade**

*Limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados.*

**Nec_01_01.** Há um mapeamento do fluxo dos dados tratados na instituição?

**Nec_02_01**. É feita a coleta de alguma informação pessoal para o fim de associar-se ao sistema cooperativista e utilizado para algum fim não informado ao titular de dados?

**Nec_02_02**. Qual a justificativa na coleta de dados pessoais para o fim de associar-se ao sistema cooperativista?

**Nec_03_01**. É feita a coleta de alguma informação pessoal para o fim de candidatar-se à vaga de emprego e utilizado para algum fim não informado ao titular de dados?

**Nec_03_02.** Qual a justificativa na coleta de dados pessoais para o fim candidatar-se à vaga de emprego?

**Nec_04_01.** É feita a coleta de alguma informação pessoal em campanhas de marketing/publicidade e utilizado para algum fim não informado ao titular de dados?

**Nec_04_02.** Qual a justificativa na coleta de dados pessoais em campanhas de marketing/publicidade?

**Princípio do Livre Acesso**

*Garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais.*

**Lia_01_01.** A instituição permite o acesso de todos os dados pessoais do titular?

**Lia_02_01.** O titular de dados tem acesso fácil através de site na internet, rede social ou aplicativo para informações sobre o tratamento dos seus dados?

**Lia_03_01.** É realizada alguma cobrança monetária para que o titular de dados tenha acesso às suas informações pessoais?

**Lia_04_01.** A instituição tem definido os processos para a garantia da integralidade dos dados pessoais na associação ao sistema cooperativista?

**Lia_04_02**. Como é feita a garantia da integralidade dos dados pessoais no processo de associação ao sistema cooperativista?

**Lia_05_01.** A instituição tem definido os processos para a garantia da integralidade dos dados pessoais no processo de recrutamento de colaboradores?

**Lia_05_02.** Como isso é feita a garantia da integralidade dos dados pessoais no processo de recrutamento de colaboradores?

**Lia_06_01.** A instituição tem definido os processos para a garantia da integralidade dos dados pessoais em campanhas de marketing/publicidade?

**Lia_06_02.** Como isso é feita a garantia da integralidade dos dados pessoais em campanhas de marketing/publicidade?

**Princípio da Qualidade dos Dados**

*Garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento.*

**Qda_01_01.** Quais as tecnologias utilizadas para a manutenção da integridade dos dados pessoais coletados?
**Qda_02_01.** Quais as ferramentas disponibilizadas ao titular de dados para que ele possa realizar a alteração ou a atualização de seus dados pessoais?

**Princípio da Transparência**

*Garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial.*

**Tra_01_01.** Há definido os papeis e as responsabilidades dos colaboradores na instituição, no tocante a Lei Geral de Proteção de Dados?
**Tra_02_01.** Os colaboradores da instituição estão cientes de seus papeis na privacidade da informação?
**Tra_03_01.** No processo de associação ao sistema cooperativista, o candidato à vaga de emprego tem acesso a informações claras no aviso legal?
**Tra_04_01.** No processo de recrutamento, o candidato à vaga de emprego tem acesso a informações claras no aviso legal?
**Tra_05_01.** Em campanhas de marketing/propaganda, o candidato à vaga de emprego tem acesso a informações claras no aviso legal?

**Princípio da Segurança**

*Utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.*

**Seg_01_01.** Há na instituição protocolos para minimizar riscos e danos em caso de vazamento de dados pessoais?
**Seg_02_01.** É realizado algum tipo de treinamento com os colaboradores da instituição sobre os procedimentos de segurança da privacidade da informação?
**Seg_03_01.** Há na instituição uma Política de Privacidade da Informação?

**Princípio da Prevenção**

Adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais.

**Pre_01_01.** Quais são as medidas técnicas e administrativas utilizadas para proteção de dados pessoais?
**Pre_02_01.** Existe um procedimento de gestão de riscos formalizado na instituição para prevenir a ocorrência de incidentes à segurança da informação?

**Princípio da Não Discriminação**

*Impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.*

**Nad_01_01.** A instituição coleta algum tipo de dado sensível?
**Nad_02_01.** Há treinamentos entre os setores para estudos e trocas de experiências e informações quanto às áreas afetadas pela privacidade de dados?
**Nad_03_01.** Há um protocolo para a utilização de dados pessoais que impossibilite a utilização para fins discriminatórios ilícitos ou abusivos?

**Princípio da Responsabilização e Prestação de Contas**

*Demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.*

**Rpc_01_01.** As ações relativas à privacidade da informação são documentadas?
**Rpc_02_01.** Há auditoria interna para atestar a eficácia das medidas para cumprimento das normas de proteção de dados pessoais?
**Rpc_02_02.** Quais procedimentos da auditoria interna são realizados?
**Rpc_03_01.** Há auditoria externa para atestar a eficácia das medidas para cumprimento das normas de proteção de dados pessoais?
**Rpc_03_02.** Quais procedimentos da auditoria externa são realizados?