UNIVERSIDADE FEDERAL DE SANTA CATARINA
CAMPUS DE ARARANGUÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO

Lucas Nascimento Martins Camargo da Silva

Cultura organizacional e LGPD na percepção de servidores do Poder Legislativo: discussão de similaridades com o diploma legal

Araranguá
2023

Lucas Nascimento Martins Camargo da Silva

Cultura organizacional e LGPD na percepção de servidores do Poder Legislativo: discussão de similaridades com o diploma legal

Dissertação submetida ao Programa de Pós-Graduação em Tecnologias da Informação e Comunicação da Universidade Federal de Santa Catarina como requisito parcial para a obtenção do título de Mestre em Tecnologias da Informação e Comunicação.
Orientador: Prof. Andréa Cristina Trierweiller

Araranguá
2023

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

Silva, Lucas Nascimento Martins Camargo da
Cultura organizacional e LGPD na percepção de servidores do Poder Legislativo : discussão de similaridades com o diploma legal / Lucas Nascimento Martins Camargo da Silva ; orientadora, Andréa Cristina Trierweiller, 2023.
105 p.

Dissertação (mestrado) - Universidade Federal de Santa Catarina, Campus Araranguá, Programa de Pós-Graduação em Tecnologias da Informação e Comunicação, Araranguá, 2023.

Inclui referências.

1. Tecnologias da Informação e Comunicação. 2. Cultura Organizacional. Segurança da Informação. 3. Lei Geral de Proteção de Dados Pessoais. 4. Poder Legislativo. I. Trierweiller, Andréa Cristina. II. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Tecnologias da Informação e Comunicação. III. Título.

Lucas Nascimento Martins Camargo da Silva

Título: Cultura organizacional e LGPD na percepção de servidores do Poder Legislativo: discussão de similaridades com o diploma legal

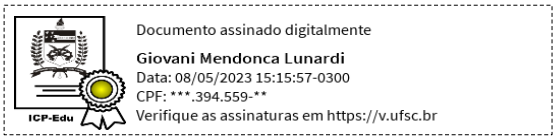
O presente trabalho em nível de mestrado foi avaliado e aprovado, pela banca examinadora composta pelos seguintes membros.

Prof.(a) Dra. Andréa Cristina Trierweiller
Orientadora

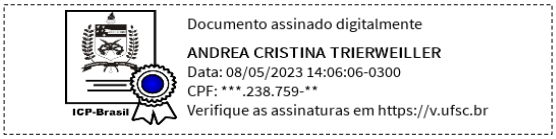
Prof.(a) Dr. Denilson Sell
Instituição UFSC

Prof.(a) Dr. Paulo César Leite Esteves
Instituição UFSC

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.



Coordenação do Programa de Pós-Graduação



Prof.(a) Dra. Andréa Cristina Trierweiller
Orientadora

Araranguá, 2023

Dedico o trabalho a todos meus colegas e familiares.

AGRADECIMENTOS

Não se faz uma caminhada sozinho. Quando se entra em uma jornada longa, o caminho conta com encontros, desencontros e reencontros. Neste ínterim, encontramos pessoas capazes de contribuir, pois estão atentas ao mundo em mudança.

A ânsia que me traz ao programa PPGTIC é o inconformismo a complacência lassa em permanecer em uma caverna, dispondo de mui fraca luz, apenas observando os respingos dos audaciosos aventureiros que se dispõem a mergulhar na ciência. E assim, o divino se faz luz durante a solidão inexorável da jornada.

À mão orientadora da Andréa Trierweiller, que gentilmente foi oferecida, mesmo sem contato prévio ao processo de ingresso ao programa, deposito os mais sinceros agradecimentos. É um relacionamento “às cegas”, arriscadíssimo, mas que se mostrou profícuo. Com suas qualidades agregadoras, fez o possível para convergir as ideias do Pedro Henrique de Moura Araújo, Yuri Borba Vefago, Felipe José Ferreira e Maurício José Ribeiro Rotta ao tema proposto. Aliás, agradeço-lhes, suas companhias respaldaram todo trabalho desenvolvido.

Aos vereadores, assessores e funcionários da Câmara Municipal de Criciúma, neste parágrafo resumo o que deveria desdobrar-se em uma lauda completa. Contei com a presença de 100%, ninguém se opôs a me receber no seu departamento/gabinete, respondendo ao questionário e expondo situações que certamente complementarão o que popularmente chamamos de “currículo oculto”. Aos meus colegas do grupo foco, Henrique, Patrícia, Giovanni, Gisele, Maiara, demonstraram comprometimento e competência nos apontamentos prestados. Possuem olhar apurado aos vieses que só a experiência ensina.

Para quem não sabe, tenho a felicidade de ser milionário. Uma sena certeira, há alguns anos, abstém-me da corrida por metais. Vou explicar:

Minha mãe, Helcy Martins e padrasto Marcial Terra, sempre me acompanhando pela vida andarilha. Dispuseram-se a mudar do pago sulino, marcaram território aqui em terra litorânea. Dizem que estão quase de “Barriga Verde” - talvez seja o chimarrão. Minha família “catarina”, Sandro, Cléa, Luís Eduardo, incontáveis tios e tias (injusto enumerar), esses tantos formam a beleza que é desfrutar da vida.

À Maiara e Nícolas, esposa e filho, que mantém os pilares familiares fortes, permitindo que a estrutura permaneça incólume mesmo diante da tempestade.

Agradeço a tudo que se passou durante esses dois anos. Nossas discussões revelaram a intensidade da vida virtual que obriga refletirmos com sabedoria sobre a condição humana, fraterna e social que compartilhamos.

RESUMO

A LGPD foi sancionada em 2018 com o objetivo de modernizar a legislação quanto ao tratamento de dados pessoais. É mister que a administração pública processe dados do cidadão, em suas redes de telemática, para conseguir cumprir seu papel de oferecer serviços ao cidadão, portanto atua como controladora de dados pessoais. Nesta pesquisa, de natureza qualiquantitativa, exploratória e descritiva, que utilizou a Teoria da Resposta ao Item - TRI para analisar o nível de cultura organizacional em segurança da informação, sob a ótica dos servidores da Câmara Municipal de Criciúma, com olhar às similaridades do texto do diploma legal. Descobriu-se que a instituição está no nível “Encaminhado”, contando com uma mentalidade que o furto de dados pode a afetar severamente, conta com servidores vigilantes a ameaças que possam colocar seus dados em risco. No entanto, carecem de uma política de segurança da informação, inexistindo diretrizes para o uso de dados pessoais, adicionado ao fato de que muitos servidores utilizam seus próprios *smartphones* nos afazeres laborativos. A eficácia da lei é discutível no Poder Legislativo, pois seu papel constitucional a exime de algumas formalidades no uso de dados de munícipes. Mesmo assim, há a necessidade de adoção de medidas na Câmara Municipal de Criciúma, a fim de mitigar os riscos advindos do manuseio inadequado de dados pessoais.

Palavras-chave: Cultura Organizacional. Segurança da Informação. Lei Geral de Proteção de Dados Pessoais. Poder Legislativo.

ABSTRACT

The LGPD was put into effect in 2018 with the aim of modernizing legislation regarding personal data. It is essential that the Government Offices processes citizen's data, in order to be able to deliver public services, therefore it acts as personal data controller. In this research used the Item Response Theory - TRI to analyze the level of Organizational Culture in Information Security from the perspective of the employees from Criciúma's City Council, with a close look at the new Lei Geral de Proteção de Dados Pessoais. Findings show that the institution is at "Encaminhado" level. It has been discovered that data leak can severely affect the whole institution. People are aware of threats that could put its data at risk. However, Criciúma's City Coucil doesn't have a defined Information Security Policy, with no guidelines for the use of personal data. In addition, many workers use their own smartphones for job. The effectiveness of the LGPD is not in a consistent way in the Legislative Branch due the fact that its constitutional role exempts it from some formalities described in the law. Even so, there is a need to adopt measures at the Criciúma's City Council in order to mitigate the risks arising from the improper handling of personal data.

Keywords: Organizational Culture in Information Security. City Council. Personal Data.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ABREVIATURAS E SIGLAS

ABNT Associação Brasileira de Normas Técnicas
ANPD Agência Nacional de Proteção de Dados
BYOD *Bring Your Own Device*
CAPES Coordenação de Aperfeiçoamento de Pessoal de Nível Superior
CMC Câmara Municipal de Criciúma
COBIT *Control Objectives for Information and Related Technologies*
CONARQ Conselho Nacional de Arquivos
CONEP Comissão Nacional de Ética em Pesquisa
CPF Cadastro de Pessoa Física
GED Gerenciador Eletrônico de Documentos
GDPR *General Data Protection Regulation*
IBGC Instituto Brasileiro de Governança Corporativa
IBGE Instituto Brasileiro de Geografia e Estatística
ICGN *International Corporate Governance Network*
ISO *Organization for Standardization*
ITIL *Technology Infrastructure Library*
LAI Lei de Acesso à Informação
LGPD Lei Geral de Proteção de Dados Pessoais
OCDE Organismo de Cooperação e Desenvolvimento Econômico
OECD *Organization for Economic Co-operation and Development*
PBD *Privacy by Design*
PCN Plano de Continuidade de Negócios
PDCA *Plan, Do, Check, Act*
PMBOK *Project Management Body of Knowledge*
PPGD Programa de Pós-Graduação em Direito
PPGTIC Programa de Pós-Graduação em Tecnologias da Informação e Comunicação
RIPD Relatório de Impacto de Dados Pessoais
SGSI Sistema de Gestão de Segurança da Informação
SUS Sistema Único de Saúde
TCC Trabalho de Conclusão de Curso

TCLE Termo de Consentimento Livre e Esclarecido

TCT Teoria Cássica de Testes

TIC Tecnologia da Informação e Comunicação

TGS Teoria Geral de Sistemas

TRI Teoria de Resposta ao Item

UFSC Universidade Federal de Santa Catarina

VPN *Virtual Private Network*

SUMÁRIO

1 INTRODUÇÃO

O governo, de maneira geral, avança em busca de tecnologias que auxiliem na aplicação de políticas públicas. Em março de 2021, foi sancionada a Lei 14.129, titulada Governo Digital, que apresenta em seu Artigo 1°:

> Esta Lei dispõe sobre princípios, regras e instrumentos para o aumento da eficiência da administração pública, especialmente por meio da desburocratização, da inovação, da transformação digital e da participação do cidadão (BRASIL, 2021).

Impulsiona a criação de demandas tecnológicas, de cunho material como *hardware* ou intelectual como *software*, todas no sentido de facilitar o contato entre órgãos públicos e cidadãos. Ela acompanha a Lei 13.709, de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD):

> Art. 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).

Um exemplo, recentemente, por razão da Covid-19, os municípios tiveram que atender exigência nacional do plano de imunização, criando um sistema de cadastro, em uma fila eletrônica, para distribuir vacinas à população. No caso de Criciúma-SC, o poder municipal desenvolveu um desses recursos, um *software*, em que o munícipe acessa o site oficial da prefeitura e insere seus dados pessoais como: nome; CPF; data de nascimento; cartão SUS; endereço; filiação; etc.

Há de se perceber crescente necessidade de endereçar corretamente o tratamento desses dados, para que não reste prejudicada a privacidade e individualidade do munícipe. O Poder Legislativo, para cumprir sua missão constitucional de fiscalizar o Poder Executivo, apropria-se dos dados gerados por este, ou seja, acessa informações pessoais, predominantemente regidas pela LGPD.

Buscando mitigar a questão acima, a Lei Geral de Proteção de Dados impõe uma série de regras à administração pública. Muitos ainda não compreenderam a abrangência dessa lei, adicionado ao fato da escassez de

técnicas, metodologias ou conscientização sobre o tema, aos que trabalham nas áreas jurídicas, tecnológicas, administrativas e análogas.

Observou-se a oportunidade de realização deste estudo, em que serão utilizadas técnicas de revisão de literatura, abarcando leis que versam sobre salvaguarda de dados pessoais, conceitos atinentes à privacidade de dados pessoais, cultura organizacional em segurança da informação, entre outros temas necessários para esta pesquisa.

O resultado desse estudo objetiva propor uma discussão a respeito da cultura organizacional de segurança da informação, no Poder Legislativo de Criciúma, por meio de técnicas metodológicas adequadas, sob viés da nova LGPD.

1.1 CONTEXTUALIZAÇÃO DO PROBLEMA DE PESQUISA

O desafio das empresas em criar e lançar inovações, muitas vezes, as pressiona a ponto de considerarem a privacidade dos dados pessoais. Ayala-Rivera e Pasquale (2018, p. 136) - nesse sentido, exemplificam que, desde a *General Data Protection Regulation* (GDPR), *de 2016, na* Europa, os profissionais de TIC[1] carecem de guias para garantir o cumprimento de *compliance*[2] entre a regulamentação *e* seus produtos. A LGPD[3] é uma lei que atua nesse sentido, no entanto ainda passa por momento de amadurecimento, editando diretrizes e normas, dado a escassez de técnicas, metodologias ou *frameworks* aos organismos submetidos à ela.

O mesmo desafio também é percebido na esfera pública, em nível federal, estadual ou municipal. O administrador público é provocado de tal forma a sensibilizar-se às novas práticas que a LGPD impõe. Recentes publicações revelaram que há necessidade de aperfeiçoar o entendimento do conceito de privacidade de dados entre os profissionais de TIC (CANEDO et al., 2020). Assim como há desconhecimento por profissionais de TIC, é razoável pressupor que as

[1] São os profissionais de tecnologia da informação como analistas, engenheiros de software,
[2] *Compliance:* cumprir, obedecer, estar de acordo com a norma.
[3] A LGPD é a versão brasileira adaptada da GDPR.

organizações públicas, sofrerão com a exígua orientação a respeito do Diploma Legal, a qual também está exposta.

Portanto, qual o nível de cultura organizacional de segurança da informação, na percepção dos servidores do Poder Legislativo e quais possíveis relações poder-se-á estabelecer entre o ente e as diretrizes da LGPD?

1.2 JUSTIFICATIVA

Este pesquisador ingressou no Programa de Pós-Graduação em Tecnologias da Informação e Comunicação em 2017, frequentando matérias isoladas do PPGTIC. Essa oportunidade permitiu o acesso às bases de dados[4], disponibilizadas pela VPN[5] UFSC.

As disciplinas isoladas demandam uma série de leituras, que com o tempo, começaram a convergir para a LGPD. A experiência profissional deste pesquisador está amplamente ligada à TIC, em segurança da informação e infraestrutura, especialmente na adoção de boas práticas dos processos de continuidade de negócio (suportados por COBIT, ITIL e ISO 27.000), incluindo processos de auditoria. Ultimamente, o autor desta dissertação percebe os conceitos de segurança da informação sendo desmistificados com extrema propriedade pelos autores dos artigos disponíveis nas bases de dados de periódicos; predominantemente pesquisadores oriundos da área jurídica. Tornou-se mister sobrepor os pontos de vista técnicos, a fim de engrandecer o tema. A isto se deve a necessidade de metodologia para esta pesquisa.

A administração pública, de maneira geral, avança em busca de tecnologias que auxiliem na aplicação de políticas públicas. A capilaridade do Estado se expande, sugerindo desenvolvimento de ferramentas modernas, que atendam a população com agilidade (DE SOUSA et al., 2017). Neste contexto, é imperativo que

---

[4] Exemplos: Scopus, Web of Science, Repositório UFSC, IEEExplore, Capes, Scielo.org, Wiley, Emerald, ProQuest.

[5] A VPN permite emular uma conexão oriunda da UFSC, isso habilita o acesso às bases sem a exigência de assinatura pessoal ao serviço.

armazene um universo de informações de toda população, seja por força legal ou para desenvolvimento do trabalho das organizações.

Este é o caso apresentado em uma publicação de Regan e Jesse (2019), que apresentam importante análise sobre dados de estudantes da educação básica (nos Estados Unidos) e levantam o aspecto ético que pode estar sendo negligenciado, quanto ao manejo dos dados das crianças. Frisa ainda, os riscos advindos do vazamento desses dados, em que a orientação sexual e religiosa são exemplos de dados sensíveis.

Reitera-se que o gestor público sofre com a exígua orientação a respeito da LGPD. Ferrão et al. (2021, p. 12) reafirmam essa constatação, em estudo entre empresas públicas e privadas, somente 16% estabeleceram procedimentos adequados para verificar se atendem aos princípios[6] da LGPD, desde o planejamento de um serviço até sua execução.

Os Poderes Legislativos municipais, representados nos mais de 5 mil municípios em todo Brasil, pelas Câmaras de Vereadores, personificam o papel fiscalizador da população, vigilantes à aplicação de recursos públicos na consecução de políticas públicas. Portanto, seu capital “econômico” está nas informações que coleta e nos relatórios que produz a partir destas fiscalizações. São dados contábeis, licitatórios, expedientes, e aqui, destacam-se os dados relacionados aos munícipes, de cunho pessoal, como matrículas, uso do serviço de saúde, ou seja, exatamente os dados os quais são alvo de regulação pela LGPD. Diante do fato que muitos servidores acessam os dados supracitados, há uma necessidade de diagnosticar os fatores relacionados à segurança da informação como os culturais, comportamentais e tecnológicos.

É difícil mensurar o grau de adequação de uma instituição à segurança da informação[7]. Portanto, faz-se necessário buscar apoio em trabalhos pregressos. Sendo assim, a principal ferramenta norteadora foi a desenvolvida pelo professor Pedro Henrique de Moura Araújo, apresentada em sua tese de doutorado, em 2018.

---

[6] Princípios constantes do Art 6° da LGPD.

[7] Segurança da Informação contempla um conjunto de ações muito abrangentes, de maneira geral, são compostos de técnicas, tecnologia e conscientização.

Trata da construção da escala de cultura organizacional em segurança da informação, utiliza a Teoria de Resposta ao Item, aborda a psicometria, já foi aplicada calibrada e validada. Seu resultado passa por uma transformação linear, o que facilita sua interpretação, portanto pode se encaixar com o que se pretende nesta dissertação.

O trabalho de Araújo (2018) foi desenvolvido nos Poderes Judiciário e Executivo. A pesquisa em tela adentra no Poder Legislativo, ambiente de trabalho do autor desta dissertação, o que facilita pelos aspectos logísticos e de tempo para realizar a pesquisa.

Sob o ponto de vista legal, há várias leis que versam sobre o cenário da publicidade e eficiência dos serviços públicos. Por exemplo:

a) Lei de Acesso à Informação (LAI), número 12.527, de 2011. Trata da divulgação das informações de interesse público, independentemente de solicitações;
b) a Lei Geral de Proteção de Dados Pessoais (LGPD), número 13.709, de 2018. Dispõe sobre o tratamento de dados pessoais; e
c) Governo Digital, número 14.129, de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital.

A legislação supracitada é central para a eficiência e publicidade na atualidade. A LGPD direciona seus esforços ao “Dado Pessoal” - é mais específica, trazendo novas exigências a todos que tratam dados pessoais[8].

Há crescente necessidade da gestão endereçar corretamente o tratamento desses dados, para que não reste prejudicada a privacidade e individualidade do munícipe, o que exige das instituições públicas e das pessoas que compõem seus quadros, cultura organizacional e ferramental técnico que os habilite a executar tal tarefa.

[8] Inclusive no ambiente onde se pretende desenvolver esta pesquisa.

1.3 OBJETIVOS

Para responder o problema de pesquisa, este estudo estruturou a análise em um objetivo geral que será desdobrado nos objetivos específicos. Serão utilizados os métodos indutivo/dedutivo para verificar as novas realidades normativas e respectivos desafios organizacionais. Há um conjunto de leis recentes que versam sobre o tema (LGPD, LAI), além de literatura sobre cultura, cultura organizacional, cultura organizacional em segurança da informação, que deverão ser revisados.

1.3.1 Objetivo Geral

Esta proposta tem como objetivo analisar uma cultura organizacional em segurança da informação, sob ótica dos servidores do Poder Legislativo de Criciúma/SC, considerando uma comparação com a Lei Geral de Proteção de Dados Pessoais (LGPD).

1.3.2 Objetivos Específicos

Para desenvolver esse objetivo, o assunto será subdividido em:

a) Proceder a revisão de literatura, para relacionar a segurança da informação com os itens de análise da ferramenta de Araújo (2018) e com o que consta na LGPD;
b) Aplicar a ferramenta de Araújo (2018), para verificar o panorama da cultura organizacional em SI, na percepção dos servidores da Câmara;
c) Elencar lacunas existentes entre o nível de cultura organizacional em segurança da informação e a LGPD, no ambiente proposto; e
d) Comparar os dados obtidos, a ferramenta de pesquisa e o texto do Diploma Legal.

1.4 INTERDISCIPLINARIDADE E ADERÊNCIA AO PPGTIC

O Programa de Pós-Graduação em Tecnologias da Informação e Comunicação (PPGTIC), visa resolver problemas de características interdisciplinares, lançando mão de ferramentas tecnológicas. O programa possui uma área de concentração intitulada Tecnologia e Inovação e três linhas de pesquisa, a saber: 1. Tecnologia Educacional; 2. Tecnologia Computacional e 3. Tecnologia, Gestão e Inovação. O Programa está inserido na área interdisciplinar da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (CAPES) e objetiva congregar várias áreas do conhecimento que apresentam interface de estudo e assim, contribuir com o avanço do conhecimento e da pesquisa.

Esta linha de pesquisa trabalhará as novas tecnologias da informação e comunicação para o desenvolvimento de novas metodologias, técnicas, processos para a gestão das organizações (UFSC, 2022).

O ensino interdisciplinar começa a ser discutido a partir de meados do século passado. Tem em sua proposta, romper com o aspecto disciplinar isolado das especialidades, aglutinando habilidades diversas em torno de um objeto de estudo (OLIVIA; RAMOS; FERREIRA, 2020).

A característica interdisciplinar foi aprofundada, buscando-se em bases de dados da Universidade Federal de Santa Catarina (UFSC), a fim de enumerar trabalhos correlatos. As buscas foram feitas em meio eletrônico, por meio da plataforma do Repositório Institucional UFSC. A *string* de busca foi ("lei geral de proteção de dados" OR "LGPD"), em 29 de junho de 2021.

A Tabela 1 contém os resultados obtidos na busca.

Tabela 1 – Busca no Repositório da UFSC

Autor	Título da Dissertação	Programa	Ano
Érico Leandro Buzzi Torres	O direito ao esquecimento e a lei geral de proteção de dados pessoais	TCC Direito	2019
Gabriela Fernandes Sulzbach	O empoderamento do consumidor em torno dos seus dados pessoais diante da pandemia: estudo do sistema legal de proteção de dados pessoais	TCC Direito	2021

Gustavo Xavier de Camargo	A vedação à gratuidade compulsória dos serviços digitais como forma de proteção dos dados pessoais dos usuários consumidores e mitigação do abuso de posição dominante pelas plataformas de dois ou múltiplos lados	Dissertação PPGD	2020
Igor Graeff Bohrer	A proteção de dados pessoais como direito da personalidade e seu risco diante do online profiling	TCC Direito	2019
Maria Victoria Antunes Krieger	A análise do instituto do consentimento frente a Lei Geral de Proteção de dados do Brasil	TCC Direito	2019
Paulo Vitor Petris Tambosi	Responsabilidade civil pelo tratamento de dados pessoais conforme a Lei Geral de Proteção de Dados (LGPD): subjetiva ou objetiva?	TCC Direito	2021
Rogério Hermínio da Silva	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	Dissertação PPGTIC	2021
Sarah Helena Linke	Sociedade de vigilância e consumo: proteção de dados pessoais relacionados à saúde em programas de fidelização de redes de farmácia	Dissertação PPGD	2019
Vanderlei Munhoz Pereira Filho	Projeto e desenvolvimento de um sistema de software de alto desempenho para execução de competições de programação com números massivos de usuários	TCC Engenharia Automação	2020

Fonte: https://repositorio.ufsc.br/discover.

Destes, 06 são Trabalhos de Conclusão de Curso de Graduação (TCC) e 03 são dissertações de mestrado. Estabelecem o marco de partida desta pesquisa, pois assimilam aspectos técnicos e práticos da LGPD, aplicados à sociedade.

Paulo Vitor Petris Tambosi (2021), detalha aspectos jurídicos, pelo viés das correntes hermenêuticas no âmbito doutrinário, com foco na responsabilidade civil dos agentes de tratamento de dados pessoais. Em sua análise, enumera as iniciativas legislativas pretéritas à LGPD, no Brasil, justificando o texto positivado no diploma legal vigente. Sugere estudo científico, para compreender a atividade de tratamento de dados pessoais e prever, nessa toada, hipóteses - melhor delimitadas - do agente de tratamento, que possam prejudicar os direitos de outrem.

Rogério Hermínio da Silva, em dissertação apresentada ao PPGTIC, em 2021, discorre sobre um plano de implementação da LGPD em uma empresa do

setor químico. Explana aspectos que alavancaram a implementação e os óbices enfrentados. Conclui sugerindo o aprimoramento do método adotado em sua implementação, onde constatou oportunidades de melhorias, de modo a construir um *framework* mais adequado às necessidades.

Mesmo com a busca no Repositório Institucional da UFSC, houve a necessidade de complementação em trabalhos pregressos, deste modo, cabe referenciá-los.

O professor Araújo, em sua tese de doutorado de 2018, construiu a escala do nível de cultura da segurança da informação. Apoia-se em técnicas de mensuração psicométricas, para aferir níveis de aptidões dos respondentes. O traço latente é o meio pelo qual a Teoria de Resposta ao Item (TRI) determina características do indivíduo, que não podem ser medidas diretamente. Neste ímpeto, o nível da escala proposta constituiu a base do que se pretende medir nesta pesquisa - o score atual do nível de cultura da segurança da informação na Câmara Municipal de Criciúma, na percepção de seus servidores.

Dentre suas sugestões de trabalho futuro, aventa a possibilidade de incrementar a ferramenta com mais itens.

Felipe José Ferreira, em dissertação de mestrado do PPGTIC, de 2021, desenvolve pesquisa exploratória e de campo, na qual lança mão da tese supracitada, para dissertar sobre a percepção da segurança da informação, privacidade da informação e proteção de dados pessoais em instituições financeiras cooperativistas. Constata a incipiência dos gestores quanto à importância que os colaboradores dão à LGPD.

Conclui sugerindo melhorias na escala de medida, no sentido de habilitá-la à aplicação em qualquer segmento do mercado. A dissertação de Ferreira serviu para pavimentar a etapa metodológica desta dissertação.

2 FUNDAMENTAÇÃO TEÓRICA

O tema proposto nesta pesquisa será desdobrado em uma fundamentação teórica, que servirá para o leitor compreender os termos utilizados. Deste modo, facilitará a discussão dos resultados obtidos por este pesquisador.

Observa-se um objeto definido, o estudo com servidores em uma organização pública. Há um arcabouço teórico a ser percorrido que os admita sob o aspecto humano e, técnico. Por isso, este capítulo compreende a cultura, cultura organizacional, cultura organizacional da segurança da informação, normas da cultura da segurança da Informação, Lei de Acesso à Informação e Lei Geral de Proteção de Dados Pessoais.

2.1 CULTURA

Ao se buscar o termo cultura no dicionário, ou mesmo como Schein (2004) define, os significados ficarão limitados à capacidade intelectual do indivíduo - aquele que detém cultura, é culto - ou poderá relacionar o termo à atividade agrária. Sendo assim, propõe-se expor este conceito no sentido a ampliá-lo.

As definições de “cultura” foram sendo construídas com a evolução dos pensadores, que analisavam as interações sociais. A linguagem, dança, hábitos, expressão artística, música, entre outros, passaram a ser introduzida nesse conceito imaterial que compõe a “cultura”, (LARAIA, 2001). Pode ser multifacetada, divergente, em grupos sociais dispersos. Ou seja, um fato pode ter um entendimento por certo grupo social, em que esse fato é perfeitamente aceitável. Por outro lado, em outro grupo, pode ser considerado inadequado para os costumes locais.

Ao se considerar a cultura dentro de uma organização/empresa, trata-se de um processo em constante evolução, um elemento orgânico, do comportamento de pessoas e, deve ser estudado de forma a reconhecer a importância das mesmas, para contribuir com a missão e valores das unidades empresariais (ARAUJO, 2018).

2.2 CULTURA ORGANIZACIONAL

Assim como a cultura está para o grupo social ou indivíduo, a cultura organizacional está para a organização. Os estudos sobre o tema datam entre 1927 e 1932, com os estudos de Hawthorne, que relata a grande influência das atitudes do grupo sobre o indivíduo (ARAUJO, 2018; FERREIRA, 2021). Ao longo do século, esse conceito evoluiu, mesmo assim não há consenso sobre sua definição e composição (PARSONS et al., 2015).

A antropologia contribui com a explicação do conceito, adicionado ao vetor “tempo”, a cultura organizacional se consolida pela experimentação contínua dos hábitos que os indivíduos adotam para resolver os problemas cotidianos. Isso forma o arcabouço de práticas e políticas. Portanto, à medida que as pessoas são substituídas, as políticas se consolidam e servem como instrumento de orientação aos novos integrantes. Há uma sinergia natural de refinamento dos hábitos; de como fazer as coisas acontecerem. Perceba que a cultura organizacional tende a não se alterar abruptamente, possui uma célula *mater* e em torno dela, as adaptações pela sobrevivência da organização se desenvolvem (SCHEIN, 2004).

Portanto, este estudo está alinhado ao conceito de Araújo (2018), em que a cultura organizacional é a mescla de comportamentos e atitudes dos indivíduos, que determinam os hábitos aceitáveis do grupo, compondo um saber coletivo tácito, a fim de garantir a sobrevivência e a eficiência da organização.

2.3 CULTURA ORGANIZACIONAL EM SEGURANÇA DA INFORMAÇÃO

A popularização da internet dos últimos 30 anos, acompanhada da globalização, expandiu as fronteiras da tecnologia pelo mundo. Abriu oportunidades para a indústria de tecnologia, no momento em que estas passaram a ser responsáveis por produzir soluções que acelerassem os processos de compartilhamento de dados. “As empresas ampliaram seus arranjos contratuais públicos, privados e mistos cada vez mais complexos, ainda fez com que países se

ocupassem de tratados de livre comércio ou organizações internacionais" (HANOFF; NIELSEN, 2020). A indústria se adaptou de forma a descentralizar sua produção e aproveitou os benefícios que cada componente da aldeia global pôde trazer. Veja, ao comprar um carro, os componentes como motor, vidros, portas, freios, são oriundos de países diversos, todos reunidos em um terceiro destino, somente com o objetivo de montá-los.

O gerenciamento de processos, com uso de tecnologia, passou a ser fundamental neste modelo de negócios. Um descontrole em somente um participante da cadeia de suprimentos impacta a produção, causando enormes prejuízos. Outros exemplos para ilustrar este tema podem ser citados, como o *e-commerce* ou plataformas de relacionamentos sociais.

Como resultado do que foi descrito acima, as organizações aceleraram o ritmo de oferta de produtos e serviços intercontinentais. Isso provocou preocupações para padronizar e regulamentar níveis de segurança da informação mais elevados (PARSONS et al., 2015).

Uma difícil lição, que acelerou este processo de regulamentação, estão relacionadas às fraudes dos executivos de empresas americanas, no início deste século, em que os balanços apresentados pelas empresas Enron eram manipulados de tal forma, que parecessem que a saúde da empresa estava hígida. Isso era possível porque não havia mecanismos de controle (administrativos, operacionais ou de controles internos), capazes de evitar tais fraudes. As ações desta empresa despencaram de US$ 81,00 em janeiro de 2001, para US$ 0,40, doze meses depois (SILVA; OTT; NASCIMENTO, 2008). Para agravar o quadro, descobriu-se que essa prática não era tão incomum como parecia.

Organizações que tratam dados, antes de tudo, são indagadas a se aparelhar, de modo efetivo, implantando um Sistema de Governança. Conforme (HANOFF; NIELSEN, 2020), os principais regramentos de abrangência internacional são oriundos da *Organization for Economic Co-operation and Development* (OECD); da Lei *Sarbanes-Oxley*, em 2002; e da *International Corporate Governance Network*

(ICGN). No Brasil, O Instituto Brasileiro de Governança Corporativa (IBGC) cunha a definição teórica, ao definir o termo Governança:

> Governança corporativa é o sistema pelo qual as empresas e demais organizações são dirigidas, monitoradas e incentivadas, envolvendo os relacionamentos entre sócios, conselho de administração, diretoria, órgãos de fiscalização e controle e demais partes interessadas (INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA, 2015).

As boas práticas de governança se fazem taxativas quando da prestação de contas (*accountability*). Os agentes de governança devem prestar contas de sua atuação de modo claro, conciso, compreensível e tempestivo, assumindo integralmente as consequências de seus atos e omissões e atuando com diligência e responsabilidade no âmbito dos seus papéis (IBGC, 2015).

A governança e a segurança da informação elevam seu nível de importância, pelas organizações, digo isto porque ambas estão se tornando imposição legal entre nações, que promovem e constroem um ambiente de confiança, transparência e responsabilidade, no uso de direitos, bens e serviços.

Anderson (2003) aprofunda o tema e descreve que a segurança da informação deve procurar levar em consideração o equilíbrio entre os riscos e o controle. Deve também propor maneiras de transparecer que os riscos estão muito bem mapeados, pelas organizações e que estratégias de controle estão implementadas para contornar esses riscos. A cultura da segurança visa o envolvimento da alta gerência definindo e propondo políticas, procedimentos e responsabilidades de segurança incentiva os colaboradores a adotarem comportamentos éticos adequados e a cumprirem os padrões organizacionais (DA VEIGA; ELOFF, 2007).

Há várias ferramentas e *frameworks* que auxiliam nessa tarefa, dentre eles: *Control Objectives for Information and Related Technologies* (COBIT), *Technology Infrastructure Library* (ITIL), ISO 27.000, ISO 27.701, etc. Elas traduzem a relação risco *versus* controle em uma documentação consistente e exequível aos que almejam alcançar alta maturidade em cultura de segurança da informação, materializando-se sob forma de um documento chamado de Política de Segurança da Informação.

2.4 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Conforme dito anteriormente, a cultura de segurança da informação demanda de envolvimento da alta gerência, de modo a disciplinar os processos existentes em sua organização. Nas Casas Legislativas, a gerência é representada pelo Presidente da Câmara, o qual é encarregado de articular a elaboração do referido documento e, posteriormente, publicando ato normativo.

Os princípios norteadores de uma boa política baseiam-se em preservar a confidencialidade, integridade e disponibilidade (CID) (FERREIRA, 2021). A confidencialidade diz respeito à garantia que os dados serão acessados somente pelas pessoas autorizadas para tal. O princípio da integridade garante que os dados mantém seu conteúdo inalterado desde a produção até seu consumo. Por fim, o princípio da disponibilidade representa os recursos que mantém os sistemas acessíveis, sem interrupções, ou seja, operacionais, independentemente da ocorrência de sinistros na plataforma que os hospeda.

Apesar de as políticas de segurança da informação não seguirem um roteiro rígido, o Guia de Boas Práticas LGPD (BRASIL, 2020) aponta sugestão que se mostra adequada. Inicialmente, a obtenção de dados exige uma organização sistemática de **coleta**, mapeando-se os processos administrativos existentes, com ajuda dos departamentos responsáveis, incluindo sistemas fornecidos por empresas terceirizadas, de gestão administrativa da Casa.

A fase de **retenção** determina qual o método de armazenamento das bases de dados, documentos, equipamentos ou sistemas. Considera sua guarda em meio físico ou em meios virtuais.

A designação dos responsáveis pelos tratamentos de dados representa a etapa de **processamento**. É nele que ficam apontados os papeis de cada um, garantindo o princípio da confidencialidade. Contempla as medidas de segurança adotadas nos equipamentos que processam os sistemas existentes na organização.

Tendo em vista que recursos computacionais operam, em grande maioria, nas redes, é imprescindível prescrição de ações de segurança que permitam o

compartilhamento de informações. A existência de sistemas interoperáveis exige estudo de quem são os agentes envolvidos no envio e recepção de informações e quais equipamentos utilizados para esta tarefa.

Por fim, a política de segurança deve contar com os procedimentos de **eliminação** de documentos. Podem ser físicos ou não. Em caso de descarte de documentos físicos, é necessário apontar o local onde ele ocorre e quais requisitos de desfazimentos destes. No caso de documentos “em nuvem”, há a necessidade de previsão contratual de procedimentos juntos às fornecedoras de soluções tecnológicas contratadas, para eliminação adequada dos dados digitais.

Como dito, os guias COBIT, ITIL e ISO 27.000 descrevem formas de lidar com o aparecimento de incidentes relacionados a tecnologia da informação. O termo “incidentes” diz respeito a falhas, problemas ou dúvidas do usuário, que de alguma forma impactam na execução de tarefas, nos meios computacionais. Este item deve estar contemplado, constando fluxograma de acionamentos de incidentes, assim como os responsáveis por tratá-los.

As ações aqui descritas não se esgotam e nem têm a pretensão de serem impositivas, mesmo assim, Igarashi (2021) relatou que poucas Casas Legislativas estabeleceram suas normas, principalmente no que diz respeito à LGPD. A adoção de uma política de segurança da informação mostra-se item diferencial entre os órgão públicos, principalente vistos à luz da separação de responsabilidades entre os poderes constitucionais, destacando-se o Legislativo, que é objeto desta pesquisa.

2.5 NORMAS DA CULTURA DE SEGURANÇA DA INFORMAÇÃO

Os casos de inconsistências nos dados financeiros descritos na seção anterior mostraram que os sistemas de informática corriam o risco de permitir fraudes. Afinal os sistemas não são imunes à má fé humana. Para remediar este problema, várias entidades procuraram normalizar procedimentos com o intuito de revestir os sistemas com recursos que evitassem esse tipo de problema no futuro.

No Brasil, o governo federal se sensibilizou com o tema e sancionou a Lei N° 13.709, de 14 de agosto de 2018 (LGPD). Esse regulamento visa o tratamento de dados não só em meio eletrônico, mas similarmente em meio físico, assunto a ser tratado adiante.

Este também é o caso da família de normas *International Organization for Standardization* (ISO) 27.000 (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2013), que descreve um modelo para estabelecer, implementar, manter e melhorar continuamente um Sistema de Gestão de Segurança da Informação (SGSI), atuando nas dimensões tecnológicas, de processos e em nível de conscientização das pessoas. Portanto, sob o ponto de vista tecnológico, busca restringir acesso de pessoas a dados ou instalações a que não tenham permissão, tanto sistemas computacionais ou dependências físicas onde equipamentos sensíveis estejam alocados. Do ponto de vista de pessoas, prevê reuniões/treinamento de conscientização com os envolvidos no tratamento de dados, tudo com devida comprovação documental de que os colaboradores tenham passado por tal treinamento. Na visão de processos, preocupa-se com a melhoria contínua e revisão das políticas de segurança implementadas pelas organizações, a fim de corrigir possíveis desvios oriundos do cotidiano das mesmas.

Os volumes desta norma recebem numeração entre 27.000 até 27.099, todos disponíveis no site oficial da entidade (https://www.iso.org). No entanto, a ABNT selecionou, traduziu e disponibilizou as publicações em território nacional, de alguns destes volumes, conforme pesquisa feita no site oficial (https://www.abntcatalogo.com.br), em 27 de outubro de 2022, Tabela 2.

Tabela 2 – Família ISO 27.000

Norma	**Título**
ISO/IEC 27001:2013	*Information security management systems — Require-ments*
ISO/IEC 27701:2019	*Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*
ISO/IEC 27002:2022	*Information security, cybersecurity and privacy protection*

	— Information security controls
ISO/IEC 27003:2017	*Information security management systems — Guidance*
ISO/IEC 27004:2016	*Information security management — Monitoring, measurement, analysis and evaluation*
ISO/IEC 27005:2018	*Information security risk management*
ISO/IEC 27007:2020	*Information security, cybersecurity and privacy protection — Guidelines for information security management systems auditing*
ISO/IEC 27014:2020	*Information security, cybersecurity and privacy protection — Governance of information security*
ISO/IEC 27017:2015	*Code of practice for information security controls based on ISO/IEC 27002 for cloud services*
ISO/IEC 27018:2019	*Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors*
ISO/IEC 27032:2012	*Guidelines for cybersecurity*
ISO/IEC 27035-3:2020	*Information security incident management — Part 3: Guidelines for ICT incident response operations*
ISO/IEC 27037:2012	*Guidelines for identification, collection, acquisition and preservation of digital evidence*
ISO/IEC 27038:2014	*Specification for digital redaction*

Fonte: https://www.abntcatalogo.com.br.

Dos volumes descritos acima, o guia ISO/IEC 27002:2022 estabelece os controles a serem seguidos para uma estrutura de segurança da informação constituindo o guia essencial à obtenção do grau de *compliance* com o referido padrão.

2.6 LEI DE ACESSO À INFORMAÇÃO

Com o objetivo fundamental de regulamentar o acesso à informação, foi editada a Lei 12.527, Lei de Acesso à Informação, de 18 de novembro de 2011, (BRASIL, 2011), dispondo sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com fim de garantir o acesso à informação

previsto no inciso XXXIII do Art. 5°, no inciso II do §3° do Art. 37° e no §2° do Art. 216° da Constituição Federal.

Em seu Art. 3°, a LAI prevê as diretrizes que deverão ser observadas para assegurar o direito fundamental de acesso à informação. Este artigo prevê os princípios básicos da administração pública, mesmo sendo desnecessário, pois a lei é aplicada justamente no exercício da função pública, o que atrai o regime jurídico administrativo e consequentemente, os princípios administrativos (RIBEIRO, 2020).

De toda sorte, a lei reforça a necessidade de o órgão público disponibilizar informação de interesse público, independentemente de solicitações. A isto, se dá o nome de transparência ativa, enquanto que a prestação de informações públicas, a pedido do interessado, é chamada de transparência passiva (BRASIL, 2020).

A LAI incentiva a difusão ampla dos atos/fatos da administração pública, buscando todos os meios possíveis de divulgação da informação. O ente não se permite ficar alheio às evoluções tecnológicas, ou a qualquer outro meio que impacte a transmissão de informações, hoje preponderantemente na internet. Como a preocupação é atingir o maior público possível, deve haver uma linguagem acessível e de fácil compreensão dos dados expostos. Tudo para coadunar com o princípio básico do estado democrático de direito, promovendo participação social, em permitir que o cidadão influencie na elaboração de atos administrativos.

A LAI também reserva-se em proteger documentos considerados imprescindíveis à segurança da sociedade ou do estado. Ela propõe classificação e restrição da informação em ultrassecreto (por até 25 anos), secreto (por até 15 anos) e reservado (por até 5 anos) (BRASIL, 2011).

Finalmente, a LAI descreve “informação pessoal” como aquela relacionada à pessoa natural, identificada ou identificável. Sua divulgação não é permitida, zelando pelo respeito à intimidade, vida privada, honra e imagem das pessoas, bem como às liberdades e garantias individuais. Mesmo assim, o Art. 31° flexibiliza a divulgação dos dados pessoais, se essas forem necessárias para fins médicos, uso científico em pesquisas, cumprimento de ordem judicial, defesa de direito humano ou à proteção do interesse público e geral preponderante (BRASIL, 2011).

Este diploma já dá sinais de que se preocupa com dados pessoais, facultando sua divulgação, por ordem do próprio titular dos dados, o qual poderá consenti-los para sua divulgação. Este item será aprofundado logo a seguir, ao se abordar a LGPD.

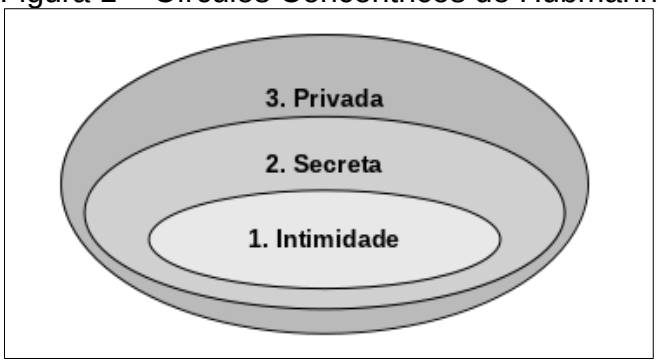
2.7 LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD)

A LGPD é resultado de longo processo histórico. Esta seção será subdividida para situar o leitor historicamente e, sem transcrever propriamente a Lei, ressaltar os aspectos disruptivos que seu texto impõe.

2.7.1 Contextualização da regulamentação da privacidade de dados

O direito geral da personalidade não é tema de estudos recentes. Heinrich Hubmann, autor alemão, em 1953, desenvolveu sua teoria dos círculos concêntricos. Ele define três círculos circunscritos um ao outro, em formato de camadas, comumente denominadas de “cebola”, onde cada camada representa um nível a mais de proteção, conforme adaptação ilustrativa (DA MOTA; TENA, 2020):

Figura 1 – Círculos Concêntricos de Hubmann



Fonte: Adaptado de Da Mota; Tena (2020).

Hubmann constrói a sua definição numa tentativa de delimitar os limites jurídicos do acesso à informação em caráter privado. O nível 1 - “Intimidade” - representa aquele no qual o indivíduo pode manter-se em total segredo diante da

coletividade. O nível 2, camada denominada “Secreta” é mais amplo, pois algumas pessoas conhecem certas intimidades do indivíduo, por participar da vida cotidiana. No nível 3, “Privada”, mais ampla de todas, em que se encontram fatos divulgados a pessoas que não fazem parte da vida do indivíduo (DA MOTA; TENA, 2020).

Concomitantemente, após a Segunda Guerra Mundial, a Declaração Universal dos Direitos Humanos (DUDH), assegura o direito individual a não interferência em sua vida privada, da família, do lar, e de sua correspondência.

Segundo Ferreira (2021, p. 38) e Bernardes, de Andrade e Novais, (2020, p. 4), a Alemanha foi pioneira ao propor um diploma legal, no sentido de salvaguardar as informações pessoais. Nas décadas de 70 e 80, definiram, pela primeira vez, autodeterminação informacional. Esse critério facultava ao cidadão, o consentimento no uso dos seus dados.

Após isso, em 1995, a norma mais saliente quanto à privacidade de dados foi a diretiva 95/46/CE, na União Europeia. Teve um efeito a padronizar as diretrizes nos estados-membros, estabelecendo um novo padrão para proteção de dados no setor da tecnologia e comunicação. Sua vida foi longeva, sendo substituída somente em 2016, quando a GDPR entrou em vigor. Seu efeito notável, pois ela transpôs o continente europeu e forçou que todos os demais continentes editassem leis no mesmo sentido, zelando pela garantia da privacidade dos dados, fazendo deste, um requisito para manter relações comerciais com a Europa (ACOCELLA; SAMPAIO, 2020).

2.7.2 Proteção de dados no Brasil

O incentivo europeu alcançou o Brasil sob a forma da Lei 13.709, de 14 de agosto de 2018 (BRASIL, 2018), conhecida como LGPD. Aplica-se tanto às pessoas naturais ou pessoas jurídicas, de direito público ou privado; às empresas estabelecidas no território nacional ou aquelas com sede no exterior, mas que tenham suas operações no país. Àquelas que a atividade de tratamento de dados tenha por objetivo a oferta ou o fornecimento de bens ou serviços.

Todo o texto da Lei é escrito de modo a cumprir os requisitos descritos nos incisos do Art. 6º, os “Princípios”. São eles: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização e prestação de contas. É perceptível que todo o desenrolar da Lei se debruça sobre os “Princípios” existentes no Art. 6º, sendo os norteadores para apontar as características salientadas a seguir.

2.7.3 Novidades que a LGPD trouxe ao Brasil

Conforme De Sousa e Da Silva, (2020, p. 8), um ponto importante da lei é que, pela primeira vez, um diploma legal resguarda o direito de privacidade oriundo da teoria dos círculos concêntricos, de Hubmann, da década de 70.

O tratamento de dados está condicionado ao consentimento dado pelo titular de forma inequívoca, informando a finalidade a que se destina. Sendo assim, a mudança de finalidade do uso dos dados desconstitui o consentimento, e, portanto, retira a permissão de uso daquele dado pessoal. A essa característica importante, dá-se o nome de autodeterminação informativa (DE SOUSA; DA SILVA, 2020).

Outro quesito inovador está no Art. 15°, os agentes de tratamento de dados, controladores ou operadores, ficam condicionados a estabelecer um prazo para o tratamento dos dados[9], de tal forma a excluí-los ao término deste prazo.

Os indivíduos que necessitarem informações detalhadas a respeito dos seus dados poderão recorrer ao encarregado de dados, Art. 41°. Ele cumprirá o papel de monitorar a forma como os dados pessoais são tratados dentro da instituição, sendo sua atribuição comunicar eventuais falhas/problemas à Agência Nacional de Proteção de Dados (ANPD).

A responsabilidade de auditar as organizações quanto ao correto cumprimento das normas referentes ao tratamento de dados pessoais fica a cargo da ANPD, estando amparada nas exigências dos Art. 46° até Art. 50°. É necessário

[9] Entende-se tratamento de dados, por toda atividade com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

a elaboração de documentação comprobatória, por parte do encarregado de dados, comumente denominado de “Mapeamento de Dados”, o qual enumera o dado coletado, sua finalidade legal, amparo para sua custódia, prazo de utilização, assim como situações particulares. A partir do mapeamento, desenvolve-se o mapeamento de risco acompanhado de ações que mitiguem os sinistros decorrentes de falhas ou violações do uso de dados pessoais. Exemplos mais comuns são sequestro de dados pessoais, ataques cibernéticos, vazamento de dados, interrupção de serviços, etc. Oportunamente, o Governo Federal deve ser comunicado em caso de eventos que envolvam a Segurança da Informação, pelos encarregados de dados.

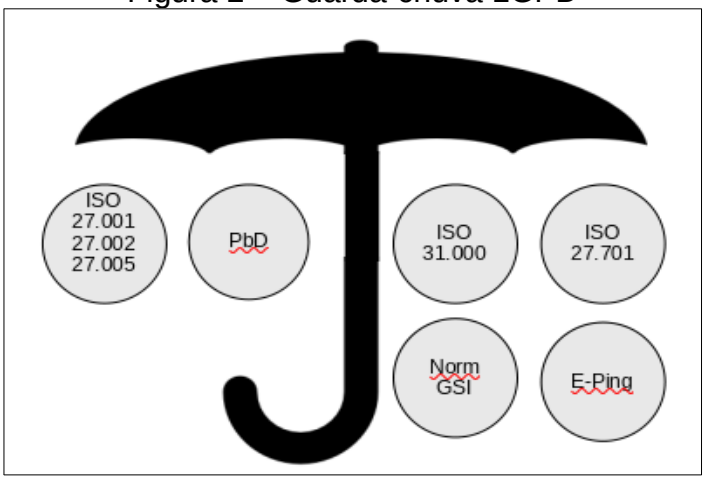
É consenso que o Poder Legislativo edita leis de alto grau de abstração e subjetividade. Porquanto normas mais diretas para tratar as especificidades são necessárias (GUNTHER; COMAR; RODRIGUES, 2020). O “Guia de Boas Práticas”, disponível em https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf, é recomendado para suprir essa necessidade.

2.7.4 Ferramentas de apoio à LGPD

Há ferramentas e *frameworks* que instruem a instrumentalização de tais ações (HANOFF; NIELSEN, 2020) fazem menção ao COBIT. O Governo Federal publicou o Guia de Boas Práticas LGPD (BRASIL, 2020), fornecendo algumas destas ferramentas (Figura 2):

a) E-ping;
b) ABNT ISO/IEC 27.001:2013;
c) ABNT ISO/IEC 27.002:2013;
d) ABNT ISO/IEC 27.005:2019;
e) ABNT ISO/IEC 31.000:2018;
f) ABNT ISO/IEC 27.701:2019; e
g) Normativos do Gabinete de Segurança Institucional da Presidência da República.

Figura 2 – Guarda-chuva LGPD



Fonte: Adaptado de (BRASIL, 2020).

2.7.5 Alcance da LGPD nos órgãos públicos

A LGPD dedicou o Capítulo IV para disciplinar o tratamento de dados pessoais pelo poder público, tanto quanto uso compartilhado entre seus órgãos e entidades. Assim, o objetivo do tratamento é, imprescindivelmente, para atendimento da finalidade pública, na persecução do interesse público, com o objetivo de executar as competências legais ou cumprir as atribuições legais do serviço público, conforme descrito no Art. 23°.

O legislador imputou o dever de obter o consentimento prévio do titular antes das operações. Esta é a regra, mas há exceções com relação à função administrativa. A dispensa da concordância anterior é plausível diante do interesse público Art. 7º inciso III. Moreira (2020, p. 289) indaga: “Mas qual seria o alcance deste dispositivo extremamente aberto?”.

Pertinente é o questionamento, pois a LGPD trouxe um arcabouço robusto para administração pública tratar dados pessoais “a bem do interesse público”, restando ao Poder Judiciário a definição dos seus limites (PACHECO Junior, 2020, p. 315).

O professor Celso Mello define o conceito de política pública como “Um conjunto de atos unificados por ato condutor que os reuniria ao objetivo, meta ou

algo comum de realizar um projeto de governo para o país.” (PACHECO Junior, 2020, p. 316).

LAI e LGPD coexistem harmonicamente no ordenamento jurídico. A LGPD no sentido de disciplinar o agente (pessoa jurídica de direito público), a capturar a informação e custodiá-la em seus bancos de dados. Cabe à lei regulamentar o direito fundamental de divulgação desta informação custodiada, consoante o inciso XXXIII do Art. 5° da Constituição Federal - princípio da transparência pública.

Aparentemente, há uma dicotomia antagônica entre os dois diplomas legais,

> É certo, porém, que há situações em que dados pessoais e até mesmo dados sensíveis não estarão protegidos e comporte-se como dados abertos, justamente por se enquadrarem em uma das hipóteses do Art. 31°, § 3 da Lei de Acesso à Informação. Nesse caso, os dados abertos, ainda que pessoais ou sensíveis, não deverão observar a LGPD, mas sim compor a transparência ativa ou passiva da administração pública (RIBEIRO, 2020, p. 307).

E finalmente, toda esta análise é exposta pois, nos Capítulos finais da LGPD (Capítulo VIII - Da Fiscalização), o Art. 52° sujeita os agentes de tratamento a uma série de sanções administrativas. Tais sanções evoluem gradativamente, desde advertência, multa pecuniária, chegando até a interrupção parcial ou total do exercício relacionado ao tratamento de dados. Multas pecuniárias podem chegar a 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, limitada ao total de R$ 50.000.000,00 (cinquenta milhões de reais) por infração. Não há menção à pessoa jurídica de direito público no referido artigo.

3 PROCEDIMENTOS METODOLÓGICOS

A presente dissertação tem por objetivo propor uma cultura organizacional em segurança da informação, sob ótica dos servidores do Poder Legislativo de Criciúma/SC, considerando uma comparação com a Lei Geral de Proteção de Dados Pessoais (LGPD). Viu-se a necessidade de mensurar, do ponto de vista quantitativo, o estado em que a Casa Legislativa está, no que tange à Segurança da Informação; por isso, adotou-se uma ferramenta: a Teoria da Resposta ao Item, capaz de suprir a questão em tela.

3.1 NATUREZA DA PESQUISA

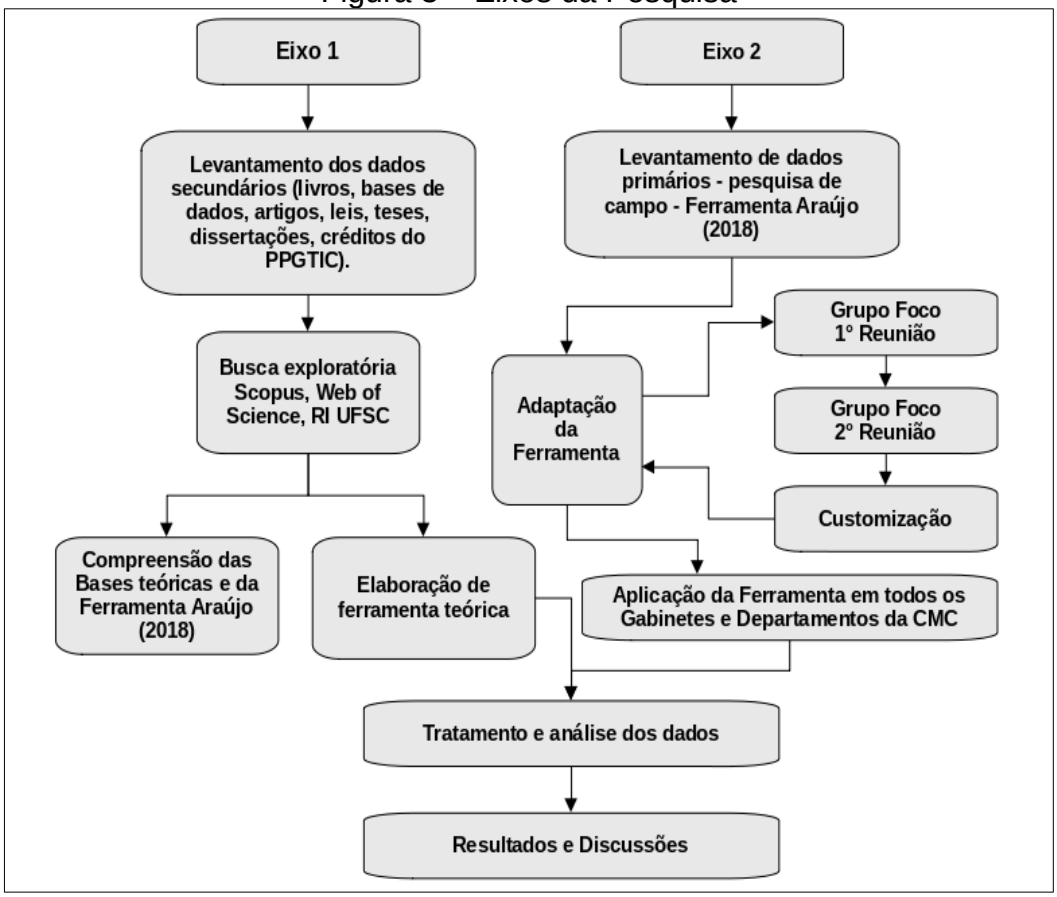
A pesquisa contém características quantitativas e qualitativas.

Como já mencionado, para mensurar o nível de cultura organizacional da Câmara de Vereadores de Criciúma, utilizou-se a Teoria da Resposta ao Item, que inerentemente, envolve abordagem qualitativa para a construção dos itens (questões); seguida de abordagem quantitativa, no momento do tratamento dos dados, resultante da aplicação do conjunto de itens (questionário) para mensurar o traço latente, aqui, o nível de cultura organizacional na percepção dos servidores da Câmara.

3.2 TIPOLOGIA DA PESQUISA

O planejamento desta pesquisa contempla levantamento de dados secundários (eixo 1), com a realização de revisão de literatura, bem como levantamento de dados primários (eixo 2), pelo estudo de campo, com a aplicação de questionário junto aos servidores da Câmara.

Figura 3 – Eixos da Pesquisa



Fonte: Próprio autor.

Para construção desta dissertação, realizou-se pesquisa exploratória, que geralmente é o primeiro passo de qualquer projeto de pesquisa, pois como o próprio nome traduz, é o momento inicial em que o pesquisador busca maior aproximação do fenômeno, para definição adequada do escopo do problema, sem exceder os limites do que se deseja pesquisar. Geralmente envolve entrevistas, incluindo análise de experiências práticas que estimulem a compreensão por parte do participante (GIL, 2002).

As pesquisas envolvem tempo de reflexão dos pesquisadores a fim de construir abstrações, hipóteses e premissas em torno do problema. A dedução, ou método dedutivo, desenvolve o raciocínio lógico, onde duas premissas são analisadas a fim de se obter uma terceira premissa conclusiva, em um exercício constante de produção de silogismos.

Há o interesse de produzir silogismos[10] a partir das premissas Segurança da Informação e LGPD, dentro do ambiente organizacional da Câmara Municipal de Criciúma. Aprofundar o tema, via estudo de caso, e eventualmente, construir hipóteses é alvo do estudo.

3.3 PROCEDIMENTOS PARA COLETA DE DADOS

Conforme já mencionado, para a realização da pesquisa desta dissertação, foram conduzidos dois tipos de levantamento: de dados secundários e primários, conforme segue.

3.3.1 Levantamento de dados secundários

Quanto aos procedimentos para a coleta de dados secundários, realizou-se revisão de literatura no repositório institucional UFSC, com vistas a levantar o que já havia sido publicado sobre o assunto na Universidade, berço do PPGTIC, bem como pesquisa em livros e artigos, inicialmente, sem um critério sistemático.

No decorrer do curso, com o amadurecimento do pesquisador, via disciplinas cursadas no Programa e maior contato com as ferramentas de pesquisa, partiu-se para busca sistemática de literatura nas bases de dados Scopus e Web of Science, em junho de 2021, com a *query* de pesquisa "*general data protection law*" e “lei geral de proteção de dados”, tendo-se obtido 33 documentos: 23 (Scopus); 10 (Web of Science). Destes, 7 eram duplicados e assim, foram removidos manualmente e 5, removidos por abordarem assuntos extemporâneos ao interesse do tema. Os 21 artigos restantes reincidem nos mesmos conceitos básicos da LGPD, sendo assim, esta pesquisa optou por considerar 6 artigos para análise mais profunda, os quais constam nas referências bibliográficas desta dissertação.

[10] (BUENO, 2007, p. 715) exemplifica o termo: “Todos os homens são mortais (premissa maior), tu és homem (premissa menor), logo, és mortal (conclusão).

3.3.2 Levantamento de dados primários

Em relação ao levantamento de dados primários, destaca-se o uso da técnica de grupo foco adaptada. Ou seja, o grupo foco ou *focusgroup*, geralmente é utilizado nas pesquisas de marketing, ao se convidar pessoas a registrar atitudes e opiniões sobre determinado produto ou serviço, sendo conduzida por um moderador (MATTAR, 2013).

Como neste estudo, decidiu-se pela aplicação de um questionário já desenvolvido por Araújo (2018), aplicado em outro tipo de organização, o grupo foco adaptado buscou reunir um conjunto reduzido de servidores da Câmara de Vereadores de Criciúma, com experiência legislativa, a fim de verificar se os termos utilizados no questionário estariam adequados às peculiaridades da Câmara e assim, para obtenção de dados condizentes com a realidade deste tipo de organização. Tendo como moderador, o autor desta dissertação.

Cinco integrantes compuseram o grupo foco. Todos graduados com mais de 15 anos de atividade profissional. Quatro deles, profundos conhecedores da atividade legislativa (Técnicos Legislativos), inclusive um ex-vereador. Um integrante com vasta experiência em desenvolvimento de software, especialmente em *Scrum*[11].

Houve duas reuniões do grupo foco, para análise do questionário e, uma reunião final para refinamento do mesmo.

O grupo foco 1 ocorreu em 20 de maio de 2022, nas dependências da Câmara Municipal de Criciúma, reunião híbrida (videoconferência/presencial). A professora orientadora fez breve explanação quanto a missão do grupo. Cada integrante recebeu uma versão impressa do *draft* de questionário, com a tarefa de respondê-lo e propor melhorias na forma e texto dos itens.

A segunda reunião, o grupo foco 2, aconteceu em 27 de maio de 2022, também híbrida, e todos os integrantes entregaram seus relatórios, que depois de

[11] *Scrum* é uma metodologia ágil de desenvolvimento de *software*. É denominada ágil porque prevê entregas incrementais (incrementos) de código, num período curto de tempo, geralmente entre duas a quatro semanas (PRESSMAN, 2006).

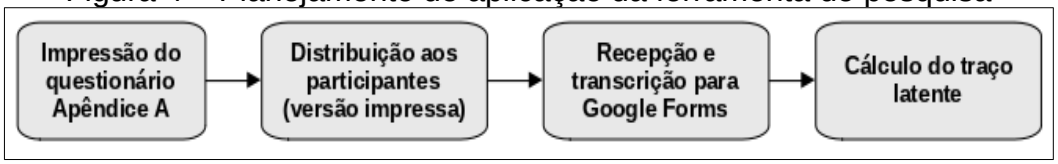
compilados, foram apresentadas ao autor da ferramenta, professor Dr. Pedro Araújo e orientadora Dra. Andréa Cristina Trierweiller.

A ferramenta resultou no constante do Apêndice “D” – Parâmetros Transformados, da tese (ARAUJO, 2018), estes indispensáveis para o cálculo do traço latente em tela. Este pesquisador ainda incluiu 3 itens àqueles existentes no apêndice, com o objetivo de levantar hábitos notadamente praticados no ambiente onde se desenvolve a pesquisa. O resultado é que a ferramenta final conta com 58 itens e está disponível para consulta no Apêndice A – Questionário.

3.4 APLICAÇÃO DA FERRAMENTA DE PESQUISA

A aplicação da ferramenta de pesquisa adotou o planejamento com as seguintes etapas:

Figura 4 – Planejamento de aplicação da ferramenta de pesquisa



Fonte: Próprio autor.

O questionário aplicado foi o constante no Apêndice A - Questionário. Todas as recomendações para o correto preenchimento estão presentes no Termo de Consentimento Livre e Esclarecido (TCLE). São os termos considerados indispensáveis à compreensão do assunto tratado. A distribuição foi feita, de maneira impressa, nos 17 gabinetes existentes na Câmara Municipal de Criciúma mais os 11 setores administrativos da Casa. O pesquisador acompanhou alguns respondentes no sentido de tirar dúvidas quanto à interpretação dos itens, buscando cuidado não interferir nas respostas.

As datas de preenchimento dos formulários foram entre 13 e 20 de setembro de 2022. O pesquisador criou um formulário no *Google Forms* e transcreveu as respostas em meio eletrônico, entre os dias 21 de setembro e 04 de outubro de 2022.

O cálculo do traço latente do nível de cultura em segurança da informação teve ajuda do professor Pedro Araújo. Ele recebeu os dados tabulados pelo *Google Forms* e retornou com os resultados. Esta fase ocorreu no período de 10 a 14 de outubro de 2022. Complementarmente, fez-se uma reunião entre Araújo (2018) e o autor desta dissertação, para análise dos dados e interpretação dos resultados.

3.5 CÂMARA MUNICIPAL DE CRICIÚMA

O sistema de 3 poderes adotado no Brasil é composto por Legislativo, Executivo e Judiciário. Independentes e harmônicos entre si. No âmbito federal, o Poder Legislativo é representado pelo Congresso Nacional[12]; nos estados, fica a cargo das Assembleias Legislativas e, nos municípios, figuram as Câmaras de Vereadores.

A Câmara Municipal de Criciúma é situada na Rua Coronel Pedro Benedet, 488, bairro Pio Corrêa, em Criciúma, Santa Catarina. O plenário ocupa o 6° andar do Edifício Centro Profissional, com os gabinetes dos vereadores dispersos entre o segundo e o oitavo andares. Este órgão é o representante pelo Poder Legislativo Municipal, portanto “Câmara Municipal de Criciúma” e “Poder Legislativo” são, habitualmente, termos análogos. A recepção está ilustrada na Figura 5:

Figura 5 – Recepção da Câmara Municipal de Criciúma

Fonte: Sítio oficial da Câmara Municipal de Criciúma[13].

[12] O Congresso nacional é composto pela Câmara de Deputados e Senado.
[13] Disponível em http://camaracriciuma.sc.gov.br, acesso em: 25 Jan. de 2023.

A estrutura administrativa existente na casa é composta de 17 servidores efetivos, distribuídos em 11 departamentos. Como há a necessidade de complementação de pessoal, há um número variável de comissionados (indicados políticos), que ocupam lugar nesses departamentos, a soma fica próximo a 22 servidores, a saber:

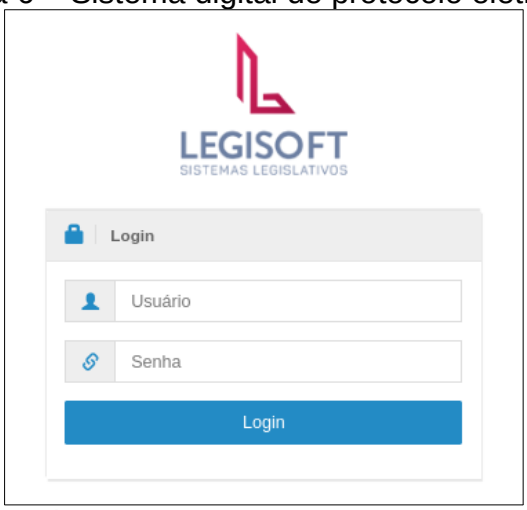
- Diretoria;
- Departamento jurídico;
- Departamento financeiro;
- Departamento de pessoal;
- Secretaria;
- Departamento de informática;
- Departamento de legística;
- Departamento de compras;
- TV Cidadã;
- Recepção; e
- Imprensa.

A composição política é de 17 gabinetes de vereadores (um vereador por gabinete), companhado de 2 assessores, compondo 51 agentes políticos, sendo que um deles acumula a função de presidência da Casa. Essa atribuição é renovada por eleição entre os pares a cada dois anos.

O sistema de Gerenciamento Eletrônico de Documentos (GED) é a plataforma principal de trabalho legislativo[14]. Os servidores têm acesso a este sistema para protocolar documentos e projetos. O mesmo está disponível na internet, dispensa o uso de papel e faz uso de assinatura eletrônica. A seguir, a tela inicial do sistema intitulado Legisoft.

[14] Popularmente este tipo de sistema recebe o nome de *Enterprise Resource Planning* (ERP).

Figura 6 – Sistema digital de protocolo eletrônico



Fonte: Sítio oficial da Câmara Municipal de Criciúma.

O munícipe também pode protocolar documentos na Câmara Municipal de Criciúma sem a necessidade de se deslocar até as dependências deste órgão público. O canal de contato está disponível no sítio oficial:

Figura 7 – Sistema digital de protocolo eletrônico

Fonte: Sítio oficial da Câmara Municipal de Criciúma.

Este canal de atendimento também aceita documentos assinados eletronicamente. Todos são recebidos na Secretaria para providências e encaminhamentos.

3.6 TEORIA DE RESPOSTA AO ITEM

A aferição de desempenho, coletivo ou individual, segue princípios majoritariamente quantitativos. É herança da Teoria Clássica de Testes (TCT), oriunda da década de 20, amplamente empregada até hoje com a finalidade de medir o nível de proficiência alcançado por um indivíduo ou organização (BAKER, 2001, tradução nossa).

Para ilustrar a Teoria de Resposta ao Item (TRI) é importante relacioná-la às provas escolares, que são compostas de um conjunto de itens (questões), aplicados a um grupo de estudantes com a finalidade de eleger aqueles que adquiriram conhecimento suficiente em determinada matéria. Os itens, ou questões, são sempre associados à prova como um todo. Portanto, o instrumento de avaliação construído sob a égide da TCT possibilitará a comparação de indivíduos, somente se a prova, ou teste, for composto pelos mesmos itens, ou seja, provas idênticas. Nesse método, é difícil de comparar grupos ou indivíduos que não tenham sido submetidos às mesmas provas, ou seja, compostas com os mesmos itens (ANDRADE; TAVARES; VALLE, 2000).

As avaliações precisam comprovar se o respondente domina determinado assunto, propondo questões que o desafiem a encontrar a resposta certa. A soma dos acertos obtidos comprova se o aluno detém as habilidades satisfatoriamente. A resposta aceita somente uma alternativa correta na TCT.

Pela ótica do conhecimento mais amplo, há variáveis adjacentes intuitivamente compreendidas, como a inteligência. Descrever alguém inteligente pode se referir à capacidade dessa mesma pessoa assimilar conhecimento rapidamente, em criar sinapses que transformam um conhecimento em sabedoria,

para resolver problemas práticos do cotidiano ou empíricos (BAKER, 2001, tradução nossa).

A velocidade de leitura, boas notas, velocidade de raciocínio podem ser exemplos de inteligência, similarmente, no ambiente escolar. Destreza em um profissional executar habilmente suas tarefas, pois a inteligência é uma variável mais robusta de ser medida - diferentemente de peso e medida que se resolveria somente com uma balança e trena (BAKER, 2001, tradução nossa).

Por isso, a TRI se dispõe a mensurar características que não são diretamente medidas por um instrumento, como a fita métrica para a altura ou uma balança, para o peso. Sendo assim, destina-se a mensurar traços psicométricos, que não são diretamente observados. Neste caso, o nível de cultura em segurança da informação da Câmara de Vereadores de Criciúma, sob a percepção de seus servidores. Sendo assim, ao auferir algo abstrato, a inteligência, como citada anteriormente, o campo da psicometria chama esta unidade de medida de traço latente.

É um conjunto de características observáveis que descrevem atributos do que se deseja medir. O conjunto é quantificável e um escore pode ser obtido após a concatenação dos valores individuais das variáveis (BAKER, 2001, tradução nossa).

Os pesquisadores dessa área reconhecem que o traço latente é a representação numérica de habilidade individual quando o indivíduo é exposto a algum teste. Pode-se dizer mais, é o índice de probabilidade de o respondente dar a resposta correta para determinado problema. Por mais que exemplifiquemos a aplicação do termo genérico “habilidade”, este é nomeado na TRI para se referir ao termo “traço latente” - é algo que se deseja medir (BAKER, 2001, tradução nossa).

3.6.1 Escala de Medida

Se é necessário medir o traço latente de uma pessoa, é necessário lançar mão de uma escala de medida, acompanhado das regras para medi-la. Por uma

série de razões técnicas é difícil definir a escala de medida, a numeração da escala e o peso que esta representa nos valores do traço latente.

(BAKER, 2001) auxilia essa questão definindo, arbitrariamente, uma escala adjacente de habilidade, apontada para zero “0”, contando com a unidade de medida um “1”, podendo variar entre positivo e negativo. Analogamente, adotamos esta escala de medida, ajustada por uma técnica matemática de transformação linear, para aplicar na presente pesquisa. Portanto, adotamos uma regra numérica que permitirá medir habilidades, o que é alvo do trabalho.

3.6.2 A abordagem de medida do Traço Latente

O comum é que se elabore um teste composto por itens/questões. Os itens são elaborados com foco em examinar alguma dimensão do objeto observado. A dimensão também pode chamar-se faceta, de tal modo que quanto mais pontos de vista do objeto observado, mais facetas há na ferramenta de análise. Lembrando que quanto mais facetas, melhor é a escala de medida e mais complexa ela fica.

É possível que o item permita resposta com texto livre – resposta onde o participante responde livremente às perguntas. A resposta também pode apresentar-se dicotômica - frequentemente referida como binária. O item dicotômico (binário), é aquele com as alternativas certo ou errado; verdadeiro ou falso; sim ou não; etc. Ainda há possibilidade de múltiplas alternativas, contemplando aquelas do tipo binária ou múltipla alternativa. Estas com a característica de terem a operacionalização da soma de correção mais fácil de ser obtida, ou seja, de mais fácil correção.

Os itens com resposta livre são conferidas pelo examinador, o qual julgará se a resposta está certa ou errada. Caso certo, recebe o score “1”, se errado o score é “0”.

Os itens dicotômicos, ou binários, seguem a mesma lógica. Evidentemente, é mais fácil a somatização das respostas do avaliador. Assim como a resposta livre, “1” para o acerto e “0” para o item errado.

A múltipla alternativa sofre um processo semelhante ao dicotômico, no sentido que há uma resposta certa e as demais estão erradas. Neste caso, há a possibilidade de estabelecer pesos às alternativas, e não somente o “0” e “1” do modelo binário. Vamos a um exemplo: podemos questionar a frequência com que alguém verifica itens de segurança no seu ambiente de trabalho. Às respostas “sempre” e “frequentemente” atribuem-se os escores “3” e “2” respectivamente, enquanto que “raramente” e “nunca” atribuem-se os escores “1” e “0” respectivamente. Veja abaixo:

Tabela 3 – Relação entre scores e pesos

Alternativa	**Peso**
Sempre	3
Frequentemente	2
Raramente	1
Nunca	0

Fonte: Próprio autor.

De um ponto de vista prático, é muito difícil corrigir uma ferramenta com resposta livre, restando os modelos binários ou múltipla escolha, preferencialmente. Evidentemente, que tudo se adéqua conforme as peculiaridades de cada caso.

3.6.3 Curva característica do item

É razoável pensar que a resposta do examinado revelará a sua habilidade quanto àquele item. O escore obtido, conforme explicação anterior, posiciona-lo-á dentro da escala de medida da TRI. Para isso, é fundamental que se considere que cada respondente possui uma quantidade de habilidade adjacente. Portanto, seu escore o posiciona dentro da escala de medida (BAKER, 2001, tradução nossa).

Habilidade é descrita na literatura pela letra grega *Theta*(θ). Cada nível de habilidade conterá a probabilidade de o participante responder corretamente ao item.

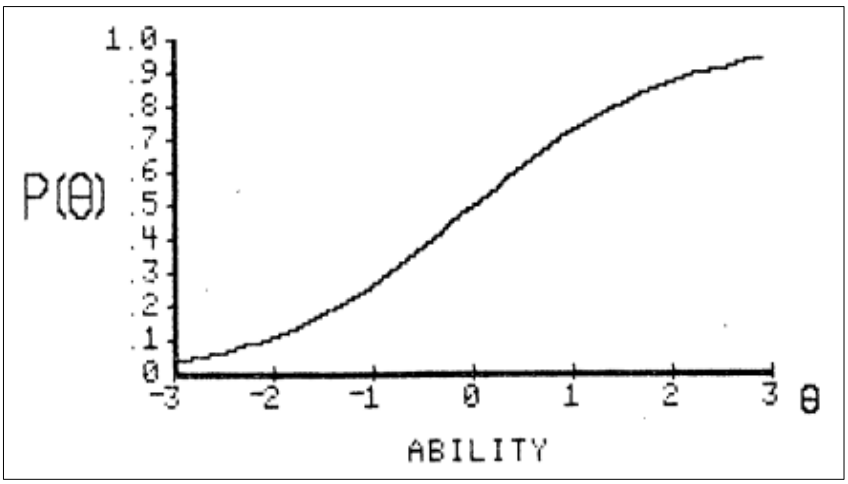
Quanto menor a habilidade, menor é a probabilidade de acertar. Quanto maior a habilidade, maior a probabilidade de acerto (BAKER, 2001, tradução nossa).

Há duas propriedades técnicas de uma curva característica do item.

1. A primeira é a dificuldade, ela funciona para posicionar o item conforme a habilidade do examinado. O Item de baixa dificuldade funciona com os participantes de baixa habilidade enquanto que os itens de alta dificuldade funcionam com os participantes de alta habilidade.
2. A segunda propriedade é a discriminação, visualmente posiciona os examinados com maior habilidade em um índice *theta* mais elevado, formando uma senoide ao longo do plano cartesiano. Em tese, o gráfico em formato de linha plana, corresponde que tanto os participantes com alta habilidade quanto com baixa habilidade forneceram a mesma resposta para um dado item.

Essa relação é descrita como “A curva característica do item” (Figura 8):

Figura 8 – A curva característica do item



Fonte: (BAKER, 2001, p. 7).

Recorda-se que a TRI, ao contrário da TCT, leva em consideração os itens individualmente, diferentemente da soma global dos valores do teste. Haverá uma curva característica do item para tantos quantos forem o número de itens do teste.

Não nos cabe neste trabalho, aprofundarmo-nos neste quesito, pois a noção já apresentada satisfaz a necessidade deste pesquisa.

3.7 ESCALA DO NÍVEL DA CULTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

A escala do nível de medida é construída seguindo princípios da Teoria de Resposta ao Item. Essa escala é aplicada em formato de formulário, constituído por itens destinados a prover condições necessárias para que o avaliado possa escolher a resposta que lhe é mais adequada. Esta escala serve para subsidiar o gestor na compreensão do comportamento dos funcionários, colaboradores de uma instituição, refletindo de modo qualitativo em resultados quantitativos.

A ferramenta em tela é oriunda de Tese de Araújo (2018), que levou diversas diretrizes em consideração, que envolvem a cultura organizacional de segurança da informação. Dentre eles, os princípios descritos pelo Organismo de Cooperação e Desenvolvimento Econômico – OCDE (Tabela 4). São dimensões baseadas na tríade existente quando o assunto é segurança da informação, ações técnicas, de comportamento e de gestão.

Tabela 4 – Princípios Diretivos de Cultura de Segurança da Informação

Princípio	**Descrição**
Sensibilização (Consciência)	Os participantes devem estar cientes da necessidade de garantir a segurança dos sistemas e redes de informação e do que podem fazer para melhorar a segurança.
Responsabilidade	Todos os participantes são responsáveis pela segurança dos sistemas e redes de informação.
Resposta (Reação)	Os participantes devem agir em tempo hábil e de maneira cooperativa para prevenir, detectar e responder a incidentes de segurança.
Ética	Os participantes devem respeitar os interesses legítimos de outros participantes.
Democracia	A segurança dos sistemas e redes de informação deve ser

	compatível com os valores essenciais de uma sociedade democrática.
Avaliação de risco	Os participantes devem realizar avaliações de risco
Projeto de segurança e implementação	Os participantes devem integrar a segurança como um elemento essencial dos sistemas e redes de informação.
Gestão de Segurança	Os participantes devem adotar uma abordagem abrangente para a gestão da segurança.
Reavaliação	Os participantes devem rever e reavaliar a segurança dos sistemas e redes de informação e fazer as modificações apropriadas nas políticas, práticas, medidas e procedimentos de segurança.

Fonte: (OCDE, 2002 apud ARAÚJO, 2018, p. 57-68).

Também se adotou a ISO 27.002, que estabelece os controles de segurança que devem ser implementados em segurança da informação. A sobreposição dos nove princípios diretivos da OCDE e os controles da ISO formam a ferramenta produzida por Araújo e que depois de validada e ajustada, resultou nos “Parâmetros Transformados” contendo 55 itens. Estes são os itens necessários para calcular o índice, por algoritmo desenvolvido pelo próprio Araújo (2018). Mesmo assim, este pesquisador incluiu 3 perguntas complementares, a fim de averiguar hábitos dos servidores da Casa Legislativa (Apêndice A).

Os resultados obtidos pela escala são números racionais (Q), linearmente ordenados, onde quanto maior o índice, maior é a proficiência do respondente.

3.7.1 Interpretação da Escala

Os valores obtidos na escala do nível da cultura de segurança da informação, enquadram-se, conforme a Tabela 5:

Tabela 5 – Interpretação da escala

Nível	**Escala**
Nível 0 (Caos)	$i \leq 65$ pontos
Nível 1 (Elementar)	$65 < i \leq 75$

Nível 2 (Em evolução)	$75 < i \leq 90$
Nível 3 (Encaminhado)	$90 < i \leq 120$
Nível 4 (Otimizado)	> 120

Fonte: (ARAÚJO, 2018, p. 111-123).

Uma breve caracterização de cada nível de cultura de segurança da informação (ARAUJO, 2018):

> Nível 0 (Caos) é o das organizações que não atingiram o nível mínimo (65 pontos) de segurança da informação. As organizações classificadas neste nível estão expostas a todos os tipos de riscos na segurança da informação. Não existe um padrão de comportamento estabelecido e há total desconhecimento sobre o assunto. Todas as iniciativas de segurança nesse nível são isoladas, pessoais, sem fundamento técnico/normativo, ou são puramente intuitivas. Trata-se do nível cujo risco é o mais alto, no qual a organização está mais vulnerável. Pode-se afirmar que não existe uma cultura formalizada sobre segurança da informação e não é possível identificar as facetas (ARAUJO, 2018, p. 111).
> Nível 1 (Elementar) acima de 65 até 75 pontos. Nesse nível, a organização contempla os requisitos mínimos de comportamentos voltados à segurança da informação. Ainda não é observada a relação entre o colaborador e a tecnologia da informação. Tais comportamentos ainda são ocasionais, não frequentes e só às vezes observados. Os seus colaboradores demostram ter preocupação com a segurança da informação, mas de forma não sistemática e empírica (ARAUJO, 2018, p. 111).
> Nível 2 (Em evolução) acima de 75 até 90 pontos. Esse nível é chamado de Em Evolução, pois se trata de organizações cujos colaboradores apresentam conhecimentos iniciais, superficiais, sobre o tema segurança da informação e também sobre tecnologia da informação. Nesse nível as organizações ainda não têm uma cultura organizacional de segurança da informação consolidada, mas dão indícios de estarem se preparando para atingir a consolidação (ARAUJO, 2018, p. 113).
> Nível 3 (Encaminhado) acima de 90 até 120 pontos. As organizações posicionadas neste nível começam a demonstrar uma preocupação com a segurança da informação. Embora ainda exista a condição ‘Às vezes’, os seus colaboradores já estão incutindo o comportamento ‘sempre’ em suas atitudes. Assim, esse nível foi chamado de Encaminhado, pois se percebe que as organizações já apresentam condições que as encaminham em direção a uma cultura de segurança da informação plena (ARAUJO, 2018, p. 116).
> Nível 4 (Otimizado) acima de 120. As organizações aqui posicionadas já estão com sua cultura de segurança da informação estabelecida. Nesse nível os colaboradores já entendem que a segurança da informação é uma questão vital para a organização. A preocupação das organizações nesse nível está em encontrar formas e procedimentos mais eficazes e eficientes para atingir uma melhor efetividade (ARAUJO, 2018, p. 121).

O posicionamento da organização, como um todo, é definido seguindo metodologia específica contida na Tabela 6:

Tabela 6 – Aferição do nível na organização

Nível	Regra
Nível 0 (Caos)	A quantidade de colaboradores nesse nível é >= 10%, independente dos níveis mais elevados.
Nível 1 (Elementar)	Ter menos de 10 % no nível anterior e a soma dos níveis 0 e 1 >= 10%.
Nível 2 (Em evolução)	A totalização dos dois níveis anteriores deve ser menor que 10% e a totalização dos níveis 0, 1e 2 >= 20%.
Nível 3 (Encaminhado)	Os níveis 0, 1, 2 devem totalizar menos que 20% e ter mais de 30% no nível 3.
Nível 4 (Otimizado)	Deve ter mais de 70% dos colaboradores no nível 4.

Fonte: (ARAÚJO, 2018, p. 125).

A organização é medida considerando a quantidade dos menores escores. Tomando-se os elos mais fracos, faz-se a contagem dos mesmos e o enquadramento do grupo de respondentes na Tabela 6, para obter-se a definição do nível..

4 RESULTADOS E DISCUSSÃO

Os resultados obtidos nesta seção confrontarão os índices de cultura organizacional em segurança da informação, oriundos do Eixo 2, ferramenta de pesquisa aplicada junto aos servidores da Câmara Municipal de Criciúma, com aqueles levantados no Eixo 1, revisão bibliográfica, considerando as regulamentações e leis.

4.1 RESULTADO DO DIAGNÓSTICO TRI

Esta dissertação contou com 28 participantes, representados por vereadores, assessores, analistas legislativos e técnicos legislativos. Todos os 17 gabinetes e os 11 departamentos administrativos responderam ao formulário. Todos são considerados servidores da Casa. Os respondentes estão anonimizados, estando enumerados para fins de análise.

Os índices obtidos pelos respondentes sofreram uma transformação linear, pelo princípio da invariância da TRI, com média 100 e desvio padrão em 10 Araújo (2018, p. 94).

Tabela 7 – *Scores* obtidos

Ordem	Abaixo de 100	Acima de 100	Nível
1	95,823		3
2	99,931		3
3		104,48	3
4		114,31	3
5	99,924		3
6		114,45	3
7	98,164		3
8		112,94	3
9	95,29		3

10	97,26		3
11	96,346		3
12	98,823		3
13		112,38	3
14	98,554		3
15	97,981		3
16	98,589		3
17		107,94	3
18	93,888		3
19		104,88	3
20		103,14	3
21	99,367		3
22	91,805		3
23	92,636		3
24		108,41	3
25	84,285		2
26	92,21		3
27	90,999		3
28		112,88	3

Fonte: Próprio autor.

Observa-se que, 35% (10 participantes) estão acima da média, enquanto que 65% (18 participantes) estão abaixo. Os participantes “6” e “4” alcançaram os maiores níveis, com 114,45 e 114,31 de média, respectivamente e os participantes “25” e “27” obtiveram os menores, com 84,28 e 90,99 respectivamente. Outra análise é a partir do viés das facetas existentes na ferramenta de Araújo (2018), conforme Tabela 4.

Todos os servidores devem estar cientes da necessidade de garantir a segurança dos sistemas telemáticos que operam e propor ações a fim de mitigar riscos, sugerindo controles para os mesmos, conforme observado por Anderson (2003).

Conhecer a configuração do parque de informática e as atualizações disponíveis do sistema pode elevar a segurança. Na faceta de **consciência**, tanto os participantes 6 e 4, quanto os participantes 25 e 27, demonstraram não ter grande conhecimento da configuração do equipamento que utilizam. Todos consideram que o furto de dados e informações afetaria a credibilidade da instituição. No entanto, um dado curioso e contraditório, os participantes que obtiveram o menor índice consideram que a quebra de sigilo da informação afetaria a credibilidade da instituição, ao contrário dos participantes que obtiveram os melhores scores, que responderam que a quebra de sigilo não afetaria a credibilidade na Câmara Municipal de Criciúma. Isso demonstra fragilizado o princípio da confidencialidade descrita por Ferreira (2021) e também os níveis de proteção da informação, como “intimidade” e “secreto”, da teoria dos círculos concêntricos de Hubmann (DA MOTA; TENA, 2020). Os níveis representam o grau de publicidade que as informações podem alcançar, conforme a própria vontade do indivíduo. Os dois níveis apontados representam aqueles de maior sigilo, proibindo pessoas não autorizadas de acessar informações que não lhe são devidas.

Desconhecer as diretrizes para classificação da informação é consenso entre os melhores e os piores escores. Por mais que se trate de uma instituição pública, sujeita às regras de transparência, há informações nas bases de dados que estão sujeitas aos Princípios descritos por (BRASIL, 2018), como as pessoais e dados de saúde.

A consciência de que os meios de informação incidem em uma série de responsabilidades morais e éticas**,** torna os usuários **responsáveis** por estar vigilantes a tudo que se passa nos sistemas que utilizam. Dentre os melhores escores 6 e 4, ficou constatado que sempre atuam no sentido de comunicar aos seus colegas ou setores responsáveis, caso identifiquem um ataque a computadores. Esse comportamento, por outro lado não se manifestou nos participantes 25 e 27. Hanoff e Nielsen (2020) descrevem a importância da adoção de Sistema de Governança, de modo a conscientizar a todos, para evitar casos

como dos participantes em destaque (25 e 27), que dizem desconhecer suas responsabilidades relacionadas à segurança da informação.

O comportamento adotado pelos indivíduos, que integram uma organização é permeado e influenciado pela cultura organizacional da mesma. A **ética** envolvida nas relações humanas deve validar este sentimento e afastar fraude como da Enron relatados por Silva, Ott e Nascimento (2008), constando práticas de atos reprováveis como adulteração de dados, podendo ser usado para fins estelionatários. Assim, como a tecnologia traz facilidades, ela também expõe os usuários ao roubo de suas identidades virtuais. Os participantes da pesquisa que obtiveram melhores escores se mostraram atentos em desligar suas estações de trabalho ou bloquear seus computadores quando se ausentarem do seu posto de trabalho. Da mesma maneira, os participantes 6 e 4 afirmaram sempre alertar seus colegas da necessidade de proteger seus documentos. Esse tipo de comportamento é nulo nos participantes com menores escores.

Ainda, no quesito ética, um fato curioso é que os participantes 6 e 4, com os maiores escores, demonstraram sempre tratar de assuntos de trabalho em ambientes fora dos seus gabinetes, ação indesejada. Este comportamento pode revelar particularidades sensíveis do ambiente de trabalho, que não devem ser divulgados ostensivamente. Já, os participantes 27 e 25 responderam que têm o cuidado em não expor assuntos sensíveis desta natureza, em locais como ônibus, táxis, elevadores, bares e etc. Por mais que a transparência pública seja incentivada pela LAI (BRASIL, 2011)[15], isto não quer dizer que há um “alvará” para tratar assuntos de natureza pública, portanto cuidados devem ser tomados.

A gestão de segurança organizacional deve ser dinâmica, global e democrática. Deve se basear na avaliação de riscos do uso da informação. Assim como os colaboradores são os elementos responsáveis por resguardar os dados de uma organização, eles também representam vulnerabilidade à segurança. Por isso, a gestão de segurança deve ser traduzida num plano com participação democrática de todos e envolta da cultura organizacional da instituição que a adotará. No quesito

[15] Em tese, todos os assuntos tratados em uma Câmara de Vereadores são públicos.

gestão de segurança e democracia ficou bastante evidente o senso de pertencimento dos participantes 6 e 4. Eles demonstraram sempre planejar, avaliar, e aperfeiçoar todas as tarefas necessárias, a fim de cumprir determinado projeto. Os participantes 25 e 27, ilustraram não praticar gestão de segurança eficaz, pois responderam que nunca tomam cuidado na etapa de planejamento, execução e monitoramento de projetos dos seus departamentos. Retomando o termo "pertencimento", a governança corporativa requer que se envolva o relacionamento entre os servidores da Casa Legislativa (IBGC, 2015), pois eles representam as partes interessadas da instituição em análise.

A **avaliação de risco** é um subconjunto de ações que deve pertencer um plano de segurança da informação. Convém que a organização mapeie riscos, avaliando os potenciais impactos que possam causar à instituição. O guia *Project Management Body of Knowledge* (PMBOK) possui uma área de conhecimento chamada de Gerenciamento de Riscos do Projeto. Considera que os riscos devem ser mapeados, categorizados e aqueles julgados prioritários devem receber tratamento adequado. As possíveis ações a um risco são: resolvê-lo; mitigá-lo; transferi-lo ou aceitá-lo.

Neste jaez, Anderson (2003) fala do equilíbrio que a segurança da informação deve ter entre o risco e as ações de controle. Contudo, esta pesquisa demonstrou que: não há preocupação com as cópias de segurança de dados (*backups*) e, não há muita preocupação com a procedência de e-mails e seus anexos.

Há a orientação, nas "Informações de Autenticação" (ISO/IEC 27.002:2022), que a composição de senhas deve obedecer a critérios para dificultar a descoberta da mesma. Este é o caso do participante número 4, que afirmou frequentemente trocar sua senha, além de incluir caracteres especiais na composição da chave. Afinal, em um ambiente com intenso uso de mídias sociais por pessoas públicas é importante que os usuários tenham o hábito de proteger suas estações de trabalho e dispositivos móveis com senhas fortes, pois já houve histórico de sequestro de perfis.

Ainda, na sequência da gestão de segurança organizacional e avaliação de risco, o **projeto de segurança e implementação** está na esteira dessas duas facetas. Uma delas trata da questão dos grupos de processos existentes no guia PMBOK, pois ao iniciar um projeto, todas as partes interessadas devem participar de sua elaboração, conforme política de segurança, seguir com o planejamento, monitorar o projeto, documentar a reavaliação para identificar oportunidades de melhoria. A pesquisa demonstrou que os participantes com melhores escores têm o hábito de sempre formalizar ao término de uma atividade do projeto, para uso futuro. Enquanto que, os participantes com menores scores responderam que raramente o fazem. É importante observar que dentro da casa Legislativa toda execução das atividades obedece ao rito regimental. Os processos dão entrada nos gabinetes, são revisados pelo setor de Legística, votados em plenário e encaminhados ao Poder Executivo. O sistema de GED registra todas essas informações para consulta, via *web*, mostrando-se satisfatoriamente alinhado com o conceito de transparência ativa descrita pela LAI (BRASIL, 2011).

Para concluir o ciclo *Plan, Do, Check, Act* (PDCA) a **reavaliação** figura de modo a rever, reavaliar e modificar todos os aspectos de segurança para lidar com esses riscos que estão em constante evolução. Neste quesito, o curioso é que somente o participante número 4 respondeu que sempre reavalia as suas atitudes, revelando que os demais não têm o hábito nem de revisar, participar ou reavaliar suas atitudes com respeito à segurança da informação. É possível que isso ocorra em decorrência do cumprimento ao rito regimental da casa, em atender as demandas dos cidadãos, depositando a preocupação da reavaliação a cargo da administração/presidência.

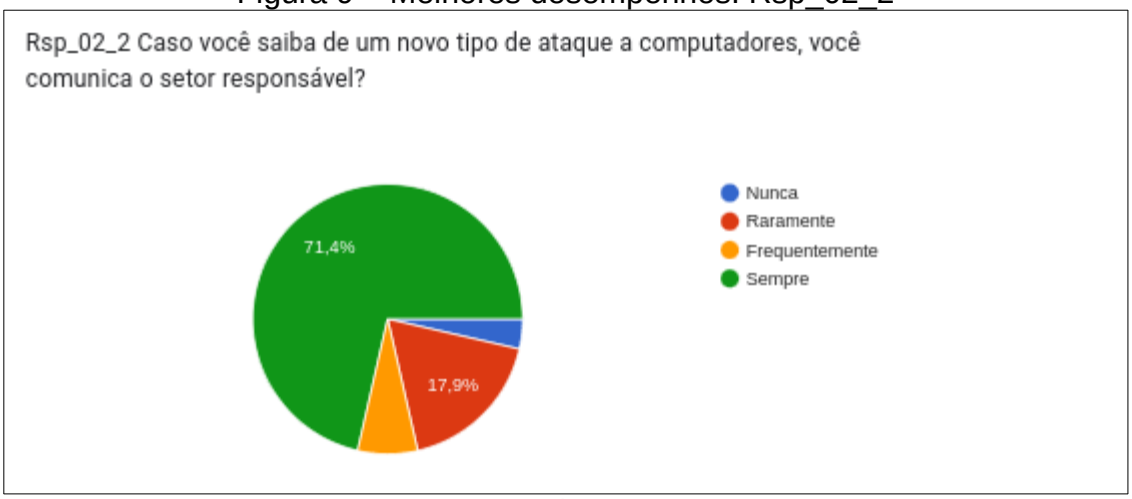
A partir de agora, parte-se para a interpretação do nível global fornecido pela ferramenta de pesquisa. Ao analisar a Tabela 7, 27 respondentes encontram-se no Nível 3 – Encaminhado, enquanto que 1 respondente está no Nível 2 – Em Evolução.

A Tabela 6 serve como referência para interpretar o valor global do índice de cultura de segurança da informação na Câmara Municipal de Criciúma. Como há

mais de 30% enquadrados no nível “3” e menos que 20% nos níveis “0”, “1” ou “2”, então a organização encontra-se no Nível 3 – Encaminhado.

Entre os itens que alavancam um score positivo, na Figura 9 há o destaque daqueles que obtiveram esse índice. Ficou claro que a maioria, 71,4% (20), sempre comunicaria casos de ciberataque ao setor responsável.

Figura 9 – Melhores desempenhos: Rsp_02_2



Fonte: Próprio autor.

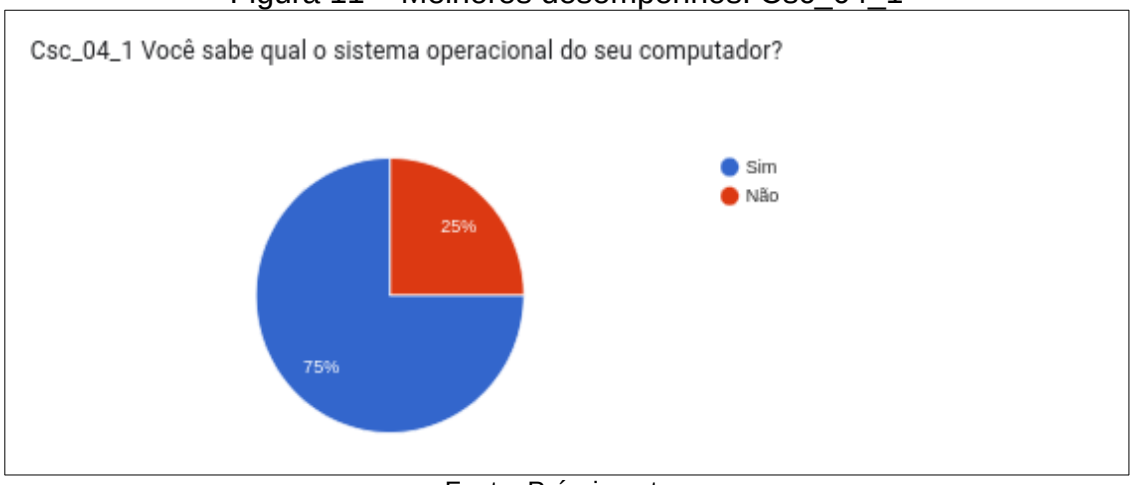
Todos os colaboradores da Câmara Municipal de Criciúma, independentemente de exercer cargos políticos ou administrativos, tem consciência que haverá impacto caso haja furto de dados e informações, como mostra a Figura 10:

Figura 10 – Melhores desempenhos: Csc_03_7

Fonte: Próprio autor.

Segundo a Figura 11, a ampla maioria, 75%, conhece o sistema computacional que opera. Apenas 7 relataram desconhecer qual o sistema operacional de suas máquinas.

Figura 11 – Melhores desempenhos: Csc_04_1



Fonte: Próprio autor.

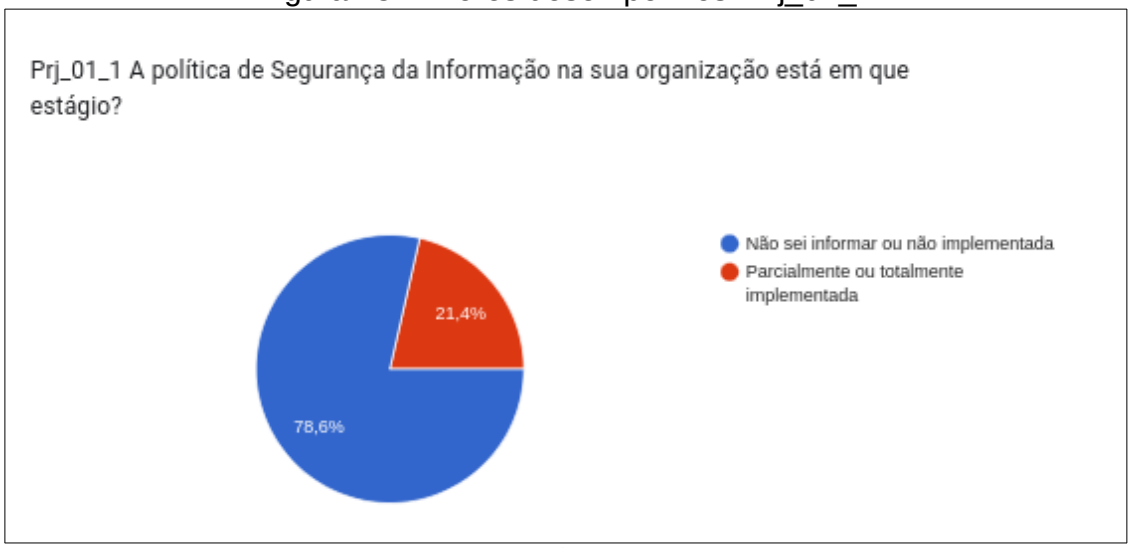
Por outro lado, há aqueles itens que demonstraram as fraquezas da instituição e que apontam para as oportunidades de melhoria. A inexistência de política de segurança da informação faz com que somente 7,1% conheçam procedimentos e diretrizes para a classificação da informação (Figura 12):

Figura 12 – Piores desempenhos: Csc_06_1

Fonte: Próprio autor.

Como dito, a instituição sequer possui política de segurança da informação, o que é constatado por 78,6% dos respondentes (Figura 13).

Figura 13 – Piores desempenhos: Prj_01_1



Fonte: Próprio autor.

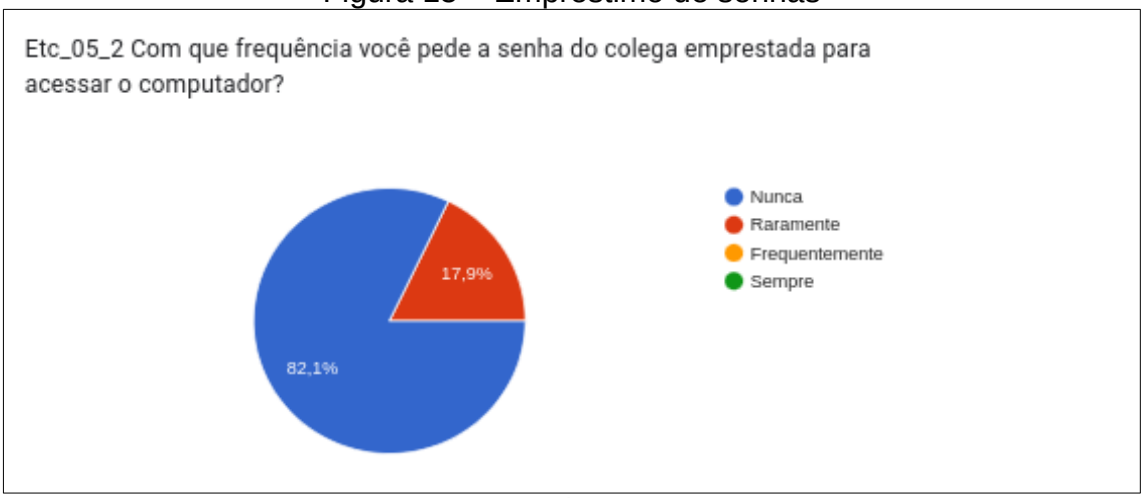
Outro hábito que merece atenção é a periodicidade de troca de senhas, pois a soma daqueles que nunca (7,1%) ou raramente (75%) alteram senhas alcançou 82,1% (Figura 14):

Figura 14 – Piores desempenhos: Rsc_12_1

Fonte: Próprio autor.

Mesmo que poucas pessoas tenham o hábito de trocar as suas senhas periodicamente, esta pesquisa teve a curiosidade de saber se os servidores emprestam as suas senhas para os colegas. Constatou-se que 82,1%, 23 participantes, nunca emprestaram suas senhas. Não houve respostas “Sempre” ou "Frequentemente", por outro lado, este hábito requer conscientização, pois se sabe que é praxe comum entre os gabinetes dos vereadores (Figura 15).

Figura 15 – Empréstimo de senhas



Fonte: Próprio autor.

A função Legislativa requer mobilidade dos agentes políticos - assessores e vereadores. Um exemplo são as ferramentas de agenda sincronizadas que auxiliam a atividade do vereador - em campo - e do assessor - no gabinete. Esta pesquisa procurou levantar o índice de uso de celular próprio para trabalho (Figura 16). Se for considerada a soma das respostas “Sempre” ou “Frequentemente”, chega-se a 92,9%. É um número elevado de dispositivos alheios ao controle patrimonial da instituição. Podem representar um risco, pois não há garantias que estes equipamentos contem com *softwares* de segurança, ratificando a necessidade de implementar controles na cadeia de segurança da informação, no aspecto mobilidade.

Figura 16 – Uso de celular próprio

Fonte: Próprio autor.

De maneira geral, a compreensão dos servidores quanto à LGPD demanda cuidado especial, pois há dicotomia dos dados obtidos nesta avaliação. Destaca-se que a soma dos que dizem não considerar a LGPD nas suas atividades[16] chega a 53,6%. Em situação oposta, a soma dos que se consideram levá-la em consideração[17] é de 46,4% (Figura 17).

Figura 17 – Aderência LGPD

Fonte: Próprio autor.

16 Trata-se da soma daqueles que responderam “Nunca” ou “Raramente”.
17 Trata-se daqueles que responderam “Sempre” ou “Frequentemente”.

Em tese, apesar da margem estreita, aqueles que se preocupam estão em minoria. Há necessidade de reforçar o trabalho de conscientização, por meio de uma política de segurança da informação ajustada à organização.

4.2 SIMILARIDADES DA FERRAMENTA E A LGPD

A construção da ferramenta de Araújo, defendida em 2018, não considerou o projeto de lei da LGPD. Isso não os faz desconectados entre si, pois seus princípios seguem as mesmas premissas. É adequado afirmar que há simetria entre os quesitos existentes, os itens de análise e as exigências da LGPD.

O nível alcançado pela Câmara Municipal de Criciúma foi o Nível 3 – Encaminhado. A ferramenta descreve os comportamentos esperados dentro deste nível, à égide das facetas: consciência; democracia; ética; gestão de segurança; projeto de segurança e implementação; resposta; análise de risco e reavaliação. A seguir, há a relação existente entre as características descritas por Araújo (2018), dentro considerando cada faceta e o texto da LGPD.

a) **Faceta Consciência**: as partes interessadas devem estar cientes da necessidade de ações visando a garantia da segurança da informação.

   LGPD

   - Art. 50°, §2°, inciso I, alínea “a”: demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais;

b) **Faceta Democracia:** há evidências de valores como liberdade, troca de ideias, pensamentos, livre fluxo de informações e confidencialidade da informação, ainda que proporcione a abertura dos dados, na forma da transparência.

   LGPD

   - Art. 2°, inciso I: o respeito à privacidade;

- Art. 2°, inciso III: a liberdade de expressão, de informação, de comunicação e de opinião;
- Art. 2°, inciso VII: os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais;
- Art. 6° 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;
- Art. 6° inciso VI: 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;
- Art. 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.

c) **Faceta Ética:** promove-se que os participantes reconheçam a necessidade de segurança da informação.

LGPD

- Art. 50°, § 2°, inciso II: demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei.

d) **Faceta Gestão de Segurança**: a organização cumpre os requisitos que subsidiam uma boa governança.

LGPD

- Art. 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;

e) **Faceta Projeto de Segurança e Implementação**: há um conjunto de políticas de segurança, mesmo que não completamente implantadas, contando com reavaliação periódica.

LGPD

- Art. 50°, §2°, inciso I, alínea “d”: estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade;
- Art. 50°, §2°, inciso I, alínea “h”: seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

f) **Faceta Resposta:** os colaboradores sempre comunicam a presença de pessoas estranhas ao local de trabalho, reduz-se o risco de acesso indevido, furto de dados ou até mesmo instalação de *malwares* nas estações de trabalho.

LGPD

- Art. 50°, §2°, inciso I, alínea “g”: conte com planos de resposta a incidentes e remediação;

g) **Faceta Análise de Risco:** mitigar todas as atitudes dos colaboradores que colocam a organização em risco.

LGPD

- A ferramenta aponta a necessidade de mitigar riscos na organização em todos os aspectos, sejam dados pessoais, política de senhas, descarte de dados (mídias, CD´s, DVD´s,…), receptação de arquivos,

cuidados com antivírus. A LGPD considera o risco advindo do vazamento somente do “dado pessoal”;

h) **Faceta Reavaliação:** igualmente como a Faceta Projeto de Segurança e Implementação, a organização precisa revisar rotineiramente suas políticas, para não se tornar ineficiente.
LGPD: Art. 50°, §2°, inciso I, alíneas “d” e“h”[18].

4.3 QUESTÕES ESPECÍFICAS DO PODER LEGISLATIVO

Para Igarashi (2021) a liberdade de atuação parlamentar é a condição necessária para a independência do Poder Legislativo e a concretização do princípio da separação dos poderes. A Constituição Federal institui prerrogativas e proibições, e, embora o legislador possa sobrepô-las, na forma da imunidade parlamentar, não se trata de uma vantagem pessoal, mas de uma condição necessária ao exercício do mandato.

Constitucionalmente, o Poder Legislativo tem o papel de criar leis e fiscalizar o Poder Executivo. O multipartidarismo fomenta a participação democrática e, ao mesmo tempo, cria unidades organizacionais isoladas dentro do Poder, independentes e autônomas entre si. Como exemplo estão os Gabinetes, Comissões Permanentes, Comissões Temporárias, Frentes Parlamentares e Comissões Parlamentares de Inquérito.

O Legislativo conta com a livre atuação, sem subserviência ao Poder Executivo. Cumpre o papel de mediador de conflitos, num sistema de freios e contrapesos. A livre atuação parlamentar implica a produção de dados pessoais assim como a obtenção durante sua atividade fiscalizadora. Esta ideia é reforçada por Lara (2021 *apud* IGARASHI, 2021, p. 24) quando escreve que “nessas hipóteses, todo o processo de manipulação de dados pessoais, desde a coleta até a eventual destruição, é realizado pelo próprio parlamentar ou integrantes de seu gabinete, sem a interferência da Casa Legislativa.”.

[18] Idem ao contido em “Projeto de Segurança e Implementação.

Embora os vereadores não sejam imunes à incidência da Lei, o cumprimento do seu dever constitucional justifica o tratamento dos dados pessoais dentro de sua estrutura administrativa autônoma.

Igarashi (2021) relata que a maioria dos parlamentos não regulamentou a LGPD, alguns apenas designaram o encarregado de dados ou instituíram grupos de trabalho destinados à adequação da Lei. Portanto abre-se uma oportunidade de fazê-lo, tomando em consideração as peculiaridades deste Poder.

4.4 DIAGNÓSTICO

A Câmara Municipal de Criciúma, semelhante à maioria das Casas Legislativas, ainda não regulamentou a aplicação das diretrizes e normas para atender a LGPD. A obtenção do nível de Cultura Organizacional de Segurança da Informação é o primeiro passo para diagnosticar em que posição ela se encontra, permitindo traçar o caminho para alcançar tal objetivo.

A revisão sistemática de literatura, reforçada por artigos complementares, ajudou a apontar sugestões que certamente elevarão o nível de segurança da informação, como colocarão a referida instituição em condições de atender as exigências que a lei exige.

Por exemplo, Moreira (2020) questiona o alcance da LGPD com relação à função administrativa pública. Pacheco Júnior (2020) retoma a mesma preocupação em uma tentativa de justificar que no “exercício do interesse público”, os órgãos e governo poderão ficar alheios à LGPD.

Igarashi (2021) trouxe a experiência da implementação da LGPD na Câmara Municipal de São Paulo. Mostrou que os gabinetes e vereadores constituem unidade autônoma de tratamento de dados e apontou a alternativas para conciliar a atividade legislativa com a referida lei.

Desta forma, a seguir estão descritos os apontamentos observados nessa pesquisa. Obviamente, não há pretensão de ações impositivas, tão pouco vislumbrar que os itens enumerados esgotarão todas as ações passíveis de implementação.

4.4.1 Elaboração de Política de Segurança da Informação

Convém que a Câmara Municipal de Criciúma defina uma política de segurança da informação, em conformidade com (BRASIL, 2020). A política deve ser devidamente aprovada pelo plenário da casa, divulgada entre os servidores e órgãos externos, com quem mantenha contato institucional. Convém que essa política dê autonomia aos gabinetes da casa, facultando a eles a opção de quem será o controlador de dados.

4.4.2 *Bring Your Own Device* (BYOD)

Convém que a política e segurança da informação da Câmara Municipal de Criciúma conte com capítulo dedicado aos procedimentos de segurança com dispositivos móveis próprios dos funcionários, aqueles empregados nas atividades laborativas. Já há diversas soluções no mercado, de softwares destinados a gerenciá-los, monitorando os riscos que possam trazer a infraestrutura tecnológica da instituição.

4.4.3 Definição do Encarregado de Dados

Convém que a Câmara Municipal de Criciúma defina seu encarregado de dados, conforme Art. 41° da LGPD. Ele será responsável por criar os processos de comunicação internos, controlando as petições, Art. 18°, e controlando os prazos previstos no Art. 19°, quando da solicitação de informações pelo munícipe. Ele é o responsável por prover os meios para criar, manter e atualizar o mapeamento de dados pessoais e o relatório de impacto de dados pessoais (RIDP).

4.4.4 Elaboração do mapeamento de dados pessoais

Convém que a Câmara Municipal de Criciúma crie o mapeamento de dados pessoais nos setores administrativos da Casa, para cumprir o disposto das obrigações do controlador de dados pessoais, na forma do Art. 37°.

Envolver os departamentos é imprescindível, pois os servidores atuam elucidando as especificidades de cada setor (Departamento de Pessoal, Secretaria, Assessoria Jurídica, Informática, Compras e Licitações, Contabilidade, Arquivo, Legística e TV Câmara).

4.4.5 Validação das questões de Arquivo

Convém conferir se o Arquivo da Casa adequa-se aos princípios previstos nos incisos III, IV e VI do Art. 6° da LGPD. Tratam da necessidade[19], o livre acesso e transparência. Traduzem-se no tempo de guarda, acesso facilitado e gratuito, bem como integralidade e acessibilidade aos dados.

4.4.6 Validação de contratos

Convém que a Assessoria Jurídica revise os contratos existentes na Casa a fim de identificar os agentes de tratamento e firmando os compromissos do uso compartilhado de dados pessoais.

4.5 LIMITAÇÕES DA PESQUISA

Por mais que a participação dos assessores e funcionários da Câmara Municipal de Criciúma seja voluntária, pode haver uma tendência de respostas chamadas “falsos” positivos. Contudo, medidas foram tomadas para tornar o

[19] Este princípio possui estreita ligação com a tabela de temporalidade, já existente nos órgãos públicos detentores de Arquivo. A tabela descreve o tempo de guarda de documentos, conforme seu tipo, destinação final e atividade-fim para a entidade ou órgão. É uma exigência que seja elaborada, aprovada e publicada. O tema é regido pelo Conselho Nacional de Arquivo (CONARQ).

questionário atrativo, ele contou com 58 itens, buscando evitar desistências por falta de interesse em completá-lo.

Ainda assim, deve-se considerar que o respondente pode responder conforme acredita que a gestão espera, ou seja, com receio de perseguições, buscando a aceitação, é o que se chama de “desejabilidade social”. “Assim sendo, os resultados para mensurar o nível da cultura de segurança da informação na unidade de estudo pode ter sofrido viés devido seu conceito e características de suas reações” (GIANGRECCO, 2002 apud BORTOLOTTI; ANDRADE, 2011).

“Desejabilidade social é a tendência do respondente de escolher a resposta socialmente desejável, politicamente correta para o momento, negligenciando a veracidade da resposta (SPECTOR, 1987, p. 438, tradução nossa).

> Respondem de forma tendenciosa aos itens apresentados em escalas de atitudes e escalas de personalidade, levando a assinalar respostas que são tidas como mais aceitáveis ou aprovadas socialmente, negando sua posição pessoal com comportamentos que seriam desaprovados socialmente (ANASTASI e URBINA, 2000 apud LIGIA; BORTOLOTTI; ANDRADE, 2011).

Os funcionários da Casa Legislativa podem se sentir constrangidos em revelar desconhecimento em LGPD. Os conceitos são novos inclusive para os legisladores, ocorrendo, inclusive, uso político da referida norma para obstrução das ações fiscalizadoras no âmbito municipal.

Os itens que compõem a ferramenta de pesquisa percorrem vasta área de conhecimento, desde técnicas até gerenciais. Nem todos os participantes dominam a linguagem particular de cada caso.

A concepção deste projeto se deu durante uma época em que a ANPD publicou diversas normas regulando os artigos existentes na LGPD. Esta dissertação se limitou a analisar somente os diplomas legais apontados no objetivo de pesquisa.

5 CONCLUSÃO

As informações já são considerados o “novo petróleo” da sociedade informacional. Os dados pessoais são um subconjunto dessas informações e as pessoas têm uma ideia nebulosa do que é a privacidade destes dados. Utilizar dados pessoais não é, na sua essência, o problema, ela viabiliza a execução de várias atividades em infindáveis áreas.

E é assim que acontece no poder público, sua atividade essencial diz respeito a promover políticas públicas, servindo ao cidadão as condições básicas, como saúde educação e segurança. Esta atividade não afere lucro, pelo contrário, obriga que o gestor aplique todo o recurso diretamente em investimentos direta ou indiretamente ligados à sociedade. Portanto, o que resta à administração pública é a obrigação, imposta pela Lei de Acesso à Informação, de prestar contas das ações empreendidas, sem a necessidade de ser provocada para isso. Fatalmente, as informações dos cidadãos figuram no arcabouço telemático dos órgão públicos, suas identidades, renda, ofícios que ocupam, podendo ainda, conter dados sensíveis como saúde, religioso e posição partidária.

O IBGE aponta que o Brasil já alcançou pouco mais de 5.500 municípios, contendo estrutura administrativa composta pelos Poderes Executivo, Legislativo e Judiciário. Legislativos municipais, além de formular leis, fiscalizam o executivo municipal, quando da prestação de contas atinente aos serviços públicos atendidos.

Pouco se sabia sobre a privacidade de dados pessoais até que o ordenamento jurídico passou a contar com a Lei Geral de Proteção de Dados Pessoais (LGPD). É a primeira lei que versa sobre a autodeterminação informativa, fundamento que garante ao titular do dado pessoal, o controle e proteção dos seus próprios dados. Na administração pública, para prestar serviços de toda natureza, não resta dúvida que há crescente necessidade de endereçar corretamente o tratamento dos dados produzidos, para que não reste prejudicada a privacidade e individualidade das pessoas.

Por isso é que se buscou tratar da cultura organizacional em segurança da informação e LGPD na percepção dos servidores do Poder Legislativo. O trabalho de natureza qualiquantitativa, desdobrou os objetivos específicos em uma RSL sobre segurança da informação e LGPD, ainda que sensível aos demais diplomas legais, com temática análoga. Aplicou ferramenta para diagnosticar o nível da cultura organizacional e segurança da informação no Poder Legislativo de Criciúma, e assim, comparar o diagnóstico em segurança da informação com a legislação em vigor.

A resposta à pergunta de pesquisa “Qual o Nível de Cultura de Segurança da Informação do Poder Legislativo de Criciúma e quais possíveis relações poder-se-á estabelecer entre o ente e as diretrizes da LGPD foi respondida. Porquanto, satisfaz-se o objetivo geral de analisar a cultura organizacional de segurança da informação, sob a ótica de servidores do Poder Legislativo de Criciúma, com olhar crítico a similaridades existentes com a LGPD.

O trabalho procurou estabelecer qual o panorama de segurança da informação, na Câmara Municipal de Criciúma, por meio de ferramenta de Araújo (2018). Esta ferramenta utiliza técnicas da psicometria, adota a Teoria de Resposta ao Item, que tem abordagem quantitativa. Constatou-se que a instituição se encontra no nível “encaminhado”, revelando hábitos que já estão incutidos na rotina dos servidores da casa. Eles demonstraram ter consciência da responsabilidade em comunicar aos responsáveis caso tomem conhecimento de ataques cibernéticos ou em avistar invasões nas instalações de trabalho por estranhos. Consideram severo o impacto à organização, caso sofram algum tipo de furto de dados.

Mesmo assim, das 9 facetas de análise, em 4 ficou com desempenho abaixo do esperado. A inexistência de política de segurança da informação foi fator que pesou contra. Esta faceta de análise arrastou outros pontos, de maneira negativa. Constatou-se a falta de classificação da informação. Como efeito, as atividades são executadas baseando-se no conhecimento tácito dos colaboradores, sem uma uniformidade de procedimentos, um fator de risco à organização. A troca frequente de senhas é pouco observada. Adicionado ao fato de que a maioria dos funcionários

utiliza seu próprio *smartphone* para o trabalho, os dispositivos não pertencem ao patrimônio da casa e podem passar ao largo de mecanismos de segurança adequados.

Como toda instituição, a cultura organizacional se baseia em tecnologias, processos e pessoas. Enquanto as tecnologias estão em constante evolução, no aspecto de processos, há de se estabelecer um caminho procedimental para o tratamento de dados pessoais. É onde figura a necessidade de uma política da segurança da informação, adequadamente aprovada, divulgada e conscientizada entre as pessoas que trabalham na Câmara Municipal de Criciúma. A pesquisa elencou as lacunas entre o nível de cultura organizacional em segurança da informação e a LGPD, na forma de um diagnóstico, apontando 6 ações bem delimitadas, que poderão representar oportunidades de melhorias no ambiente proposto.

A ferramenta de Araújo (2018) adotada é muito assertiva para a tarefa a que se destina. Conta com uma variedade de itens (categorizados em dimensões/facetas), oriundos dos princípios do Organismo de Cooperação e Desenvolvimento Econômico (OCDE) e da família de padrões, que são internacionalmente conhecidos na segurança da informação, ISO/IEC 27.000. Constatou-se que a ferramenta se alinha com o diploma legal positivado na forma da Lei 13.709 – Lei Geral de Proteção de Dados Pessoais (LGPD), pois ambas se debruçam sobre os mesmos princípios de segurança. Para essa análise, a pesquisa comparou as facetas da ferramenta com o texto da LGPD.

Diante disso, descobriu-se peculiaridades nesta Lei, quando adotadas no ambiente de pesquisa ora apresentados. A LGPD dedica uma seção versando sobre sanções para aqueles que descumprirem à norma legal. Partem desde advertência até multas de alto valor. O que acontece é que o poder público fica albergado em condições que o afasta de tais sanções. De certa forma, para a “consecução de políticas públicas”, devidamente regulamentados, a custódia de dados pessoais independe do consentimento do titular dos mesmos, desconstruindo a ideia de que a pessoa natural ou jurídica tem absoluta autonomia sobre os seus dados.

Outro fator peculiar é que a atividade legislativa gera, necessariamente, unidades autônomas de tratamento de dados pessoais - elas se amoldam nos Gabinetes, Comissões Permanentes, Comissões Temporárias, Frentes Parlamentares e Comissões Parlamentares de Inquérito. Formam-se devido à inerente função fiscalizadora do edil. Por isso, as políticas de segurança que envolvem dados pessoais podem ficar descentralizadas por gabinetes, nos casos das casas legislativas.

Replicar a análise desta dissertação é perfeitamente viável em outras Câmaras de Vereadores[20], não somente para diagnosticar a segurança da informação, mas para alertar o real valor dos dados armazenados em suas estruturas. A simples aplicação de uma ferramenta de diagnóstico liga o alerta nos servidores da Casa, que lidam com informações, dentre elas os dados pessoais. Os integrantes da Câmara Municipal de Criciúma passaram a reavaliar suas rotinas, adotando práticas mais responsáveis no dia a dia.

A adequação dos órgãos públicos à LGPD é imperiosa. O percurso inicia por um diagnóstico assertivo do estado em que a organização se encontra, para saber onde se quer chegar. Como sugestão de trabalho futuro, há a oportunidade de inclusão de itens na ferramenta de análise, que a faça apontar diretamente para a segurança da informação à égide da LGPD. A privacidade de dados pessoais deve trilhar o princípio norteador desta tarefa, com olhar à possibilidade de replicação do estudo em outros órgãos públicos de mesma natureza desta dissertação.

Outra sugestão é a incipiência da LGPD em atingir a administração pública. É oportuno aprofundar mais este tema, com literatura mais robusta, estabelecendo uma relação de causa/efeito e propondo soluções para esta questão.

[20] O uso da mesma ferramenta, em ambiente análogo ao desta pesquisa, exigiria exígua necessidade de alterações.

REFERÊNCIAS

ACOCELLA, J.; SAMPAIO, R. Impactos da LGPD sobre a atuação da administração pública: alguns desafios e sua efetividade. In: DAL POZZO, A. N.; MARTINS, R. M. (Eds.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters, 2020. p. 359–376.

ANDERSON, J. M. Why we need a new definition of information security. **Computers and Security**, v. 22, n. 4. Disponível em : http://www.sciencedirect.com/science/article/pii/S0167404803 004073., p. 308–313, 2003.

ARAUJO, P. H. DE M. **Construção da Escala do Nível da Cultura Organizacional de Segurança da Informação**. 2018. 205 f. Tese (Doutorado) - Programa de Pós-Graduação em Engenharia de Produção, Universidade Federal de Santa Catarina, Florianópolis, , 2018. Disponível em: <https://repositorio.ufsc.br/handle/123456789/191171>

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001: Sistemas de gestão da segurança da informação Requisitos**. 2. ed. Rio de Janeiro: ABNT, 2013.

AYALA-RIVERA, V.; PASQUALE, L. The grace period has ended: An approach to operationalize GDPR requirements. **Proceedings - 2018 IEEE 26th International Requirements Engineering Conference, RE 2018**, p. 136–146, 2018.

BAKER, F. B. **The Basics of Item Response Theory**. 2. ed. Wisconsin: ERIC Clearinghouse on Assessment and Evaluation, 2001.

BERNARDES, M. B.; DE ANDRADE, F. P.; NOVAIS, P. **Data protection in public sector: Normative analysis of portuguese and brazilian legal orders**. (A. Rocha et al., Eds.)8th World Conference on Information Systems and Technologies, WorldCIST 2020. **Anais**...Braga: Springer, 2020. Disponível em: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85086254440&doi=10.1007%2F978-3-030-45691-7_76&partnerID=40&md5=92191047f01d005e2a91c37396cf9b55>

BRASIL. **Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do Art. 5º.** , 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>

BRASIL. **Lei n° 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoas.** , 2018. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>

BRASIL. Guia de boas práticas da LGPD. In: [s.l: s.n.].

BRASIL. **Lei nº 14.129, de 29 de março de 2021. Dispõe sobre princípios, regras e instrumentos para o Governo Digital e para o aumento da eficiência pública.** , 2021. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14129.htm>

CANEDO, E. D. et al. Perceptions of ICT practitioners regarding software privacy. **Entropy**, v. 22, n. 4, p. 1–23, 2020.

DA MOTA, I. D.; TENA, L. P. Fundamentos da LGPD: Círculos concênctricos e sociedade de informação no contexto de direitos da personalidade. **Revista Juridica**, v. 2, n. 59, p. 538–576, 2020.

DA VEIGA, A.; ELOFF, J. H. P. An information security governance framework. **Information Systems Management**, v. 24, n. 4, p. 361–372, 2007.

DE SOUSA, R. P. M. et al. Necessidades de informação do operador do direito como usuário do processo judicial eletrônico no estado da Paraíba. **Perspectivas em Ciencia da Informacao**, v. 22, n. 1, p. 186–201, 2017.

DE SOUSA, R. P. M.; DA SILVA, P. H. T. Proteção de dados pessoais e os contornos da autodeterminação informativa. **Informacao e Sociedade**, v. 30, n. 2, p. 1–19, 2020.

FERRÃO, S. É. R. et al. Diagnostic of data processing by brazilian organizations—a low compliance issue. **Information (Switzerland)**, v. 12, n. 4, 2021.

FERREIRA, F. J. **Cultura Organizacional De Segurança Da Informação, Privacidade E Proteção De Dados: Estudo de caso em instituições financeiras cooperativistas**. [s.l.] Universidade Federal De Santa Catarina, 2021.

GUNTHER, L. E.; COMAR, R. T.; RODRIGUES, L. E. **A proteção e o tratamento dos dados pessoais sensíveis na era digital e o direito à privacidade: Os limites da intervenção do estado**. Relações Internacionais no Mundo Atual. **Anais**...Curitiba: Centro Universitário Curitiba - UNICURITIBA, 2020. Disponível em: <http://revista.unicuritiba.edu.br/index.php/RIMA/article/download/3972/371372300>

HANOFF, R. V.; NIELSEN, T. H. A Lei Geral de Proteção de Dados Pessoais na administração pública brasileira: é possível implementar governança de dados antes de se implementar a governança em gestão? In: DAL POZZO, A. N.; MARTINS, R. M. (Eds.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters, 2020. p. 391–406.

IGARASHI, R. T. **LGPD: a figura do controlador no poder legislativo**. **Revista Procuradoria da Câmara Municipal de São Paulo,**São Paulo, v. 9, n. 1, p. 15-28, dez., 2021. Disponível em: <http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/2022_Periodicos/Revista-Procuradoria-n.09.pdf.Acesso em: 16 dez. 2022.>

INSTITUTO BRASILEIRO DE GOVERNANÇA CORPORATIVA. **Código das Melhores Práticas de Governança Corporativa**. 5. ed. Sao Paulo: Instituto Brasileiro de Governança Corporativa, 2015.

JUNIOR, F. G. P. O tratamento de dados pessoais pelo setor público e o alcance da LGPD. In: DAL POZZO, A. N.; MARTINS, R. M. (Eds.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters, 2020. p. 311–320.

LARAIA, R. D. B. **Cultura: um conceito antropológico**. 14. ed. Rio de Janeiro: [s.n.].

LIGIA, S.; BORTOLOTTI, V.; ANDRADE, D. F. DE. Resistência À Mudança Organizacional : Avaliação de Atitudes e Reações em Grupo de Indivíduos. **VIII Simposio de Excelência em Gestão e Tecnologia**, 2011.

MATTAR, F. N. **Pesquisa de Marketing:** Metodologia, Planejamento, Execução e Análise. 7. ed. São Paulo: Atlas, 2013.

MOREIRA, P. P. Tratamento e uso compartilhado de dados pessoais pela administração pública na execução de políticas públicas. In: DAL POZZO, A. N.;

MARTINS, R. M. (Eds.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters, 2020. p. 275–292.

OLIVIA, L.; RAMOS, L.; FERREIRA, R. A. Sobre uma práxis interdisciplinar: aproximações e proposições conceituais. **Revista Brasileira de Estudos Pedagógicos**, v. 101, n. 257, p. 197–216, 2020.

PARSONS, K. M. et al. The influence of organizational information security culture on information security decision making. **Journal of Cognitive Engineering and Decision Making**, v. 9, n. 2, p. 117–129, 2015.

PRESSMAN, R. **Engenharia de Software**. 6. ed. São Paulo: Makron, 2006.

REGAN, P. M.; JESSE, J. Ethical challenges of edtech, big data and personalized learning: twenty-first century student sorting and tracking. **Ethics and Information Technology**, v. 21, n. 3, p. 167–179, 2019.

RIBEIRO, G. B. Compatibilidade entre a proteção de dados pessoais e o dever de transparência pública. In: DAL POZZO, A. N.; MARTINS, R. M. (Eds.). **LGPD & Administração Pública**. São Paulo: Thomson Reuters, 2020. p. 293–309.

SCHEIN, E. H. **Organisational culture and leadership**. 3. ed. San Francisco: Jossey-Bass, 2004.

SILVA, L. M.; OTT, E.; NASCIMENTO, A. M. Lei Sarbanes-Oxley e Código Civil: os efeitos nos procedimentos de controle adotados por empresas localizadas no Brasil. **Revista do Conselho Regional de Contabilidade do Rio Grande do Sul**, v. 133, n. mar., p. 16–29, 2008.

SPECTOR, P. E. Method variance as an artifact in self-reported affect and perceptions at work: Myth or significant problem? **Journal of Applied Psychology**, v. 72, n. 3, p. 438–443, 1987.

UFSC. **Linhas de Pesquisa**. Disponível em: <https://ppgtic.ufsc.br/linhas-de-pesquisa/. Acesso em 18 Jan. 2023.>.

Termo de Consentimento Livre e Esclarecido - TCLE
Título: Cultura organizacional e LGPD na percepção de servidores do Poder Legislativo: discussão de similaridades com o diploma legal

Olá!

Você está sendo convidado, autorizado pela Presidência desta Casa Legislativa, a participar de uma pesquisa que auxiliará na elaboração da minha dissertação de Mestrado, na linha de Tecnologia, Gestão e Inovação, do Programa de Pós-Graduação em Tecnologia da Informação e Comunicação (PPGTIC), da Universidade Federal de Santa Catarina (UFSC).

O objetivo desta pesquisa é analisar a cultura organizacional em segurança da informação, no Poder Legislativo de Criciúma/SC, com olhar crítico às similaridades existentes com a Lei Geral de Proteção de Dados Pessoais (LGPD). Com isso, o benefício almejado é de levantar aspectos organizacionais que podem ser aperfeiçoados no sentido de atender segurança da informação e a Lei Geral de Proteção de Dados Pessoais.

Entende-se por cultura organizacional em segurança da informação, todas as atitudes de um grupo para mitigar os riscos quando do uso de dados em uma organização. Uma governança de segurança da informação na organização, com o envolvimento da alta gerência incentiva os colaboradores a adotarem comportamentos éticos adequados e a cumprirem os padrões organizacionais destinados a esse fim.

Entende-se por Lei Geral de Proteção de Dados Pessoais, Lei N° 13.709, um diploma legal que implementa alguns dos controles alinhados à cultura organizacional em segurança da informação, por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados.

Mapeamos alguns riscos ligados a esta etapa, a saber:

Risco: O sigilo da identidade dos participantes.

Ação de controle: A coleta de dados serão em formulário físico, sem campo de identificação do participante. As respostas serão agrupadas e apresentadas estatisticamente, exibindo somente valores agregados;

Risco: Descontinuidade de participação por motivos diversos.

Ação de controle: Os formulários serão entregues aos participantes, em meio físico impresso. Será estipulado um cronograma de preenchimento e acompanhamento/ajuda do pesquisador, caso necessário;

Risco Perda/descarte dos formulários de resposta.

Ação de controle: Os formulários deverão permanecer no ambiente organizacional da Câmara, durante o preenchimento. Os formulários permanecerão arquivados com o pesquisador, por 5 anos e serão destruídos, em conformidade à Resolução 466/2012.

Não há obrigação de responder todas as perguntas, sendo possível desistir a qualquer momento. Mesmo assim, incentivamos que responda todas as questões, da maneira mais realista possível. Dessa forma, é essencial que considere exatamente a realidade vivenciada na Câmara de Vereadores ou no seu gabinete e não, o que seria ideal que ocorresse.

As informações obtidas durante essa pesquisa serão confidenciais e asseguramos o sigilo sobre sua participação. Apenas o pesquisador envolvido nesta pesquisa e sua orientadora terão acesso aos dados. Os resultados ficarão disponíveis no Repositório Institucional da UFSC. O participante terá acesso ao registro do consentimento sempre que soli-

citado. Serão indenizados os danos, desde que comprovadamente oriundos da pesquisa, nos termos da lei. As despesas decorrentes da pesquisa, como alimentação e transporte, desde que devidamente comprovadas pelo participante de pesquisa serão ressarcidas. Qualquer informação que possibilite a identificação dos participantes será modificada, garantido a confidencialidade de sua identidade.

Pesquisa submetida ao Comitê de Ética em Pesquisa com Seres Humanos. O CEPSH é um órgão colegiado interdisciplinar, deliberativo, consultivo e educativo, vinculado à Universidade Federal de Santa Catarina, mas independente na tomada de decisões, criado para defender os interesses dos participantes da pesquisa em sua integridade e dignidade e para contribuir no desenvolvimento da pesquisa dentro de padrões éticos. Localiza-se no Prédio Reitoria II, 7º andar, sala 701, Rua Desembargador Vitor Lima, nº 222, Trindade, Florianópolis/SC. Telefone 3721-6094. E-mail: cep.propesq@contato.ufsc.br

Adequação a Lei 13.709/2018 - LGPD: Por se tratar de pesquisa acadêmica, de acordo com o Art. 4º, a Lei não se aplica ao tratamento de dados pessoais:

II - realizado para fins exclusivamente: b) acadêmicos, aplicando-se a esta hipótese os artigos 7º e 11 º desta Lei; aos quais especificam Art. 7 º I - mediante o fornecimento de consentimento pelo titular; Art. 11º I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas.

Mestrando: Lucas Nascimento Martins Camargo da Silva, (UFSC)
http://lattes.cnpq.br/0137879715217286
Câmara Municipal de Criciúma
Rua Cel. Pedro Benedet, 488, 6° Andar, Criciúma/SC
88811-508
(48) 9 9167 1120
martins@camaracriciuma.sc.gov.br

Orientadora: Andréa Cristina Trierweiller, Drª. (UFSC)
http://lattes.cnpq.br/0540194149670095
Universidade Federal de Santa Catarina
Secretaria de Planejamento e Orçamento (SEPLAN)
R. Desembargador Vitor Lima, 222, 7º andar, Sala 702, Bairro Trindade, Florianópolis/SC
88040-400
(48) 3721-4225

O prazo de entrega é no dia _____/_____/_____

ASSINATURAS

_____
Lucas N. Martins C. Silva
Pesquisador

_____
Participante

Nome:_____

DECLARAÇÃO

Câmara Municipal de Vereadores de Criciúma

Declaro para os devidos fins e efeitos legais que, objetivando atender as exigências para a obtenção de parecer do Comitê de Ética em Pesquisa com Seres Humanos, e como representante legal da Câmara Municipal de Vereadores de Criciúma, tomei conhecimento do projeto de pesquisa: "Cultura organizacional e LGPD na percepção de servidores do poder legislativo: discussão de similaridades com o diploma legal.", sob responsabilidade de Lucas Nascimento Martins Camargo da Silva e cumprirei os termos da Resolução CNS 510/16 e suas complementares, e como esta instituição tem condição para o desenvolvimento deste projeto, autorizo a sua execução nos termos propostos.

Criciúma, 02/08/2022

ASSINATURA: .....
NOME: Roseli de Lucca Pizzolo
CARGO: Presidente
CARIMBO DO/A RESPONSÁVEL

CÂMARA MUNICIPAL DE CRICIÚMA
ROSELI DE LUCCA PIZZOLO
Presidente

Cultura Organizacional de Segurança da Informação no Poder Legislativo

1. Com que frequência você verifica se o antivírus do seu computador está atualizado?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

2. Com que frequência você verifica o histórico (relatório) do antivírus do seu computador?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

3. Em sua opinião, qual seria o impacto na sua organização caso ocorresse quebra do sigilo da informação?
( )Nenhum ( )Leve – não afeta a credibilidade ( )Severa – afeta a credibilidade

4. Em sua opinião,qual seria o impacto na sua organização caso ocorresse furto dos dados e informações?
( )Nenhum ( )Leve – não afeta a credibilidade ( )Severa – afeta a credibilidade

5. Você sabe qual o sistema operacional do seu computador?
( )Sim ( )Não

6. Você sabe qual a versão do sistema operacional do seu computador?
( )Sim ( )Não

7. No computador do trabalho, você sabe qual é a quantidade de memória RAM?
( )Sim ( )Não

8. No computador do trabalho, você sabe qual a capacidade de armazenamento do disco?
( )Sim ( )Não

9. No computador do trabalho, você sabe o tipo de conexão do seu computador com a rede?
( )Sim ( )Não

10. Você sabe se sua organização há procedimentos e diretrizes para classificação da informação?
( )Não sei informar ( )Não há classificação ( )Sim, há classificação da informação

11. Caso você saiba de um novo tipo de ataque a computadores, você alerta os colegas de equipe?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

12. Caso você saiba de um novo tipo de ataque a computadores, você comunica o setor responsável?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

13. Caso você saiba de um novo tipo de ataque a computadores, você verifica se seu computador está vulnerável/fragilizado a esse ataque?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

14. Você conhece suas responsabilidades e atribuições relacionadas a Segurança da Informação na Câmara de Vereadores de Criciúma?
( )Não sei informar ( ) Não ( ) Sim

15. Você está no seu local de trabalho e percebe a presença de uma pessoa desconhecida, você comunica à Presidência da Casa?
( )Não ( )Raramente ( )Frequentemente ( )Sempre

16. Com que frequência você trata de assuntos relacionados à sua organização em ambientes como (aviões, ônibus, taxi, elevador, sala de cafezinho, redes sociais, bares, etc.)?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

17. Com que frequência você pede a senha do colega emprestada para acessar o computador?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

18. Com que frequência você costuma alertar os seus colegas sobre a necessidade de desligar o computador quando não estiver em uso?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

19. Com que frequência você costuma alertar os seus colegas sobre a necessidade de bloquear o computador quando sai da sala?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

20. Com que frequência você costuma alertar os seus colegas sobre a necessidade de manter a mesa limpa/organizada?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

21. Com que frequência você costuma alertar os seus colegas sobre a necessidade de proteger os documentos de trabalho de acesso não autorizado?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

22. Durante o processo de manuseio dos dados do Gabinete (agenda, cadastros, dados de pessoas, etc.) você avalia os riscos de danos ou incidentes como, perda, roubo, adulteração e acesso indevido aos dados?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

23. Durante o processo de manuseio dos dados do Gabinete (agenda, cadastros, dados de pessoas, etc.) você planeja a forma, o local, como os dados serão armazenados e acessados levando-se em consideração a avaliação dos riscos?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

24. Durante o processo de manuseio dos dados do Gabinete (agenda, cadastros, dados de pessoas, etc.) você leva em consideração as diretrizes estabelecidas pela sua organização no planejamento?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

25. Durante o processo de manuseio dos dados do Gabinete (agenda, cadastros, dados de pessoas, etc.) você executa os processos conforme planejado?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

26. Durante o processo de manuseio dos dados do Gabinete (agenda, cadastros, dados de pessoas, etc.) você avalia-se os procedimentos adotados estão atendendo as necessidades de Segurança da Informação?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

27. Durante o processo de manuseio dos dados do Gabinete (agenda, cadastros, dados de pessoas, etc.) você executa as modificações necessárias para adequar às novas necessidades?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

28. 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 Gabinete/Departamento estimula os colegas a emitirem opiniões, promovendo um ambiente participativo?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

29. Com respeito à cópia de segurança dos seus arquivos de trabalho, com que frequência você realiza cópia de segurança em mídias externas. (CD, DVD, nuvem, *pendrive*, etc.)?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

30. Com respeito à cópia de segurança dos seus arquivos de trabalho, com que frequência você verifica se as cópias de segurança estão atualizadas?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

31. Com que frequência você utiliza o celular próprio para trabalho?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

32. Quando você recebe um email com o arquivo anexo, com que frequência você passa o antivírus antes de abrir o anexo?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

33. Quando você recebe um email com o arquivo anexo, com que frequência você verifica a procedência do e-mail antes de abrir o anexo?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

34. Ao receber uma mídia (CD, DVD, *pendrive*, etc.) com que frequência você passa o antivírus antes de abrir ou executar programas da mídia?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

35. No momento da composição da sua senha de acesso você costuma utilizar números, letra e caracteres especiais misturados (!@#$%¨&*()_=+-/.)?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

36. Independente de o equipamento ser pessoal ou profissional, você tem por hábito trocar a sua senha de acesso?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

37. Independente de o equipamento ser pessoal ou profissional, você tem por hábito criptografar (colocar senha) nos dados importantes?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

38. Independente de o equipamento ser pessoal ou profissional, você tem por hábito limpar e higienizar seu equipamento de trabalho?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

39. Ao acessar uma página na internet, você verifica se a página é segura?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

40. Ao acessar uma página na internet, você verifica se a rede de computadores é segura?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

41. Independente da atividade que está fazendo, você verifica se alguém está lhe observando ao utilizar a sua senha?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

42. Independente da atividade que está fazendo, você verifica se está sendo filmado ao utilizar a sua senha?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

43. Independente da atividade que está fazendo, você verifica se o dispositivo que está utilizando está em bom estado de conservação, ao utilizar a sua senha?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

44. Durante o processo de instalação de um aplicativo, você procura saber a procedência do mesmo?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

45. Ao descartar uma mídia (CD, DVD, *pendrive*), com que frequência você confirma o conteúdo dela antes de descartar?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

46. Ao descartar uma mídia (CD, DVD, *pendrive*), com que frequência você destrói a mídia?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

47. Ao descartar uma mídia (CD, DVD, *pendrive*), com que frequência você registra o descarte ou a sua baixa?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

48. Ao descartar uma mídia (CD, DVD, *pendrive*), com que frequência você verifica se a mídia está em conformidade com os requisitos para o seu descarte?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

49. A política de Segurança da Informação na sua organização está em que estágio?
( ) Não sei informar ou não implementada ( ) Parcialmente ou totalmente implementada

50. Com que frequência a Segurança da Informação é considerada na fase de definição e elaboração do projeto?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

51. Com que frequência a Segurança da Informação é considerada na fase de execução do projeto?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

52. Com que frequência a Segurança da Informação é considerada na fase de gerenciamento do projeto?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

53. Durante um projeto ou trabalho, com que frequencia você reavalia os procedimentos em busca de falhas?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

54. Após a conclusão da atividade, projeto ou trabalho, você o formaliza para registro e uso futuro?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

55. Com que frequência você ou sua equipe revisa as políticas de segurança da informação da sua organização?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

56. Você é convidado(a) a participar da reavaliação das políticas de Segurança da Informação?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre ( )NA

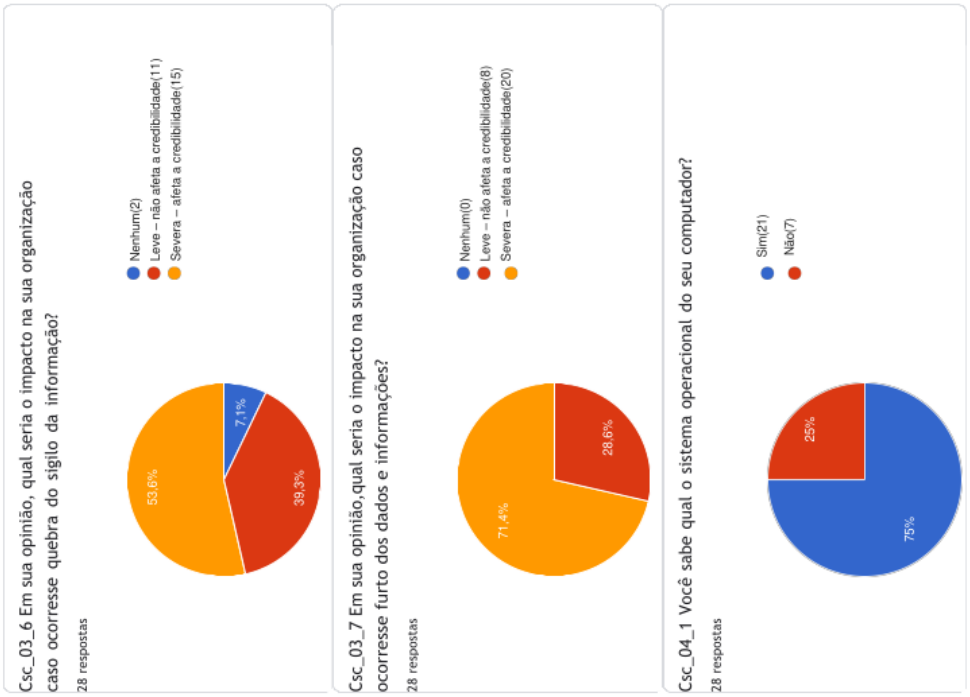
57. Com que frequência você reavalia as suas atitudes com respeito a Segurança da Informação?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

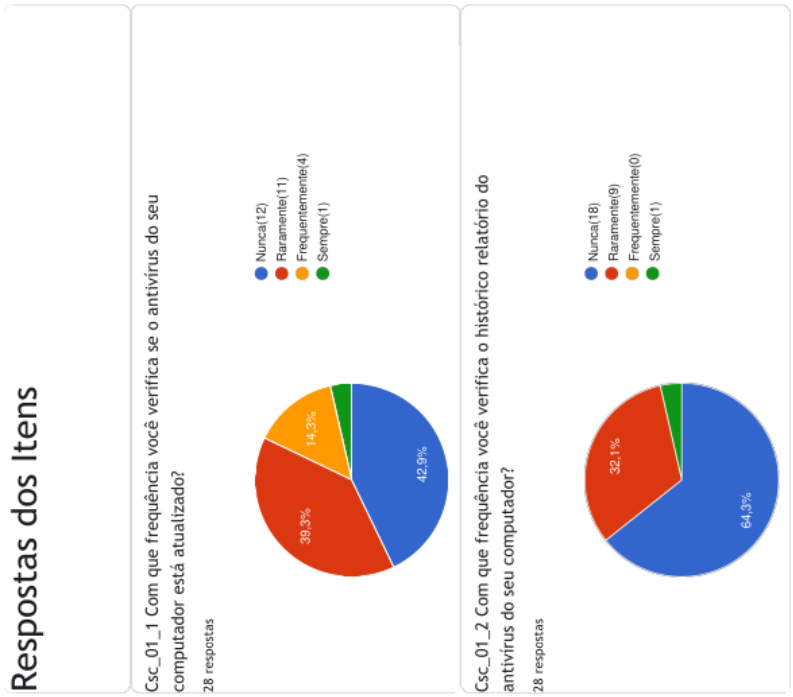
58. Com que frequência você leva em consideração a Lei Geral de Proteção de Dados Pessoais (LGPD), para os trabalhos do Gabinete/Departamento?
( )Nunca ( )Raramente ( )Frequentemente ( )Sempre

Grato pela participação!

Observações:

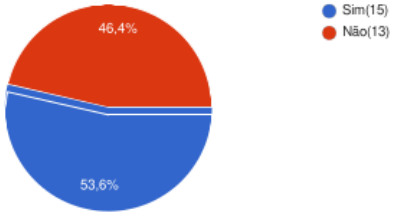
APÊNDICE B – Respostas dos Itens





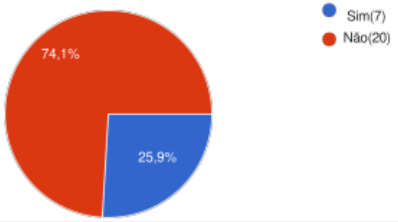
Csc_04_2 Você sabe qual a versão do sistema operacional do seu computador?

28 respostas



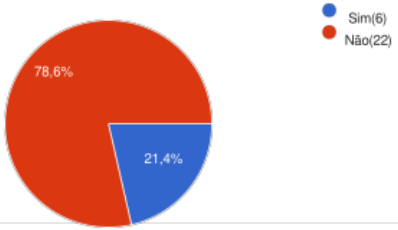
Csc_05_2 No computador do trabalho, você sabe qual é a quantidade de memória RAM?

27 respostas



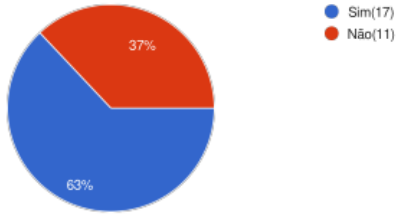
Csc_05_3 No computador do trabalho, você sabe qual a capacidade de armazenamento do disco?

28 respostas



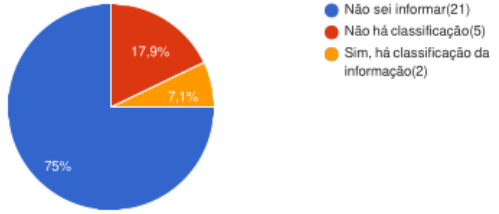
Csc_05_4 No computador do trabalho, você sabe o tipo de conexão do seu computador com a rede?

28 respostas



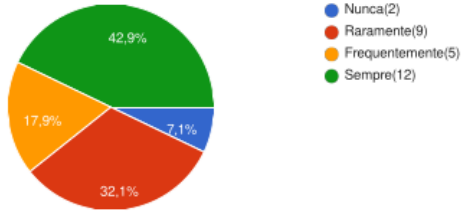
Csc_06_1 Você sabe se sua organização há procedimentos e diretrizes para classificação da informação?

28 respostas



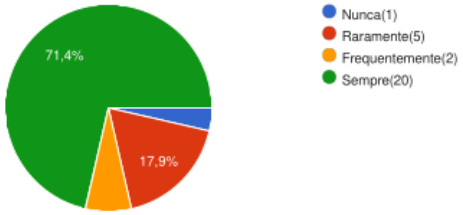
Rsp_02_1 Caso você saiba de um novo tipo de ataque a computadores, você alerta os colegas de equipe?

28 respostas



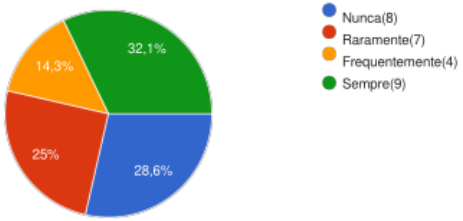
Rsp_02_2 Caso você saiba de um novo tipo de ataque a computadores, você comunica o setor responsável?

28 respostas



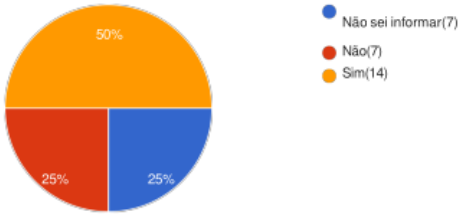
Rsp_02_3 Caso você saiba de um novo tipo de ataque a computadores, você verifica se seu computador está vulnerável/fragilizado a esse ataque?

28 respostas



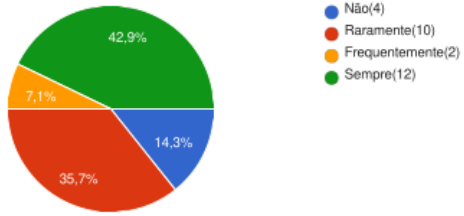
Rsp_03_1 Você conhece suas responsabilidades e atribuições relacionadas a Segurança da Informação na Câmara de Vereadores de Criciúma?

28 respostas



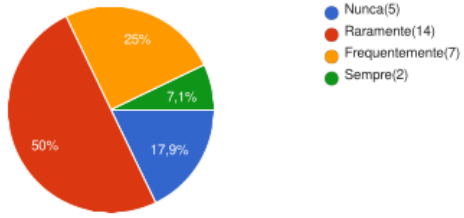
Rpt_03_3 Você está no seu local de trabalho e percebe a presença de uma pessoa desconhecida, você comunica à Presidência da Casa?

28 respostas



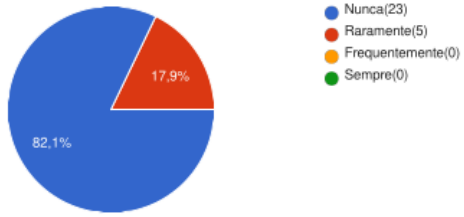
Etc_01_1 Com que frequência você trata de assuntos relacionados à sua organização em ambientes como aviões, ônibus, taxi, elevador, sala de cafezinho, redes sociais, bares, etc. ?

28 respostas



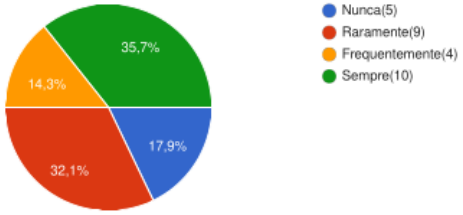
Etc_05_2 Com que frequência você pede a senha do colega emprestada para acessar o computador?

28 respostas



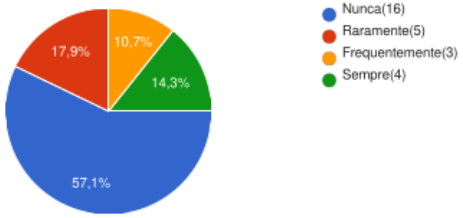
Etc_06_1 Com que frequência você costuma alertar os seus colegas sobre a necessidade de desligar o computador quando não estiver em uso?

28 respostas



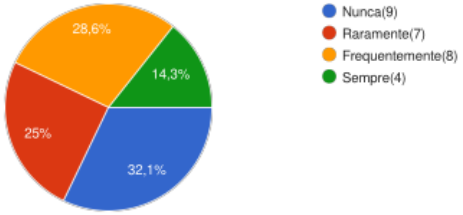
Etc_06_2 Com que frequência você costuma alertar os seus colegas sobre a necessidade de bloquear o computador quando sai da sala?

28 respostas



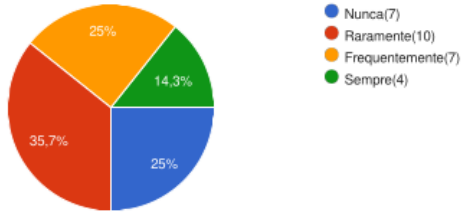
Etc_06_3 Com que frequência você costuma alertar os seus colegas sobre a necessidade de manter a mesa limpa/organizada?

28 respostas



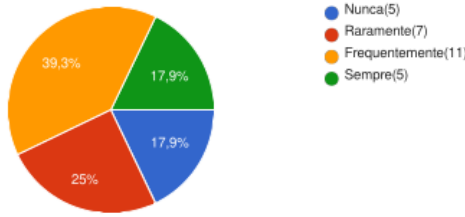
Etc_06_4 Com que frequência você costuma alertar os seus colegas sobre a necessidade de proteger os documentos de trabalho de acesso não autorizado?

28 respostas



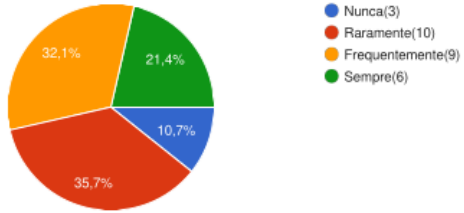
Gts_01_1 Durante o processo de manuseio dos dados do Gabinete agenda, cadastros, dados de pessoas, etc. você avalia os riscos de danos ou incidentes como, perda, roubo, adulteração e aces so indevido aos dados?

28 respostas



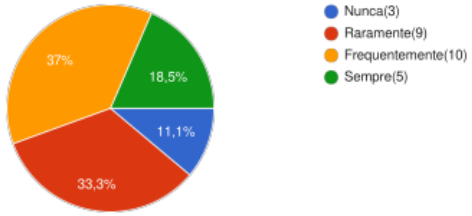
Gts_01_2 Durante o processo de manuseio dos dados do Gabinete agenda, cadastros, dados de pessoas, etc. você planeja a forma, o local, como os dados serão armazenados e acessados levan do-se em consideração a avaliação dos riscos?

28 respostas



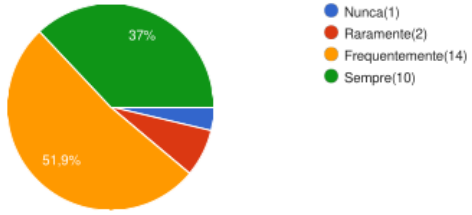
Gts_01_3 Durante o processo de manuseio dos dados do Gabinete agenda, cadastros, dados de pessoas, etc. você leva em consideração as diretrizes estabelecidas pela sua organização no plane jamento?

27 respostas



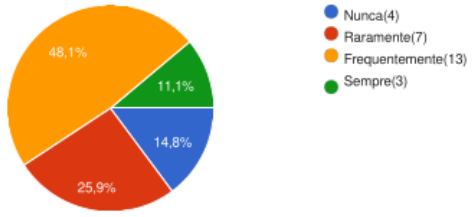
Gts_01_4 Durante o processo de manuseio dos dados do Gabinete agenda, cadastros, dados de pessoas, etc. você executa os processos conforme planejado?

27 respostas



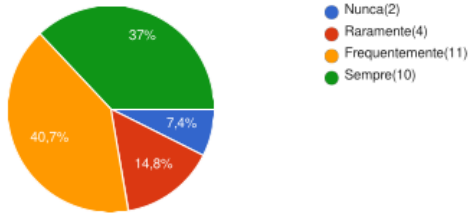
Gts_01_5 Durante o processo de manuseio dos dados do Gabinete agenda, cadastros, dados de pessoas, etc. você avalia-se os procedimentos adotados estão atendendo as necessidades de Segurança da Informação?

27 respostas



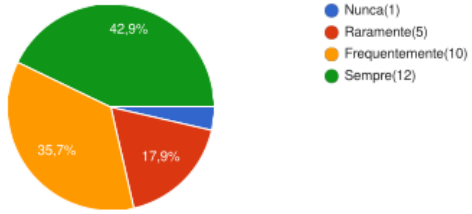
Gts_01_6 Durante o processo de manuseio dos dados do Gabinete agenda, cadastros, dados de pessoas, etc. você executa as modificações necessárias para adequar às novas necessidades?

27 respostas



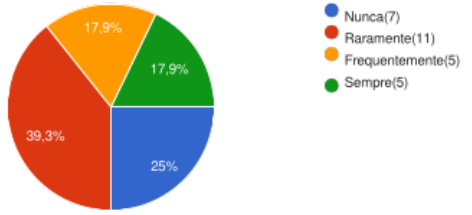
Dmc_02_2 Durante um processo de tomada de decisão que tem como consequência mudanças de hábitos e comportamentos da sua equipe ou grupo de trabalho, o seu Gabinete/Departamento estimula os colegas a emitirem opiniões, promovendo um ambiente participativo?

28 respostas



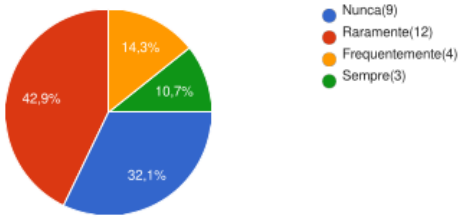
Rsc_01_1 Com respeito à cópia de segurança dos seus arquivos de trabalho, com que frequência você realiza cópia de segurança em mídias externas. CD, DVD, nuvem, pendrive, etc. ?

28 respostas



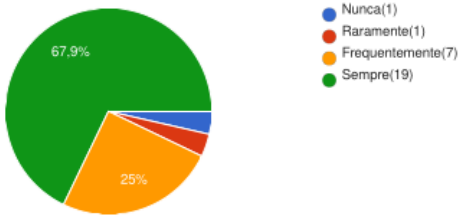
Rsc_01_3. Com respeito à cópia de segurança dos seus arquivos de trabalho, com que frequência você verifica se as cópias de segurança estão atualizadas?

28 respostas



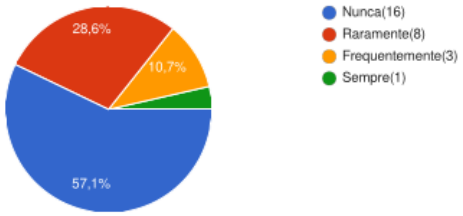
PRÓPRIO. Com que frequência você utiliza o celular próprio para trabalho?

28 respostas



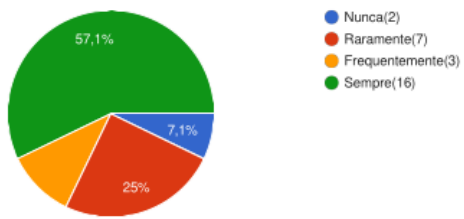
Rsc_04_2 Quando você recebe um email com o arquivo anexo, com que frequência você passa o antivírus antes de abrir o anexo?

28 respostas



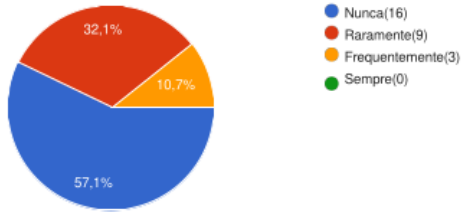
Rsc_04_3 Quando você recebe um email com o arquivo anexo, com que frequência você verifica a procedência do e-mail antes de abrir o anexo?

28 respostas



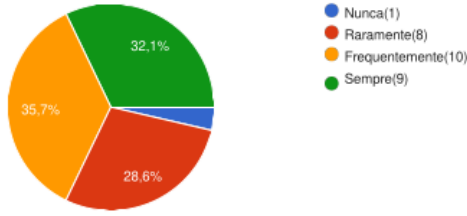
Rsc_06_3 Ao receber uma mídia CD, DVD, pendrive, etc. com que frequência você passa o antivírus antes de abrir ou executar programas da mídia?

28 respostas



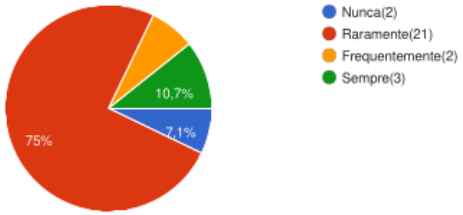
Rsc_11_3 No momento da composição da sua senha de acesso você costuma utilizar números, letra e caracteres especiais misturados (!@#$%¨&*_=+-/.)?

28 respostas



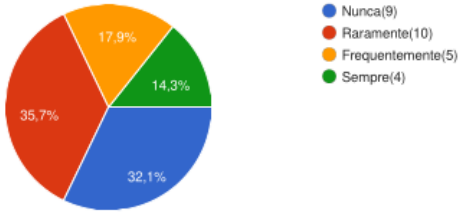
Rsc_12_1 Independente de o equipamento ser pessoal ou profissional, você tem por hábito trocar a sua senha de acesso?

28 respostas



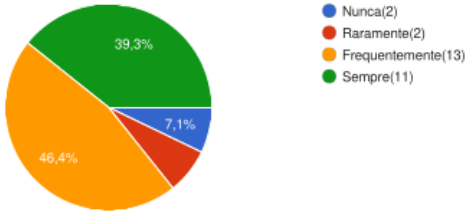
Rsc_12_2 Independente de o equipamento ser pessoal ou profissional, você tem por hábito criptografar colocar senha nos dados importantes?

28 respostas



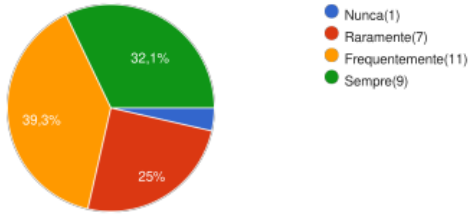
Rsc_12_6 Independente de o equipamento ser pessoal ou profissional, você tem por hábito limpar e higienizar seu equipamento de trabalho?

28 respostas



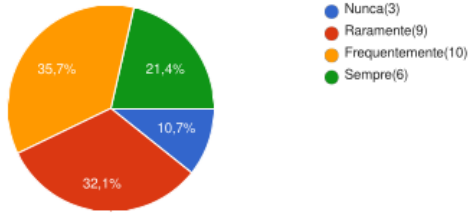
Rsc_13_1 Ao acessar uma página na internet, você verifica se a página é segura?

28 respostas



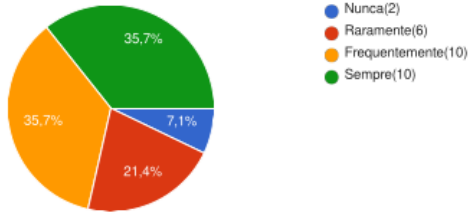
Rsc_13_2 Ao acessar uma página na internet, você verifica se a rede de computadores é segura?

28 respostas



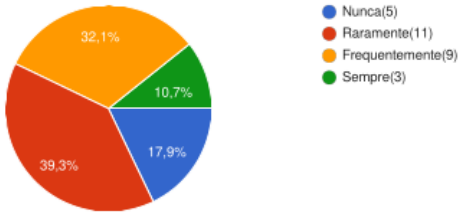
Rsc_14_1 Independente da atividade que está fazendo, você verifica se alguém está lhe observando ao utilizar a sua senha?

28 respostas



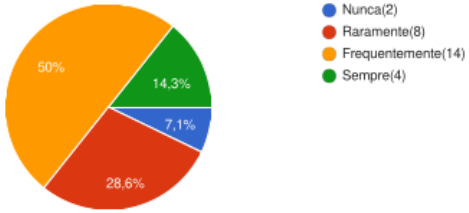
Rsc_14_2 Independente da atividade que está fazendo, você verifica se está sendo filmado ao utilizar a sua senha?

28 respostas



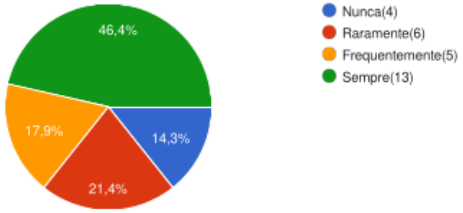
Rsc_14_3 Independente da atividade que está fazendo, você verifica se o dispositivo que está utilizando está em bom estado de conservação, ao utilizar a sua senha?

28 respostas



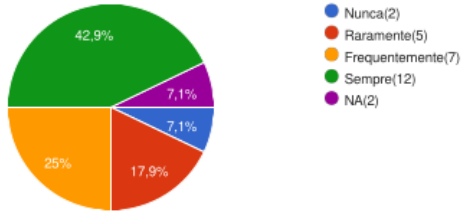
Rsc_15_2 Durante o processo de instalação de um aplicativo, você procura saber a procedência do mesmo?

28 respostas



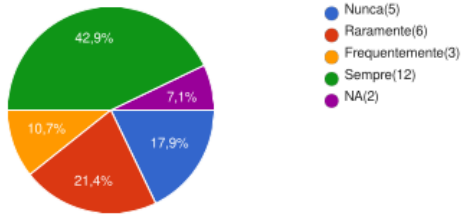
Rsc_16_1 Ao descartar uma mídia CD, DVD, pendrive, com que frequência você confirma o conteúdo dela antes de descartar?

28 respostas



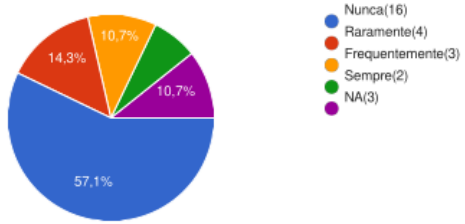
Rsc_16_2 Ao descartar uma mídia CD, DVD, pendrive, com que frequência você destrói a mídia?

28 respostas



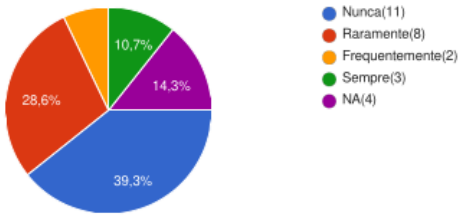
Rsc_16_3 Ao descartar uma mídia CD, DVD, pendrive, com que frequência você registra o descarte ou a sua baixa?

28 respostas



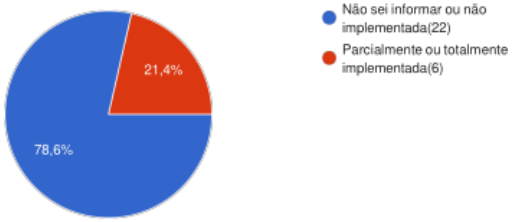
Rsc_16_4 Ao descartar uma mídia CD, DVD, pendrive, com que frequência você verifica se a mídia está em conformidade com os requisitos para o seu descarte?

28 respostas



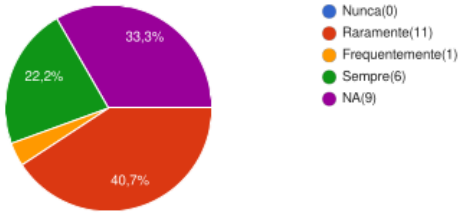
Prj_01_1 A política de Segurança da Informação na sua organização está em que estágio?

28 respostas



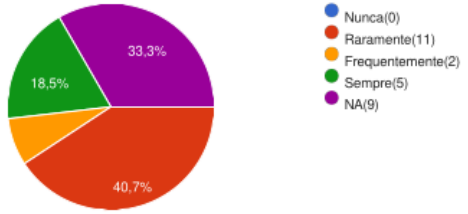
Prj_02_1 Com que frequência a Segurança da Informação é considerada na fase de definição e elaboração do projeto?

27 respostas



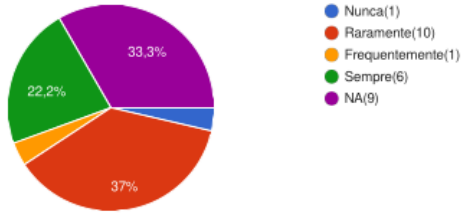
Prj_02_2 Com que frequência a Segurança da Informação é considerada na fase de execução do projeto?

27 respostas



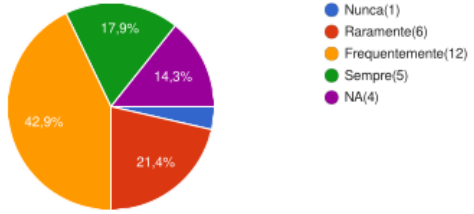
Prj_02_3 Com que frequência a Segurança da Informação é considerada na fase de gerenciamento do projeto?

27 respostas



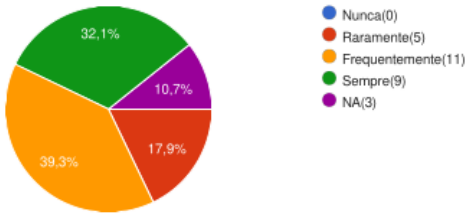
Prj_03_2 Durante um projeto ou trabalho, com que frequencia você reavalia os procedimentos em busca de falhas?

28 respostas



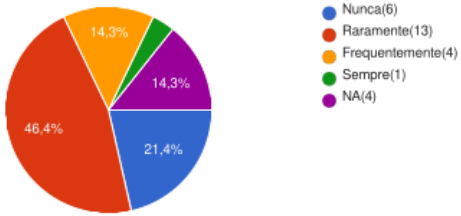
Prj_03_3 Após a conclusão da atividade, projeto ou trabalho, você o formaliza para registro e uso futuro?

28 respostas



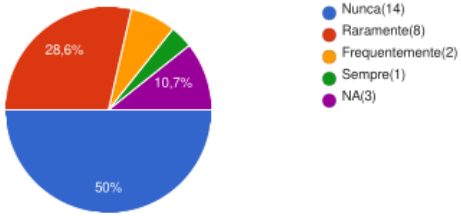
Rvl_01_1 Com que frequência você ou sua equipe revisa as políticas de segurança da informação da sua organização?

28 respostas



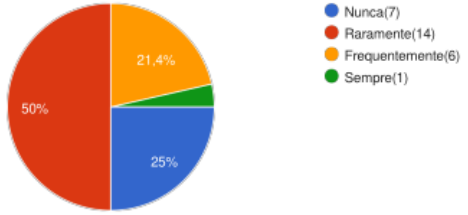
Rvl_01_2 Você é convidadoa a participar da reavaliação das políticas de Segurança da Informação?

28 respostas



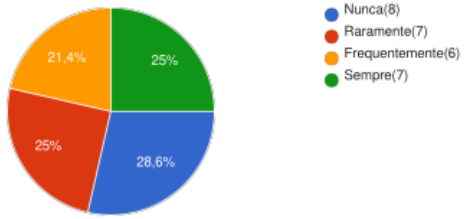
Rvl_02_1 Com que frequência você reavalia as suas atitudes com respeito a Segurança da Informação?

28 respostas



PRÓPRIO Com que frequência você leva em consideração a Lei Geral de Proteção de Dados Pessoais LGPD, para os trabalhos do Gabinete/Departamento?

28 respostas



ANEXO A – Autorização CONEP

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

PARECER CONSUBSTANCIADO DO CEP

DADOS DO PROJETO DE PESQUISA

Título da Pesquisa: Cultura organizacional e LGPD na percepção de servidores do poder legislativo: discussão de similaridades com o diploma legal.

Pesquisador: LUCAS NASCIMENTO MARTINS CAMARGO DA SILVA

Área Temática:

Versão: 2

CAAE: 61802822.2.0000.0121

Instituição Proponente: Universidade Federal de Santa Catarina

Patrocinador Principal: Financiamento Próprio

DADOS DO PARECER

Número do Parecer: 5.637.709

Apresentação do Projeto:

Cultura organizacional e LGPD na percepção de servidores do poder legislativo: discussão de similaridades com o diploma legal.

Resumo: O trabalho apresentado nesta dissertação utiliza a Câmara de Vereadores de Criciúma, SC, como ambiente para explorar e aprofundar questões que envolvem a cultura organizacional em segurança da informação e a nova Lei Geral de Proteção de Dados Pessoais (LGPD). O ambiente legislativo contêm características ímpares quando da utilização de dados. A atribuição principal do legislador é legislar e fiscalizar o Poder Executivo, por esta razão há a necessidade de livre acesso à informação e transparência dos seus atos administrativos. Por outro lado a LGPD, diploma recente, de 2018, traz requisitos quanto ao uso de informações pessoais, ainda incomuns no campo da tecnologia, também utilizadas no Poder Legislativo, quando do exercício de sua função constitucional. Diante deste fato, buscou-se uma ferramenta capaz de aferir numericamente a cultura de segurança da informação, na Casa Legislativa de Criciúma e contrastá-la com os ditames legais da nova lei. As similaridades, ou a inexistência delas, podem provocar a reflexão quanto ao cumprimento da lei e a contribuir na missão do Poder Legislativo, fomentando seu papel na promoção da cidadania e transparência pública.

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 701
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Objetivo da Pesquisa:

Objetivo Geral Esta proposta tem como objetivo analisar a cultura organizacional em segurança da informação, no Poder Legislativo de Criciúma/SC, com olhar crítico às similaridades existentes com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Objetivos Específicos

Para desenvolver esse objetivo, o assunto será subdividido em:

- Proceder revisão de literatura quanto a Lei Geral de Proteção de Dados Pessoais, cultura, cultura organizacional, cultura organizacional em segurança da informação;
- Proceder aplicação de ferramenta específica e calibrada, no grupo alvo de análise;
- Elencar lacunas existentes entre o nível de cultura organizacional em segurança da informação e a LGPD, dentro do ambiente proposto; e
- Discutir similaridades entre os dados obtidos entre a ferramenta de pesquisa e texto do Diploma Legal.

Avaliação dos Riscos e Benefícios:

Risco: O sigilo da identidade dos participantes. Ação de controle: A coleta de dados será em formulário físico, sem campo de identificação do participante. As respostas serão agrupadas e apresentadas estatisticamente, exibindo somente valores agregados; Risco: Descontinuidade de participação por motivos diversos. Ação de controle: Os formulários serão entregues aos participantes, em meio físico impresso. Será estipulado um cronograma de preenchimento e acompanhamento/ajuda do pesquisador, caso necessário; Risco Perda/descarte dos formulários de resposta. Ação de controle: Os formulários deverão permanecer no ambiente organizacional da Câmara, durante o preenchimento. Os formulários serão destruídos após a contabilização das respostas.

Benefícios: Levantar aspectos organizacionais que podem ser aperfeiçoados no sentido de atender segurança da informação e a Lei Geral de Proteção de Dados Pessoais.

Comentários e Considerações sobre a Pesquisa:

A pesquisa apresenta pertinência, fundamentação bibliográfica e uma vez obtido os dados conclusivos proporcionará uma visão mais abrangente sobre o tema proposto.

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 701
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Considerações sobre os Termos de apresentação obrigatória:

Documentos de acordo com as solicitações do CEPSH-UFSC.

Recomendações:

Não se aplica.

Conclusões ou Pendências e Lista de Inadequações:

Foram elaboradas alterações na Folha de Rosto e adequações no TCLE, com os itens obrigatórios inclusos.

Considerações Finais a critério do CEP:

Este parecer foi elaborado baseado nos documentos abaixo relacionados:

Tipo Documento	Arquivo	Postagem	Autor	Situação
Informações Básicas do Projeto	PB_INFORMAÇÕES_BÁSICAS_DO_PROJETO_1979185.pdf	30/08/2022 15:58:30		Aceito
TCLE / Termos de Assentimento / Justificativa de Ausência	PlatBrasil_TCLE.pdf	30/08/2022 15:57:57	LUCAS NASCIMENTO MARTINS CAMARGO DA SILVA	Aceito
Folha de Rosto	folhaDeRosto_assinado_assinadoP.pdf	30/08/2022 15:57:15	LUCAS NASCIMENTO MARTINS CAMARGO DA SILVA	Aceito
Outros	Lucas_Ferramenta.pdf	11/08/2022 13:57:16	LUCAS NASCIMENTO MARTINS CAMARGO DA SILVA	Aceito
Projeto Detalhado / Brochura Investigador	LucasPESH.pdf	04/08/2022 14:32:48	LUCAS NASCIMENTO MARTINS CAMARGO DA SILVA	Aceito
Declaração de Instituição e Infraestrutura	PlatBrasil_Decl.pdf	03/08/2022 09:14:42	LUCAS NASCIMENTO MARTINS CAMARGO DA SILVA	Aceito
Cronograma	PlatBrasil_Cron.pdf	03/08/2022 09:13:12	LUCAS NASCIMENTO	Aceito

UNIVERSIDADE FEDERAL DE SANTA CATARINA - UFSC

Continuação do Parecer: 5.637.709

Cronograma	PlatBrasil_Cron.pdf	03/08/2022 09:13:12	MARTINS CAMARGO DA SILVA	Aceito

Situação do Parecer:
Aprovado

Necessita Apreciação da CONEP:
Não

FLORIANOPOLIS, 12 de Setembro de 2022

Assinado por:
Luciana C Antunes
(Coordenador(a))

Endereço: Universidade Federal de Santa Catarina, Prédio Reitoria II, R: Desembargador Vitor Lima, nº 222, sala 701
Bairro: Trindade **CEP:** 88.040-400
UF: SC **Município:** FLORIANOPOLIS
Telefone: (48)3721-6094 **E-mail:** cep.propesq@contato.ufsc.br

ANEXO B – Consentimento da CMC

ESTADO DE SANTA CATARINA
CÂMARA MUNICIPAL DE CRICIÚMA
PODER LEGISLATIVO MUNICIPAL

Memorando 255/2022

Memorando

Criciúma, 4 de maio de 2022

À
Presidência

Remeto expediente sobre consentimento para pesquisa em pós-graduação em nível de mestrado.

Informo que estou matriculado no programa de pós-graduação, em Tecnologias da Informação e Comunicação, nível mestrado, da UFSC, desde 2021, conforme atestado de matrícula anexo. O programa tem duração de 2 anos, com previsão de término em abril de 2023, e com a orientação da professora doutora Andréa Cristina Trierweiller.

O trabalho desenvolvido tem como tema: Privacidade de dados, busca do Traço Latente com uso da Teoria de Resposta ao Item. Por essa razão, dirijo-me a esta presidência, solicitando proceder tal pesquisa nesta Casa Legislativa. As atividades envolvem ações de calibração e aplicação de ferramenta de pesquisa (questionário), entre outras julgadas necessárias, com os membros da unidade organizacional (gabinetes dos vereadores).

Ressalto que todos os dados obtidos na pesquisa acadêmica serão anonimizados, impossibilitando identificação dos participantes ou agentes políticos envolvidos. O objetivo final é descobrir o nível de maturidade organizacional, quanto à segurança do tratamento de dados, físicos ou não, resultando oportunidades de melhorias quanto às práticas adotadas por esta instituição.

Atenciosamente,

Lucas Martins
Técnico Legislativo

ESTADO DE SANTA CATARINA
CÂMARA MUNICIPAL DE CRICIÚMA
PODER LEGISLATIVO MUNICIPAL

Anexo 1/2022
do(a) Memorando 255/2022

Em resposta ao Memorando 255/2022, de 04 de maio de 2022, em que o servidor Lucas Nascimento Martins Camargo da Silva, servidor desta Casa Legislativa, atestando estar matriculado regularmente no Programa de Pós-Graduação em Tecnologias da Informação e Comunicação, em nível de mestrado, no município de Araranguá, pela Universidade Federal de Santa Catarina (UFSC), sob orientação da professora doutora Andréa Cristina Trierweiller, requer consentimento para proceder pesquisa científica nesta Casa Legislativa.

Tal solicitação foi apreciada por esta presidência e tendo em vista as características da pesquisa, optou-se por dar parecer favorável ao que se requere, podendo este a proceder as atividades atinentes à pesquisa descrita na solicitação.

Atenciosamente,

Roseli Maria De Lucca Pizzolo
Presidente

ESTADO DE SANTA CATARINA

CÂMARA MUNICIPAL DE CRICIÚMA

PODER LEGISLATIVO MUNICIPAL

MANIFESTO DO DOCUMENTO

Anexo

Protocolo Nº: 67527
Protocolo Data: 16/05/2022
Documento Nº: 1/2022
Processo Nº: 175/2022

Gerado por Lucas Nascimento Martins Camargo da Silva na repartição Informática dia 16/05/2022 às 13:33

CHAVE DE AUTENTICAÇÃO DO DOCUMENTO

KZVPM-PF81A-4EMAI-ZDEP2-F2DZZ

Para confirmar a autenticidade acesse https://www.camaracriciuma.sc.gov.br/validador-assinatura

Documento eletrônico assinado digitalmente conforme DOC-ICP-15 de 25/8/2015.

Nome Roseli Maria De Lucca Pizzolo
CPF/CNPJ 39849384972
Data 16/05/2022 14:40

Esta folha foi gerada automaticamente em 03/08/2022 às 17:34