



UDESC
UNIVERSIDADE
DO ESTADO DE
SANTA CATARINA



**UNIVERSIDADE DO ESTADO DE SANTA CATARINA
CENTRO DE CIÊNCIAS DA ADMINISTRAÇÃO E SOCIOECONÔMICAS - ESAG
PROGRAMA DE PÓS-GRADUAÇÃO EM ADMINISTRAÇÃO**

Curso: MESTRADO PROFISSIONAL EM ADMINISTRAÇÃO

Área de Especialidade:

Tecnologias de gestão em organizações intensivas em conhecimento e em TICs

**MODELO DE GESTÃO DO CONHECIMENTO EM SEGURANÇA CIBERNÉTICA
PARA O PODER JUDICIÁRIO DE SANTA CATARINA**

CPF: 000.222.169-10

**Florianópolis
2023**

1 INTRODUÇÃO

Atualmente, a tecnologia da informação e de comunicação (TIC) está presente em quase todas as atividades desenvolvidas pelos órgãos e entidades da Administração Pública, haja vista a regulamentação da transformação digital do setor público no Brasil: Decreto n. 8.936/2016, que criou a Plataforma de Cidadania Digital para oferta de serviços públicos digitais; Decreto n. 8638/2016, que instituiu a Política de Governança Digital a fim de propagar o uso da TIC na prestação dos serviços públicos e estimular o monitoramento desses serviços pelo cidadão; Decreto n. 9.319/2018, que instituiu o Sistema Nacional de Transformação Digital com o objetivo de harmonizar as iniciativas do Executivo federal no ambiente digital; e, por fim, Decreto n. 10.332/2020, que instituiu a Estratégia de Governo Digital com princípios, objetivos e iniciativas da transformação digital no governo federal (MACIEL, 2020).

Diante dos avanços da transformação digital do setor público, o Conselho Nacional de Justiça (CNJ) lançou o Programa Justiça 4.0 para o sistema judiciário brasileiro com o propósito de garantir serviços mais rápidos, eficazes e acessíveis e tornar a justiça brasileira mais inovadora, eficiente, inteligente, colaborativa, integrada e transparente (CNJ, 2020b).

Nesse contexto, as ferramentas tecnológicas estão revestidas de grande importância ao proporcionar mais rapidez ao serviço prestado para a sociedade que, por sua vez, exige mais efetividade, eficácia, eficiência e transparência dos entes públicos. Em contrapartida, com os avanços no uso de soluções tecnológicas pelas organizações públicas e privadas, incluindo o Poder Judiciário, aumentam também as ameaças à segurança da informação, especialmente no espaço cibernético, já que este constitui novo e promissor ambiente de exposição ao risco, o que torna necessária a implementação de ações para assegurar a confidencialidade, a integridade e a disponibilidade das informações das organizações (KILLMEYER, 2006, apud AZAMBUJA & NETO, 2020).

Demonstrando preocupação com o tema, o Conselho Nacional de Justiça (CNJ) instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ) por meio da Resolução CNJ n. 396, de 7 de junho de 2021, com o objetivo de aprimorar o nível de maturidade em segurança cibernética nos órgãos do Poder Judiciário (CNJ, 2021).

De acordo com esse objetivo, as ações de governança cibernética devem ser fortalecidas por meio de um *Sistema de Gestão em Segurança da Informação* baseado em riscos, assim como elevar o nível de segurança das infraestruturas críticas, estabelecer uma rede

de cooperação no Judiciário e um modelo centralizado de governança cibernética nacional (CNJ, 2021).

No cenário global, é notório que os ataques bem-sucedidos nem sempre dizem respeito às vulnerabilidades de equipamentos e sistemas, mas sim a ações humanas mal executadas, seja intencionalmente ou não. Inúmeras empresas se preocupam em instalar bons softwares para evitar esses ataques, além disso criam políticas de segurança e procedimentos padrão, mas ainda não conseguem evitar incidentes de segurança da informação. A razão disso é a falta de conscientização e treinamento dos seus colaboradores (MORETTI, 2022).

Um exemplo que ratifica essa situação é a definição em uma política de senhas da exigência de um número mínimo de caracteres com números, letras maiúsculas e minúsculas, enquanto o usuário cria essa senha, escreve num papel e cola no seu computador (MORETTI, 2022).

Por mais que os usuários saibam que os ataques maliciosos às informações estão cada vez mais comuns na atualidade e por mais que sejam cuidadosos na maior parte do tempo, eles são humanos. Por isso, muitas vezes são movidos pela emoção, pelo cansaço e pelo excesso de atividades do dia, ficando suscetíveis e expostos a ataques (ALBUQUERQUE E RIBEIRO, 2002).

Portanto, acima de todas as ações voltadas para a segurança cibernética, a principal é gerar conhecimento para que os usuários dos serviços de tecnologia da informação e comunicação do PJSC estejam conscientes acerca dos riscos, ameaças, golpes e invasões, e dos prejuízos financeiros e de imagem que podem ser causados, caso algum ataque cibernético se concretize.

Para atender a necessidade do judiciário catarinense, este trabalho tem como objetivo geral: *construir um modelo de gestão do conhecimento para a área de segurança cibernética no PJSC*. Os objetivos específicos são: i) desenvolver o modelo de gestão do conhecimento de acordo com as diretrizes da ENSEC-JUD; ii) mapear os processos de gestão do conhecimento; iii) elaborar um plano de gestão do conhecimento em segurança cibernética para o PJSC; iv) levantar técnicas inovadoras de aprendizagem; e v) apresentar um programa de programa continuado de educação e capacitação em segurança cibernética para o PJSC.

2 JUSTIFICATIVA

Considerando as circunstâncias globais acerca do aumento exponencial dos ataques cibernéticos no contexto de um juízo 100% digital, – que é a possibilidade de o cidadão valer-se da tecnologia para ter acesso à Justiça sem precisar comparecer fisicamente nos Fóruns, onde todos os atos processuais, além de audiências e sessões de julgamento, serão praticados exclusivamente por meio eletrônico e remoto, pela Internet (CNJ, 2020c).

Considerando que o Tribunal de Justiça de Santa Catarina (TJSC) concluiu a digitalização e a migração de todo o seu acervo de processos físicos em tramitação, suspensos e sobrestados, passando a atuar com a integralidade de seus processos em meio eletrônico (TJSC, 2022).

Convém que todos os indivíduos que trabalham com serviços informatizados e sistemas de TIC do judiciário catarinense recebam, de forma contínua, treinamento, educação e conscientização apropriados, além de atualizações regulares das políticas e procedimentos organizacionais relevantes para garantir a segurança da informação, principalmente no ambiente cibernético.

A necessidade da compreensão de que a informação é o ativo mais importante de qualquer atividade nas organizações é uma das razões que tornam importante a gestão do conhecimento em segurança cibernética. Assim, implementar ações que sensibilizem todos os colaboradores do Poder Judiciário de Santa Catarina (PJSC) a desenvolverem uma cultura voltada para esse assunto é imprescindível para garantir a proteção de dados e informações da instituição.

Justifica-se, portanto, a realização desta pesquisa, dada a importância da gestão do conhecimento (GC), como um “conjunto de técnicas e ferramentas para identificar e utilizar os ativos de informação, por meio de uma abordagem sistemática e organizada para melhorar a capacidade da organização de impulsionar o conhecimento” (KPMG apud BATISTA, 2012, p. 9).

Ademais a gestão do conhecimento em segurança cibernética no PJSC vem ao encontro das ações necessárias para atender as diretrizes da ENSEC-JUD e, sobretudo, para criar uma cultura de cibersegurança, assegurar o treinamento e a conscientização dos usuários com as habilidades necessárias ao enfrentamento dos riscos e ameaças comumente explorados no ambiente digital.

Diante do atual contexto de riscos que as organizações estão submetidas e do exponencial crescimento do número de ameaças cibernéticas, é necessário inovar na gestão do conhecimento no PJSC, com foco em resultados específicos para elevar o nível de maturidade dos seus usuários com relação a ameaças e minimizar os riscos associados à gestão da segurança da informação, além de promover o uso eficiente, eficaz e efetivo dos recursos de tecnologia da informação e comunicação (TIC).

3 FUNDAMENTAÇÃO TEÓRICA

Na pesquisa inicial da literatura foram encontradas as seguintes obras literárias e acadêmicas que serão a teoria base deste projeto de pesquisa:

- a) Livro digital: Modelo de gestão do conhecimento para a administração pública brasileira: como implementar a gestão do conhecimento para produzir resultados em benefício do cidadão (BATISTA, 2012).
- b) Tese de doutorado: Gestão do Conhecimento em Organizações: proposta de mapeamento conceitual integrativo (ALVARENGA NETO, 2005).
- c) Dissertação de mestrado: O fator humano da cibersegurança nas organizações (GONÇALVES, 2019).
- d) Dissertação de mestrado: Engajamento de Gestores Públicos e Cidadãos Através de uma Métrica Baseada em Elementos de Gamificação (ZOTTI, 2014).
- e) ABNT NBR ISO/IEC 27001 e 27002: Segurança da informação, segurança cibernética e proteção à privacidade. Sistemas de gestão de segurança da informação e controles de segurança da informação (ABNT, 2022).

Batista (2012) apresenta um modelo de gestão do conhecimento concebido essencialmente para a administração pública com a finalidade de orientar essas organizações a implementá-lo de tal forma que o alcance dos objetivos estratégicos e a melhoria de processos, produtos e serviços sejam assegurados em benefício dos cidadãos, usuários e sociedade em geral. A proposta descreve um modelo de gestão do conhecimento formado por seis componentes: (1) direcionadores estratégicos: visão, missão, objetivos estratégicos e metas; (2) viabilizadores: liderança, tecnologia, pessoas e processos; (3) processo de gestão do conhecimento: identificar, criar, armazenar, compartilhar e aplicar; (4) ciclo KDCA: knowledge – conhecimento, do – executar, check – verificar, e action – atuar corretivamente; (5) resultados de gestão do conhecimento; e (6) partes interessadas: cidadão-usuário e sociedade.

Por sua vez, Alvarenga Neto (2005), investigou a temática da gestão do conhecimento em três grandes organizações atuantes no Brasil, discutindo seu conceito, elementos constituintes, áreas fronteiriças e interfaces, origens, abordagens gerenciais e ferramentas, dinâmica e demais aspectos com a finalidade de apresentar um modelo ou mapa conceitual integrativo. Como resultado desse trabalho, o autor identificou que os principais desafios impostos às organizações comprometidas com a gestão do conhecimento estão concentrados na gestão de mudanças culturais e comportamentais e na constituição de um contexto organizacional favorável à criação, uso e compartilhamento de informações e conhecimentos.

A segurança da informação e todos os seus conceitos e boas práticas são decorrentes das normativas que compõem a “família ISO 27000”, publicadas pela Associação Brasileira de Normas Técnicas, que é membro fundadora da ISO (Organização Internacional de Normalização)¹. De acordo com a norma ABNT NBR ISO/IEC 27002 (2013), a segurança da informação visa a proteção da informação que tem valor para o negócio contra vários tipos de ameaças e vulnerabilidades, tanto acidentais como deliberadas, a fim de minimizar os riscos de segurança da informação e o impacto aos seus ativos nas organizações. A norma estabelece diretrizes e requisitos para a adoção de um sistema de gestão de segurança da informação, como uma decisão estratégica das organizações. Esse sistema tem o propósito de preservar a confidencialidade, integridade e disponibilidade da informação por meio da aplicação de um processo de gestão de riscos e fornece confiança para as partes interessadas de que os riscos são adequadamente gerenciados.

Com relação à segurança cibernética, Gonçalves (2019) estudou a influência que o fator humano tem nessa área peculiar das organizações. Foram identificadas características e comportamentos humanos que repercutem na segurança cibernética, além do impacto nos níveis de cibersegurança alcançados e das respectivas soluções para estes comportamentos. A conclusão do trabalho aponta que as pessoas têm realmente uma grande influência e, conseqüentemente, importância, na gestão da segurança cibernética das organizações.

¹ A Organização Internacional de Normalização – ISO, com sede em Genebra – Suíça, é uma organização internacional não governamental independente, associada a 165 organismos de normalização nacionais. Por meio de seus membros, ela reúne especialistas para compartilhar conhecimento e desenvolver Normas Internacionais voluntárias, baseadas em consenso e relevantes para o mercado que apoiam a inovação e fornecem soluções para os desafios globais. Disponível em: <https://www.iso.org/about-us.html>. Acesso em 30 nov. 2023.

No âmbito da inovação na aprendizagem organizacional, Zotti (2014) aborda o engajamento dos agentes públicos com a aplicação de mecanismos e dinâmicas de jogos (gamificação) no contexto de não jogo, a fim de preparar as pessoas envolvidas nos serviços prestados à sociedade pela Administração Pública a responder às exigências de um público cada vez mais conectado em novas tecnologias digitais. Na pesquisa, a gamificação é apresentada como uma oportunidade de transformar tarefas maçantes e repetitivas dos processos burocráticos e hierárquicos em tarefas mais divertidas, produtivas e colaborativas. Como objetivo geral, o trabalho se propõe a apresentar uma métrica de engajamento baseada em elementos de gamificação, com a finalidade de motivar a participação de cidadãos e funcionários públicos em processos de gestão colaborativa.

4 PROCEDIMENTOS METODOLÓGICOS

Segundo Vergara (2010), este trabalho é classificado como uma pesquisa aplicada quanto à sua natureza, pois é motivado pela necessidade de resolver um problema concreto com a finalidade prática de identificar uma solução específica.

Apresenta, ainda, natureza qualitativa (GODOY, 1995, apud ALMEIDA, 2014), uma vez que busca uma resposta para a pergunta de pesquisa por meio da análise, compreensão e interpretação dos dados de forma indutiva.

Considerando os seus objetivos, a pesquisa é exploratória, sendo associada à pesquisa bibliográfica para produção do conhecimento sobre o tema e as hipóteses resultantes da fundamentação teórica levantada no estudo por meio da coleta de dados de fontes secundárias: materiais publicados em livros, artigos, dissertações e teses (GIL, 2010).

Quanto aos fins, a pesquisa é caracterizada como um estudo descritivo, pois estuda e descreve características próprias do ambiente organizacional do PJSC a fim de estabelecer relações entre as variáveis apresentadas no estudo (FILHO & FILHO, 2015).

5 VIABILIDADE / IMPLEMENTAÇÃO

Do ponto de vista prático, o tema da pesquisa contém relevância organizacional e científica, conforme já exposto na justificativa.

Com relação à viabilidade de implementação, o projeto vai ao encontro de diretrizes nacionais para a segurança cibernética do Poder Judiciário estabelecidas pelo Conselho Nacional de Justiça (CNJ), pois aprimorar a segurança da informação é um objetivo estratégico

7 REFERÊNCIAS

ALBUQUERQUE, Ricardo e RIBEIRO, Bruno. **Segurança no Desenvolvimento de Software** – Como desenvolver sistemas seguros e avaliar a segurança de aplicações desenvolvidas com base na ISO 15.408. Editora Campus. Rio de Janeiro, 2002.

ALVARENGA NETO, R. C. D. **Gestão do conhecimento em organizações**: proposta de mapeamento conceitual integrativo. 2005. 400 p. Tese (Doutorado) - Universidade Federal de Minas Gerais, Programa de Pós-Graduação em Ciência da Informação, Belo Horizonte, 2005. Disponível em: <http://hdl.handle.net/1843/EARM-6ZGNE6>. Acesso em: 28 nov. 2023.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001** - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão de segurança da informação - Requisitos. Rio de Janeiro, 2022a. Disponível em: <https://www.abntcolecao.com.br/normavw.aspx?Q=dmN0Z2ZNNnFzS3l0akF5UGxWMjlqSkZ2RzZJTG9kcVZ2WWFoU0k0cm1jYz0=>> Acesso em 29 nov. 2023.

_____. **NBR ISO/IEC 27002** - Segurança da Informação, segurança cibernética e proteção à privacidade - Controles de segurança da informação. Rio de Janeiro, 2022. Disponível em: <https://www.abntcolecao.com.br/normavw.aspx?Q=T2JVQ1FZQkZsejBHTW9ybE1EdTRoSXRtb2kyWk4xV0FUS0M5MUdJeTVQT0=>> Acesso em 28 nov. 2023b.

ALMEIDA, Mário de Souza. **Elaboração de projeto, CC, dissertação e tese**: uma abordagem simples, prática e objetiva. 2ª ed. São Paulo: Atlas, 2014.

AZAMBUJA, Antônio João; NETO, João Souza (2020). Modelo de maturidade de segurança cibernética para os órgãos da administração pública federal. **Revista do Serviço Público**, 71(3), 660-712. Disponível em: <https://doi.org/10.21874/rsp.v71i3.3210>. Acesso em: 26 nov. 2023.

BATISTA, Fábio Ferreira. **Modelo de gestão do conhecimento para a administração pública brasileira**: como implementar a gestão do conhecimento para produzir resultados em benefício do cidadão/Fábio Ferreira Batista. – Brasília: Ipea, 2012. 132 p. Disponível em: <http://repositorio.ipea.gov.br/handle/11058/754>. Acesso em 27 nov. 2023.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA (CNJ). **Resolução n. 396**, de 7 de junho de 2021. Disponível em <https://atos.cnj.jus.br/atos/detalhar/3975>. Acesso em 30 nov. 2023.

_____. **Resolução n. 370**, de 28 de janeiro de 2021. 2021b. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/3706>. Acesso em 30 nov. 2023.

_____. **Justiça 4.0**. 2020b. Disponível em: <https://www.cnj.jus.br/tecnologia-da-informacao-e-comunicacao/justica-4-0/>. Acesso em 18 jan. 2023.

_____. **Juízo 100% Digital: tudo o que você precisa saber**. 2020c. Disponível em: https://www.cnj.jus.br/wp-content/uploads/2020/10/WEB_cartilha_Juizo_100porcento_digital_v3.pdf. Acesso em 26 nov. 2023.

FILHO, Milton Cordeiro F.; FILHO, Emílio J. M A. **Planejamento da Pesquisa Científica**, 2ª edição. [Digite o Local da Editora]: Grupo GEN, 2015. E-book. ISBN 9788522495351. Disponível em: <<https://integrada.minhabiblioteca.com.br/#/books/9788522495351/>>. Acesso em: 10 out. 2022.

GIL, Antônio Carlos. **Como elaborar projetos de pesquisa**. 7ª ed. São Paulo: Atlas, 2022.

GONÇALVES, Rita Santos. **O fator humano da cibersegurança nas organizações**. 2019. 52 p. Dissertação (Mestrado em Gestão de Sistemas de Informação) - Universidade de Lisboa. Instituto Superior de Economia e Gestão, 2019. Disponível em: <http://hdl.handle.net/10400.5/19248>. Acesso em: 27 mar. 2023. GUNS, Bob. A organização que aprende rápido: seja competitivo utilizando o aprendizado organizacional. São Paulo: Editora Futura, 1998.

MACIEL, Caroline Stéphanie Francis dos Santos. Governança digital e transparência pública: avanços, desafios e oportunidades. **Liinc em Revista**, [S. l.], v. 16, n. 2, p. e5240, 2020. DOI: 10.18617/liinc.v16i2.5240. Disponível em: <<https://revista.ibict.br/liinc/article/view/5240>>. Acesso em: 27 nov. 2023.

MURR, Caroline Elisa; FERRARI, Gabriel. **Entendendo e aplicando a gamificação**: o que é, para que serve, potencialidades e desafios. Florianópolis: UFSC – UAB, 2020. Ebook disponível em: <<https://sead.paginas.ufsc.br/files/2020/04/eBOOK-Gamificacao.pdf>>. Acesso em 26 nov. 2023.

SANTA CATARINA. TRIBUNAL DE JUSTIÇA (TJSC). **Tribunal de Justiça conclui digitalização de seu acervo de processos físicos**. 2022. Disponível em: <<https://www.tjsc.jus.br/web/imprensa/-/tribunal-de-justica-conclui-digitalizacao-de-seu-acervo-de-processos-fisicos>>. Acesso em: 26 nov. 2023.

_____. **Planejamento estratégico 2021-2026**. 2021a. Disponível em: <https://www.tjsc.jus.br/documents/27424/34827/Relat%C3%B3rio+planejamento_estrategico_2021_2026.pdf/051ed3ab-21f0-f49d-8310-4e602e0d622f?t=1625679373163>. Acesso em: 30 nov. 2023.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa em administração**. 12. ed. São Paulo: Atlas, 2010.

ZOTTI, Ângela Iara. **Engajamento de gestores públicos e cidadãos através de uma métrica baseada em elementos de gamificação**. 2014. 130 p. Dissertação (Mestrado) - Universidade Federal de Santa Catarina, Centro Tecnológico. Programa de Pós-Graduação em Engenharia e Gestão do Conhecimento, Florianópolis, 2014. Disponível em: <https://repositorio.ufsc.br/xmlui/handle/123456789/129588>. Acesso em: 28 nov. 2023.