INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA
CURSO SUPERIOR DE TECNOLOGIA EM GESTÃO PÚBLICA

MARCELO JOSÉ DE LIMA

SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NA ADMINISTRAÇÃO PÚBLICA NO BRASIL: UMA BREVE REVISÃO BIBLIOGRÁFICA

CACOAL-RONDÔNIA
2024

MARCELO JOSÉ DE LIMA

SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NA ADMINISTRAÇÃO PÚBLICA NO BRASIL: UMA BREVE REVISÃO BIBLIOGRÁFICA

Trabalho de Conclusão de Curso apresentado como requisito parcial para aprovação no Curso Superior de Tecnologia em Gestão Pública.

Orientador(a): Prof(ª). Dr(ª). Josiane Silva.

CACOAL-RONDÔNIA

2024

Ficha catalográfica elaborada pelo Sistema Gerador de Ficha Catalográfica do IFRO, com dados informados pelo(a) próprio(a) autor(a).

Lima, Marcelo José de.
Segurança da tecnologia da informação e comunicação na administração pública no Brasil: uma breve revisão bibliográfica / Marcelo José de Lima, Cacoal-RO, 2024.
28 f.

Orientador(a): Profª. Dra. Josiane Silva.

Trabalho de Conclusão de Curso (Superior de Tecnologia em Gestão Pública EAD) – Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO, Cacoal-RO, 2024.

1. Tecnologias. 2. Informação. 3. Internet. 4. Administração Pública. 5. Segurança. I. Silva, Josiane (orient.). II. Instituto Federal de Educação, Ciência e Tecnologia de Rondônia - IFRO. III. Título.

Bibliotecário(a) Responsável: Fernanda de Oliveira Freitas Cavalcante, CRB-11/762 (Campus Cacoal)

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE RONDÔNIA
Cacoal - Código INEP: 11109815
Rodovia BR 364, Lote 2A, CEP 76960-970, Cacoal (RO)
CNPJ: 10.817.343/0008-73 - Telefone: (69) 2182-9641

ATA DE DEFESA DE TRABALHO DE CONCLUSÃO DE CURSO

Na data 27/04/2024 realizou-se a sessão pública de defesa do Trabalho de Conclusão de Curso intitulada **SEGURANÇA DA TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO NA ADMINISTRAÇÃO PÚBLICA NO BRASIL: UMA BREVE REVISÃO BIBLIOGRÁFICA** apresentada pelo aluno **Marcelo Jose de Lima (2020208110009)** do Curso **Superior de Tecnologia em Gestão Pública (Cacoal)**. Os trabalhos foram iniciados às **09:00** pelo Professor **Josiane Silva** presidente da banca examinadora, constituída pelos seguintes membros:

- **Josiane Silva** (Orientadora)
- **Magno Batista Amorim** (Examinador Interno)
- **Fabiano Rodrigues de Carvalho** (Examinador Externo)
- **Poliana Santos** (Examinadora Externa)

A banca examinadora, tendo terminado a apresentação do conteúdo do Trabalho de Conclusão de Curso, passou à arguição do candidato. Em seguida, os examinadores reuniram-se para avaliação e deram o parecer final sobre o trabalho apresentado pelo aluno, tendo sido atribuído o seguinte resultado:

[X] APROVADO **Nota: 9**

Proclamados os resultados pelo presidente da banca examinadora, foram encerrados os trabalhos e, para constar, eu **Josiane Silva** lavrei a presente ata que assino juntamente com os demais membros da banca examinadora.

CACOAL / RO, 27/04/2024

Documento assinado eletronicamente por **MARCELO JOSE DE LIMA**, Discente, em 09/07/2024, às 09:38, conforme horário oficial de Rondônia, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Josiane Silva**, Orientador, em 09/07/2024, às 08:41, conforme horário oficial de Rondônia, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **FABIANO RODRIGUES DE CARVALHO**, Examinador Externo, em 10/07/2024, às 08:01, conforme horário oficial de Rondônia, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Documento assinado eletronicamente por **Poliana Santos**, Examinador Externo, em 10/07/2024, às 07:38, conforme horário oficial de Rondônia, com fundamento no art. 6º, § 1º, do Decreto nº 8.539, de 8 de outubro de 2015.

Dedico este trabalho a todas as pessoas que fizeram e fazem parte do meu convívio: familiares, amigos, colegas de profissão, professores e a todos, que ao longo da minha carreira acadêmica me inspiraram e me ajudaram de alguma forma na concretização dessa importante etapa.

AGRADECIMENTOS

Agradeço, primeiramente, ao Deus Criador pela oportunidade de poder concluir mais essa etapa em minha vida e por me cuidar, fortalecendo-me nos momentos de dificuldades.

À minha família por toda a compreensão e apoio a mim dispensados, mesmo em meio a tantas dificuldades que tivemos nesses últimos anos. Obrigado por acreditarem que seria possível dar mais esse passo e que seria possível a conquista.

Aos meus colegas da graduação, que me ajudaram e que sempre estiveram dispostos a unir forças para que pudéssemos realizar de forma coordenada, em equipe, as atividades e trabalhos acadêmicos ao longo desses anos de jornada e aprendizagem.

À minha professora orientadora Drª. Josiane Silva pela dedicação e presteza e por ter me dado um direcionamento na produção desse trabalho acadêmico. Estou profundamente grato.

Aos demais professores, coordenadores, profissionais e servidores do *campus* do IFRO de Cacoal-RO e também aos professores Marialva de Souza Silva, Reuria da Silva Moreira, Magno Amorim e Gabriel Tenório dos Santos pela prontidão a mim dispensada.

RESUMO

O presente trabalho busca fazer uma concisa revisão de bibliografias acerca das tecnologias da informação e comunicação -TICs, abordando a evolução dessas tecnologias nas últimas duas décadas e a aplicação delas no setor público. Buscou-se ainda discorrer sobre o conceito de tecnologia, o avanço da internet, perpassando pela *Web 1.0*, seguindo para a *Web 2.0* bem como a aplicação dessas ferramentas pela Administração Pública, que se tornaram fundamentais dentro de qualquer organização. Tratou ainda a respeito da importância da segurança digital desses dados, informações e comunicações principalmente pelas entidades, públicas e privadas, detentoras de grandes bancos de dados, uma vez que o mundo vem se transformando com essas novas tecnologias digitais, que ganharam mais e mais espaço dentro das organizações e na vida das pessoas. A metodologia utilizada embasou-se essencialmente em pesquisas de literaturas publicadas sobre o tema, usando o Google Acadêmico e o Scielo como base para as consultas. Por fim, buscou-se com este trabalho levantar uma reflexão sobre a importância do uso seguro das TICs.

Palavras-chave: Tecnologias; Informação; Internet; Administração Pública; Segurança.

ABSTRACT

The present work seeks to make a concise review of bibliographies about information and communication technologies - ICTs, addressing the evolution of these technologies in the last two decades and their application in the public sector. We also sought to discuss the concept of technology, the advancement of the internet, going through Web 1.0, moving on to Web 2.0, as well as the application of these tools by Public Administration, which have become fundamental within any organization. It also discussed the importance of digital security of these data, information and communications, mainly by public and private entities, holders of large databases, since the world has been transforming with these new digital technologies, which have gained more and more space. within organizations and in people's lives. The methodology used was basically based on research into published literature on the topic, using Google Scholar and Scielo as a basis for queries. Finally, this work sought to raise a reflection on the importance of safe use of ICTs.

Keywords: Technologies; Information; Internet; Public administration; Security.

.

LISTA DE ABREVIATURAS E SIGLAS

AGU	Advocacia Geral da União
APS	Agência da Previdência Social
CPEMS	Central de Protocolo Externo para Mandado de Segurança
CPF	Cadastro de Pessoa Física
Dataprev	Empresa de Tecnologia e Informações da Previdência Social
Facimed	Faculdade de Ciências Biomédicas de Cacoal
HRC	Hospital Regional de Cacoal
LGPD	Lei Geral de Proteção de Dados
IFRO	Instituto Federal de Educação, Ciência e Tecnologia de Rondônia
INSS	Instituto Nacional de Seguro Social
PAP	Processo Administrativo Previdenciário
Same	Serviço de Arquivamento Médico e Estatística
SEI	Sistema Eletrônico de Informações
TDICs	Tecnologias Digitais da Informação e Comunicação
TICs	Tecnologias da Informação e Comunicação

Sumário

1. INTRODUÇÃO

O tema abordado no presente trabalho acadêmico foi pensado a partir do estudo de algumas das disciplinas constantes na grade curricular do Curso Superior de Tecnologia em Gestão Pública, tais como as de Organização, Processos e Tomadas de Decisão e Planejamento e Gestão Estratégica, realizadas ainda nos primeiros módulos da graduação e que me chamaram mais atenção. Com isso em mente, comecei então a fazer algumas leituras de pesquisas e trabalhos realizados nessas áreas e notei que elas têm uma considerável relação com a temática do governo eletrônico, atualmente denominado governo digital, que utiliza como base as tecnologias da informação e comunicação - TICs. Também tinha em mente realizar um trabalho acadêmico de conclusão de curso voltado para aquelas áreas em que eu já tive uma certa experiência profissional, como a da Saúde Pública ou da Previdência Social, que, à guisa de conhecimento, fazem parte do chamado tripé da Seguridade Social: Saúde, Previdência Social e Assistência Social. Então, na minha concepção, o curso de Gestão Pública coaduna-se com a qualidade e a melhoria na prestação desses principais serviços públicos disponibilizados à sociedade brasileira.

Desde o começo, a tecnologia e os seus avanços vêm auxiliando a humanidade a processar dados e informações, bem como trazendo comodidade e transformando o dia a dia das pessoas, quer seja no âmbito pessoal, quer seja no âmbito profissional ou social. Assim sendo, é inegável que a tecnologia tem influenciado constantemente o comportamento dos indivíduos em nossa sociedade, ajudando inclusive a resolver diversos problemas e situações. Por exemplo: para que seja construída qualquer coisa, como uma lâmpada, um móvel ou até mesmo um computador, é necessário que haja pesquisa, planejamento e, por fim, criação do produto, gerando assim todo um serviço, que é chamado de tecnologia.

O uso da tecnologia vai depender também do contexto em que ela se encontra. No campo da Biologia, por exemplo, a tecnologia envolve, entre outras coisas, a criação de ferramentas que facilitem o estudo das células e da evolução animal e vegetal. Já no contexto da Arqueologia, a tecnologia pode ser entendida como a evolução dos equipamentos que possibilitam o conhecimento e a investigação de elementos históricos. Na área da Educação, a tecnologia envolve a metodologia de ensino, os recursos didáticos como o quadro-negro, os livros didáticos, o giz, o projetor de multimídia, entre outros, e até mesmo o processo de planejamento de uma aula, de um curso ou de uma disciplina. Portanto, pode-se afirmar que

existem diversos tipos de tecnologia, tais como a tecnologia militar, a tecnologia de construção, a tecnologia medicinal, a tecnologia educacional, a tecnologia industrial, a tecnologia da informação e comunicação e assim por diante.

Por seu turno, as tecnologias da informação e comunicação (TICs) também promoveram inovações dentro da nossa sociedade. A área da tecnologia da informação e da comunicação começou, de certa forma, a se destacar mais que as outras porque houve o desenvolvimento de equipamentos e sistemas que lidam com a distribuição e processamento da informação de modo cada vez mais veloz, abrangendo assim um número crescente de pessoas, instituições e realizando cálculos ainda mais avançados.

No setor governamental, principalmente com o advento da internet ocorrido nas últimas duas décadas, como por exemplo a transição da *Web 1.0* para a chamada *Web 2.0*, acarretou o surgimento do denominado governo eletrônico que, por conseguinte, evoluiu para o governo digital.

1.1 Justificativa

Ao pesquisar sobre o tema de segurança da informação no governo eletrônico no Brasil nas duas últimas décadas e da evolução tecnológica ocorrida nesse período, percebi que esse é uma tendência que eu particularmente presenciei e estou vivenciando na minha carreira profissional dentro do serviço público, pois sou servidor desde o ano de 2008. Essas inovações tecnológicas nos afetam direta ou indiretamente, fazendo com que devemos nos adaptar a essa nova realidade e com isso faz-se necessária também a evolução na segurança da informação e comunicações, já que as ameaças cibernéticas também acompanharam e acompanham a evolução tecnológica e podem vir de todas as partes.

1.2 Objetivos

O objetivo do presente trabalho acadêmico foi discorrer, sem a pretensão de exaurir o assunto, a respeito da segurança da informação e comunicações no governo eletrônico por meio de um recorte de revisão de literatura das últimas duas décadas. Pretende-se assim fazer uma reflexão sobre a importância da segurança da informação e comunicações dentro dos sistemas informatizados utilizados pela Administração Pública. Dessa forma, a presente composição acadêmica visa contribuir no campo da gestão pública no que tange à segurança da informação no âmbito do governo eletrônico, além de contribuir como fonte para consultas e estudos nesta

área e fornecer ao leitor e demais interessados uma base expositiva informativa sobre um pouco do que já tem sido publicado a respeito do tema.

1.3 Definição do Problema de Pesquisa

No nosso dia a dia, existem dados e informações pessoais que preferimos não compartilhar por diversos motivos, mas uma vez compartilhados, você considera importante que as organizações também utilizem uma gestão de segurança dessas informações e dados? Que importância as informações tratadas por uma organização, seja ela pública ou privada, têm e de que forma devem ser encaradas? Devemos lembrar que aquilo que é importante para nós e para os outros deve ser protegido.

2. MEMORIAL FORMATIVO DO PESQUISADOR

Sou discente do Curso Superior de Tecnologia em Gestão Pública do Instituto Federal de Educação, Ciência e Tecnologia de Rondônia (IFRO), *campus* de Cacoal - Rondônia, ingresso na turma 2020/2. Nascido e criado em Cacoal-RO, minha formação básica escolar ocorreu toda em escolas públicas e a minha primeira graduação foi feita na área da Saúde, quando cursei o bacharelado em Enfermagem por meio de bolsa de estudos do Governo Federal na então FACIMED – Faculdade de Ciências Biomédicas de Cacoal, hoje denominada UNINASSAU, tendo concluído o curso em 2010, obtendo assim o título de bacharel em Enfermagem.

Trabalho no setor público há 15 anos. Iniciei a minha trajetória profissional na administração pública em 2008 aos vinte anos de idade, mediante aprovação em concurso público, trabalhando na Secretaria Municipal de Saúde da Prefeitura de Cacoal, onde laborei até o ano de 2010. Nesse período, trabalhei com a equipe do setor administrativo do Hospital Municipal Materno Infantil, antigamente conhecido como SESP, e também no Ambulatório Municipal de Saúde, onde fiquei até o mês de agosto de 2010, quando então me transferi, através de aprovação em um novo concurso público, para o recém inaugurado Hospital Regional de Cacoal – HRC, pertencente ao Governo do Estado de Rondônia. No HRC trabalhei no Serviço de Arquivamento Médico e Estatística (SAME), lidando com os prontuários dos pacientes, que são documentos compilados contendo os dados e o histórico de atendimento do paciente na unidade hospitalar, tais como consultas, patologias, exames, solicitação de exames, cirurgias realizadas e agendadas etc., ou seja, documentos que contêm muitas informações e dados pessoais dos usuários do serviço de saúde. Na época em que trabalhei, tanto no Município de Cacoal quanto na Secretaria de Estado da Saúde de Rondônia, a maior parte das informações ainda eram armazenadas em papel, em que a segurança desses dados era feita de maneira relativamente simples. Aos arquivos das unidades hospitalares, onde a documentação ficava guardada em armários de arquivos chaveados, só tinham acesso os servidores e pessoas autorizadas.

Trabalhei no HRC até o final do ano de 2012, quando então fui convocado, mediante aprovação em concurso público para provimento de cargo efetivo, para trabalhar no Instituto Nacional de Seguro Social (INSS) e onde sigo trabalhando até o presente momento, perfazendo assim onze anos que laboro nesta autarquia previdenciária.

Ao longo desses anos trabalhando no setor público, percebi que algumas melhorias advindas da evolução da tecnologia demoram a chegar, a virar realidade para os usuários de serviços públicos. No INSS, por exemplo, quando comecei a trabalhar, boa parte do serviço ainda era realizada manualmente, os processos administrativos previdenciários – chamados de PAP – eram formalizados em papel. O requerente chegava até à Agência da Previdência Social (APS) no horário previamente agendado, portando os documentos originais acompanhados de suas cópias, e com isso dava-se início ao atendimento e à instrução processual. As cópias, que não precisavam ser autenticadas em cartório perante o tabelião, eram cotejadas por nós servidores públicos com os documentos originais, documentos estes que eram devolvidos e as cópias retidas para compor o processo administrativo, dando-se o carimbo de "confere com o original". Os dados eram lançados nos mais diversos sistemas corporativos e os processos físicos, em papel, que, depois de terem sidos analisados, enumerados e carimbados, seguiam para o arquivo da unidade. Isso tudo, de uma certa forma, atrasava o andamento dos trabalhos na autarquia.

Hoje a realidade da maior instituição previdenciária da América Latina é outra no que diz respeito à tecnologia, pois obteve grandes avanços na parte da informatização. No ano de 2018 houve a chamada "virada de chave", marcando o início da implantação do projeto "INSS Digital" com o lançamento da plataforma MEU INSS (site e aplicativo de celular). E a partir de então os processos concessórios na autarquia foram gradativamente deixando de ser físicos e se tornando digitais e, dessa forma, foram necessários investimentos na infraestrutura tecnológica da instituição. Os processos internos da instituição também passaram por mudanças com a adoção do SEI (Sistema Eletrônico de Informações), uma ferramenta tecnológica que foi desenvolvida por servidores do Judiciário federal e que depois se estendeu para todo o Executivo federal e que também foi implantado em alguns estados da federação, gerando assim uma grande economia de papel e, portanto, de recursos públicos.

Há que se destacar ainda que, com o contexto da pandemia de COVID-19, uma vez que os atendimentos presenciais ficaram restritos à perícia médica e à avaliação social, a entidade se viu obrigada a ter que acelerar essa migração para o processo digital, impactando sobremaneira na sua expansão tecnológica.

Atualmente todos os serviços da autarquia previdenciária são requeridos pela internet ou pelo aplicativo, bem como o envio *online* de documentos. Não existe mais processo físico, em papel, já que os documentos são todos digitalizados, gerando assim redução de tempo,

primando pela celeridade e economicidade na prestação dos serviços públicos à sociedade e reduzindo a burocracia por meio da transformação digital.

Por isso, a autarquia previdenciária, detentora de um dos maiores bancos de dados pessoais do país, por meio da empresa pública Dataprev (Empresa de Tecnologia e Informações da Previdência Social), deve atuar como uma guardiã da confiança e do direito à privacidade de seus segurados e usuários. Os dados pessoais que são geridos por ela merecem o mais alto nível de proteção em conformidade com a Lei Geral de Proteção de Dados (LGPD).

No momento, desde o ano de 2021, estou cedido para a Procuradoria Regional Federal junto à Advocacia Geral da União (AGU), atuando nas demandas judiciais que envolvem o INSS, participando de um grupo de trabalho de forma remota chamado Central de Protocolo Externo para Mandado de Segurança (CPEMS), da Superintendência Regional Norte – Centro-Oeste do INSS, criado por meio da Portaria SR-V/INSS nº 276, de 20 de outubro de 2021.

Para termos acessos aos sistemas corporativos, tanto da instituição previdenciária como da Justiça Federal, e ao *e-mail* institucional, foram realizadas algumas alterações na segurança, em que é necessário o uso de *token* e o chamado segundo fator de autenticação. O duplo fator de autenticação, por sua vez, é um recurso digital utilizado para garantir mais segurança na autenticação de quem realiza o acesso aos sistemas, inserindo assim mais uma camada de proteção, além do usual registro de usuário e senha.

O Curso Superior de Tecnologia em Gestão Pública me interessou devido ao fato de eu estar trabalhando no setor público, prestando serviços à sociedade já há um certo tempo, e também pela vontade de ingressar numa instituição pública federal renomada como o IFRO. O curso do IFRO tem como um dos seus objetivos capacitar o discente para atuar de forma estratégica, ajudando a acompanhar e a construir políticas públicas, implementando mudanças progressivas e melhorias na nossa sociedade de uma forma geral. É um curso que prepara o aluno para se tornar um agente transformador, um profissional para atuar nas mais diversas áreas e demandas da sociedade. Por isso, além de agregar conhecimentos, esse curso é uma excelente ferramenta que proporciona aprimoramento e capacitação para quem também já faz parte da administração pública.

3. REVISÃO DA LITERATURA

3.1 Conceito de Tecnologia

A palavra “tecnologia” tem origem em dois vocábulos do grego antigo, em que o vocábulo “tecno” de *tekhné* significa arte, técnica ou ofício, e o termo “logia”, oriundo de *logos,* que tem o significado de razão ou estudo de algo.

É um termo muito abrangente, mas que pode ser definido basicamente como o conjunto de técnicas, processos, métodos, meios e instrumentos de um ou mais domínios das atividades humanas. É uma aplicação prática do conhecimento científico em diversas áreas e setores da sociedade (BASTOS *et al.*, 2008).

É notável que ocorreu um enorme avanço no mundo com as novas tecnologias e que isso mudou a forma como as pessoas interagem entre si, pensam, estudam, trabalham etc. e na administração pública idem, pois houve mudanças na maneira de o Poder Público prestar seus serviços à sociedade. Tendo isso em consideração, o fato de estarmos vivendo numa sociedade cada vez mais digital, conectada e com inovações tecnológicas constantes, a gestão da segurança da informação e comunicações no chamado governo eletrônico se tornou indispensável, uma vez que ela visa à proteção de dados e informações pessoais, nas organizações públicas e nas privadas que detêm dados pessoais armazenados em seus servidores e sistemas.

O campo da tecnologia da informação e comunicação evoluiu muito, exigindo assim um gerenciamento constante sobre a segurança dos dados e informações, haja vista que as ameaças a essas informações e dados vão sempre existir e as vulnerabilidades podem acontecer a todo momento. Portanto, é um tema bastante relevante considerando o contexto da era tecnológica em que vivemos.

O termo governo eletrônico, em síntese, baseia-se no uso de novas tecnologias de informação e comunicação (TICs), que são aplicadas a um amplo segmento das funções governamentais e na prestação de serviços públicos direcionados à sociedade (RUEDIGER, 2002, p. 01).

Segundo Agune e Carlos (2005, *apud* Diniz *et al.,* 2009, p. 24), a ideia de governo eletrônico, conquanto esteja associada ao uso de tecnologia de informação no setor público,

está vinculada à modernização da administração pública através do uso de TICs bem como na melhoria e eficiência dos processos operacionais e administrativos dentro da gestão pública.

Dentre os motivos que determinaram estrategicamente a adoção das TICs pela administração pública em seus processos internos, predominam-se: o uso intensivo das tecnologias pelas pessoas, pelas empresas privadas e pelas organizações não governamentais; a migração da informação e de dados baseados em papel para mídias eletrônico-digitais e serviços *online* assim como o avanço e a universalização da infraestrutura pública de telecomunicações e da rede mundial de computadores, no intuito de melhorar a prestação dos serviços públicos destinados aos cidadãos. Outros motivos envolvidos são o próprio movimento de reforma do Estado, da modernização da administração pública e da necessidade de eficiência dos gestores públicos. Por consequência, tópicos como desempenho, eficiência, eficácia, transparência, mecanismos de controle, qualidade do gasto público e de prestação de contas, relacionados ao processo de modernização da função administrativa, foram associados ao processo de construção de programas de governo eletrônico. E tudo isso, portanto, demandou e vem demandando o uso de tecnologias, tornando os programas de governo eletrônico elementos que promovem a eficiência dentro da administração pública (DINIZ *et al.,* 2009, p. 24).

3.2 Web 2.0

A *Web 2.0* é considerada a segunda geração da internet, uma evolução que se iniciou a partir da chamada *Web 1.0*, em que as páginas da internet eram praticamente estáticas e unidirecionais, significando que, ao carregá-las, eram mostrados conteúdos sem nenhum tipo de interação com o usuário nem havia necessidade de se fazer algum *login* para ter acesso a eles. Sendo assim, os sites também não monetizavam com anúncios e publicidade. Isso perdurou por mais ou menos entre os anos de 1991 e 2004. Até então, as pessoas eram apenas consumidores passivos de conteúdos e informações da rede mundial de computadores e também não havia necessidade de realizar nenhuma ação para contribuir com a funcionalidade das páginas. A *Web 2.0* foi uma quebra de paradigma muito grande no campo da internet, alterando o processo histórico de comunicação e interação entre as pessoas e as páginas da *web*.

Com o passar do tempo, foram adicionados às páginas alguns recursos mais tecnológicos, como o *Flash* e *Java Script*. Foi então que, com essas e várias outras ferramentas, surgiu a conhecida *Web 2.0* por volta do ano de 2004, uma internet muito mais dinâmica em que os conteúdos são feitos por milhões de usuários que se conectam entre si, permanecendo

assim até os dias atuais. Desde então a internet evoluiu bastante, permitindo a interatividade entre os sites que produzem conteúdos e os seus diversos usuários.

Conforme Machado (2008, p. 02), a *Web 2.0* tornou a internet mais dinâmica, interativa, flexível para os conteúdos e publicações, deixando de ter uma característica inerte e podendo ser editada tanto por profissionais da área como pelos próprios usuários. Mas o principal aproveitamento é o da inteligência coletiva baseada em uma rede de informações em que cada usuário passa a ser criador de conteúdos.

Pode-se afirmar então que a *Web 2.0* é também considerada a internet da era da publicidade. Porém, apesar de toda essa evolução, abrimos mão, de certa forma, da nossa privacidade para que a inteligência artificial dos sites e aplicativos nos entregue exatamente aquilo que queremos ver, pesquisar etc. Dessa forma, para cada usuário da *Web 2.0*, a experiência é única, uma vez que ocorre de acordo com aquilo que é consumido, e isso determina o que será mais ou menos relevante, por meio da lógica de programação e algoritmos, para o que irá ser sugerido, causando uma verdadeira revolução na internet. Tudo isso veio através da interatividade possibilitada pelos novos recursos tecnológicos adicionados às plataformas.

Por meio da internet, uma gama de sistemas de distribuição de informações, tornou-se possível inclusive a participação da sociedade nos atos do governo, proporcionando a capacidade do exercício do controle social, mais interação entre os diversos atores, mais tráfego de informações entre as pessoas, enfim.

3.3 Tecnologias da Informação e Comunicação e Tecnologias Digitais da Informação e Comunicação – TICs e TDICs

A utilização da tecnologia no nosso dia a dia, destarte, tornou-se algo habitual, e nas organizações da mesma forma. Estamos vivendo em um mundo que se encontra em constante transformação, no qual a evolução tecnológica vem influenciando o comportamento da sociedade, cujas informações produzidas vêm se tornando mais e mais presentes no universo digital. Em meio a essa evolução tecnológica surgiu um novo conceito: tecnologias digitais da informação e comunicação, as TDICs. As TICs, ou seja, as tecnologias da informação e comunicação, correspondem a tecnologias que interferem e mediam os processos informacionais e comunicativos das pessoas, como por exemplo, o rádio, o jornal, a tv etc. Já as TDICs, tecnologias digitais da informação e comunicação, referem-se a um conjunto de

diferentes mídias que se diferenciam pela presença de tecnologia digital, ou seja, são equipamentos que se utilizam de processamento de dados armazenados que funcionam através da decodificação de códigos numéricos. Porém, há muitos autores que não diferenciam os dois termos - TICs x TDICs, e os utilizam como sinônimos. E já para outros, as TDICs são uma evolução das TICs.

As organizações públicas, por sua vez, vêm utilizando essas ferramentas que as tecnologias digitais da informação e comunicação disponibilizam, de forma a se adequar e acompanhar a evolução pela qual a sociedade vem passando, buscando aproximar o serviço público dos cidadãos com foco na eficiência na prestação estatal. A tecnologia, consequentemente, está facilitando a gestão pública e auxiliando os usuários dos diversos serviços públicos.

O governo digital implementou assim um novo modelo de gestão na administração pública e modificou o relacionamento entre os órgãos públicos e a sociedade por meio da modernização do Estado. É válido afirmar, portanto, que estamos vivendo em um mundo cada vez mais digital.

3.4 Governo, Privacidade de Dados e Segurança

As informações, por seu turno, são a base para o trabalho das mais diversas instituições. Em sua obra intitulada Gestão da Informação, Beato (2004, p. 08) contextualiza que:

> "as informações constituem o insumo básico para o trabalho das organizações [...], e a forma como elas a produzem, organizam, disponibilizam e utilizam é que determinarão a natureza e efetividade das atividades desenvolvidas" (BEATO, 2004, p. 08).

Assim, os funcionários das organizações, no decorrer de suas atividades, lidam frequentemente com informações e dados pessoais importantes tanto do público externo como do público interno, o que torna essencial a disseminação dos conceitos e implementação de práticas voltadas à gestão da segurança da informação e comunicações dentro das organizações assim como na vida pessoal e profissional de seus colaboradores. Nesse sentido, Neves *et al*. (2021, p. 186) descreve que:

> "a contínua expansão dos negócios gera diariamente uma enorme massa de dados, com informações pessoais e organizacionais, públicas ou privadas. Sobre essa massa há uma grande necessidade de atenção e cuidados, pois nela transita qualquer tipo de informação como fotos, vídeos, relatórios médicos, policiais e judiciais, dados que devem ser mantidos sob sigilo" (NEVES *et al.*, 2021, p. 186)

A segurança da informação está associada à proteção de informações, sistemas, recursos e serviços contra incidentes, erros e acessos indevidos ou manipulação não autorizados (MELLO, 2010, p. 15).

Ao confiar seus dados e informações às instituições, a pessoa continua sendo a proprietária desses dados e informações e é por esse motivo que a coleta e o tratamento de dados e informações pelas organizações devem ser mantidos de forma mais segura possível.

Na administração pública digital – conceito amplo que reflete a inserção do setor público na era dos dados e da comunicação – o Estado se posiciona como um importante agente de tratamento, que coleta e processa os mais diversos dados (independentemente da tipologia do dado) em busca de uma atuação de forma mais eficiente, transparente, participativa e que busca fomentar a política baseada em evidências (MENDES *et al*., 2023, p. 05).

A Constituição Federal do Brasil de 1988, por sua vez, ao tratar dos direitos e garantias fundamentais em seu Título II, disciplina que a intimidade e a vida privada dos indivíduos são invioláveis, sob pena de indenização por danos morais e materiais nos casos de violação. Com isso, podemos inferir que nossos dados pessoais foram salvaguardados no bojo da Lei Maior do nosso País. Determina, então, o texto constitucional que "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, [Constituição 1988]).

A privacidade está intrinsecamente ligada ao direito de uma pessoa poder controlar as informações e os dados que são compartilhados sobre si mesma. Por isso, a nossa Carta Magna é muitas vezes denominada de Constituição Cidadã, haja vista que a dignidade da pessoa humana é tida como um dos seus fundamentos, um alicerce da nossa República Federativa.

Baião e Gonçalves (2014, p. 13) complementam o assunto ora estudado mencionando que “no universo das sociedades tecnologicamente avançadas, o respeito à privacidade como direito fundamental se apresenta como exigência cada vez mais urgente, vez que essencial à própria dignidade humana”. Daí a imprescindibilidade da gestão da segurança da informação e comunicações, composta de ações que objetivam viabilizar bem como assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

Como seria, por exemplo, o trabalho de um servidor que atua na maior autarquia pública do País, qual seja, o Instituto Nacional do Seguro Social (INSS), que possui um dos maiores bancos de dados pessoais de toda a Administração Pública Federal, laborando na análise e concessão de benefícios e serviços previdenciários e assistenciais, sem acesso aos dados pessoais dos segurados e usuários? É extremamente difícil imaginar essa situação e, por isso mesmo, o colaborador integrante desta eminente autarquia pública deve se encarregar de protegê-los. O INSS, por ser uma instituição pública e por deter um dos maiores bancos de dados pessoais, deve, como as demais instituições públicas, preservar a integridade dessas informações, protegendo assim os direitos fundamentais de liberdade e privacidade insculpidos na nossa Carta Política. Todo CPF informado em um requerimento de benefício ou serviço previdenciário ou assistencial, por exemplo, representa uma pessoa e sua história. Não é apenas um número, pois traz consigo a representatividade de cada cidadão que vai em busca de um direito, em prol de oferecer uma vida digna para si e seus dependentes.

Muitos dos requerimentos de benefícios e serviços previdenciários requeridos perante a instituição previdenciária trazem consigo, portanto, dados sensíveis dos solicitantes. À guisa de exemplo, um requerimento de benefício por incapacidade, o antigo benefício de auxílio-doença, na maior parte das vezes, contém exames ou atestados médicos em anexo, com dados sobre a saúde do cidadão e, por vezes, a indicação da patologia que ocasionou a incapacidade laborativa do segurado. Por isso, cada pessoa confia que a sua privacidade será respeitada ao fornecer informações dessa natureza.

De acordo com Mendes *et al.* (2023, p. 04), faz-se necessário então que os órgãos públicos, principalmente os que possuem dados coletados e tratados em grande escala, como no caso do INSS, estabeleçam mecanismos e uma gestão permanente de segurança com consistência e efetividade para regular o uso de dados pessoais, como por exemplo fomentação de programas voltados para a governança em privacidade de dados.

Desde o ano 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) visa oferecer ao cidadão o controle sobre o tratamento de seus dados pessoais e, para isso, estabelece princípios e cria regras a serem observadas por organizações públicas e privadas.

A recente Lei nº 13.709, de 14 de agosto de 2018, apresenta as classificações dos dados em: pessoais, sensíveis e públicos. Os dados pessoais são aqueles fornecidos em um cadastro, possibilitando a identificação direta ou indireta como nome, identidade, CPF, gênero, data e local de nascimento, filiação, telefone etc. Já os dados pessoais sensíveis são as informações que podem causar algum tipo de vulnerabilidade ou discriminação, como, por exemplo, de estado civil, religião, etnia, escolaridade, orientação sexual, biometria, entre outros - daí a classificação como dados pessoais sensíveis (BRASIL, 2018).

Além desses, há, ainda, os dados públicos, que podem ser disponibilizados obedecendo-se ao princípio constitucional da publicidade, desde que presentes a boa-fé e o interesse público, e os dados chamados anonimizados, assim classificados quando não é possível construir um caminho para identificar a titularidade de um dado (BRASIL, 2018). A título de conhecimento, conforme Pinheiro (2020, p. 15), os dados anonimizados são aqueles relativos a uma pessoa que não possa ser identificada, considerando a utilização de meios técnicos razoáveis e disponíveis no momento de seu manuseio.

As informações tratadas por uma instituição, seja ela pública ou privada, em muitos casos contêm dados sensíveis e/ou privados e, por isso, devem ser protegidas, mantidas com a devida segurança. Contudo, essa tarefa se constitui num verdadeiro desafio, pois 100% de segurança é algo que não existe, tendo em vista que sempre haverá a possibilidade de ocorrer falhas tanto no sistema de segurança da informação e comunicações quanto falhas humanas; falhas essas conhecidas como vulnerabilidades. Daí o relevante papel da gestão da segurança da informação e comunicações nas organizações, uma vez que se deve sempre estar atento a possíveis vulnerabilidades.

Temos acompanhado quase diariamente notícias de ciberataques e vazamentos de dados. À medida que mais pessoas têm acesso às TDICs, mais recorrentes vão se tornando os incidentes envolvendo ataques de cibercriminosos, como vazamentos e roubo de informações etc. Segundo Prokisch (2023, p. 05):

> “Vivemos hoje a era da conectividade. São inúmeros dispositivos conectados às redes de computadores, milhões de sistemas e dados armazenados em nuvem. Mas a praticidade proporcionada pela tecnologia tem um preço: o aumento de ameaças e ataques cibernéticos” (PROKISCH, 2023, p. 05).

Conforme explica Oliveira (2017, p. 05), a segurança da informação, portanto, é um tema que as instituições devem ter como prioridade, pois existem brechas que, por mínimas que sejam, podem abrir caminho para que indivíduos mal-intencionados causem diversos prejuízos a organizações de pequeno a grande porte, e às pessoas que têm seus dados e informações guardados nelas. No entanto, com o auxílio da própria tecnologia, pois há várias ferramentas, e do próprio ambiente organizacional, a segurança digital pode ser garantida de modo satisfatório.

A sociedade de modo geral deposita confiança no serviço público e nas organizações e espera um comprometimento ético das pessoas que acessam equipamentos e sistemas contendo suas informações e dados, bem como que as organizações garantam a redução dos riscos de quebra da segurança dessas informações e dados que estão sob sua guarda. Nesse sentido, no entendimento de De Castro *et al.* (2019, p. 01), a segurança e a privacidade são de interesse de boa parte dos usuários de serviços *online* e, assim sendo, eles confiam que, quando fornecidos, seus dados estejam protegidos nos sistemas dessas organizações. Da mesma forma, Neves *et al*. (2021, p. 186) argumenta que “a garantia da segurança dos dados fica sob a responsabilidade das empresas que realizam a coleta”.

4. METODOLOGIA

O presente trabalho de conclusão de curso constitui-se essencialmente em uma sinóptica revisão bibliográfica, na qual o conteúdo foi desenvolvido por meio de uma síntese narrativa das ideias centrais dos autores contidas nas produções referenciadas na temática da segurança da informação no governo digital. Os métodos de pesquisa que foram empregados baseiam-se, portanto, em consultas a literaturas especializadas tais como artigos, monografias, revistas científicas, livros digitais e demais periódicos publicados no interregno de 2002 a 2023.

Foram utilizados como base de dados para a composição do presente trabalho o Google Acadêmico e o Scielo, nos quais foram identificadas e selecionadas as obras por meio de uma lista de palavras-chave para facilitar a localização das produções bibliográficas e sua leitura para então ser feito o compêndio dos textos com vistas à realização deste estudo.

5. CONSIDERAÇÕES FINAIS

A internet e as TDICs são ferramentas de comunicação e interação imprescindíveis que abrangem praticamente toda a sociedade. No tocante à gestão pública, num primeiro momento, as ações governamentais feitas através das TICs eram mais voltadas para a parte operacional, ou seja, quando a administração pública passou a fazer uso dessas tecnologias, o objetivo era mais voltado para as questões operacionais internas do próprio governo e dos seus órgãos.

Com o avanço tecnológico dessas ferramentas, o governo tornou possível à população ter mais acesso à informação pública e a ter mais proveito dos serviços públicos disponibilizados por meio da tecnologia digital da informação e comunicação, a conhecida TDIC, e a internet. Assim, foi-se ampliando o leque de possibilidades entre o governo e a sociedade, uma vez que, com o avanço das TICs e da internet, foram criados novos canais de relacionamento e de interação entre o setor público e os seus usuários bem como entre as próprias pessoas e as organizações de um modo geral.

À medida que as TICs foram evoluindo, o governo digital também foi incorporando, acompanhando, mesmo que de forma um tanto lenta, os avanços dessa tecnologia e assim foi possível ampliar a atuação estratégica do Estado, trazendo mais qualidade, eficiência, agilidade e, por consequência, gerando economia de recursos públicos. Houve também a promoção do fortalecimento do exercício da cidadania, possibilitando a realização das práticas democráticas pela população, a melhoria da governança pública e a integração entre os níveis de governo. Proporcionou ainda um incremento no processo de tomada de decisão pelos gestores públicos, trazendo mais transparência na sua gestão e facilitando a prestação de contas aos órgãos de controle e principalmente à própria sociedade.

Apesar de todos esses benefícios e vantagens que a evolução da tecnologia da informação proporcionou para a população e à administração pública, vieram também as ameaças digitais. Por isso, é de fundamental importância a adoção de técnicas e ferramentas para identificar, estimar, monitorar e administrar os acontecimentos que possam colocar em risco a segurança digital das informações e comunicações, uma vez que os impactos causados pelos acessos indevidos e roubos de informações pessoais e institucionais podem ser inestimáveis.

Embora haja incontáveis riscos à segurança da informação e comunicação, enquanto usuários de tecnologia da informação e comunicação, há a necessidade de tomarmos algumas precauções que dificultarão a atuação de pessoas mal intencionadas. Portanto, deve-se ter muito cuidado ao passar informações por telefone, ao receber e-mail, mensagens de redes sociais etc. Deve-se também sempre criar senhas difíceis de serem descobertas, fazer alterações nelas frequentemente, usar redes de internet confiáveis, manter os programas antivírus sempre atualizados etc.

REFERÊNCIAS

BAIÃO, Kelly C. Sampaio; GONÇALVES, Kalline Carvalho. **A garantia da privacidade na sociedade tecnológica: um imperativo à concretização do princípio da dignidade da pessoa humana**. Civilistica. com, v. 3, n. 2, p. 01-24, 2014.

BASTOS, Maria do Socorro Rocha *et al*. **Ferramentas da ciência e tecnologia para a segurança dos alimentos**. Fortaleza: Embrapa/BNB, 2008.

BEATO, Cláudio. **Gestão da informação**. Coleção Segurança, p. 08-47, 2004.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil**. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 de outubro de 2023.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, ano 155, n. 157, p. 59-64, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 12 de outubro de 2023.

DE CASTRO, Ariel Góes *et al*. **Os meus dados de fato vazaram? Uma análise de serviços que monitoram vazamentos de dados na Internet**, p. 01-06, 2019.

DINIZ, Eduardo Henrique *et al*. **O governo eletrônico no Brasil: perspectiva histórica a partir de um modelo estruturado de análise**. Revista de Administração Pública, v. 43, p. 23-48, 2009.

MACHADO, Ana Claudia Teixeira. **Novas formas de produção de conhecimento: utilização de ferramentas da web 2.0 como recurso pedagógico**. Revista Udesc Virtu@ l, v. 1, n. 2, 2008.

MELLO, Cláudio Oscílio Santos de. **Gestão de riscos em segurança da informação utilizando o "risk manager"**, p. 13-61, 2010.

MENDES, Cássia Isabel Costa *et al*. **Programa de governança em privacidade e proteção de dados pessoais na Administração Pública Federal**, p. 01-38, 2023.

NEVES, Denise Lemes Fernandes *et al*. A segurança da informação de encontro às conformidades da LGPD. **Revista Processando o Saber**, v. 13, p. 186-198, 2021.

OLIVEIRA, Warlisson Costa de. **Implementação de políticas de segurança da Informação na Empresa PNEUCAR com base nas diretrizes da ABNT NBR ISO/IEC 27005**, p. 05-90, 2017.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais: Comentários à lei n. 13.709/2018-lgpd**. Saraiva Educação S.A, p. 01-152, 2020.

PROKISCH, Carlos A. **Soluções para a proteção de redes e sistemas**. Senac São Paulo, p. 05-128, 2023.

RUEDIGER, Marco Aurélio. **Governo eletrônico ou governança eletrônica: conceitos alternativos no uso das tecnologias de informação para o provimento de acesso cívico aos mecanismos de governo e da reforma do Estado**. In: Anais do Congresso del CLAD, Caracas, Venezuela, p. 01-34. 2002.