UNIVERSIDADE FEDERAL DO TOCANTINS
CAMPUS UNIVERSITÁRIO DE PALMAS
PROGRAMA DE PÓS-GRADUAÇÃO PROFISSIONAL EM
MODELAGEM COMPUTACIONAL DE SISTEMAS

JOÃO CARLOS VILELA BATELLO

ESTUDO DE VIABILIDADE PARA A IMPLANTAÇÃO DO PLANO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO TOCANTINS

Palmas-TO
2020

JOÃO CARLOS VILELA BATELLO

ESTUDO DE VIABILIDADE PARA A IMPLANTAÇÃO DO PLANO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO TOCANTINS

Dissertação apresentada ao Programa de Pós-Graduação em Modelagem Computacional de Sistemas. Foi avaliada para obtenção do título de Mestre em Modelagem Computacional de Sistemas e aprovada em sua forma final pelo orientador e pela Banca Examinadora.

Orientador: Professor Doutor Gentil Veloso Barbosa

Palmas-TO
2020

Dados Internacionais de Catalogação na Publicação (CIP)
Sistema de Bibliotecas da Universidade Federal do Tocantins

B328e Batello, João Carlos Vilela.

Estudo de Viabilidade para a Implantação do Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins. / João Carlos Vilela Batello. – Palmas, TO, 2020.

116 f.

Dissertação (Mestrado Acadêmico) - Universidade Federal do Tocantins – Câmpus Universitário de Palmas - Curso de Pós-Graduação (Mestrado) em Modelagem Computacional de Sistemas, 2020.

Orientador: Gentil Veloso Barbosa

1. Segurança da Informação. 2. Fluxo do Processo. 3. Plano de Conscientização. 4. Cultura de Boas Práticas. I. Título

CDD 004

Elaborado pelo sistema de geração automática de ficha catalográfica da UFT com os dados fornecidos pelo(a) autor(a).

FOLHA DE APROVAÇÃO

JOÃO CARLOS VILELA BATELLO

ESTUDO DE VIABILIDADE PARA A IMPLANTAÇÃO DO PLANO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO NO PODER JUDICIÁRIO DO TOCANTINS

Dissertação apresentada ao Programa de Pós-Graduação em Modelagem Computacional de Sistemas. Foi avaliada para obtenção do título de Mestre em Modelagem Computacional de Sistemas e aprovada em sua forma final pelo orientador epela Banca Examinadora.

Data de Aprovação: 01 / 07 / 2020

Banca Examinadora

Professor Doutor Gentil Veloso Barbosa, UFT

Professor Doutor George Lauro Ribeiro de Brito, UFT

Professor Doutor Gerson Pesente Focking, IFTO

Palmas-TO
2020

Dedico este trabalho primeiramente a Deus e a Nossa Senhora Aparecida, que não me deixaram fraquejar perante as adversidades.
À minha esposa, Guiomar Batello, pelas orientações, incentivo e paciência.
Às minhas filhas, Sophia e Gabrielly, que são a dose diária de incentivo para a conclusão deste trabalho.
Aos meus pais, José Carlos e Lucineá, meus irmãos e cunhadas Luciano e Katiuscy, Marco Aurélio e Adriana, e a toda minha família que sempre me apoiaram.

AGRADECIMENTOS

A Deus pelo dom da vida e por me possibilitar a conclusão deste trabalho.

Ao Tribunal de Justiça do Estado do Tocantins e à Escola Superior da Magistratura Tocantinense (ESMAT) pelo apoio institucional e financeiro para realização deste trabalho.

Ao meu orientador professor Doutor Gentil Veloso Barbosa pela paciência, disponibilidade, dedicação e orientação.

Aos professores e colegas da primeira turma do Mestrado em Modelagem Computacional de Sistemas da Universidade Federal do Tocantins em parceria com a Escola Superior da Magistratura Tocantinense, pelo aprendizado.

À equipe da Divisão de Administração e Segurança de Redes, Marcelo Leal, Ricardo Marx, Danillo Lustosa e Tiago Luz, que me apoiaram no desenvolvimento desta pesquisa e pela troca de experiências na área de Segurança da Informação.

E a todos aqueles que de alguma forma, direta ou indiretamente, contrubuíram para a conclusão dessa etapa.

Muito obrigado!

RESUMO

O presente estudo visa conscientizar e disseminar a cultura de boas práticas relacionadas à segurança da informação para magistrados e servidores do Poder Judiciário do Tocantins, por meio de um plano de conscientização. Esta pesquisa se caracteriza como exploratória, com abordagem Quali-quantitativa e de natureza aplicada. Para o alcance dos objetivos desta pesquisa, foram realizadas revisões bibliográficas, documental e estudo de caso com vista a apresentar embasamento teórico sobre o assunto tratato. Dessa forma, visando à normatização do Plano de Conscientização em Segurança da Informação, foi elaborada a Minuta com a Norma TIC-09, e para cumprir o propósito desta, foram elaborados o Fluxo do Processo, o Formulário de Conscientização e o Termo de Ciência da PSI. Para subsidiar este trabalho, foi realizado o levantamento dos meios de comunicação existente no PJTO, bem como a aplicação de um instrumento de pesquisa – questionário – com 21 perguntas divididas em três dimensões: Comportamento; Conscientização e Perfil, obtendo resultado satisfatório quanto ao seu objetivo. Ao ser institucionalizado o Plano de Conscientização em Segurança da Informação no Tribunal de Justiça do Estado do Tocantins, este estará de acordo com o recomendado pelas Normas ISO 27001 e 27002; e atendendo às Resoluções do Conselho Nacional de Justiça (CNJ); Portarias nº 3.433 e 1.660 e Resolução nº 22 do TJTO. Assim, este trabalho tem contribuíção fundamental ao cumprimento das normas, resoluções, portarias, metas e principalmente na disseminação da cultura de boas práticas voltadas à Segurança da Informação entre magistrados e servidores do Poder Judiciário do Tocantins.

Palavras-chave: Segurança da Informação. Fluxo do Processo. Plano de Conscientização. Cultura de Boas Práticas.

ABSTRACT

This study aims to raise awareness and disseminate the culture of good practices related to information security for magistrates and civil servants of the Judiciary of Tocantins, through an awareness plan. This research is characterized as exploratory, with a qualitative approach and applied nature. To achieve the objectives of this research, bibliographic, documentary and case study reviews were carried out with a view to presenting theoretical basis on the subject. Thus, aiming at the standardization of the Information Security Awareness Plan, the Draft was prepared with the ICT-09 Standard, and to fulfill its purpose, the Process Flow, the Awareness Form and the PSI Science Term were elaborated. To support this work, the survey of the media existing in the PJTO was carried out, as well as the application of a research instrument - questionnaire - with 21 questions divided into three dimensions: Behavior; Awareness and Profile, obtaining satisfactory result regarding its objective.When the Information Security Awareness Plan is institutionalized at the Court of Justice of the State of Tocantins, it will be in accordance with the recommended by ISO 27001 and 27002; and taking into account the Resolutions of the National Council of Justice (CNJ); Ordinances No. 3,433 and 1,660 and Resolution No. 22 of the TJTO. Thus, this work has a fundamental contribution to compliance with the norms, resolutions, ordinances, goals and especially in the dissemination of the culture of good practices aimed at Information Security among magistrates and civil servants of the Judiciary of Tocantins.

Keywords: Information Security. Process Flow. Awareness Plan. Culture of Good Practices.

LISTA DE ILUSTRAÇÃO

LISTA DE GRÁFICOS

LISTA DE TABELAS

LISTA DE QUADRO

LISTA DE SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CERT.br	Grupo de Resposta a Incidentes de Segurança para a Internet
CGSI	Comitê Gestor de Segurança da Informação Multidisciplinar
CNJ	Conselho Nacional de Justiça
DISI	Dia Internacional de Segurança em Informática
DTINF	Diretoria de Tecnologia da Informação
ENTIC-JUD	Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário
GRSI	Gestão de Riscos de Segurança da Informação
IM	Mensagem Instantânea
NBR	Norma Brasileira
NIC.br	Comitê Gestor da Internet no Brasil
NIST	National Institute of Standards and Technology
PJTO	Poder Judiciário do Tocantins
PSI	Política de Segurança da Informação
RNP	Rede Nacional de Ensino e Pesquisa
SI	Segurança da Informação
SEI	Sistema Eletrônico de Informações
TCU	Tribunal de Contas da União
TI	Tecnologia da Informação
TJTO	Tribunal de Justiça do Estado do Tocantins
USB	Universal Serial Bus
XMPP	Extensible Messaging and Presence Protocol

SUMÁRIO

1. INTRODUÇÃO

Com o crescimento de ameaças – a Segurança da Informação – as quais afetam setores públicos e privados, e recentemente atingiram níveis alarmantes, o grande desafio das organizações é a incansável luta para manter em segurança seus e ativos e suas informações.

De acordo com a Norma ABNT NBR ISO/IEC 17799:2005, a informação "é um ativo que, como qualquer outro ativo, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegido".

Conforme Sêmola (2004), a Segurança da Informação pode ser definida como área do conhecimento dedicada à proteção de ativos de informação contra acessos e alterações indevidas, de forma a garantir a confiabilidade, integridade e disponibilidade das informações.

A segurança da Informação se tornou nos últimos anos um dos assuntos mais relevantes no meio organizacional, pois com os avanços da tecnologia, mais dados e informações passam a ser armazenados, e assim disponibilizados a qualquer lugar do Planeta de forma rápida e eficiente. Com esse avanço digital, o mundo vem passando por transformações contínuas, em que a globalização é fundamentada pelas conexões em rede, contribuindo cada vez mais com o crescimento das transações eletrônicas que incluem correspondências digitais, operações comerciais, bancárias, entre outras (FERREIRA, 2013).

Segundo Sêmola (2014), a política de Segurança da Informação tem papel fundamental e, guardadas as devidas proporções, tem importância similar à da Constituição Federal de um país. Dessa forma, pode-se observar a tamanha relevância de uma política de Segurança da Informação nas organizações, para garantir a preservação desta contra futuras eventualidades.

Conforme a ABNT NBR ISO/IEC 27002:2013, a política de Segurança da Informação tem por objetivo prover orientação da direção e apoio à Segurança da Informação, de acordo com os requisitos do negócio e com as leis e regulamentos pertinentes à organização.

Nesse sentido e com o objetivo de melhorar os aspectos relacionados à Gestão e Governança de Tecnologia da Informação e Comunicação nos Tribunais de Justiça do País, o Conselho Nacional de Justiça (CNJ), pela Resolução nº 211, de 2015, instituiu a

Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) para o período 2015-2020.

Dentre os objetivos e princípios dessa Estratégia, em seu artigo 7º, ela diz que cada órgão deverá constituir um Comitê de Governança de Tecnologia da Informação e Comunicação que ficará responsável, entre outros, pelo estabelecimento de estratégias, indicadores e metas institucionais, aprovação de planos de ações, bem como pela orientação das iniciativas e dos investimentos tecnológicos no âmbito institucional. Dessarte, o Tribunal de Justiça do Estado do Tocantins (TJTO), por meio da Resolução nº 22, de 16 de outubro de 2014, criou o Comitê Gestor de Segurança da Informação Multidisciplinar (CGSI), no âmbito do Poder Judiciário do Tocantinense.

A Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário, em seu artigo 9º, diz que cada órgão deverá elaborar e aplicar política, gestão e processo de segurança da informação a serem desenvolvidos em todos os níveis da instituição, por meio de um Comitê Gestor de Segurança da Informação, e em harmonia com as diretrizes nacionais preconizadas pelo Conselho Nacional de Justiça.

Assim, em meados de 2017, por meio do Comitê Gestor de Segurança da Informação e pela Portaria nº 3.433, de 2017, instituiu-se a Política de Segurança da Informação (PSI) no âmbito do Poder Judiciário do Tocantins.

Nessa ocasião, a Política de Segurança da Informação do Tribunal de Justiça do Estado do Tocantins foi composta por seis normas complementares:

1. Norma-TIC-01: Responsabilidades do Usuário;
2. Norma-TIC-02: Troca de Informações com Partes Externas;
3. Norma-TIC-03: Responsabilidade dos Ativos;
4. Norma-TIC-04: Controle de Acesso do Usuário;
5. Norma-TIC-05: Manuseio de Mídias;
6. Norma-TIC-06: Controle de Acesso ao Conteúdo *Web*;

Em agosto de 2019, pela Portaria nº 1.660, a Política de Segurança da Informação passou a contar com mais duas novas normas complementares, conforme seguem abaixo**:**

7. Norma-TIC-07: Gestão de Riscos de Segurança da Informação (GRSI);
8. Norma-TIC-08: Gestão de Processos de *Backup*;

De acordo com a pesquisa realizada pela empresa *Software Advice* (2015), no relatório sobre *Phishing Scam*, publicada em 2015, os funcionários das organizações ainda são o elo mais fraco sobre os incidentes relacionados à Segurança da Informação.

Nesse sentido, um estudo mundial realizado pela empresa de consultoria e auditoria *Price Waterhouse Coopers – PWC* (2014), juntamente com 9.600 executivos de 115 países concluíram que os funcionários e ex-funcionários representam 57% aos incidentes de origem interna, e que os *hackers* respondem por 32% dos ataques externos (PWC, 2014).

Segundo o *Gartner Group* (2016), mais de 70% dos incidentes de segurança da informação que causam prejuízos financeiros para organizações envolvem *insiders.*

Os reflexos desse resultado, de acordo com o *Norton Cyber Security Insights Report* 2017, divulgado pela *Norton by Symantec*, mostra que o Brasil, em 2017, foi o segundo país do mundo mais vulnerável a vírus que captam informações, estimando ainda para o mesmo ano uma perda de 22 bilhões de dólares em ataques cibernéticos no País.

Esse mesmo ano ainda foi marcado por dois importantes ataques, quais sejam:

a) O *cyber* ataque que paralisou as atividades do Instituto Nacional de Seguridade Social (INSS) por cerca de três dias.

b) O caso do Tribunal de Justiça do Estado de São Paulo, que teve mais de mil computadores afetados e precisou interromper seus atendimentos.

Esse resultado reflete fortemente a necessidade de investimentos em infraestrutura de segurança, criação de Políticas de Segurança da Informação e principalmente a necessidade de criar plano para a conscientização para funcionários e colaboradores das organizações sobre os temas ligados à Segurança da Informação.

1.1. Problema

Os inúmeros casos de incidentes de Segurança da Informação, divulgados na mídia, possibilitaram identificar que os ataques, em sua grande maioria, foram realizados por dispositivos dos próprios funcionários ou colaboradores. Essa identificação reflete fortemente que os recursos humanos das organizações são considerados por diversos especialistas o elo mais fraco da Segurança da Informação.

Beal (2008) também afirma que o conceito de Segurança da Informação abrange, além da tecnologia, processos e pessoas, sendo estes o elo mais frágil no comprometimento do ativo informacional. Campos (2007) acrescenta que as próprias pessoas são os ativos mais importantes das organizações, pois executam processos, geram e consomem informações, podem, portanto, oferecer os maiores riscos.

Assim, reconhecendo a importância da necessidade de conscientização das normas instituídas e treinamentos sobre assuntos ligados à Segurança da Informação no âmbito das

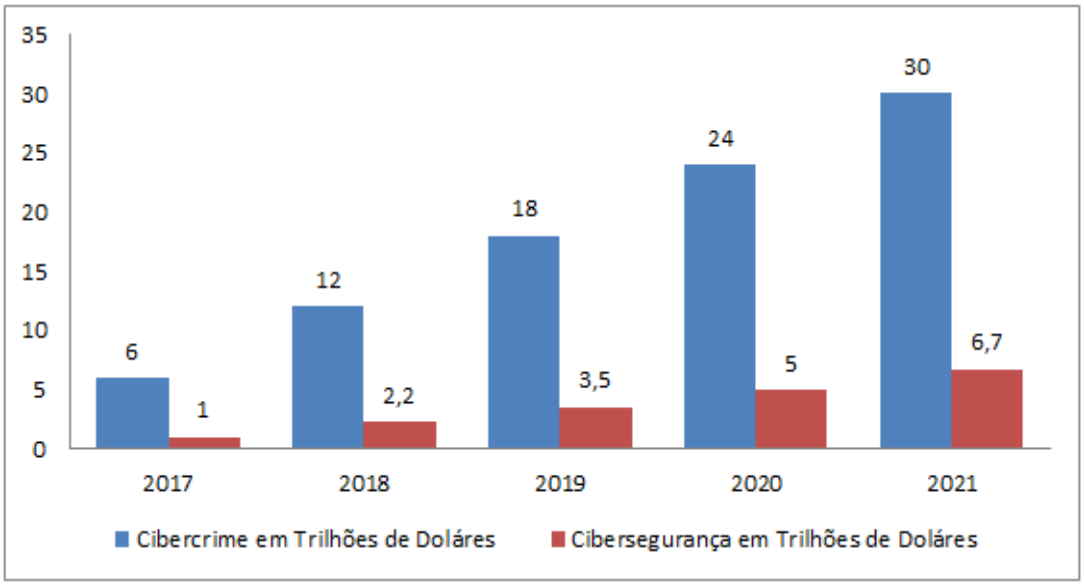
organizações, sejam elas públicas ou privadas, surgiu o seguinte problema de pesquisa: Como elaborar um plano para institucionalizar a conscientização em Segurança da Informação para magistrados e servidores do Poder Judiciário do Tocantins?

1.2. Justificativa

Nos últimos anos, o cenário de ameaças à Segurança da Informação mudou drasticamente, e os números são bem alarmantes, uma vez que a indústria do cibercrime movimenta anualmente bilhões de dólares, e a tendência é que continue crescendo cada vez mais.

A *Cyber Security Ventures*, empresa com foco principal em pesquisa da economia voltada à cibersegurança global, por meio de fonte confiável de fatos, números e estatísticas de segurança cibernética, publicou em seu relatório anual de 2017, que os investimentos das empresas em cibersegurança serão um acumulado de um trilhão de dólares nos próximos cinco anos, de 2017 a 2021. No mesmo relatório observa-se ainda um crescimento entre 12 e 15% de investimento ao ano, para o mesmo período. Em contrapartida, estima-se que o custo às empresas, oriundas de ataques de cibercrime no mundo, cresça cerca de 6 trilhões de dólares por ano até 2021. O Gráfico 1 representa aproximadamente os valores em trilhões de dólares de custos causados por cibercrimes *versus* investimentos em cibersegurança para os anos de 2017 a 2021.

Gráfico 1. Cibercrime *versus* Cibersegurança Global. (*Cyber Security Ventures*, 2017, adaptado).



Para visualizar as ameaças no mundo em tempo real, a *Kaspersky*, empresa russa produtora de *softwares* de segurança para a Internet, disponibilizou em sua *website* o *cybermap*[1] "*M*apa interativo de ameaças cibernéticas", que visualiza incidentes de segurança virtuais que ocorrem em todo o mundo em tempo real.

Os tipos de ameaças exibidos incluem objetos maliciosos detectados durante *on-access* e varreduras sob demanda, e-mail e detecções de antivírus da *web*, bem como objetos identificados por vulnerabilidade e detecção de subsistemas de intrusão da *Kaspersky*.

Diante das estatísticas apresentadas por meio da consulta realizada no mapa interativo, foi possível observar que boas partes dos *cyberataques* são provenientes dos usuários. Assim, inseri-los no contexto da Segurança da Informação é de suma importância.

Os guias de boas práticas de Gestão de Segurança da Informação apontam para a necessidade de envolver os usuários no processo de segurança. E, por isso, assim como *Firewall*,[2] *AntiSpam*[3] e Antivírus[4], a conscientização em Segurança é parte essencial em qualquer processo de Segurança da Informação de qualquer organização.

A conscientização em Segurança da Informação é capaz de gerar mudança no comportamento de todos; por isso, é vista como uma ferramenta com grande potencial para beneficiar as organizações.

Segundo Kim e Solomon (2014), as pessoas são os ativos mais importantes da organização, e que um forte programa de conscientização se torna um dos melhores controles de Segurança da Informação.

Corroborando com o mesmo entendimento, RAMOS (2015) afirma que essas pessoas transmitem, processam e armazenam informações; logo, também são alvos de ataques. Nesse sentido, é fundamental a criação de processo contínuo de conscientização nas organizações.

Dessa forma, e diante da necessidade de conscientizar as pessoas sobre assuntos relacionados à segurança da informação no âmbito das organizações, pretende-se, por meio deste trabalho, realizar um estudo de viabilidade para instituir um plano de conscientização

---

[1] https://cybermap.kaspersky.com/pt

[2] Um *firewall* é um dispositivo de segurança da rede que monitora o tráfego de rede de entrada e saída, permitindo ou bloqueando tráfegos específicos de acordo com um conjunto definido de regras de segurança.

[3] *AntiSpam* é um serviço que analisa as mensagens, por meio da aplicação de uma série de camadas de segurança, reduzindo o recebimento de mensagens de e-mails com *spams*.

[4] Antivírus é um programa ou um conjunto de programas que tem como função detectar e remover virus e *software* malicioso em computadores e redes.

em Segurança da Informação para magistrados e servidores do Poder Judiciário do Tocantins.

Em suma, atendendo aos termos da Resolução nº 211, de 15 de dezembro de 2015, do Conselho Nacional de Justiça (CNJ), que institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD), e também à Portaria nº 3.433, de 2017, deste Tribunal de Justiça do Estado do Tocantins, que institui a Política de Segurança da Informação (PSI), pretende-se, principalmente, fomentar a cultura em Segurança da Informação.

1.3. Objetivo Geral

Apresentar uma proposta para conscientizar e disseminar a cultura de boas práticas relacionadas à Segurança da Informação para magistrados e servidores do Poder Judiciário do Tocantins, por meio da institucionalização de um plano de conscientização em Segurança da Informação.

1.3.1. Objetivos Específicos

1. Analisar as principais Resoluções, Portarias e Normas de Segurança da Informação, com vista à construção da minuta e dos artefatos de conscientização em Segurança da Informação;
2. Definir a proposta da minuta do plano de conscientização em Segurança da Informação;
3. Elaborar os artefatos que compõem a proposta do plano de conscientização em Segurança da Informação do Poder Judiciário Tocantins.

1.4. Metodologia

Para este estudo, está sendo realizada uma revisão bibliográfica que permitirá o embasamento teórico sobre os assuntos, normas e conceitos aqui tratados. As coletas dos materiais literários estão sendo feitas por meio de buscas nas bases: ACM, IEEE e *google* acadêmico, e sendo utilizados os seguintes descritores para a pesquisa: conceitos de Segurança da Informação; conscientização em Segurança da Informação.

Para as seleções dos materiais literários a serem usados no estudo, estão sendo considerados os seguintes critérios: a) conceitos de gestão da segurança da informação, conscientização; b) sem delimitação do tempo de publicação; c) idiomas em português e inglês.

De acordo com Waslawick (2014), o método de pesquisa descreve o caminho para se atingir o objetivo proposto, ou seja, se os passos definidos no método forem executados, os resultados obtidos serão satisfatórios. A metodologia utilizada pode ser observada no Quadro 1.

Quadro 1. Metodologia Científica Aplicada à Pesquisa. (Elaborado pelo Autor).

METODOLOGIA	ESPECIFICAÇÕES
Natureza	Aplicada
Objetivo	Exploratório
Abordagem	Quali-quantitativa
Procedimentos Utilizados	Levantamento Bibliográfico, Documental e Estudo de Caso
Perspectiva e Área de Concentração	Gestão da Segurança da Informação - Conscientização em Segurança da Informação

Segundo Waslawick (2014) e Silva e Menezes (2005), a classificação de uma pesquisa pode ter os seguintes pontos de vista quanto: à sua natureza; aos objetivos; à abordagem; e aos procedimentos. Assim, de acordo com os mesmos autores, a presente pesquisa foi classificada de acordo com os itens abaixo.

1.4.1. Quanto à Natureza

A pesquisa será de natureza aplicada, pois possibilitará gerar informações e novos conhecimentos a partir de estudo de viabilidade de implantação do plano de conscientização em Segurança da Informação no Poder Judiciário Tocantins.

1.4.2. Quanto aos Objetivos

A pesquisa será exploratória, pois visa proporcionar mais familiaridade com o problema e torná-lo mais explícito ou para construir hipóteses. Pretende-se fazer pesquisas bibliográficas e documentais, revisão de literaturas, consultas internas e externas, buscando

identificar os principais pontos apresentados nos estudos, bem como a melhor compreensão e aplicabilidade acerca do assunto tratado na pesquisa.

1.4.3. Quanto à Abordagem

A abordagem desta pesquisa é do tipo Quali-quantitativa, pois envolve o estudo das metodologias existentes na área de gestão e conscientização em Segurança da Informação, buscando o entendimento do problema.

Os materiais pesquisados são vistos como elementos com capacidade de produzir conhecimentos e de intervir no resultado. Esse tipo de abordagem visa compreender o objeto e os fenômenos que estão sendo investigados (LAKATOS e MARCONI, 2017).

A interpretação dos fenômenos e a atribuição de significados serão alcançadas por meio da revisão sistemática da literatura, levantamento bibliográfico, documentos oficiais e nas informações adquiridas no estudo de caso. Dessa forma, será possível alcançar os fatores críticos para a disseminação da cultura e o aprimoramento da Segurança da Informação no Tribunal de Justiça do Estado do Tocantins.

1.4.4. Quanto aos Procedimentos

Para este trabalho, foram utilizados os métodos de pesquisa bibliográfica, pesquisa documental e estudo de caso, conforme descrito a seguir:

Pesquisa Bibliográfica

O procedimento bibliográfico implica estudo de artigos, teses, livros e outras publicações usualmente disponibilizadas por fontes indexadas. Inicialmente, foi realizado um levantamento bibliográfico, em que foi possível identificar diversos trabalhos científicos e normas mais relevantes para o tema pesquisado.

Pesquisa Documental

O procedimento documental implica estudo de materiais que ainda não receberam tratamento analítico. Nesse caso, foram utilizados documentos oficiais do próprio Tribunal de Justiça do Estado do Tocantins, Conselho Nacional de Justiça, Tribunal de Contas da União, normas, diretrizes e boas práticas de Segurança da Informação disponibilizadas pela

ABNT. Assim foram analisados: Instruções Normativas, Resoluções, Decretos, Leis relacionadas à Segurança da Informação e Normas Técnicas.

Estudo de Caso

Para Gil (2010, p. 37), o estudo de caso consiste “no estudo profundo e exaustivo de um ou poucos objetos, de maneira que permita seu amplo e detalhado conhecimento”. Para realização do estudo de caso foi elaborado um instrumento de pesquisa para coleta de dados, com o objetivo de obter um panorama do conhecimento sobre a Segurança da Informação no Poder Judiciário do Tocantins.

Dessa forma, o instrumento de pesquisa foi encaminhado para algumas Unidades Organizacionais do Tribunal de Justiça do Estado do Tocantins, com o objetivo de obter um panorama do conhecimento sobre a Segurança da Informação no Poder Judiciário do Tocantins.

1.5. Estruturação do Trabalho

Este trabalho tem como propósito elaborar uma proposta do plano de conscientização em Segurança da Informação para magistrados e servidores do Poder Judiciário do Tocantins, e está estruturado com base em 7 capítulos.

O Capítulo 1 descreve o percurso metodológico usado por está pesquisa, para atingir os objetivos propostos. Dessa forma, são apresentados: introdução, problema, justificativa, objetivo geral e específico e a metodologia.

O Capítulo 2 tem como objetivo apresentar a temática Segurança da Informação nas organizações. Também foram abordadas as principais normas de gestão de Segurança da Informação, ciclos de melhoria contínua da gestão, incidentes de Segurança da Informação e por fim a conscientização em Segurança da Informação.

Já no capítulo 3 são apresentados estudos técnicos preliminares que embasaram a necessidade deste trabalho, sendo abordados dois artigos e os principais canais de comunicação existentes no Poder Judiciário do Tocantins, com vista à execução inicial do plano de conscientização em Segurança da Informação, bem como apresetação de outras ferramentas existentes no mercado a fim de potencializar as atividades e ações de conscientização.

No Capítulo 4 é apresentada a Norma TIC-09 por meio da proposta da Minuta do Plano de Conscientização em Segurança da Informação no Poder Judiciário Tocantins.

Também são apresentados no mesmo capítulo os artefatos elaborados, compostos por: Fluxo do Processo e sua Estrutura Analítica; Formulário para Conscientização e Termo de Ciência da PSI. Visando ainda ao detalhamento do fluxo do processo, foram apresentados os papéis e as responsabilidades; ferramentas e meios de comunicação; indicadores do processo; controle de execução; descrição das atividades; temas relevantes; periodicidades e revisões; pessoas envolvidas e recursos necessários.

O Capítulo 5 traz o estudo de caso, por meio de um instrumento de pesquisa – questionário –, com o objetivo de obter um panorama do conhecimento sobre a Segurança da Informação no Poder Judiciário Tocantins, com vista à necessidade da implantação do plano de conscientização em Segurança da Informação.

Já no Capítulo 6 são apresentadas as conclusões e a continuidade do estudo, tendo como sugestão o encaminhamento da Norma-TIC 09 – Proposta da Minuta do Plano de Conscientização em Segurança da Informação – para conhecimento, aprovação e publicação no Comitê Gestor de Segurança da Informação.

2. REVISÃO DE LITERATURA

As Normas ABNT NBR ISO/IEC 17799 e ABNT NBR ISO/IEC 27001, ambas de 2005, tratam sobre Tecnologia da Informação – Código de Prática para a Gestão da Segurança da Informação e Técnicas de Segurança, Sistema de Gestão de Segurança da Informação –, respectivamente, e ambas se dividem em 10 áreas de controles.

A ABNT NBR ISO/IEC 27001:2005 pode ser implementada em qualquer tipo de organização, com ou sem fins lucrativos, privada ou pública, pequena ou grande. Ela é escrita pelos melhores especialistas mundiais no campo de Segurança da Informação e provê metodologia para a gestão da Segurança da Informação em uma organização.

A versão mais recente desta Norma foi publicada em 2013, e seu título completo é ABNT NBR ISO/IEC 27001:2013, cujo foco é proteger a confidencialidade, integridade e disponibilidade da informação de uma organização. As salvaguardas ou controles implementados, em geral, estão na forma de políticas, procedimentos e implementações técnicas (*software* e equipamento). Contudo, em muitos casos, as organizações já possuem *hardware* e *software* instalados, porém sem definições corretas de regras organizacionais (documentos escritos, normas, procedimentos, portarias, políticas) necessárias, de modo a prevenir brechas de segurança.

Para as definições de gestão de múltiplas políticas, procedimentos, pessoas e ativos, a ABNT NBR ISO/IEC 27001:2013 define como encaixar todos esses elementos de forma coerente no Sistema de Gestão de Segurança da Informação.

Dessa forma, gerir a Segurança da Informação não se trata apenas de segurança em Tecnologia da Informação (*firewalls*, antivírus etc.), mas também sobre gerenciar processos, proteção legal, recursos humanos, proteção física, dentre outros.

2.1. Segurança em Tecnologia da Informação

A segurança em tecnologia da informação tem foco principal em manter a segurança da infraestrutura de tecnologia da informação e sistemas operacionais das organizações. Sendo considerada de papel altamente estratégico dentro das organizações, a segurança em tecnologia da informação demandam os investimentos relacionados segurança, por meio de softwares e hardwares, além de adotar práticas de segurança nas organizações.

Segundo Oliveira et. al., (2014), existe dois tipos de segurança envolvendo a tecnologia da informação, fator humano e computacional, ou seja, **segurança física** dos equipamentos de informática e **segurança lógica**.

Ainda conforme os autores, a segurança física se refere a danos causados por descuidos, danos de origem acidentais ou criminais, fatores naturais ou pela falta de manutenções nos equipamentos que contemplam a infraestrutura física da organização. Já a segurança lógica, é feita por meio de softwares que se constituem através dos controles existentes e os níveis de acesso à informação.

Por ora, a Tecnologia da Informação, em muitos dos casos é sempre responsabilizada pelos incidentes de segurança ocorridos nas organizações. Contudo partes dos incidentes de segurança nas organizações estão relacionadas ao fator humano. Assim, a relevância do fator humano para a segurança das organizações fica evidenciada quanto ás origens dos incidentes de segurança.

Segundo a Pesquisa Global de Segurança da Informação realizada em 2018 (PwC, 2018), 35% dos incidentes de segurança são causados por agentes internos, como funcionários, e 34% por ex-funcionários. Para os incidentes de causa externa, 43% foram causados por *Hackers* desconhecidos, 27% por concorrentes e 29% por fornecedores atuais. Dessarte é notório observar que os incidentes de segurança nas organizações estão fortemente relacionados ao fator humano do que diretamente relacionado à falha da própria Tecnologia da Informação.

Segundo Araújo e Ferreira (2008), as ações de treinamento e conscientização dos colaboradores, são itens fundamentais para o sucesso da Segurança da Informação dentro das organizações, e destacam que esse tema tornou-se um dos mais importantes dentro das organizações, devido às necessidades de proteção e preservação das informações.

Assim, ressalta-se que os assuntos relacionados à Segurança da Informação deste trabalho estão diretamente relacionados à conscientização do fator humano (magistrados, servidores e colaboradores) do Poder Judiciário do Tocantins.

2.2. Segurança da Informação

A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Pode-se declarar que a informação é um ativo de suma importância para as

organizações, pois tem valor para o negócio e, dessa forma deve ser protegida contra vários riscos.

Sendo especialmente importante em ambientes de negócios, pois os ambientes estão cada vez mais interconectados, assim como resultado deste aumento, a informação está exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades (SILVA, 2012).

Conforme Ferreira (2003), a informação e os processos de apoio, os sistemas e as redes são

> Importantes ativos para os negócios. **Confidencialidade, integridade e disponibilidade** da informação podem ser essências para preservar a competitividade, o faturamento, a lucratividade, o atendimento aos requisitos legais e a imagem da organização perante o mercado e os clientes. (FERREIRA, 2003, p. 3).

Segundo Foina (2015), a Tecnologia da Informação é fundamental para as operações das empresas, assim como a necessidade de se preservarem os serviços e sistemas dos ataques de *hackers,* como também dos vazamentos de informações não autorizadas. Portanto, é importante tratar a Segurança da Informação em todos os níveis das organizações e não deixar a cargo apenas da área técnica especializada.

De acordo com Sêmola (2014), a Segurança da Informação pode ser definida como sendo a área do conhecimento dedicada à proteção de ativos da informação contra acessos não autorizados, alterações indevidas ou sua indisponibilidade.

O autor enfatiza que a Segurança da Informação pode ser definida com uma área que necessita de conhecimentos específicos por parte dos profissionais que nela atuam. Esses profissionais terão de garantir que a informação não sofrerá alteração ou acesso inadequado, garantindo sempre à disposição as informações para acessos autorizados.

Ainda de acordo com Lima (2013), a Segurança da Informação deve existir para proteger as informações das organizações, contra divulgação indevida, seja ela intencional ou não, alteração não autorizada, destruição não desejada, negação de serviço, fraudes financeiras, apropriação indevida de informações ou reputação da imagem da instituição. Essa proteção é feita pela implantação de controles de segurança definidos em políticas e procedimentos.

Um desses controles é a Política de Segurança, a qual, por meio dela, possibilita que as organizações criem suas próprias Políticas de Segurança da Informação (PSI). Segundo Beal (2005), a Política de Segurança da Informação é

> O documento que registra os princípios e as diretrizes de seguranças adotados pela organização, a serem observados por todos os seus integrantes e

> colaboradores e aplicados a todos os sistemas de informação e processo corporativos. (BEAL, 2005, p. 43).

De acordo com Fontes (2012), em toda organização existe a necessidade da implantação da Política de Segurança da Informação:

> É estrutural que a organização tenha uma política de segurança da informação para que o processo de proteção da informação possa ser elaborado, implementado e mantido. Essa política (ou conjunto de políticas) definira as diretrizes, os limites e o direcionamento que a organização deseja para os controles que serão implantados na proteção da sua informação. (FONTES, 2012, p. 12).

A Política de Segurança da Informação, segundo Araújo e Ferreira (2008), deve ser criada nas organizações antes da ocorrência de problemas com a Segurança da Informação, ou depois, para evitar reincidências. A PSI é uma ferramenta para prevenir problemas legais, como também para documentar a aderência ao processo de controle de qualidade nas organizações.

Dessa forma, é de extrema importância que as organizações tenham suas Políticas de Segurança da Informação, a fim de garantir que suas informações não sofram alterações indesejadas ou inadequadas. Ainda de acordo com o Tribunal de Contas da União (TCU), 2012:

> Política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela instituição para que sejam assegurados seus recursos computacionais e suas informações. (TRIBUNAL DE CONTAS DA UNIÃO, 2012, p. 10).

Araújo et. al. (2014) ressaltam que a Segurança da Informação tem um dos grandes desafios, qual seja, conscientizar o fator humano. Um desafio importante é conscientizar o fator humano em manter suas senhas como sendo confidenciais, não devendo ser permitido compartilhá-las, nem acessar sistemas de outros colaboradores sem autorização expressa.

Nesse mesmo sentido, Santos et. al. (2016) afirmam que a Segurança da Informação não pode ser tratada ou garantida apenas tecnicamente por meio do uso de antivírus, *firewall* e outras ferramentas similares. É preciso levar em consideração o fator humano, pois este é o mais fraco dos três pilares que a sustentam.

O primeiro pilar é a **Tecnologia**, que envolve as ferramentas e soluções; o segundo são os **Processos**, que implica normas e procedimentos envolvidos na estratégia de Segurança da Informação, e, por último, as **Pessoas**, que interagem com a tecnologia e se envolvem com os processos.

Ultimamente muito se fala em espionagem, privacidade e engenharia social, temas estes que tornam necessário avaliar de que forma empresas e empregados estão

contribuindo para que informações estratégicas e sigilosas vazem ao mercado. O sucesso de técnicas de engenharia social depende exclusivamente de o usuário ou empregado não conseguir identificar a situação em que está sendo exposto (Santos et. al., 2016).

Para que os pilares da Segurança da Informação sejam eficazes, é preciso investir no item “pessoas” para que este fortaleça os outros dois itens. Os esforços para investir em soluções, ferramentas, políticas e normas bem definidas serão ineficazes se o usuário não for instruído corretamente.

As organizações estão cada vez mais dependentes dos sistemas informatizados e, consequentemente, novas vulnerabilidades vão aparecendo a cada momento. A Segurança da Informação tem como objetivos protegê-las das informações contra as ameaças físicas e lógicas.

A dependência dos sistemas e serviços de informações significa que as organizações estão mais vulneráveis às ameaças de segurança. Segundo FERREIRA (2003), a conexão de redes públicas e privadas e o compartilhamento de recursos aumentam as dificuldades de ser controlarem os acessos. A tendência da computação distribuída dificulta a implementação de um controle de acesso centralizado realmente eficiente.

Desarte, essa dificuldade, contribuem para o aumento das possibilidades de que as organizações sejam alvos de cyberataques, por meio dos incidentes de Segurança da Informação, podendo resultar em perdas, roubos ou fraudes das informações que estas detêm.

2.3. Incidentes de Segurança da Informação

As ações concretizadas ocorridas pelas ameaças, causando a perda dos princípios da Segurança da Informação, resultando, assim, em prejuízos para a organização, são denominadas incidentes de Segurança da Informação.

De acordo com Sêmola (2003), o incidente de Segurança da Informação pode ser caracterizado como um evento decorrente da ação de uma ameaça, que explora uma ou mais vulnerabilidades, levando à perda dos princípios da Segurança da Informação: confidencialidade, integridade e disponibilidade.

Ainda de acordo com o autor, a todo instante os negócios, os processos, ativos físicos, tecnológicos e humanos são alvos de investidas de ameaças de toda ordem, que buscam identificar um ponto fraco compatível, uma vulnerabilidade capaz de potencializar

sua ação. Quando essa possibilidade aparece, a quebra de Segurança da Informação é consumada.

Para Moreira (2001), incidente pode ser qualquer evento que impacta no andamento da infraestrutura da organização:

> Incidente de segurança é qualquer evento que prejudique o bom andamento dos sistemas, das redes ou do próprio negócio. Esse incidente pode ser o resultado de uma violação de segurança concretizada, um acesso não autorizado a determinadas informações confidenciais ou até mesmo um site tirado do ar pela ação de um hacker. (MOREIRA, 2001, p.30).

Quando uma organização tem implementado um modelo de SGSI, este assegura que as operações e informações estejam protegidas, minimizando os incidentes de Segurança da Informação.

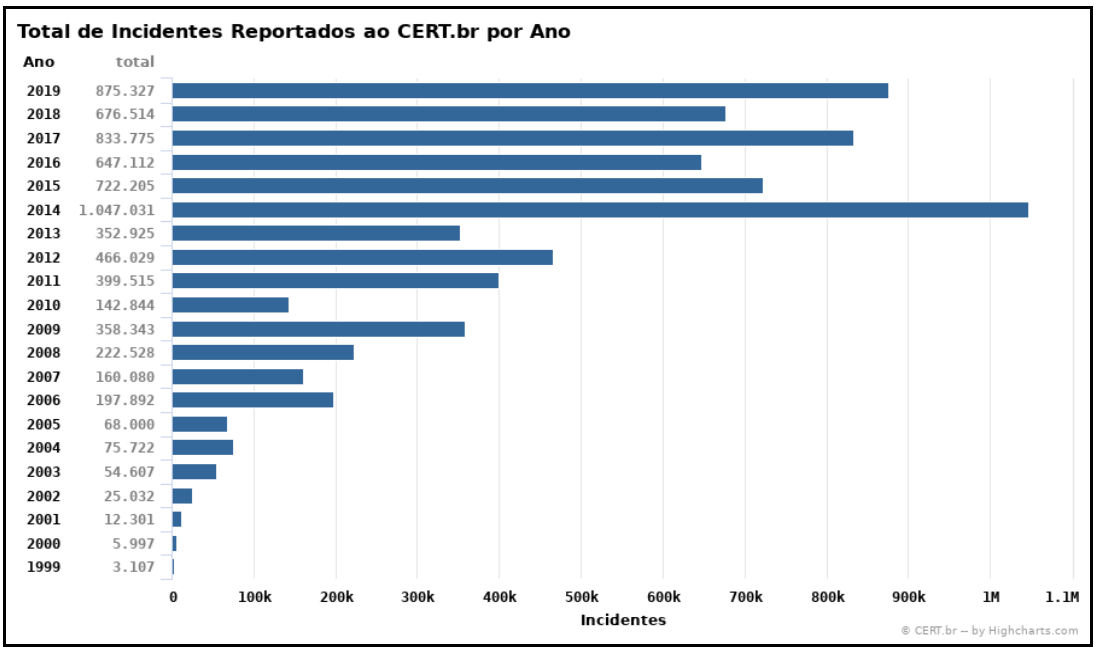
No Brasil, o CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, sendo responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil.

Atua como um ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando sempre as partes envolvidas em contato para resolução dos incidentes.

O Grupo de Resposta a Incidentes de Segurança para a Internet Brasileira tem como objetivo estratégico aumentar os níveis de segurança e de capacidade de tratamento de incidentes das redes conectadas à Internet no Brasil.

No Gráfico 2, é representado o relatório das Estatísticas dos Incidentes Reportados ao CERT.br, desde 1999 até 2019.

Gráfico 2 - Incidentes Reportados ao CERT.br, anos 1999 a 2019. (Fonte: Cert.br. Estatísticas dos Incidentes Reportados ao CERT.br).



Fica evidenciado, no Gráfico 2, que os incidentes de Segurança da Informação vêm aumentando a cada ano. A exemplo, pode-se observar que o total de notificações recebidas pelo CERT.br, em 2019, foi de 875.327, número 29% maior que o total de 2018.

O CERT.br, além do processo de tratamento a incidentes, também atua por meio do trabalho de conscientização sobre os problemas de segurança, da análise de tendências e correlação entre eventos na Internet brasileira e no auxílio ao estabelecimento de novos Grupos de Resposta a Incidentes de Segurança em Computadores no Brasil.

Assim, gerir a Segurança da Informação não se trata apenas de segurança em Tecnologia da Informação (*firewalls*, antivírus etc.), mas também sobre gerenciar processos, recursos humanos, proteção legal, proteção física, dentre outros.

Segundo Lyra (2015), um dos principais problemas que a Segurança da Informação deve tratar é a segurança em pessoas. A cooperação dos usuários é essencial para a eficácia da Segurança da Informação.

Nesse mesmo sentido, Fontes (2015) ressalta que cada colaborador é parte integrante do processo de Segurança da Informação, buscando sempre a proteção das informações que este detém, com vista à continuidade da organização no mercado.

Já Pinheiro (2009) se manifesta acerca do tema, afirmando que as políticas de Segurança da Informação têm um viés jurídico, uma vez que ela define que todos os

colaboradores são responsáveis pelo cumprimento de suas regras e ainda as punições caso contrário; portanto, faz-se necessária a formalização de ciência e aceite dos documentos. A autora ainda complementa que deve existir a etapa de divulgação e conscientização dos usuários, evitando assim a ocorrência de incidentes e a garantia de que os usuários saibam o seu papel perante o uso correto das informações na empresa.

Segundo Oliveira (2015), a implantação das Políticas de Segurança da Informação é extremamente essencial para a criação de um Sistema de Gestão de Segurança da Informação (SGSI), que pode conter a gestão de múltiplas políticas, procedimentos, pessoas e ativos.

2.4. Gestão de Segurança da Informação

De acordo com a ABNT NBR ISO/IEC 27002:2013, a Segurança da Informação poderá ser alcançada por meio da implementação de um conjunto adequado de controles. Tais controles podem ser as políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*.

Segundo a ABNT NBR ISO/IEC 27001:2013, um Sistema de Gestão de Segurança da Informação (SGSI), visa prover um modelo de gestão, dentro de uma perspectiva estratégica da organização, para estabelecer, implementar, manter e melhorar continuamente os controles de segurança e garantir que os controles sejam adequados para proteger os ativos de informação.

A importância na implantação de um SGSI permite que a organização identifique os pontos vulneráveis e as falhas nos sistemas e subsistemas, que deverão ser analisados e corrigidos. Para isso é imprescindível que o SGSI tenha apoio do nível estratégico da organização, e ainda se possível do departamento jurídico, que tem a função de conferir e validar a legitimidade do SGSI.

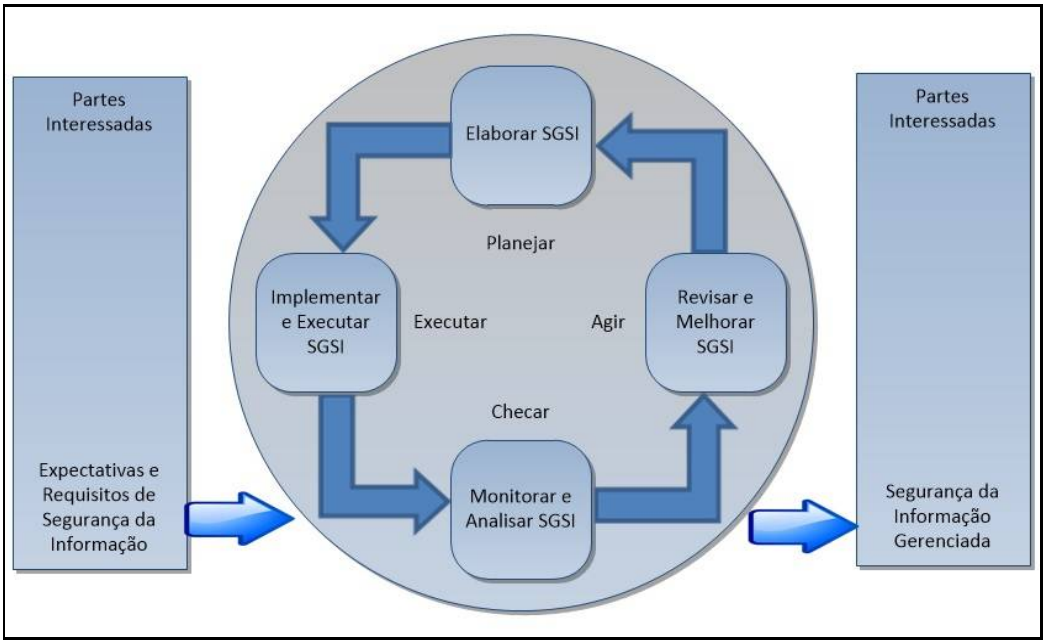
A ABNT NBR ISO/IEC 27001:2013 é dividida em 11 seções, sendo que as de 0 a 3 são introdutórias (não obrigatórias para a implementação), enquanto que as de 4 a 10 são obrigatórias. Na seção de número 7, a norma orienta que o SGSI deve embasar-se em um ciclo de melhoria contínua baseado no ciclo “Plan-Do-Check-Act” (PDCA). O ciclo PDCA, conhecido como ciclo de *Shewhart* ou ciclo de Deming, é um ciclo de desenvolvimento e tem seu foco voltado na melhoria contínua da Gestão da Segurança da Informação.

O PDCA é aplicado para atingir resultados dentro de um sistema de gestão, podendo ser utilizado em qualquer organização, de forma a buscar o sucesso nos procedimentos, independentemente da área de atuação, sendo dividido em quatro etapas:

- **Plan (Planejar):** consiste em elaborar as metas e objetivos, bem como os métodos que serão utilizados para que sejam implementados;
- **Do (Executar):** é a etapa de implementação de acordo com o que foi elaborado anteriormente no planejamento;
- **Check (Checar):** analisar os dados e medir se os objetivos e metas foram alcançados da forma desejada;
- **Act (Agir):** revisar as mudanças necessárias para garantir a melhoria contínua do projeto.

Para melhor entendimento deste modelo, na Figura 1 são representados todos os passos do ciclo PDCA, com uma breve explicação em cada uma das etapas.

Figura 1. Modelo PDCA aplicado aos Processos do SGSI. (ABNT NBR ISO/IEC 27001:2013, adaptado).



Por meio das etapas envolvidadas no ciclo do PDCA, a norma orienta que o SGSI deve ter o foco no planejamento, execução, verificação e na melhoria contínua, minimizando, dessa forma, os incidentes de Segurança da Informação.

Assim, pode-se afirmar que a definição, implantação, divulgação e conscientização das Políticas de Segurança da Informação a todos os seus usuários devem ser consideradas uma ferramenta indispensável para qualquer organização que visa tratar o vazamento de

informações corporativas, sendo este um meio inibidor e de prevenção desse problema, que é cada vez mais recorrente e impactante nas organizações.

2.5. Conscientização em Segurança da Informação

Segundo Mitnick e Simon (2003), devemos nos tornar mais conscientes das técnicas que estão sendo utilizadas por aqueles que tentam atacar a confidencialidade, integridade e disponibilidade das informações. Esses autores enfatizam ainda que

> Nós nos acostumamos a aceitar a necessidade da direção segura; agora está na hora de aceitar e aprender a prática da computação defensiva. A ameaça de uma invasão que viola a nossa privacidade, a nossa mente ou os sistemas de informações da nossa empresa pode não parecer real até que aconteça. Para evitar tamanha dose de realidade, precisamos nos conscientizar, educar, vigiar e proteger os nossos ativos de informações, as nossas informações pessoais e as infra-estruturas críticas da nossa nação. E devemos implementar essas precauções hoje mesmo. (MITNICK e SIMON, 2003, p. 7).

Nesse sentido, torna-se necessário que as pessoas e suas características individuais não sejam ignoradas pelas Políticas de Segurança da Informação, uma vez que programar sistemas e manter as informações em segurança torna-se um exercício muito mais complicado quando os problemas individuais comprometem o processo.

Uma cultura de segurança pressupõe que a segurança faça parte integral do trabalho das pessoas e que o tema esteja embutido em sua conduta e em suas atividades do dia a dia, permitindo que identifiquem situações suspeitas, mesmo que não conheçam a fundo como essas situações operam.

Um dos objetivos das ações de conscientização sobre Segurança da Informação é demonstrar para o colaborador da importância das Políticas de Segurança da Informação e os riscos em não seguir as normas estabelecidas nas PSIs podem causar ao colaborador e à organização.

Com vista à conscientização em Segurança da Informação, o *National Institute of Standards and Technology* (NIST), 1998, esclarece que a conscientização é o catalisador que, por meio de uma informação sobre determinado assunto, alguém passa a tomar conhecimento e a se conscientizar. Por esse motivo, é correto afirmar que a conscientização nas organizações é de suma importância, ainda mais quando se trata de assuntos relacionados à Segurança da Informação. Ainda conforme NIST (1998), a conscientização em Segurança da Informação é obrigatória a todos os colaboradores que estejam envolvidos de alguma forma com Sistemas de Tecnologia da Informação.

A Norma ABNT NBR ISO/IEC 27001:2013 recomenda que todas as pessoas da organização devam estar cientes da política de Segurança da Informação e colaborar com suas melhorias, reportando implicações de não conformidade com a gestão da Segurança da Informação.

Já a Norma ABNT NBR ISO/IEC 27002:2013 recomenda às organizações que a política de Segurança da Informação seja definida, aprovada pela Direção, publicada e comunicada a todos os funcionários e partes externas quando necessário.

Ainda a Norma, em seu item 7.2.2, que aborda sobre a conscientização, educação e treinamento em Segurança da Informação, diz:

> Convém que todos os funcionários da organização e, onde pertinente, partes externas devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções. ABNT NBR ISO/IEC 27002:2013, item 7.2.2.

O estudo de Parsons et. al. (2015) sugere que a melhoria da cultura de segurança de uma organização influencia positivamente os comportamentos dos empregados, que, por sua vez, possibilitam a melhor conformidade com políticas de segurança, atenuando o risco para dados e sistemas de informação da organização.

Um programa de conscientização em Segurança da Informação deve estar alinhado com as políticas e procedimentos relevantes de Segurança da Informação da organização. Para realização dos programas de conscientização, deve-se sempre considerar uma ou mais atividades de conscientização, como, por exemplo, campanhas (dia da Segurança da Informação), publicação de boletins na página *web*, mídias da organização e folhetos.

Outro ponto importante para o sucesso da conscientização é que ela deve ser planejada ao longo do tempo, de forma regular e contínua, de modo que contemple todos os funcionários, e deve estar sempre alinhada com as políticas e os procedimentos da organização.

3. ESTUDOS TÉCNICOS PRELIMINARES PARA SUBSIDIAR A CONSTRUÇÃO DO PLANO DE CONSCIENTIZAÇÃO

3.1. Epidemia de Vírus Computacionais no Poder Judiciário do Tocantins

Com ciberataques cada vez mais sofisticados, as empresas devem estar atentas para a adoção de soluções de segurança, de modo a prevenir os perigos vindos da Internet e, com isso, proteger os pontos de extremidade da rede. Entende-se por pontos de extremidade todos os dispositivos nos quais o trabalho é realizado, ou seja, servidores, estações de trabalho e dispositivos móveis (GRIFFIN, 2018).

Para proteção dos pontos de extremidade, é necessário garantir que eles estejam utilizando as mais recentes tecnologias de defesas contra ameaças. Um exemplo de contramedida a ameaças digitais são os *softwares* antivírus.

Segundo Nascimento (2015), os vírus e outras ferramentas de sabotagem digitais estão sempre alguns passos à frente das medidas de defesa, burlando as regras de *firewall* e os mecanismos de detecção dos antivírus, tornando frequentes as invasões às redes corporativas.

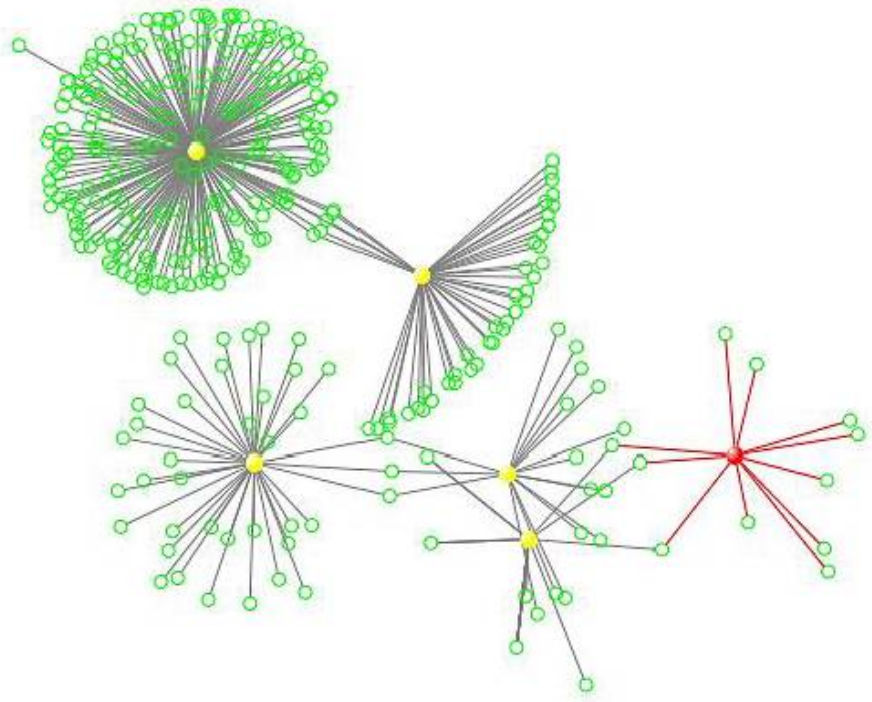
Em recente estudo realizado por WANDERLEY et. al. (2018), foram analisadas as principais ameaças à rede do Poder Judiciário do Tocantins, visando identificar suas ocorrências, os possíveis danos e as formas de contágio das estações de trabalho. Ultilizando-se do modelo epidemiológico SIR, desenvolvido por Kermack e McKendrick (1927), no qual cada indivíduo, considerado saudável, foi representado por um computador, podendo ser suscetível à infecção (S), ser infectado (I) e assim transmitir a doença a indivíduos saudáveis e, por fim, removidos (R), que não têm a doença nem podem transmiti-la, pois adquiriram imunidade. A Figura 2 representa a transição do modelo SIR.

Figura 2. Transição de um indivíduo da rede para o estado removido. (WANDERLEY et. al 2018).

Para o estudo, os autores, utlizaram duas ferramentas: a solução corporativa de antivírus e o *NodeXL*, que é uma ferramenta de análise de redes sociais, para expressar graficamente a infecção causada pelos *malwares*. A Figura 3 apresenta uma rede de

infecções, em que as estações de trabalho são representadas pelos círculos verdes e os *malwares* pelas esferas amarelas.

Figura 3: Rede de infecção causada pelo *malware*. (WANDERLEY et. al 2018).



Ainda de acordo com os autores, esse trabalho possibilitou observar que os ataques na maioria das vezes ocorreram por conta de comportamentos inadequados dos próprios usuários, por causa do acesso indevido à Internet e do uso incorreto de dispositivos USB (Universal Serial Bus).

Os autores ainda ressaltam que, segundo Alencar et. al. (2013), as pessoas podem se tornar uma ameaça interna à Segurança da Informação por diversos motivos, sendo importante ressaltar o quanto a variável pessoa pode ser prejudicial para a Instituição, uma vez que a maioria dos incidentes, direta ou indiretamente, envolve a participação humana, gerando assim muitos prejuízos.

Desse modo, fica evidenciado no estudo que, se o usuário possuir um melhor entendimento das ameaças e ataques de redes, ele pode colaborar para uma mudança positiva em relação à Segurança da Informação, pois assim criaria dificuldades para exploração de vulnerabilidades, diminuiria os riscos e aumentaria a segurança do ambiente.

Por fim, vale ressaltar que o referido estudo vai ao encontro do trabalho aqui proposto, tornando-se necessário a implantação de um plano de conscientização em Segurança da informação no Poder Judiciário do Tocantins.

3.2. Mapeamento de Riscos no Poder Judiciário do Tocantins

Preservar a confidencialidade, a integridade, a disponibilidade e a autenticidade dos dados são fatores primordiais para qualquer organização, seja pública ou privada. Por isso, gerenciar riscos é de suma importância para proteger a informação.

Segundo Bezerra (2013), risco é a combinação da probabilidade de um evento indesejado ocorrer e de suas consequências para a organização. Ou seja, é a incerteza no alcance dos objetivos. Ainda segundo o autor, em Segurança da Informação, a incerteza reside nos aspectos tecnológicos, nos processos executados e, principalmente, nas pessoas que interagem com a tecnologia e se envolvem com os processos.

Em estudo realizado, WANDERLEY et. al. (2019) abordaram os riscos relacionados à infraestrutura de TI do Poder Judiciário do Tocantins, em que eventos críticos foram pontuados com chance de ocorrência e seu impacto ante o negócio. Utilizando-se da tecnica de estudo de caso, o estudo teve como objetivo identificar as ameaças nas quais a infraestrutura de TI está sujeita e os riscos que elas impõem sobre a atividade-fim do Judiciário, bem assim a construção de um mapa de respostas aos riscos relacionados ao estudo com a implementação de controles, visando mitigar riscos e garantir os princípios da Segurança da Informação: confidencialidade, integridade, disponibilidade e autenticidade.

Segundo os autores, para o estudo foi utilizada a metodologia de gestão de riscos baseada nas Normas ABNT NBR ISO/IEC 27005, que é basicamente divida em três etapas, sendo a definição do contexto, o processo de avaliação de riscos e o tratamento de riscos, e também a Norma ABNT NBR ISO/IEC 31000, que fornece orientações sobre a seleção e aplicação de técnicas sistemáticas para o processo de avaliação de riscos.

De acordo com os autores, conforme Figura 4, foi levado em consideração o contexto interno do Tribunal de Justiça do Estado do Tocantins, que é composto pelas pessoas que desenvolvem as atividades judiciárias, e pelo ambiente computacional com os ativos que contribuem para que o Poder Judiciário do Tocantins cumpra sua missão, qual seja, "garantir a cidadania através da distribuição de uma justiça célere, segura e eficaz".

Como a maior parte das operações do Tribunal de Justiça do Estado do Tocantins é digital, incluindo o Sistema de Processo Judicial, chamado de e-Proc/TJTO, e o Sistema de Processo Administrativo, chamado de SEI/TJTO, o ambiente computacional apresenta uma relevância muito alta para a realização da atividade precípua do órgão em questão. A indisponibilidade dos recursos de TIC afeta sobremaneira o funcionamento do Judiciário, pois causa atrasos e interrompe atividades realizadas rotineiramente.

Assim, a adoção de procedimentos que garantam a Segurança da Informação é uma prioridade constante no Poder Judiciário, de forma a reduzir falhas e danos que possam comprometer a imagem da Justiça ou trazer prejuízos à sociedade.

Figura 4. Contexto Interno do TJTO composto pelas pessoas que utilizam os recursos de TIC como meio para promover os serviços prestados pelo Judiciário. (Fonte: WANDERLEY et. al. 2019).

Como resultado do estudo, foi construído e apresentado pelos autores um mapa de respostas aos riscos identificados, bem como definidos os controles, com vista a tratá-los, a fim de garantir a Segurança da Informação. Por fim, os autores concluem que a adoção de procedimentos que garantam a Segurança da Informação deve ser prioridade constante no Poder Judiciário, de forma a reduzir falhas e danos que possam comprometer a imagem da Justiça ou trazer prejuízos à sociedade.

Tendo como referência os dois artigos mencionados acima, em que ambos tratam sobre as vulnerabilidades e riscos à Segurança da Informação no Poder Judiciário do Tocantins, sendo por meio de vírus computacionais ou por riscos relacionados à infraestrutura de TI, que de uma forma ou de outra são operados por seres humanos, ambos os estudos demostram que fica evidenciada a necessidade de implantação de ações de conscientização em Segurança da Informação para criar uma cultura de boas práticas relacionada a esta Segurança no Poder Judiciario do Tocantins.

3.3. Ferramentas e Meios de Comunicação do Poder Judiciário do Tocantins

O Poder Judiciário do Tocantins possui diversos canais de comunicação com os magistrados e servidores, o que propicia maior abrangência na divulgação de suas ações e informações. Dentre os canais de comunicação desta Instituição serão destacados os principais canais visando inicialmente à execução do plano de conscientização em Segurança da Informação neste Poder.

3.3.1. Serviço de Mensagem Instantânea (*Spark*)

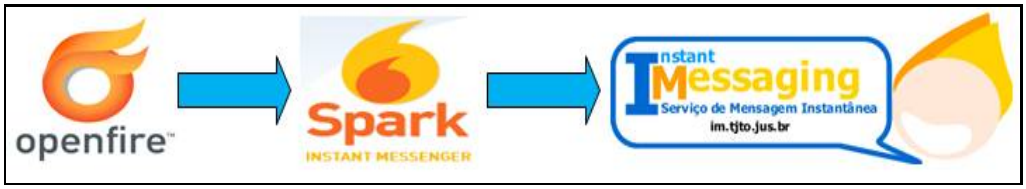
Implementado no Poder Judiciário do Tocantins, em 2009, o serviço de mensagem instantânea (*Spark*), teve como propósito reduzir as "distâncias" interpessoais da comunicação entre os magistrados e servidores das Comarcas, Juizados, Anexos e o Tribunal de Justiça, utilizando a rede de computadores do Poder Judiciário deste Poder.

O *Spark* tem como objetivo proporcionar aos magistrados e servidores do Poder Judiciário do Tocantins uma ferramenta que possa servir como meio de comunicação instantânea (*IM*). Esse serviço tem como meta principal permitir a comunicação por meio de mensagem instantânea (*IM*), como também possibilita a transferência de arquivos entre os participantes de uma comunicação.

O serviço possibilita economizar com ligações telefônicas, pois a comunicação é feita via texto, por *chat*, pela rede de computadores, independentemente de o magistrado ou de o servidor estarem no Tribunal de Justiça, Comarcas ou Anexos.

A ferramenta e o cliente de comunição são *software livre*, sem ônus para o Tribunal de Justiça, baseada no protocolo de comunicação *XMPP* (*Extensible Messaging and Presence Protocol*). A Figura 5 abaixo apresenta a ferramenta *Openfire* e o cliente *Spark* de comunicação, resultando no serviço instante mensagem (*IM*) do TJTO.

Figura 5. Ferramenta *Openfire* e cliente *Spark* (TJTO, 2010, adaptado).



Todos os magistrados e os servidores ativos no Poder Judiciário do Tocantins possuem cadastro para utilização do serviço de comunicação instantânea (*IM*). No entanto, aproximadamente 1.100 usuários utilizam diariamente o serviço de mensagem instantânea (*IM*) deste Poder.

Esse serviço contribuirá com as ações de conscientização em Segurança da Informação, alcançando diversos magistrados e servidores em todas as localidades do estado do Tocantins.

3.3.2. *Webmail* Institucional (Zimbra)

O Zimbra é uma plataforma corporativa de e-mail, calendário e colaboração de código aberto, baseada em navegação *web* e que trabalha no modelo “cliente e servidor”.

Implantado, em 2017, no âmbito do Poder Judiciário do Estado do Tocantins, a plataforma é a ferramenta de e-mail oficial utilizada por todos os magistrados e servidores, e contribuirá para a conscientização por meio de envio dos materiais educativos, divulgação das Normas da (PSI) e dicas de Segurança da Informação para todas as contas de e-mails cadastrados na plataforma.

3.3.3. TVs *Indoor*

Em 2018, mais um produto de comunicação foi implementado no Poder Judiciário do Tocantins, conhecido como Rede Justiça, que funciona por meio do sistema de mídia TV *Indoor*. Os equipamentos de transmissão foram instalados em locais estratégicos no Tribunal de Justiça, fóruns e nos prédios anexos, tendo como objetivo transmitir para magistrados, servidores e população em geral notícias do mundo jurídico, serviço de utilidade pública e conteúdo institucional.

O projeto contempla onze locais de exibição, sendo sete no Tribunal de Justiça, um no prédio do Anexo I, um na Corregedoria Geral de Justiça, um na Escola Superior da Magistratura Tocantinense e um no Fórum de Palmas.

A programação é 100% produzida pela Diretoria de Comunicação Social do TJTO e é composta de informação qualificada, notícias do mundo jurídico, serviço de utilidade pública e conteúdo institucional.

3.3.4. Zap Justiça

Um produto de comunicação interna para transmitir as notícias do Judiciário de forma rápida, dinâmica, econômica e acessível. Foi assim que, em abril de 2015, o Poder Judiciário do Tocantins lançou o Zap Justiça, um canal para promover a interação entre servidores e magistrados do Tribunal de Justiça do Estado do Tocantins (TJTO), das unidades administrativas e das 40 comarcas do interior.

Por meio de vídeos curtos produzidos com o celular e enviados duas vezes por semana pelo aplicativo *Whatsapp*, em 2017, mais de 1.100 magistrados e servidores estavam cadastrados para receber informações institucionais, avisos, dicas de cursos, alertas de prazos, coberturas de eventos e exemplos de boas práticas no Judiciário.

O Zap Justiça foi vencedor do Prêmio Nacional de Comunicação e Justiça, durante o XII Congresso Brasileiro dos Assessores de Comunicação da Justiça, realizado em junho de 2016, sendo premiado na categoria Comunicação Interna, o canal foi considerado pelos jurados uma inovação na forma de se fazer comunicação institucional, pelo alcance preciso e pelo baixo custo de produção.

Atualmente o Zap Justiça do TJTO possui aproximadamente 1.475 contas cadastradas entre magistrados e servidores, e com certeza será uma ferramenta de grande importância nas atividades e ações de conscientização em Segurança da Informação.

3.3.5. Portais Internet e Intranet

No portal internet, são disponibilizadas, além dos diversos serviços e sistemas, as principais notícias do Tribunal de Justiça do Estado do Tocantins para o público interno e externo. Já no portal intranet, o acesso é limitado apenas a magistrados e servidores e tem o conteúdo específico para o público interno.

A utilização desses dois meios de comunicação visa possuir canais independentes de divulgação, principalmente em relação à divulgação de *banners* informativos e educativos sobre Segurança da Informação.

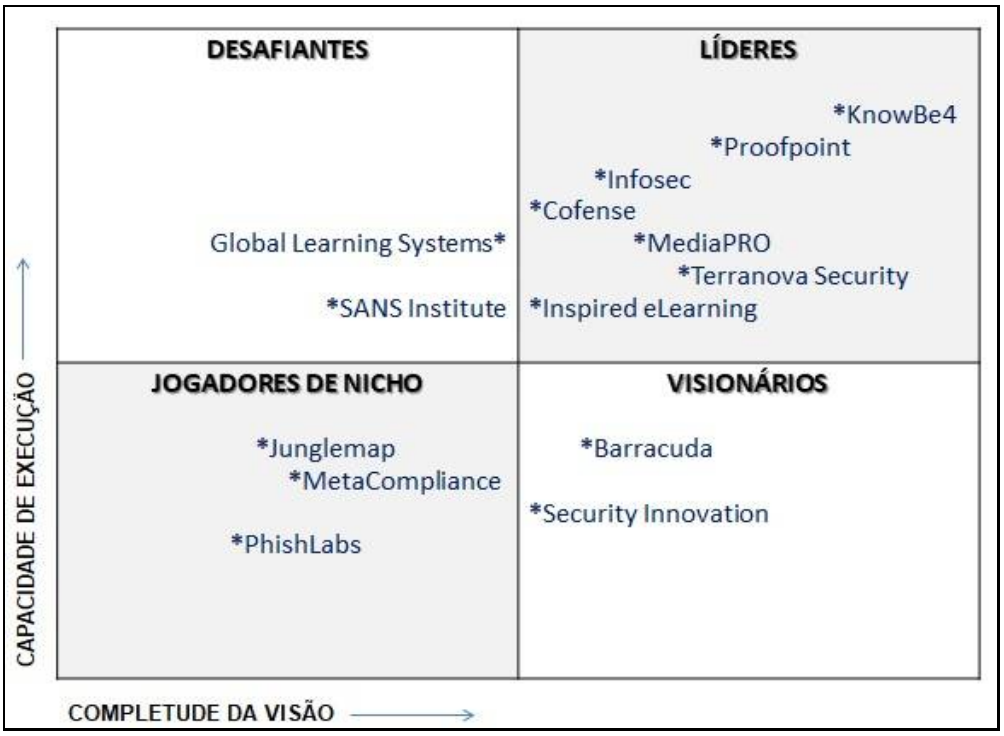
3.4. Outras Ferramentas e Meios de Comunicação

Além desses meios de divulgação existestentes no PJTO, e pensando em potencializar as atividades e ações de conscientização em Segurança da Informação, poderão ser ultilizadas outras ferramentas existentes no mercado para tal fim. Seguindo as

recomendações do Gartner Group (2019), em seu Quadrante Mágico na categoria de treinamento e conscientização em Segurança da Informação, a empresa *KnowBe4* é considerada a atual líder nesta categoria por três anos consecutivos. Considerada, ainda, a empresa com a maior plataforma de treinamento, conscientização em segurança e simulação de *phishing* do mundo.

O quadrante mágico do Gartner Group é uma metodologia de pesquisa cada vez mais importante na transformação digital, que tem como foco o monitoramento, a avaliação do progresso e das posições das empresas – com base na tecnologia – em um mercado específico. Já os líderes que compõem o quadrante mágico são as empresas tecnologicamente mais avançadas. São elas que ditam as regras dentro do seu segmento por ter uma melhor visão de mercado e capacidade de levar adiante as suas promessas. Na Figura 9 é representado o quadrante mágico da categoria de treinamento e conscientização em Segurança da Informação, para 2019.

Figura 6. Quadrante Mágico na categoria de treinamento e conscientização em Segurança da Informação. (Gartner.com, 2019, adaptado).



Diante do cenário apresentado neste capítulo, foram discutidas ameaças que põem em risco a Segurança da Informação no Poder Judiciário do Tocantins, como também foram apresentados os meios de comunicação que visam à divulgação das atividades e

ações de conscientização, torna-se necessária a apresentação de uma proposta para implantação do plano de conscientização em Segurança da Informação no Poder Judiciário do Tocantins. Esse assunto será abordado detalhadamente a partir do Capítulo 4.

4. PROPOSTA DO PLANO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Campos e Prado (2013) afirmam que não adianta fazer altos investimentos em tecnologias de última geração e deixar de lado o fator humano, já que este é ainda o elo mais fraco na Segurança da Informação. Por esse motivo, devem ter mais atenção na tentativa de conscientizá-los sobre a importância que possuem sobre esta Segurança nas organizações.

Portanto, há grande necessidade de conscientizar os usuários sobre os conceitos e as boas práticas de Segurança da Informação.

4.1. Contextualização da Conscientização

Em uma recente pesquisa global de Segurança da Informação (*Global Stateof Information Security Servey*), desenvolvida pela empresa *Price Waterhouse Coopers* (*PWC),* 2018, foi apresentado um cenário de que colaboradores atuais continuam a ser a principal fonte de incidentes de segurança nas organizações. Na referida pesquisa, foi possível observar que 35% desses incidentes são provenientes de colaboradores atuais.

Corroborando com essa pesquisa, Richard Mogull, analista de Segurança da Informação o do Instituto de Pesquisa *Gartner*, declara que é preciso observar e conhecer rotinas e procedimentos dentro das próprias empresas. Segundo pesquisa realizada pela *Gartner*, apenas 30% dos ataques são provenientes de invasões externas, e cerca de 70% são oriundos de dentro das próprias instituições.

As vulnerabilidades, em sua maioria, são decorrentes do não atendimento às práticas, normas e regulamentações vigentes que orientam sobre os referidos assuntos, como a não conscientização das políticas existentes na organização. Neste sentido a ABNT ISO/IEC 27002:2013, recomenda que os treinamentos e conscientização das políticas e procedimentos organizacionais devem serem feitos por todos os funcionários da organização, e onde, pertinente, parte externas.

A adoção de práticas e de tecnologias na Segurança da Informação não poderá ser considerada efetiva, se não houver a abordagem relacionada ao aspecto humano, por meio da conscientização. Conforme observa Rocha (2008), em muitos dos incidentes de segurança divulgados na mídia, em princípio, a grande maioria não teria sido ocasionada por questões tecnológicas nem por *hackers* mal-intencionados, mas sim pelo fator humano.

Corroborando com a mesma observação, Silva (2012, p. 69) elenca algumas iniciativas necessárias para disseminar a cultura da Segurança da Informação nas instituições, dentre elas podemos destacar:

- Realizar periodicamente palestras de conscientização;
- Capacitar o novo funcionário nas questões de Segurança da Informação;
- Enviar lembretes ou avisos importantes de Segurança da Informação com textos curtos, por e-mail;
- Divulgar notícias publicadas na mídia sobre incidentes de Segurança da Informação ocorridos com outras empresas;
- Criar na intranet da instituição um *banner* da área de Segurança da Informação, no qual possam ser disponibilizadas informações;
- Criar os alertas de Segurança da Informação para os casos de e-mails indesejados e, com isso, combater o *phishingscam*, pois muitas ações de engenharia social fazem uso desses recursos;
- Criar um canal para críticas, sugestões e reportes para os incidentes de Segurança da Informação.

Nesse sentido, para a conscientização, podem-se usar os exemplos de sucesso das ações voltadas à Segurança da Informação, praticadas por outras instituições brasileiras, a exemplo:

- ✓ Dia Internacional de Segurança em Informática (DISI), instituído na Rede Nacional de Ensino e Pesquisa (RNP);
- ✓ Dia da Segurança da Informação, instituído no Tribunal de Contas da União (TCU);
- ✓ Cartilha de Segurança para Internet, publicada pelo Comitê Gestor da Internet no Brasil (CGI.br), dentre outros.

Para composição de um plano de conscientização em Segurança da Informação, segundo a ABNT NBR ISO/IEC 27002:2013, é de extrema importância que todos os funcionários entendam os objetivos desta Segurança, bem como os impactos positivos e negativos dos seus próprios comportamentos dentro da organização.

Conforme entendimento dos autores MITNICK e SIMON (2003), é importane que os funcionários da organização reconheçam o seu papel na Segurança da Informação das organizações. Portanto, os planos de conscientização em Segurança da Informação devem

convencer os funcionários de que os comportamentos inadequados podem gerar prejuízos à organização, aos colegas e ao próprio funcionário.

Assim, a mudança de comportamento exige mudar antigos hábitos por novos, e, possivelmente para que a absorção seja satisfatória, faz-se necessário que todos os funcionários da organização participem das ações de conscientização em Segurança da Informação, com o objetivo de assegurar que não haja alegação de desconhecimento quanto às regras desta Segurança instituídas na organização.

4.2. Norma TIC-09 – Proposta da Minuta do Plano de Conscientização

Para que um plano seja institucionalizado na organização, é necessário que seja realizada sua normatização, por meio de documento próprio. Assim, foi elaborada a Minuta do Plano de Conscientização em Segurança da Informação, com vocabulários, conceitos e a Norma TIC-09, a serem inseridos na Política de Segurança da Informação do Tribunal de Justiça do Estado do Tocantins.

Nesta seção será apresentada a Norma TIC-09 com a proposta da Minuta do Plano de Conscientização de maneira simplificada; porém, sua íntegra está disposta no APÊNDICE B – Norma TIC-09 – Proposta da Minuta do Plano de Conscientização em SI no PJTO, página 94 deste trabalho.

Dessa forma, com o objetivo de normatizar e institucionalizar o Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins, a Minuta foi dividida em duas seções: a primeira representa os vocabulários; a segunda, o plano de conscientização em Segurança da Informação.

A primeira seção apresenta os novos conceitos (vocabulários) que devem fazer parte do MANUAL DE ORGANIZAÇÃO DE CONCEITOS, Anexo I, da Portaria nº 3.433, de 26 de junho de 2017. A lista de vocabulários é composta pelas palavras: Conscientização em Segurança da Informação; Plano; Elo mais Fraco; Ciclo PDCA; *Phishing*; Estrutura Analítica; Fluxo do Processo; Ciberataques; Cibersegurança e Cultura em Segurança da Informação.

A segunda seção apresenta o Plano de Conscientização em Segurança da Informação, distribuído em quatros eixos: Disposições Iniciais, Sistematização, Responsabilidades, Disposições Finais.

Nas disposiões iniciais, são apresentados os objetivos do Plano de Conscientização em Segurança da Informação que são as divulgações das normas instituídas na Política da

Segurança da Informação e de assuntos voltados a esta para magistrados e servidores do Poder Judiciário do Tocantins, para incentivar a cultura de boas práticas em Segurança da Informação, por meio das ações de conscientização.

O proximo eixo é a Sistematização, que foi estruturada em quatro etapas, conforme descritas abaixo.

- **Planejamento:** Etapa inicial do fluxo do processo, sendo constituída de nove processos, com vista à identificação das necessidades, elaboração dos assuntos e conteúdos, editoração e diagramação. É responsabilidade de o Comitê Gestor de Tecnologia da Informação e Comunicação e de o Comitê Gestor de Segurança da Informação coordenar e validarem todas as ações dessa etapa, antes que o processo passe para a etapa de execução;
- **Execução:** Esta etapa é composta por quatro processos, com vista á realização das divulgações das ações de conscientização pelos meios de comunicação existentes e divulgação das normas da Política de Segurança da Informação para os novos magistrados e servidores. Pretende-se, ainda nesta etapa, que todos os magistrados e servidores participem das ações de conscientização, conheçam e respeitem as normas existentes na Política de Segurança da Informação;
- **Registros:** Visa identificar a participação nas ações de conscientização, por meio dos registros ou *logs* coletados das ferramentas de divulgação. Esta etapa possui apenas dois processos;
- **Validar:** Etapa conta com apenas um processo que tem como função validar e tabular os registros e *logs*;
- **Resultados:** É a etapa final do fluxo do processo e tem como objetivo cientificar e divulgar os resultados das ações de conscientização em Segurança da Informação no Poder Judiciário do Tocantins, para que sejam tabuladas nos indicadores do macroprocesso de Gestão de Segurança da Informação, visando ao acompanhamento dos resultados e melhoria contínua do processo.

Ja no eixo Responsabilidades são apresentadas as seis unidades que integram o plano de conscientização em Segurança da Informação, quais sejam: Unidades da Diretoria de Tecnologia da Informação; Comitê Gestor de Tecnologia da Informação e Comunicação; Comitê Gestor de Segurança da Informação; Diretoria de Comunicação Social; Diretoria

de Gestão de Pessoas; Gabinetes, demais Diretorias, Setores e Comarcas do PJTO. Sendo posteriormente descritas as responsabilidades de cada unidade integrante.

Por fim, o eixo Disposições Finais traz o fechamento da Minuta com as informações de que o Comitê Gestor de Segurança da Informação deverá ser comunicado de todas as ações que compõem o plano de conscientização em Segurança da Informação, assim também indicará um dia do ano para ser destinado ao "Dia da Conscientização em Segurança da Informação do Poder Judiciário do Tocantins", com ações totalmente voltadas à Segurança da Informação. O eixo ainda informa que a Diretoria de Gestão Estratégica será a responsável pela compilação e tabulação dos indicadores do macroprocesso de Gestão de Segurança da Informação. Esse eixo finaliza a Minuta com a informação de que o Plano de Conscientização deverá ser atualizado periodicamente, no mínimo uma vez por ano, ou quando se fizer necessário.

4.3. Estrutura Analítica do Plano de Conscientização

A estrutura analítica é uma técnica de estudo, construído de maneira a organizar um conjunto de informações, tornando-a compreensível e de fácil memorização. Seu principal objetivo é organizar os conteúdos e facilitar associações entre as informações destacadas.

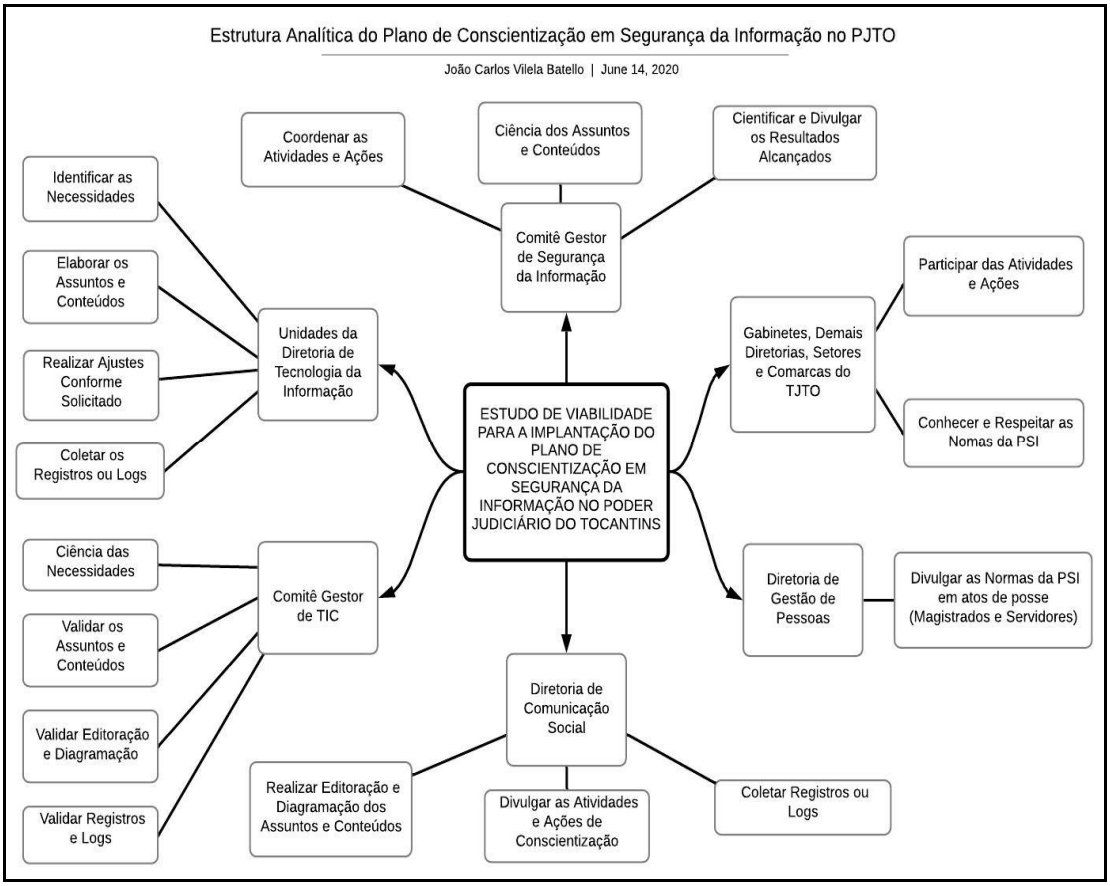
Sabendo da necessidade de que todos os funcionários devem ser conscientizados em Segurança da Informação com objetivo de garantir o efetivo cumprimento da Política de Segurança da Informação e normas de Segurança da Informação do Tribunal de Justiça do Estado do Tocantins, foi elaborada, por meio da ferramenta *Lucidchart*[5], a Estrutura Analítica do Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins.

A estrutura analítica é composta por seis unidades que serão responsáveis pela elaboração, implantação e execução do Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins, bem como traz as informações dos dezessete processos que compõem o plano de conscientização.

Dessa forma, é representada, na Figura 7, a Estrutura Analítica do Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins.

[5] https://www.lucidchart.com/pages/pt

Figura 7. Estrutura Analítica do Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins. (Elaborado pelo Autor).



Com a estrutura analítica elaborada, foi realizada reunião com a Coordenadoria de Gestão e Estratégia do Tribunal de Justiça do Estado do Tocantins, para que o escritório de projeto elaborasse, por meio de fluxogramas, o mapeamento do fluxo do processo de conscientização em Segurança da Informação.

4.4. Fluxo do Processo de Conscientização no Poder Judiciário do Tocantins

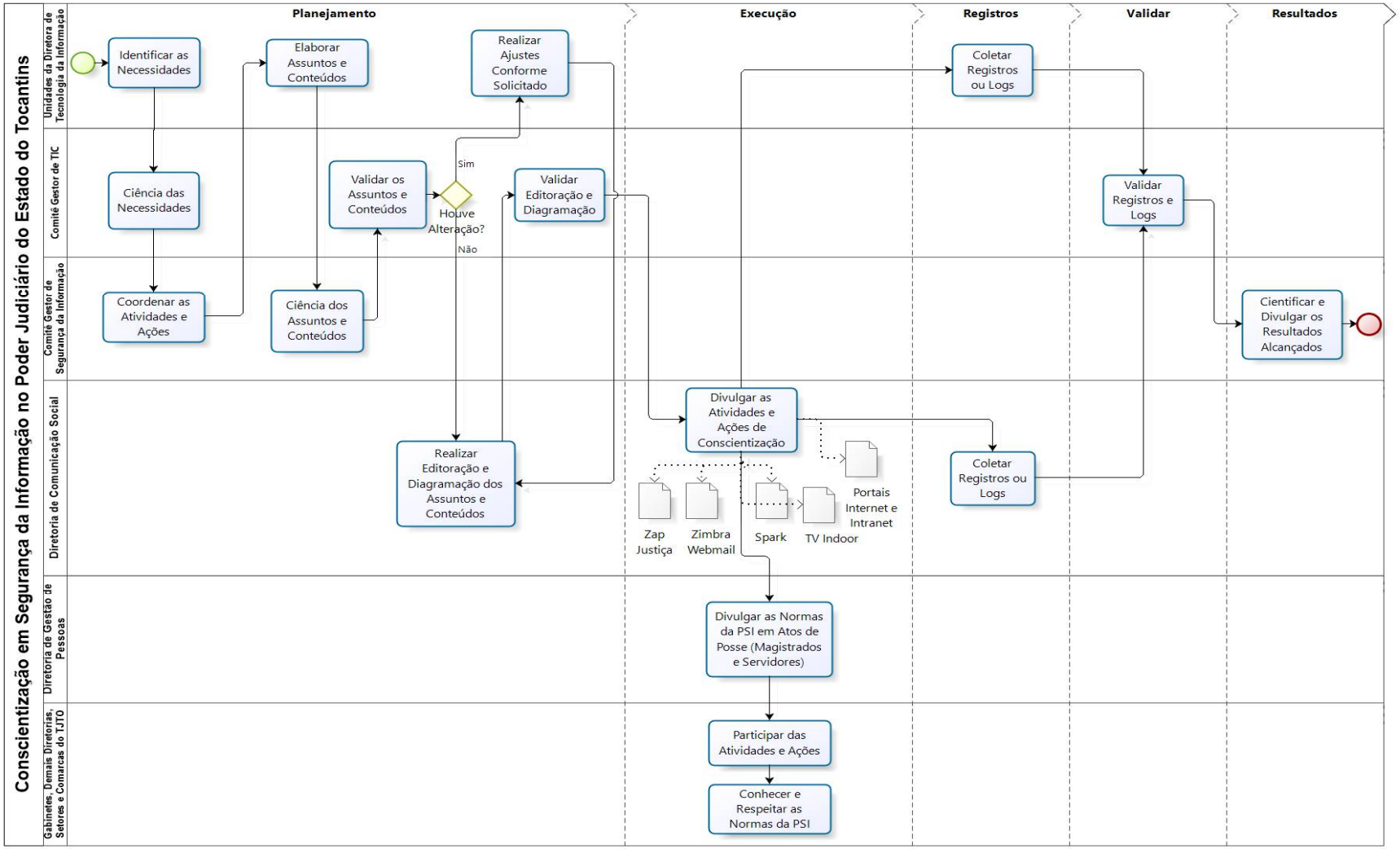
Os fluxogramas são ferramentas utilizadas para a organização sequencial dos processos das empresas, a fim de deixar clara a padronização da execução dos processos; melhorar a comunicação; aumentar a produtividade; e reduzir retrabalhos e custos de operação. São representados por etapas que compõem qualquer tipo de processo especificando as que merecem atenção especial por parte dos envolvidos na execução, identificando as rotinas da organização e deixando claros os pontos de alertas que podem ser melhorados continuamente.

Dessarte, para modelar o processo de conscientização, foram utilizados fluxogramas – representação gráfica que descreve os passos e etapas sequenciais de determinado processo – por meio de figuras geométricas e outros elementos similares. Para elaboração do fluxo do processo foi utilizada a ferramenta de modelagem de processos *Bizagi Process Modeler*[6].

Assim, a Figura 7 representa o fluxo do processo para a conscientização em Segurança da Informação no Poder Judiciário do Tocantins.

[6] https://www.bizagi.com

Figura 8. Fluxo do Processo de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins. (TJTO, 2020).



4.5. Papéis e Responsabilidades

O fluxo do processo que compõe o Plano de Conscientização em Segurança da Informação é composto por dezessete processos distribuídos entre seis unidades.

Essa atividade visa ao acompanhamento na elaboração e execução de cada etapa do processo, delineando entre as unidades envolvidas, garantindo o fiel cumprimento na execução das ações de conscientização em Segurança da Informação.

Assim, na Tabela 1, são representados os papéis e as responsabilidades das unidades envolvidas no processo.

Tabela 1. Papéis de Responsabilidades das Unidades. (Elaborado pelo Autor).

Papéis		Responsabilidades
Unidades da DTINF	Unidades Setoriais da Diretoria de Tecnologia da Informação do PJTO	Identificar as necessidades
		Elaborar assuntos e conteúdos
		Coletar registros e *logs*
		Realizar ajustes conforme solicitado
Comitê Gestor de TIC	Comitê é formado pelo diretor de Tecnologia da Informação e pelos chefes de Divisões, responsáveis pelos processos e macroprocessos de TIC do PJTO	Ciência das necessidades
		Validar assuntos e conteúdos
		Validar diagramação e editoração de assuntos e conteúdos
		Validar registros e *logs*
Comitê Gestor de Segurança da Informação	Comitê Gestor de Segurança da Informação do PJTO	Coordenar e estar ciente das atividades e ações sobre segurança da informação
		Ciência dos assuntos e dos conteúdos
		Cientificar e divulgar os resultados obtidos com as ações de conscientização
Diretoria de Comunicação Social	Diretoria de Comunicação Social do PJTO	Realizar a diagramação e editoração dos assuntos e dos conteúdos.
		Divulgar as atividades e ações de conscientização pelos meios de comunicação (Zap Justiça, Zimbra *Webmail*, *Spark*, Tv *Indoor*, Portais Intranet e Internet), dentre outros.
		Coletar registros ou logs
Diretoria de Gestão de Pessoas	Diretoria de Gestão de Pessoas do PJTO	Divulgar as Normas da Política de Segurança da Informação para novos magistrados e servidores por meio do Termo de Ciência

Gabinetes, demais Diretorias, Setores e Comarcas	Gabinetes, demais Diretorias, Setores e Comarcas do PJTO	Participar das atividades e das ações de conscientização em segurança da informação
		Conhecer e respeitar as normas contidas na Política de Segurança da Informação do Poder Judiciário do Tocantins

4.6. Ferramentas e Meios de Comunicação

O Poder Judiciário do Tocantins possui diversos canais de comunicação com os magistrados e servidores, o que propicia maior abrangência na divulgação de suas ações e informações. A Tabela 2 representa as ferramentas e os meios de comunicação que deverão ser utilizados para a execução do plano de conscientização em Segurança da Informação no Poder Judiciário do Tocantins.

Tabela 2. Ferramentas e Meios de Comunicação. (Elaborado pelo Autor).

Ferramentas e Meios de Comunicação	
Serviço de Mensagem Instantânea (*Spark*)	Ferramenta de comunicação interna entre os usuários do PJTO. (Vide item 3.3.1).
Webmail Institucional (Zimbra)	Plataforma zimbra é a ferramenta de e-mail oficial utilizada por todos os magistrados e servidores do PJTO. (Vide item 3.3.2).
TV *Indoor*	Sistema de mídia por meio de TV *Indoor*. As Tvs estão instaladas em locais estratégicos no Tribunal de Justiça, fóruns e nos prédios anexos, com o objetivo de divulgação de notícias do mundo jurídico, serviço de utilidade pública e conteúdo institucional. (Vide item 3.3.3).
Zap Justiça	Produto de comunicação interna para transmisão de notícias do Judiciário, de forma rápida, dinâmica, econômica e acessível. Por meio da produção de pequenos vídeos ou fotos, essas notícias são enviadas duas vezes por semana pelo aplicativo *Whatsapp*, para magistrados e servidores do PJTO. (Vide item 3.3.4).
Portais Internet e Intranet	Portais do PJTO, em que são divulgadas notícias, informes e demais assuntos. Esses dois meios de comunicação visam contribuir para divulgação de *banners* informativos e educativos sobre Segurança da Informação. (Vide item 3.3.5).
Projeto Justiça Cidadã	Projeto que visa visitar *in loco* as comarcas do Estado, levando informações e capacitações aos magistrados, servidores e para toda a comunidade.
Semana do Servidor	Semana dedicada aos servidores do PJTO. Tem por objetivo realizar atividades, palestras e ações focadas no servidor.

***Folders*/Panfletos**	Visa ampliar a divulgação e a conscientização sobre Segurança da Informação.

4.7. Indicador do Processo

O indicador do processo de conscientização é parte integrante do macroprocesso de Gestão de Segurança da Informação. Assim, a Tabela 3 representa o método de apuração e a fórmula de cálculo do indicador, sendo que a compilação e tabulação dessas informações é responsabilidade da Diretoria de Gestão Estratégica.

Tabela 3. Indicador do Processo. (Elaborado pelo Autor).

Descrição	Método de Apuração / Fórmula de Cálculo	Frequência
Percentual de Usuários Conscientizados	Usuários que visualizaram ou acessaram informações sobre a conscientização em Segurança da Informação. **Fórmula:** Total de usuários conscientizados / Total de usuários do TJTO * 100.	Anual

4.8. Controle de Execução

O controle de execução visa revisar melhor o processo de conscientização em Segurança da Informação. A Tabela 4 representa o controle, o método de execução que será feito pelas reuniões periódicas com todas as equipes envolvidas no processo, e a frequência que poderá ser no mínimo uma vez por ano, ou quando se fizer necessário.

Tabela 4. Controle de Execução. (Elaborado pelo Autor).

Controle	Método de Execução	Frequência
Reavaliar o Plano de Conscientização	Realizar reunião com representantes das Unidades de Diretoria de Tecnologia da Informação, do Comitê Gestor de TIC, da Diretoria de Comunicação Social, da Diretoria de Gestão de Pessoas, da Coordenação de Gestão Estratégica e do Comitê Gestor Segurança da Informação, para avaliar a aderência, os benefícios gerados e as oportunidades de melhoria do processo. Essa avaliação deve identificar se o processo necessita de revisão ou melhorias, e deverá ocorrer periodicamente, no mínimo uma vez por ano, ou quando se fizer necessário.	Anual

4.9. Descrição das Atividades

As descrições das atividades dos dezessete processos que compõem o fluxo do processo de conscientização em Segurança da Informação, conforme apresentado na Figura 7, serão detalhados a seguir, destacando-se os autores, suas responsabilidades, entradas, saídas e suas atividades.

Detalhamentos do Fluxo do Processo de Conscientização em Segurança da Informação

a) Identificar as Necessidades: considerada a atividade inicial do processo de conscientização, esta atividade compreende identificar as necessidades voltadas à segurança da informação, para embasamento da construção das ações de conscientização em segurança da Informação no Poder Judiciário do Tocantins.

Responsáveis: unidades setoriais da Diretoria de Tecnologia da Informação.

Considerações: realizar reunião com um representante de cada unidade para identificação das necessidades.

Entradas: normativas, resoluções, ocorrências ou incidentes que mereçam divulgação, recomendações oriundas de órgãos de controle externo ou interno, Política de Segurança da Informação do PJTO.

Saídas: formulário final com as necessidades para as ações de conscientização em Segurança da Informação.

Atividades:

- Levantamento documental: analisar os documentos levantados.
- Indentificação: identificar nos documentos analisados as necessidades para serem inseridas nas ações de conscientização do PJTO.

b) Ciência das Necessidades: Essa atividade consiste no conhecimento das necessidades levantadas pelas unidades setoriais da Diretoria de Tecnologia da Informação.

Responsável: Comitê Gestor de Tecnologia da Informação.

Entradas: formulário com as necessidades para as ações de conscientização em Segurança da Informação.

Saídas: ciência no formulário com as necessidades para as ações de conscientização em Segurança da Informação.

Atividades:

- Analisar o formulário com as necessidades.
- Ciência no formulário com as necessidades.

c) Coordenar as Atividades e as Ações:

Responsável: Comitê Gestor de Segurança da Informação.

Entradas: atividades e ações que farão parte do plano de conscientização.

Saídas: estabelecer metas e prazos para os trabalhos que serão realizados.

Atividades:

- Analisar atividades e ações.
- Aprovar ou sugerir alterações.
- Estabelecer metas e prazos para o desenvolvimento dos trabalhos.

d) Elaborar Assuntos e Conteúdos: consiste na elaboração e detalhamento de assuntos e conteúdos para as atividades e ações de conscientização.

Responsáveis: unidades da Diretoria de Tecnologia da Informação

Considerações: realizar reunião com um representante de cada unidade para que em conjunto sejam elaborados os assuntos e os conteúdos.

Entradas: normativas, resoluções, ocorrências ou incidentes que mereçam divulgação, recomendações oriundas de órgãos de controle externo ou interno e a Política de Segurança da Informação do PJTO.

Saídas: formulário finalizado com assuntos e conteúdos.

Atividades:

- Definir tópicos a serem abordados com assuntos e conteúdos para conscientização.
- Realizar o detalhamento de assuntos e conteúdos.
- Definir o público-alvo das atividades e das ações.
- Definir os meios de comunicação para a disponibilização dos assuntos e conteúdos.

e) Ciência dos Assuntos e Conteúdos: atividade consiste no conhecimento de assuntos e conteúdos detalhados pelas unidades.

Responsável: Comitê Gestor de Segurança da Informação.

Entradas: formulário finalizado com assuntos e conteúdos.

Saídas: formulário finalizado com assuntos, conteúdos e a ciência do Comitê Gestor de Segurança da Informação.

Atividades:

- Analisar o formulário finalizado.
- Dar ciência e conhecimento aos assuntos e conteúdos.

f) Validar Assuntos e Conteúdos: validar assuntos e conteúdos apresentados pelas unidades da Diretoria da Tecnologia da Informação para as atividades e ações de conscientização.

Responsável: Comitê Gestor de Tecnologia da Informação.

Considerações: a validação deverá ocorrer nas reuniões que ocorrem mensalmente.

Entradas: formulário com assuntos e conteúdos levantados pelas unidades da Diretoria da Tecnologia da Informação, para as atividades e ações de conscientização.

Saídas: assuntos e conteúdos validados ou com indicação de ajustes.

Atividades:

- Analisar assuntos e conteúdos para as atividades e ações de conscientização.
- Aprovar ou indicar ajustes que se fizerem necessários.

g) Realizar Ajustes: realizar os ajustes indicados pelo Comitê Gestor de Tecnologia da Informação.

Responsáveis: unidades de Diretoria de Tecnologia da Informação.

Entradas: indicação dos ajustes propostos pelo Comitê Gestor de Tecnologia da Informação.

Saídas: formulário finalizado com assuntos e conteúdos ajustados, conforme indicação.

Atividades:

- Analisar as indicações dos ajustes necessários.
- Realizar os ajustes conforme solicitado.

h) Realizar Editoração e Diagramação: atividade consiste na editoração e diagramação de assuntos e conteúdos produzidos pelas unidades de Diretoria de Tecnologia da Informação.

Responsável: Diretoria de Comunicação Social.

Entradas: formulário com assuntos e conteúdos.

Saídas: material editorado e diagramado, finalizado.

Atividades:

- Realizar a editoração de assuntos e conteúdos, de acordo com o canal de comunicação a ser utilizado nas atividades e ações de conscientização.
- Realizar a diagramação de assuntos e conteúdos, de acordo com o canal de comunicação a ser utilizado nas atividades e ações de conscientização.

i) Validar Editoração e Diagramação: atividade consiste na validação de editorações e diagramações realizadas pela Diretoria de Comunicação Social.

Responsável: Comitê Gestor de Tecnologia da Informação.

Considerações: validar editoração e diagramação.

Entradas: material editorado e diagramado, finalizado.

Saídas: validação do material editorado e diagramado.

Atividades:

- Validar a editoração de assuntos e conteúdos.
- Validar a diagramação de assuntos e conteúdos.
- Validar os meios de comunicação de cada assunto e conteúdo.

j) Divulgar os Assuntos e Conteúdos: atividade consiste na realização da divulgação dos materiais de conscientização em Segurança da Informação, por meio dos canais de comunicação existentes no PJTO.

Responsável: Diretoria de Comunicação Social.

Entradas: materiais com assuntos e conteúdos para as atividades e ações de conscientização.

Saídas: divulgação e disponibilização dos materiais de conscientização pelos meios de comunicação existentes no PJTO.

Atividades:

- Comunicar os Comitês Gestor de Segurança da Informação e Tecnologia da Informação, sobre o início das atividades de divulgação.
- Divulgar os materiais de conscientização. Esta atividade compreende a disponibilização ao público interno (magistrados, servidores e colaboradores) do material de conscientização produzido e diagramado.
- Podem ocorrer situações em que outras áreas também sejam responsáveis pela divulgação dos materiais.

k) Divulgar as Normas da PSI em Atos de Possse: atividade consiste na apresentação do Termo de Ciência da Política de Segurança da Informação para novos magistrados e servidores.

Responsável: Diretoria de Gestão de Pessoas.

Considerações: atividade visa ampliar ainda mais as ações de conscientização e divulgação das normas contidas na PSI do PJTO.

Entradas: Política de Segurança da Informação, novos magistrados e servidores.

Saídas: novos magistrados e servidores conscientizados desde o ato de posse, com vista à mudança de cultura voltada às boas práticas em Segurança da Informação.

Atividades:

- Receber os novos magistrados e servidores para os atos de posse.
- Realizar a entrega do Termo de Ciência da PSI.
- Orientação quanto às dúvidas e reportes de incidentes de Segurança da Informação deverá ser encaminhada à Diretoria de Tecnologia da Informação.

l) Participar das Atividades e Ações: atividade consiste na participação de ações e atividades de conscientização em Segurança da Informação do PJTO.

Responsáveis: todos os Gabinetes, Diretorias, Setores e Comarcas do PJTO.

Entradas: atividades e ações de conscientização em Segurança da Informação.

Saídas: magistrados e servidores conscientizados.

Atividades:

- Participar das atividades ações de conscientização em Segurança da Informação, por meio dos canais de comunicação do PJTO.

m) Conhecer e Respeitar as Normas da PSI:

Responsáveis: todos os magistrados e servidores do PJTO.

Entrada: Política de Segurança da Informação.

Saídas: magistrados e servidores conscientizados sobre as Normas existentes na PSI do PJTO.

Atividades:

- Acessar a PSI disponível no sítio do TJTO.
- Fazer a leitura da PSI e de suas normas.
- Conhecer e respeitar as informações nela contidas.
- Comunicar a Diretoria de Tecnologia da Informação qualquer evento que possa infringir a Segurança da Informação.

n) Coletar Registros e *Logs*: coletar os registros e *logs* dos participantes de atividades e ações realizadas.

Responsáveis: Diretoria de Comunicação Social e Unidades da Diretoria de Tecnologia da Informação.

Considerações: Essa atividade é essencial para alimentar os indicadores do macroprocesso de Gestão de Segurança da Informação.

Entradas: Dados sobre atividades ações de conscientização.

Saídas: Registros de *logs* de acesso às atividades e ações de conscientização

Atividades:

- Coletar os registros de acesso aos materiais disponibilizados nas atividades e ações de conscientização.
- Coletar os *logs* de acessos aos materiais disponibilizados nas atividades e ações de conscientização.

o) Validar Registros e *Logs*: atividade consite na validação dos registros e *logs*.

Responsável: Comitê Gestor de Tecnologia da Informação.

Entradas: registros e *logs* de acesso aos materiais disponibilizados.

Saídas: eegistros e *logs* de acesso aos materiais disponibilizados validados e prontos para serem divulgados.

Atividades:

- Analisar registros e *logs.*
- Validar registros e *logs* de acesso aos materiais disponibilizados nas ações e atividades de conscientização.

p) Cientificar e Divulgar os Resultados Alcançados: atividade consiste no conhecimento dos resultados das atividades e ações de conscientização em Segurança da Informação, por meio de registros e *logs* de acesso aos materiais.

Responsável: Comitê Gestor de Segurança da Informação.

Entradas: registros e *logs* de acesso aos materiais disponibilizados nas atividades e ações de conscientização.

Saídas: conhecimento e divulgação dos resultados, bem como inserções nos indicadores dos processos vinculados ao macroprocesso de Gestão de Segurança da Informação.

Atividades:

- Conhecimento dos resultados alcançados.
- Divulgar os resultados ao público interno (magistrados, servidores e colaboradores).
- Encaminhar os resultados para que a Coordenação de Gestão Estratégica alimente os indicadores dos processos vinculados ao macroprocesso de Gestão de Segurança da Informação.

4.10. Formulário para Conscientização

Nesta seção, será apresentado o Formulário para Concientização em Segurança da Informação de maneira simplificada, porém sua íntegra está disposta no APÊNDICE D – Formulário para o Plano de Conscientização em SI do PJTO –, página 101 deste trabalho.

Para padronizar e facilitar a tramitação entre as áreas envolvidas no processo de conscientização, foi desenvolvido um modelo de formulário com os campos para as indicações das necessidades, detalhamentos dos assuntos e conteúdos e apreciação das informações pelo Comitê Gestor de Tecnologia da Informação.

O formulário possui também dois anexos para preenchimento das informações. O Anexo I visa à indicação dos assuntos e conteúdos, prioridade, público-alvo e a

periodicidade de execução das atividades e ações de conscientização. Já o anexo II tem como função realizar os detalhamentos de cada assunto e conteúdo indicados no anexo anterior.

4.11. Termo de Ciência da PSI do PJTO

Nesta seção, será apresentado o Termo de Ciência da Política de Segurança da Informação do PJTO de maneira simplificada, porém sua íntegra está disposta no APÊNDICE E – Termo de Ciência da PSI do PJTO –, página 105 deste trabalho.

Visando ampliar ainda mais as ações de conscientização, principalmente na divulgação das normas da Política de Segurança da Informação do PJTO, atendendo à Resolução nº 211 do Conselho Nacional de Justiça, de 2015, e Portaria nº 3.433 do Tribunal de Justiça do Estado do Tocantins, de 2017, foi desenvolvido o Termo de Ciência da PSI do PJTO com informações, como: *link* de disponibilidade da PSI e os contatos para dúvidas e reportes de possíveis incidentes de Segurança da Informação, para serem entregues aos novos magistrados e servidores nos atos de posse.

Dessa forma, o Termo de Ciência da PSI objetiva que os novos membros do PJTO, desde o ato de posse, já tenham conhecimento da existência da PSI e se comprometam a realizar o acesso e leitura desta. Acretida-se que, com esse simples gesto e alinhado às atividades e ações de conscientização, seja possível iniciar entre os novos membros o processo de mudança da cultura voltada às boas praticas em Segurança da Informação, no PJTO.

4.12. Temas Relevantes para Conscientização

É imprescindível que os usuários aprendam as boas práticas de comportamento e uso da Internet, a fim de evitar que as ameaças afetem o negócio da organização.

Além dos assuntos contidos na Política de Segurança da Informação do Tribunal, principalmente em relação às normas: TIC-01: Responsabilidades do Usuário e TIC-04: Controle de Acesso do Usuário, é necessário também abordar outros assuntos que poderão ser incluídos na conscientização em Segurança da Informação, garantindo assim mais segurança não só para magistrados e servidores, mas principalmente para o Tribunal de Justiça do Estado do Tocantins:

1. Uso correto de *logins* e senhas.
2. Ataques de *phishing*. Saber verificar atentamente remetente, assunto, anexos dos e-mails.
3. Bloqueio do computador ao se ausentar do local de trabalho.
4. Política de mesa e tela limpa.
5. Uso do Antivírus Institucional.

4.13. Periodicidade e Revisões dos Conteúdos

O Plano de Conscientização em Segurança da Informação deve ser contínuo e recorrente, para que se atinja tanto os novos magistrados e servidores quanto relembrar os usuários antigos da importância da SI. Assim os conteúdos do plano de conscientização deverão ser revisados pelo menos uma vez por ano, ou quando se fizer necessário.

Portanto, a periodicidade de revisões dos conteúdos do plano de conscientização em Segurança da Informação do Poder Judiciário do Tocantins será anualmente, ou quando se fizer necessário.

4.14. Pessoas envolvidas na Conscientização

Para que um plano de conscientização seja eficiente e bem-sucedido, é necessário o envolvimento de outros departamentos da organização, os quais devem ter interesse mútuo, possibilitando a contribuíção no planejamento e execução.

Posto isso, para que o plano de conscientização em Segurança da Informação do Tribunal de Justiça do Estado do Tocantins seja bem-sucedido, é necessário o envolvimento de todos os Gabinetes, Diretorias, Setores e Comarcas que compõem o Poder Judiciário do Tocantins.

Além das unidades mencionadas, é necessário que todos os usuários da organização entendam a importância da Segurança da Informação.

Dessa forma**,** é necessária a participação de todos os magistrados e servidores nas atividades e ações de conscientização em Segurança da Informação.

4.15. Recursos Necessários para Conscientização

Considerando que os crimes cibernéticos ultimamente podem ter diversos meios de ataque, é notório que o plano de conscientização em Segurança da Informação também precisa ser tão abrangente quanto possível.

Segundo a empresa *High Security Center* (*HSC)*, 2018, os funcionários das organizações devem fazer parte do plano de conscientização, além de terem a possibilidade de diálogos abertos com a equipe de segurança por vários meios de comunicação.

Ainda conforme a *HSC*, os planos de conscientização não têm um padrão fechado e definido, pois é construído conforme as necessidades da organização, possibilitando, assim, que os funcionários recebam as ações de conscientização por diversos meios: simulações de *phishing*, *newsfeeds*, boletins informativos, *blogs*, jogos, dentre outros.

Assim, como já abordado anteriormente no Capítulo 3, as atividades e as ações do plano de conscientização em Segurança da Informação pretendem ser executadas por meio dos canais de comunicação já existentes e institucionalizados no Poder Judiciário do Tocantins. Vejamos:

- **Divulgação das Atividades e Ações de Conscientização em Segurança da Informação:** Serviço de Mensagem Instantânea (*Spark*), *Webmail* Institucional (Zimbra), TV *Indoor*, Zap Justiça, Portais Internet e Intranet, Projeto Justiça Cidadã, Semana do Servidor e *Folders*/Panfletos.

O fator humano desempenha um papel crítico na postura geral de Segurança da Informação de uma organização. Assim a conscientização visa mitigar os incidentes de Segurança da Informação. Segundo o Gartner Group (2019), até 2022, 60% das grandes organizações e empresas terão programas abrangentes de treinamento e conscientização sobre Segurança da Informação. Dessa forma, fazendo o uso de programas específicos para conscientização, à disseminação da cultura em Segurança da Informação no Tribunal de Justiça do Estado do Tocantins, poderá ser cada vez mais eficiente.

Assim, para obter um panorama do conhecimento sobre Segurança da Informação no Poder Judiciário do Tocantins, o próximo Capítulo aborda sobre o estudo de caso realizado nesta pesquisa.

5. ESTUDO DE CASO

Para a realização do estudo de caso, foi elaborado um instrumento de pesquisa para coleta de dados, com o objetivo de obter um panorama do conhecimento sobre a Segurança da Informação no Poder Judiciário do Tocantins. O instrumento de pesquisa foi composto por 21 perguntas, sendo todas fechadas e elaboradas tendo por base o estudo desenvolvido por Alexandria (2009) em sua tese de doutorado.

Nessa pesquisa, foram distribuídos 205 questionários via Sistema Eletrônico de Informações (SEI), dos quais 180 foram respondidos no período de 30/4/2020 a 15/0/2020, totalizando 16 dias de disponibilidade.

Dentro do SEI, um departamento, setor, escrivania civel ou criminal, diretorias, gabinetes, dentre outros setores, são representados como sendo uma Unidade Organizacional, que em sua grande maioria possui mais de um servidor (a). Contudo foi solicitada que apenas um magistrado (a) ou servidor (a) de cada Unidade Organizacional respondesse ao questionário, assim a resposta obtida não representa a ideia de todos os demais servidores de tal Unidade Organizacional.

Receberam os questionários as Unidades Organizacionais das áreas meio e fim do Poder Judiciário do Tocantins, obtendo uma representatividade das unidades, sendo possível obter uma opnião de este Poder quase como um todo.

5.1. Autorização de envio do Instrumento de Pesquisa

Para que o instrumento de pesquisa fosse encaminhado às Unidades Organizacionais do Poder Judiciário, foi necessário abrir um processo administrativo por meio do Sistema Eletrônico de Informações (SEI), a ser remetido à Diretoria de Tecnologia da Informação (DTINF) para conhecimento e manifestação do envio do instrumento de pesquisa. Nessa mesma solicitação, foi reforçada a informação de que o instrumento de pesquisa tinha apenas finalidades acadêmicas, no intuito de salvaguardar a proteção dos direitos dos respondentes desse instrumento. Informando ainda que os dados obtidos não serão utilizados para outros fins que não aqueles constantes nos objetivos do estudo.

Ao receber o processo, a DTINF acolheu a solicitação e encaminhou os autos à Diretoria Geral para providências necessárias, que manifestou pelo envio dos autos à

douta Presidência do TJTO para conhecimento e deliberação, tendo em vista que o público-alvo da pesquisa envolvia a própria Presidência, Gabinetes dos Desembargadores, Gabinete da Corregedoria Geral de Justiça, Diretoria Geral da Esmat, Diretorias dos Fóruns e Coordenadoria de Gestão Estratégica. Assim, a Presidência acolheu a manifestação da DTINF e autorizou a aplicação do instrumento de coleta de dados (questionário).

5.2. Instrumento de Pesquisa

O questionário foi dividido em três dimensões, sendo a primeira composta por perguntas relacionadas ao comportamento do respondente ante a Segurança da Informação, com o propósito de identificar os possíveis comportamentos inadequados dos respondentes sobre o tema apresentado.

A segunda abordou perguntas pertinentes à concordância da implantação do plano de ações de conscientização em Segurança da Informação, bem como o interesse de participação do respondente, com vista à busca pela cultura de boas práticas em Segurança da Informação no Poder Judiciário do Tocantins.

Já a terceira e última dimensão, por sua vez, teve como objetivo identificar o local de ocupação dos servidores lotados nas repartições para onde foram encaminhados os instrumentos, bem como o tempo de serviço e os serviços e sistemas que utilizam ou têm acesso. Nessa dimensão, também consta a escolha de três assuntos, para possíveis prioridades na composição inicial do plano de conscientização em Segurança da Informação no Tribunal de Justiça do Estado do Tocantins, além de identificar se o respondente já havia participado de algum programa voltado à Segurança da Informação.

O instrumento de pesquisa foi baseado por meio da escala *Likert*, que, de acordo com Dzazali e Zolait (2012), é amplamente utilizado para medição de atitudes, crenças e opiniões. Assim foram definidas cinco categorias de escolha, sendo: na dimensão 1, correspondentes às perguntas de 1 até 7, foram utilizadas como respostas as seguintes representações: 1 (muita frequência), 2 (frequentemente), 3 (ocasionalmente), 4 (raramente) e 5 (nunca). Na dimensão 2, correspondentes às perguntas de 8 até 14, foram utilizadas como respostas as seguintes representações: 1 (concordo totalmente), 2 (concordo), 3 (indeciso), 4 (discordo) e 5 (discordo totalmente).

Quanto à definição do público-alvo do instrumento de pesquisa, esta levou em consideração que a administração do TJTO tivesse o conhecimento e a importância deste trabalho para o Tribunal de Justiça do Estado do Tocantins. Dessa forma, e em conjunto com o professor orientador, foram definidas como público-alvo deste estudo algumas Unidades Organizacionais do Poder Judiciário do Tocantins, inicialmente compostas por 64 Unidades Organizacionais, a saber: Presidência, Gabinetes dos Desembargadores, Gabinete da Corregedoria Geral de Justiça, Diretoria Geral da Esmat, Diretorias dos Fóruns, Coordenadoria de Gestão Estratégica, Diretoria Geral e demais Diretorias do Poder Judiciário do Tocantins.

Após autorização do envio do instrumento de pesquisa pelo presidente do TJTO, desembargador-presidente em exercício, o processo SEI, com o *link* para acesso e preenchimento do questionário, foi encaminhado em 30/4/2020, para as 64 Unidades Organizacionais pré-definidas. No envio do instrumento de pesquisa, foi reforçado que era necessário que apenas um (a) magistrado (a) ou servidor (a) de cada Unidade Organizacional respondesse ao questionário.

Contudo, algumas Unidades Organizacionais, ao receberem o Processo SEI, contendo o questionário, reencaminharam-no para suas Subunidades. O instrumento de pesquisa foi recebido por 205 Unidades Organizacionais, porém respondido por 180 delas, totalizando um percentual de 88,78% respondentes.

Para destacar a seriedade desse estudo, foram inseridas duas informações no Processo SEI tratando da importância do tema "Segurança da Informação para o Tribunal de Justiça do Estado Tocantins", bem como a necessidade de obter o máximo de respostas possíveis a serem analisadas.

5.3. Resultados e Análises

Para melhor classificação, os resultados e análises serão divididos conforme as três dimensões do instrumento de pesquisa: Comportamento, Conscientização e Perfil.

5.3.1. Dimensão 1: Comportamento

A dimensão 1 é composta por sete perguntas, com objetivo de coletar informações acerca do comportamento dos respondentes em relação à Segurança da Informação.

Os resultados correspondentes às perguntas de número 1 a 7 foram explicitados em tabela e gráfico para melhor entendimento. Na tabela 5, os dados se encontram em porcentagem exata ao número de respostas em cada categoria da escala *likert*. No Gráfico 3, os dados foram baseados nas informações da tabela supracitada representando de forma ilustrativa os resultados das perguntas de número 1 a 7.

As perguntas de número 1 a 3 tratam sobre o uso de senhas: utiliza senhas fáceis de lembrar (compostas por nomes ou suas iniciais, datas de aniversários, sequências de letras ou números); anotação de senhas em locais de fácil acesso (agendas, monitores, debaixo do teclado ou sobre a mesa); compartilhamento de senha com terceiros (colegas de trabalho, sala ou gabinete), respectivamente. Observou-se a predominância das respostas nunca e raramente em comparação às demais, o que permite deduzir que grande parte dos respondentes faz o uso adequado de senhas, evitando anotá-las ou compartilha-las, inferindo assim certo grau de segurança.

A pergunta de número 1, que tratava do uso de senhas fáceis de lembrar (compostas por nomes ou suas iniciais, datas de aniversários, sequências de letras ou números), obteve em 65% dos respondentes a categoria nunca ou raramente utilizam senhas fáceis; 16,1% ocasionalmente utilizam essa prática; enquanto 18,9% dos respondentes fazem o uso frequente ou muito frequente. Tal comportamento torna os usuários alvos fáceis para os *cybers* criminosos, que utilizando de técnicas de ataque de força-bruta, conseguem com certa facilidade quebrar as senhas desses usuários.

A pergunta de número 2 abordava sobre a anotação de senhas em agendas, monitores, teclados, ou sobre a mesa de trabalho. O resultado dessa pergunta foi que 79,4% dos respondentes afirmam que nunca ou raramente anotam suas senhas. Em contrapartida, outros 20,6% afirmam que ocasionalmente, frequentemente ou com muita frequência fazem o uso desse comportamento anotando suas senhas. Esse comportamento fere as boas práticas de Segurança da Informação, pois a perda, roubo ou cópia dessas senhas por pessoas desconhecidas podem gerar danos ao usuário e ao TJTO.

A pergunta de número 3 almejava saber sobre o compartilhamento de senha com colegas de trabalho, sala ou gabinete, em que 92,7% dos respondentes afirmaram que nunca ou raramente compartilham suas senhas com terceiros. Apesar da grande maioria dos magistrados e servidores se atentar para esse comportamento, observou-se que 7,3% dos respondentes faz o uso de compartilhamento de suas senhas com colegas de trabalho, o que não vai ao encontro ao recomendado pelas boas práticas de Segurança da Informação, em que senhas devem ser consideradas pessoais e intransferíveis.

Na pergunta de número 4, os resultados obtidos demonstraram que 93,9% dos respondentes nunca ou raramente fornecem dados pessoais por e-mail, quando solicitados por órgãos públicos ou de empresas conceituadas do mercado. Este comportamento positivo merece atenção especial, pois os ataques de *spams* e *phishing* são de fato concluídos com sucesso, após os usuários que recebem esses tipos de e-mails fornecerem seus dados pessoais. Ainda assim houve 6,1% que ocasionalmente, frequentemente ou com muita frequência fornece seus dados pessoais quando solicitados por e-mail.

Outro comportamento que pode evidenciar possíveis incidentes de Segurança da Informação foi abordado na pergunta de número 5, que tinha o objetivo de saber se ao se ausentar do local de trabalho o respondente encerra a sessão aberta no computador (faz *logout*), bloqueia a sessão com uso de senha. Dentre os respondestes 86,1% se atentam a essa prática, porém os outros 13,9% afirmaram que ocasionalmente, raramente ou nunca fazem o bloqueio de sessão por meio de uso de senha. Esse comportamento pode ser considerado um ponto inicial para os incidentes de Segurança da Informação nas organizações.

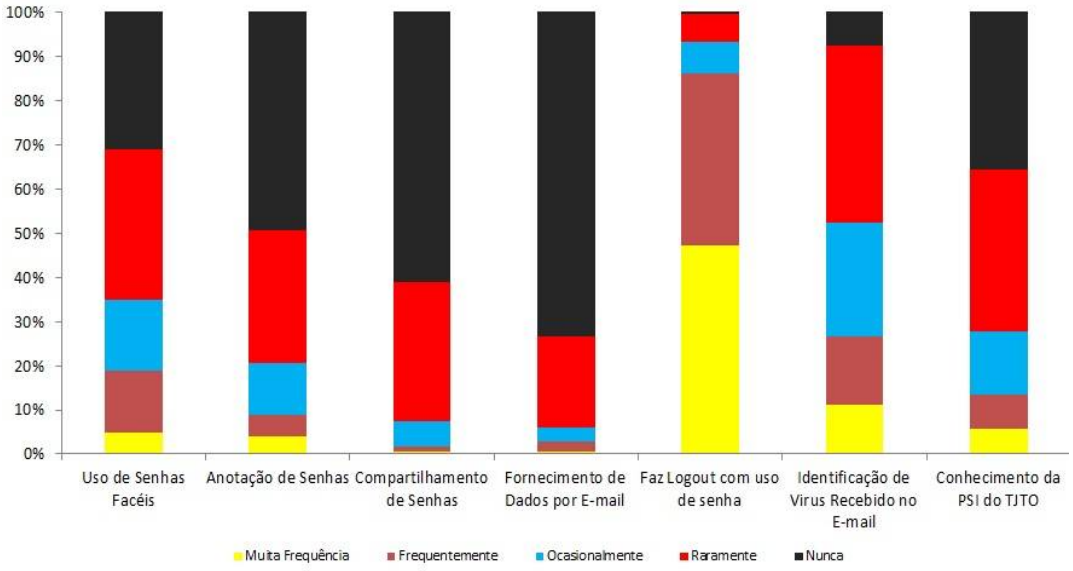
A pergunta de número 6 aborda sobre a possibilidade de identificação de um vírus de computador, quando recebido por meio de mensagens de correio eletrônico (e-mail). O resultado já era de se esperar, pois 47,7% dos respondentes raramente ou nunca conseguem identificá-lo. Contudo, mais de um terço (25,6%) dos respondentes ocasionalmente identificam-no, enquanto outro terço (26,7%) dos respondentes consegue frequentemente ou com muita frequência identificar um vírus de computador recebido por e-mail.

Com foco na Política de Segurança da Informação, a sétima e última pergunta dessa dimensão visa identificar se o respondente tem conhecimento das Normas da PSI do Tribunal de Justiça do Estado do Tocantins. Assim, o resultado perante a pergunta,

vem ao encontro com os objetivos deste trabalho, pois 72,2% dos respondentes nunca ou raramente têm conhecimento das Normas da PSI, e apenas 27,8% têm conhecimento ocasional ou frequente sobre a Norma.

Dessa forma, o Gráfico 3 representa, de forma ilustrativa, as respostas obtidas nas perguntas de números 1 a 7, que correspondem à dimensão 1.

Gráfico 3. Perguntas de 1 a 7 da Dimensão 1 – Comportamento. (Elaborado pelo Autor).



Os resultados em porcentagem exata ao número de respostas em cada categoria da escala *likert*, das perguntas de números 1 a 7, correspondentes à dimensão 1, são confirmadas na Tabela 5 abaixo.

Tabela 5. Perguntas de 1 a 7 da Dimensão 1 – Comportamento. (Elaborada pelo Autor).

Representações	Muita Frequência	Frequentemente	Ocasionalmente	Raramente	Nunca	Total de Respostas
Uso de Senhas Facéis	5,0%	13,9%	16,1%	33,9%	31,1%	100,0%
Anotação de Senhas	3,9%	5,0%	11,7%	30,0%	49,4%	100,0%
Compartilhamento de Senhas	0,6%	1,1%	5,6%	31,6%	61,1%	100,0%
Fornecimento de dados por E-mail	0,6%	2,2%	3,3%	20,6%	73,3%	100,0%
Faz Logout com uso de Senha	47,2%	38,9%	7,2%	6,1%	0,6%	100,0%
Identificação de Vírus Recebido no E-mail	11,1%	15,6%	25,6%	39,9%	7,8%	100,0%
Conhecimento da PSI do TJTO	5,6%	7,8%	14,4%	36,6%	35,6%	100,0%

5.3.2. Dimensão 2 – Conscientização

A Dimensão 2 foi composta por 7 perguntas, com objetivo de coletar informações sobre a conscientização em Segurança da Informação. Dessa forma, as perguntas de números 8 a 14 tratavam das Responsabilidades das Ações SI; Instituição do Plano de Conscientização SI; Participação das Ações de Conscientização; Importância da Criação do dia "D" em SI; Objetivos das Ações de Conscientização; Cultura de Boas Práticas em SI; Sucesso da Conscientização para a Organização, respectivamente.

Dessarte, dos resultados coletados, pode ser observado um alto índice de aceitação e de concordância com as perguntas apresentadas. Cabe destacar que todas as respostas concordam e concordam totalmente somaram-se juntas à média de 95,9% dos respondentes, seguida por 2,8% de indecisos, 0,9% que discordam e apenas 0,4% dos respondentes que discordam totalmente.

Os resultados correspondentes às referidas perguntas encontram-se representados na Tabela 6 em porcentagem exata ao número de respostas em cada categoria da escala *likert*. Assim os dados do Gráfico 2 foram baseados nas informações contidas na Tabela supracitada representando de forma ilustrativa os resultados das perguntas de números 8 a 14.

A pergunta de número 8 se refere à opinião dos respondentes, em relação a cada magistrado e servidor terem a consciência de suas responsabilidades sobre ações que envolvam a Segurança da Informação. Quase todos os respondentes (97,7%) concordam ou concordam totalmente com essa afirmativa; apenas 1,7% de indecisos; e 0,6% discordam da afirmação.

As perguntas de números 9 e 10 abordaram assuntos bem parecidos; a de número 9 almejava a opinião do respondente quanto à instituição de um plano de conscientização em Segurança da Informação no Tribunal de Justiça do Estado do Tocantins, enquanto a pergunta de número 10 tinha por meta a concordância do respondente em participar das ações de conscientização. Assim os que concordaram com a implantação do plano de conscientização em Segurança da Informação somaram-se 97,8% e os que concordaram em participar das ações somaram 93,3% respectivamente. Porém, o resultado dos indecisos, chamou a atenção, obtendo 2,2% na nona pergunta, enquanto o resultado da décima pergunta, foi mais que o dobro, ficando

na casa dos 5,6% de indecisos. Ainda assim 1,1% dos respondentes discordam em participar das ações de conscientização.

Em relação à pergunta de número 11, vale destacar, foi à única da dimensão 2 em que todas as alternativas receberam indicação. Tal pergunta investigava saber se os respondentes consideravam importante que o Tribunal de Justiça do Estado do Tocantins criasse o dia "D", com ações voltadas à conscientização em Segurança da Informação por meio de palestras, mesas redondas, *workshops*. Grande parte dos respondentes (87,2%) considera importante a criação do “D”, sendo assim um resultado positivo mediante o estabelecimento de boas práticas de Segurança da Informação, opinando como concordam ou concordam totalmente. Contudo, 6,1% responderam que estavam indecisos seguidos de 3,9% que discordam e 2,8% que discordam totalmente.

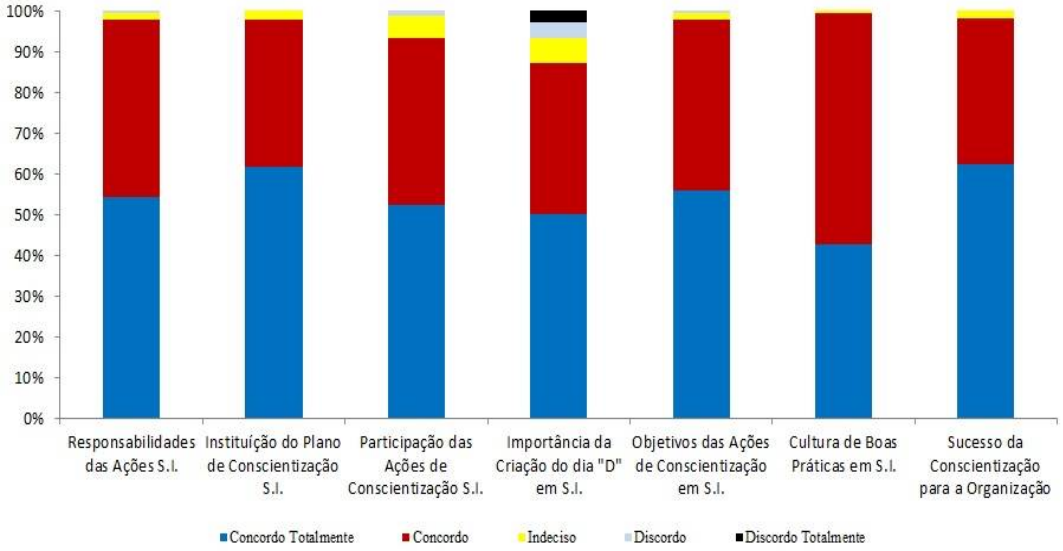
Em relação à pergunta de número 12, afirmando que o objetivo das ações de conscientização em Segurança da Informação é munir as pessoas com informações e experiências, a fim de que elas construam consciência própria e saibam como agir perante a identificação de ameaça, 97,7% concordaram com a afirmação, 1,7% estavam indecisos, e 0,6% discordaram do objetivo das ações de conscientização.

Já na pergunta de número 13, praticamente 100% (99,4%) dos respondentes concordam que a conscientização visa criar uma cultura de boas práticas voltadas à Segurança da Informação no Poder Judiciário do Estado do Tocantins e apenas 0,6% discordaram dessa afirmação.

Finalizando a 2ª dimensão, a pergunta de número 14 afirma que o sucesso de um plano de conscientização em Segurança da Informação só terá efeito se houver políticas e práticas de segurança bem definidas, aparatos tecnológicos capazes de identificar e impedir ataques e principalmente o engajamento de todos os membros da organização, pois uma equipe desta, se conscientizada, educada e engajada na importância da proteção das informações dificilmente sofrerá prejuízos causados por ciberataques. O expressivo resultado dessa afirmação corrobora com o objetivo deste trabalho, em que 98,3% dos respondentes concordaram ou concordaram totalmente com a afirmação e apenas 1,7% ficaram indecisos.

O Gráfico 4 representa de forma ilustrativa as respostas obtidas nas perguntas de números 8 a 14, que correspondem à dimensão 2.

Gráfico 4. Perguntas de 8 a 14 da Dimensão 2 – Conscientização. (Elaborado pelo Autor).



Os resultados em porcentagem exata ao número de respostas em cada categoria da escala *likert*, das perguntas de números 8 a 14 correspondentes à dimensão 2 são confirmadas na Tabela 6 abaixo.

Tabela 6. Perguntas de 8 a 14 da Dimensão 2 – Conscientização. (Elaborada pelo Autor).

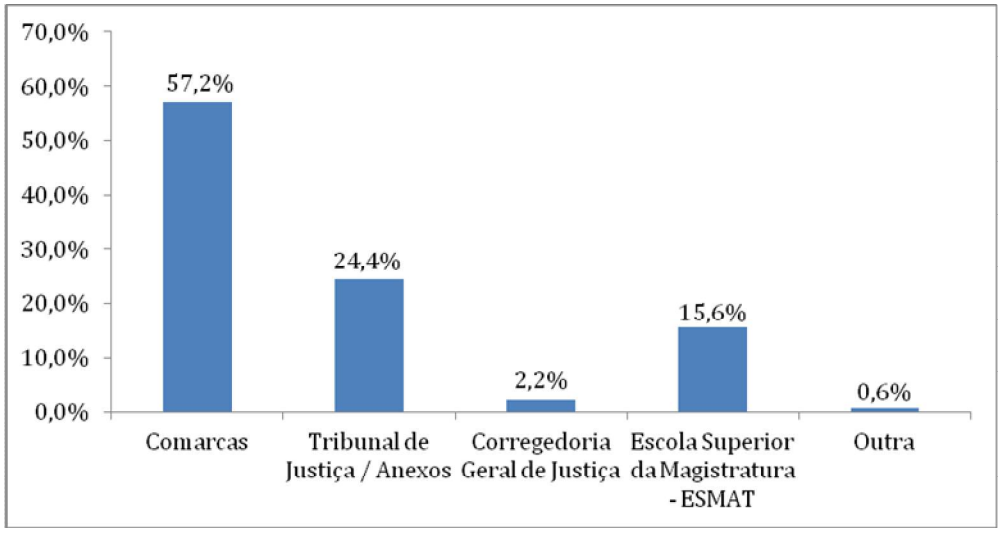
Representações	Concordo Totalmente	Concordo	Indeciso	Discordo	Discordo Totalmente	Total de Respostas
Responsabilidades das Ações S.I.	54,4%	43,3%	1,7%	0,6%	0,0%	100,0%
Instituição do Plano de Conscientização S.I.	61,7%	36,1%	2,2%	0,0%	0,0%	100,0%
Participação das Ações de Conscientização S.I.	52,2%	41,1%	5,6%	1,1%	0,0%	100,0%
Importância da Criação do dia "D" em S.I.	50,0%	37,2%	6,1%	3,9%	2,8%	100,0%
Objetivos das Ações de Conscientização em S.I.	56,1%	41,6%	1,7%	0,6%	0,0%	100,0%
Cultura de Boas Práticas em S.I.	42,8%	56,6%	0,6%	0,0%	0,0%	100,0%
Sucesso da Conscientização para a Organização	62,2%	36,1%	1,7%	0,0%	0,0%	100,0%

5.3.3. Dimensão 3 – Perfil

A Dimensão 3 foi composta por 7 perguntas, com objetivo de coletar informação quanto ao perfil dos respondentes, por meio do fornecimento das seguintes informações: local de ocupação; tempo de serviço; serviços e sistemas que utilizam ou têm acesso; pela escolha de três assuntos para compor as ações iniciais do plano de conscientização; e se já havia participado de algum programa voltado à Segurança da Informação.

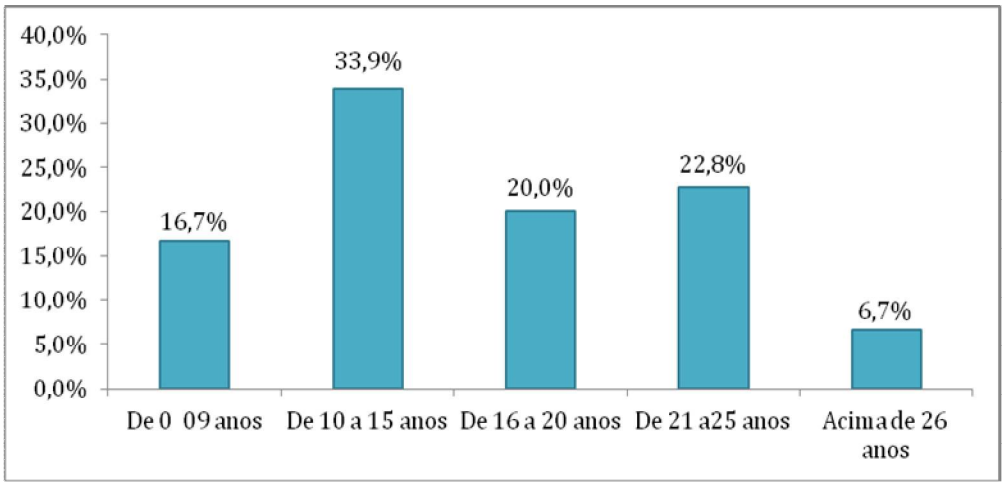
Na pergunta de número 15, foi solicitado ao respondente para informar em qual localidade exerce sua atividade laboral. Assim, conforme representado no Gráfico 5, o maior percentual de respondentes exerce suas atividades nas comarcas do estado do Tocantins, totalizando 57,2% dos respondentes, seguidos por 24,4% no Tribunal de Justiça e Anexos, 15,6% na Escola Superior da Magistratura Tocantinense, 2,2% na Corregedoria Geral de Justiça, e apenas 0,6% exercem suas atividades laborais em outra localidade. Com esse resultado, pode-se afirmar que o instrumento de pesquisa encaminhado às 205 Unidades Organizacionais abrangeu todas as regiões do estado do Tocantins (capital e interior).

Gráfico 5. Dimensão 3 – Local que exerce atividade laboral. (Elaborado pelo Autor).



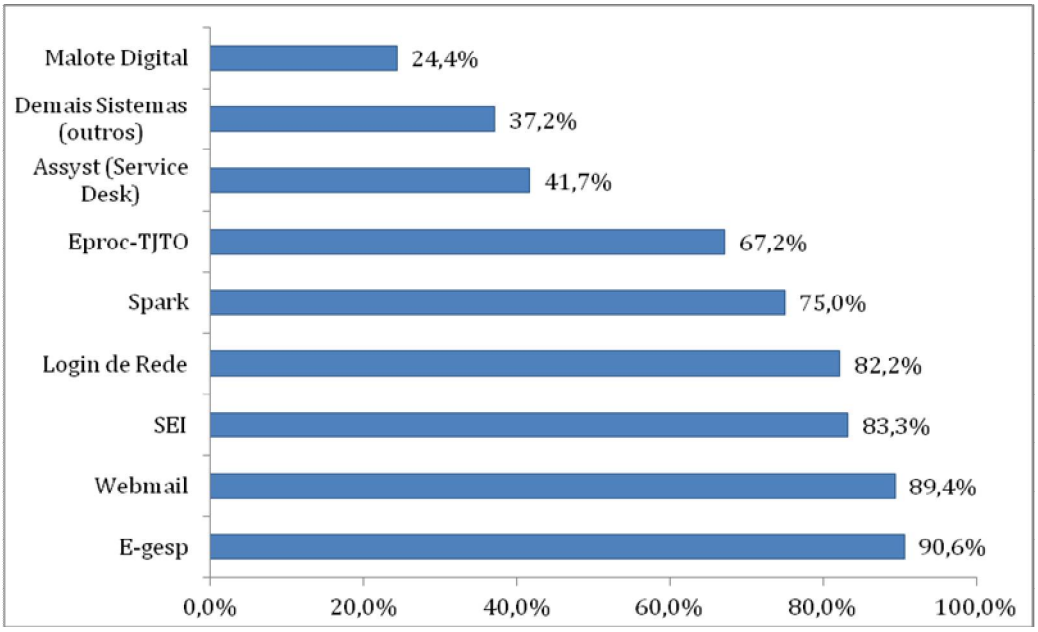
Com o intuito de identificar o tempo em anos em que o respondente exerce suas funções no Poder Judiciário do Tocantins, a pergunta de número 16 demonstrou que os servidores têm tempos aleatórios, e o tempo predominante foi de 10 a 15 anos (33,9%), seguido de 21 anos a 25 anos (22,8%) e de 16 a 20 anos (20%), seguidos 0 a 9 anos (16,7%) e acima de 26 anos (6,7%) de prestação de serviço no PJTO. Os resultados estão representados no Gráfico 6.

Gráfico 6. Dimensão 3 – Tempo de serviço no PJTO. (Elaborado pelo Autor).



Na pergunta de número 17, foi solicitado que o respondente selecionasse quais serviços e sistemas ele utiliza ou tem acesso. Dentre os serviços e sistemas elencados, destacam-se os dois serviços que serão utilizados nas ações de conscientização em Segurança da Informação: *Webmail* e *Spark*. Como representado no Gráfico 7, o *Webmail* é utilizado por 89,4% dos respondentes e o *Spark* por 75%. Esse resultado torna-se muito relevante, pois assegura que as ações de conscientização atinjam um grande número de magistrados e servidores do TJTO.

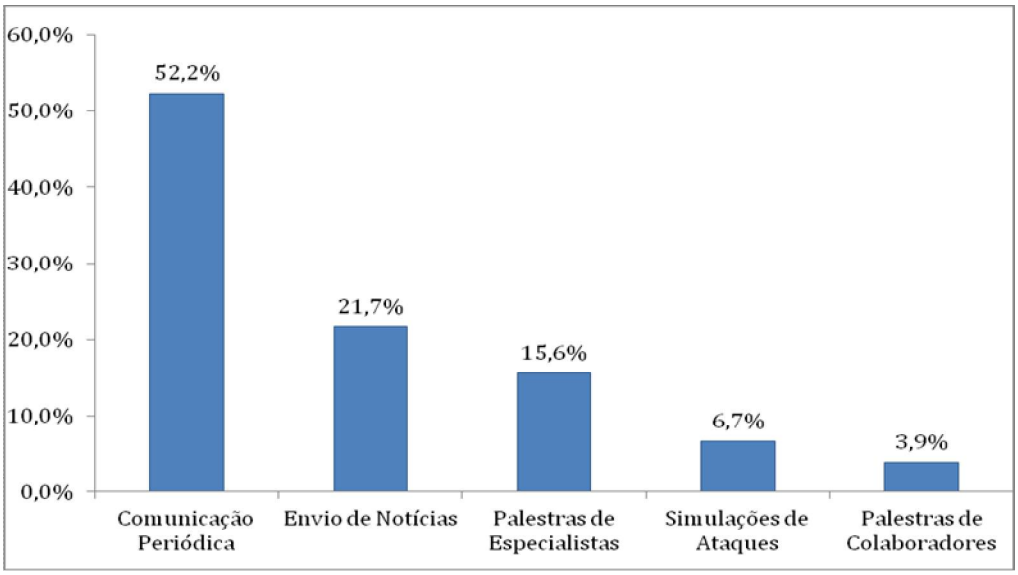
Gráfico 7. Dimensão 3 – Serviços e Sistemas utilizados. (Elaborado pelo Autor).



A pergunta de número 18 almejava saber quais das ações listadas (comunicação periódica, envio de notícias, palestras de especialistas, simulações de ataques e palestras de colaboradores) o respondente acreditava ser a mais efetiva, quando se trata de conscientizar os membros internos do Poder Judiciário do Tocantins. Assim, 52,2% afirmaram que as comunicações periódicas são as ações mais efetivas para conscientizar, seguido por 21,7% que afirmaram que o envio de notícias são as ações mais efetivas, totalizando 73,9% das ações. Esse resultado é satisfatório, pois se levarmos em consideração os dois serviços mais utilizados pelos respondentes registrados na pergunta anterior (*Webmail* e *Spark*), estas duas ações atingiriam uma média de aproximadamente 82% dos respondentes.

Dentre as outras ações listadas, 15,6% dos respondentes informaram as palestras com especialistas, 6,7% simulações de ataques e apenas 3,9% informaram as palestras de colaboradores como sendo as ações mais efetivas para conscientizar os membros internos do Poder Judiciário do Tocantins. O Gráfico 8 representa o resultado da pergunta 18 do instrumento de pesquisa.

Gráfico 8. Dimensão 3 – Ações mais efetivas para conscientização. (Elaborado pelo Autor).



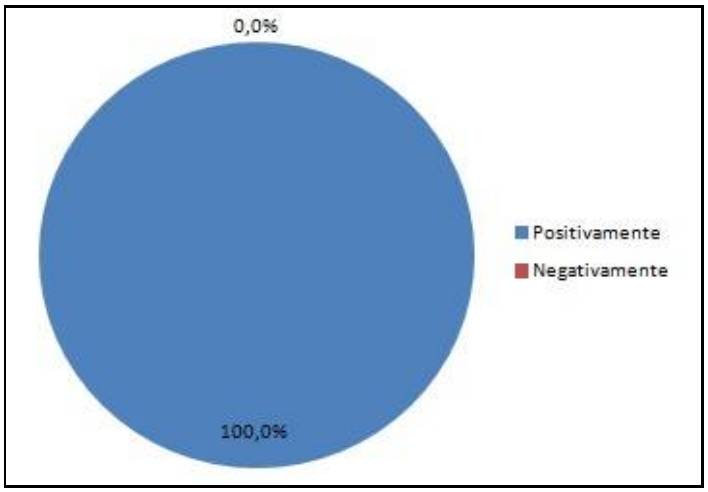
Na pergunta de número 19, observou-se a opinião do respondente quanto ao impacto positivo e negativo que as ações de conscientização voltadas à Segurança da Informação iriam trazer em seu trabalho. Assim os respondentes foram unânimes

(100%) em afirmar que as ações de conscientização irão impactar positivamente em seus trabalhos.

Porém, verificou-se que ao elaborar essa questão, faltou um pequeno detalhe, onde deveríamos ter acrescentado mais possibilidades de respostas para os respondentes, como segue nas seguintes opções: “Não Sei”, e, ou “Estou Indeciso”. Portanto, nós, não podemos afirmar que realmente 100% das pessoas entendam que as ações de conscientização são importantes e que irão impactar positivamente em seu trabalho.

O Gráfico 9 representa o resultado da pergunta 19 do instrumento de pesquisa.

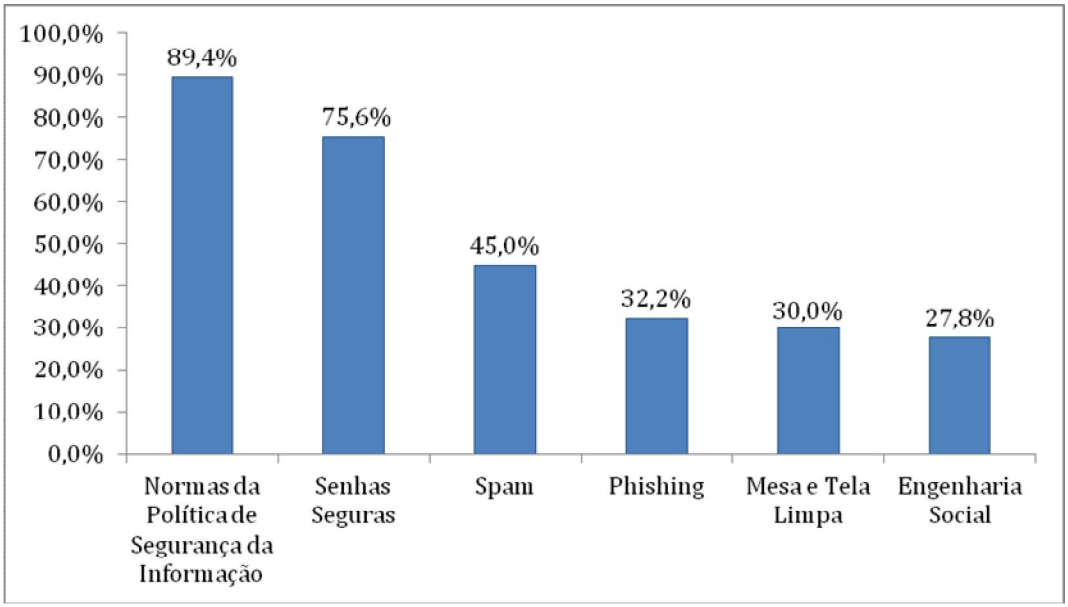
Gráfico 9. Dimensão 3 – Impacto das ações de conscientização. (Elaborado pelo Autor).



A pergunta de número 20 solicitava que o respondente marcasse três assuntos dentre os apresentados (*Phishing*, Mesa e Tela Limpa, Engenharia Social, *Spam*, Senhas Seguras e Normas da Política de Segurança da Informação), que considerava prioritários na composição inicial do plano de conscientização em Segurança da Informação do Tribunal de Justiça do Estado do Tocantins. Conforme apresentado no Gráfico 10, os três assuntos com maior percentual de indicação pelos respondentes para fazerem parte inicial das ações de conscientização foram: as Normas da Política de Segurança da Informação com 89,4%, seguidas pelas Senhas Seguras com 75,6% e *Spam* com 45%. Ressalta-se que todos os assuntos constantes nas alternativas da pergunta de número 20 são extremamente importantes e devem fazer parte das atividades e ações de conscientização em Segurança da Informação do Poder Judiciário do Estado do Tocantins. Nesse sentido, apesar de serem indicados com menor porcentagem os

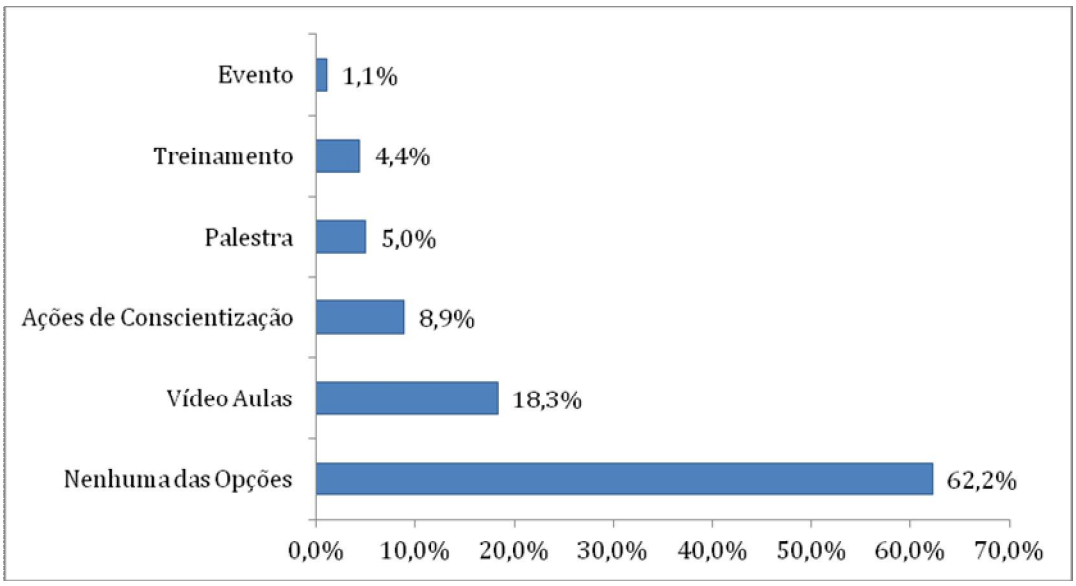
assuntos *phishing*, Mesa e Tela Limpa e Engenharia Social foram apontados com 32,2%, 30% e 27,8%, respectivamente, são assuntos que devem compor a Norma.

Gráfico 10. Dimensão 3 – Assuntos prioritários para o plano de conscientização em Segurança da Informação do PJTO. (Elaborado pelo Autor).



Por fim, a pergunta de número 21 da dimensão 3 solicitava que o respondente indicasse em qual dos programas voltados à Segurança da Informação já tenha participado (Treinamento, Palestra, Evento, Videoaulas e Ações de Conscientização ou Nenhuma das Opções). O resultado apresentado fortalece ainda mais o presente estudo, sendo que 62,2% dos respondentes ainda não participaram de nenhum dos programas informados. Outro dado importante foi que 18,3% informaram já terem participado por meio de videoaulas; essa informação torna-se valiosa, pois é mais uma alternativa que pode ser adotada como meio de realização das atividades e ações de conscientização. De outro modo, apenas 8,9% dos respondentes já participaram de ações de conscientização; seguidos de 5% que participaram de palestras; 4,4%, de treinamento; e apenas 1,1% de eventos voltados à Segurança da Informação. Os dados estão representados no Gráfico 11, abaixo.

Gráfico 11. Dimensão 3 – Programa de Segurança da Informação que tenha participado. (Elaborado pelo Autor).



Ao analisar as três dimensões que compõem o instrumento de pesquisa, pode-se concluir que, no tocante à dimensão 1, temos os seguintes temas que poderão fazer parte das ações de conscientização:

- Criando e memorizando senhas complexas;
- Técnicas para identificar falsos e-mails;
- Normas da Política de Segurança da Informação do PJTO.

Na dimensão 2, foi possível identificar que, para a grande maioria dos respondentes, o usuário é responsável por suas ações no que tange à Segurança da Informação. Fica também evidenciado que os respondentes estão dispostos a participar das atividades e ações de conscientização.

Por fim, com os resultados da dimensão 3, foi possível verificar que o instrumento de pesquisa encaminhado às 205 Unidades Organizacionais abrangeu todas as regiões do estado do Tocantins (capital e interior), sendo que todos os respondentes acreditam que as ações de conscientização irão impactar positivamente em seu trabalho. Ainda foi possível identificar que mais de 62% dos respondentes ainda não participaram de nenhum programa voltado à Segurança da Informação; contudo, mais de 73% acreditam que as mensagens periódicas e o envio de notícias são as ações mais efetivas, quando se trata de conscientizar os membros internos do Poder Judiciário do Tocantins. Ainda

nessa dimensão, foi possível identificar, por meio dos resultados, que os três assuntos mais relevantes que poderão fazer parte das ações de conscientização são:

- Normas da Política de Segurança da Informação do PJTO;
- Senhas Seguras;
- *Spam*.

Diante dos resultados apresentados por este estudo de caso, fica evidenciada a necessidade de implementação do Plano de Conscientização em Segurança da Informação no âmbito do Poder Judiciário do Tocantins.

6. CONCLUSÕES

Manter em segurança seus ativos e suas informações tornou-se um grande desafio para as organizações, uma vez que as ameaças e vulnerabilidades existentes colocam em risco a continuidade dos negócios. O Poder Judiciário do Tocantins, há alguns anos vem trabalhando com seus processos jurídicos e administrativos 100% eletrônicos, tornando assim relevante que sejam implantadas atividades e ações voltadas à Segurança da Informação para magistrados e servidores.

Nesse contexto, este estudo foi desenvolvido com o ojetivo de responder ao seguinte problema de pesquisa: Como elaborar um plano para instruir a conscientização da Política de Segurança da Informação e assuntos relacionados à Segurança da Informação para magistrados e servidores do Poder Judiciário do Tocantins? Para obtençao da resposta, foi realizada uma pesquisa quantitativo-exploratória com Levantamento Bibliográfico, Documental e Estudo de Caso.

Com base na pesquisa realizada, foram construídos e apresentados os seguintes artefatos:

- **Norma-TIC-09 – Proposta da Minuta para o Plano de Conscientização:** Por meio de uma Minuta, a proposta tem como objetivo normatizar e institucionalizar o Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins. A Minuta é composta por vocabulários, conceitos e a Norma TIC-09, a serem inseridas na Política de Segurança da Informação do TJTO. A Norma TIC-09 define a sistematização e as responsabilidades na execução de cada processo do plano de conscientização, sendo apresentada em quatro grandes eixos: Disposições Iniciais; Sistematização do Plano de Conscientização em Segurança da Informação; Responsabilidades; e Disposições Finais.

- **Fluxo do Processo de Conscientização**: Visa à execução do Plano de Conscientização em Segurança da Informação, sendo composto por 17 processos, distribuídos entre 6 Unidades. O fluxo do processo tem por objetivo a organização sequencial, a padronização do plano, melhorar a comunicação entre as áreas envolvidas e minimizar retrabalhos.

- **Formulário para o Plano de Conscientização:** Será utilizado para levantar as necessidades, indicação e detalhamentos dos assuntos que irão compor o Plano de Conscientização em Segurança da Informação. O formulário é composto por três seções, sendo que a seção 1 trata da indicação dos assuntos para o plano de atividades e ações. A indicação deve ser feita no respectivo anexo I. Já a seção 2 aborda os detalhamentos dos assuntos indicados, os quais devem ser preenchidos no respectivo anexo II. Por fim, a seção 3 trata da apreciação das informações contidas nas seções anteriores pelo Comitê Gestor de TIC. Sendo aprovado o formulário, este será encaminhado para editoração e diagramação dos assuntos propostos.

- **Termo de Ciência da PSI:** O Termo de Ciência da PSI com as informações como: *link* de disponibilidade da PSI e contatos para dúvidas e reportes de possíveis incidentes de Segurança da Informação, para serem entregues aos novos magistrados e servidores no ato de posse. O documento tem por objetivo de que os novos membros do PJTO, desde o ato de posse, já tenham conhecimento da existência da PSI e se comprometam a realizar o acesso e leitura desta.

- **Instrumento de Coleta de Dados – Questionário:** Por meio de um questionário eletrônico, a amostra foi encaminhada para 205 Unidades Organizacionais do PJTO, sendo obtidas 180 respostas, com resultados muito satisfatórios em porcentagem de 87,80% de respostas. O instrumento de pesquisa foi composto por 21 perguntas, todas fechadas, e dividido em três dimensões: A primeira foi composta por perguntas relacionadas ao comportamento do respondente mediante a Segurança da Informação, com o propósito de identificar os possíveis comportamentos inadequados dos respondentes sobre o tema. A segunda abordou perguntas pertinentes à concordância da implantação do plano de ações de conscientização em Segurança da Informação, bem como o interesse de participação do respondente, com vista à busca pela cultura de boas práticas em Segurança da Informação no Poder Judiciário do Tocantins. A terceira e última dimensão, por sua vez, teve como objetivo identificar o local de ocupação dos servidores lotados nas repartições para onde foram encaminhados os instrumentos, bem como o tempo de serviço e os serviços e sistemas que

> utilizam ou têm acesso. Nessa dimensão, também consta a escolha de três assuntos, para possíveis prioridades na composição inicial do plano de conscientização em Segurança da Informação no Tribunal de Justiça do Estado do Tocantins, além de identificar o local de ocupação, tempo de serviço, serviços e sistemas que utilizam ou têm acesso, escolha de três assuntos, bem como se já havia participado de ações relacionadas à Segurança da Informação.

Nesse contexo, entende-se que o primeiro objetivo específico proposto para este trabalho foi atingido, uma vez que foi possivel pelas pesquisas realizadas analisar os principais artigos, teses, livros, instruções normativas, resoluções, decretos, normas técnicas, dentre outras publicações relacionadas à Segurança da Informação, que embasaram a construção da proposta de Minuta e dos artefatos que compõem este trabalho.

As principais contribuições deste trabalho estão relacionadas ao segundo e ao terceiro objetivo específico. O segundo objetivo específico foi atingido por meio da definição e construção da Norma TIC-09, composta pela Proposta da Minuta do Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins. Já o terceiro objetivo específico que trata da elaboração dos artefatos que compõem a proposta do plano de conscientização foi concluído por meio da elaboração do Fluxo do Processo de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins, composto por 17 processos, sendo distribuídos entre 6 unidades; do Formulário para o plano de conscientização, documento este específico que tramitará entre as unidades envolvidas para indicação, detalhamentos e aprovação dos assuntos e conteúdos das atividades e ações de conscientização; e, por fim, a elaboração do Termo de Ciência da PSI do Poder Judiciário do Tocantins a ser entregue para magistrados e servidores em ato de posse.

Na mesma linha de contribuiçao, vale destacar o resultado obtido por meio do questionário, ficando evidenciada a necessidade de se implantarem ações de conscientização em Segurança da Informação no PJTO. Destaca-se também o resultado positivo quanto à intenção de magistrados e servidores em participarem das ações de conscientização.

Dessa forma, considera-se que esta pesquisa foi concluída de forma satisfatória, uma vez que o problema de pesquisa sugerido foi respondido adequadamente, e o

objetivo geral e os objetivos específicos propostos foram atingidos por meio dos levantamentos bibliográficos e elaboração da Norma TIC-09 e dos artefatos produzidos.

Assim, os resultados desta pesquisa, demonstraram-se viável a implantação do plano de conscientização em Segurança da Informação no PJTO, o qual possibilitará minimizar a incidência de ameaças a SI; divulgar as Normas da PSI e contribuir com as mudanças de hábitos, criando uma cultura de boas práticas voltada à Segurança da Informação no âmbito do Poder Judiciário do Tocantins.

Trabalhos Futuros

Esta pesquisa não encerra esta discussão, pelo contrário, essa temática precisa de mais compreensão e participação, de modo a gerar considerações consistentes a esse assunto tão presente e significativo.

Como pontos de trabalhos futuros podem ser considerados os seguintes assuntos:

- Assim, pretente-se submeter à Norma TIC-09 proposta da Minuta do Plano de Conscientização em Seguraça da Informação ao Comitê Gestor de Segurança da Informação para conhecimento, aprovação e publicação;
- Pretende-se, ainda, apoiar, acompanhar e mensurar as atividades e ações voltadas à conscientização em Segurança da Informação a serem realizadas pelos meios de comunicação existentes no PJTO;
- Acompanhar magistrados e servidores que realizaram as atividades e ações de conscientização em Segurança da Informação de modo a avaliar se houve, ou não, mudança de comportamento, e se essas mudanças estão contribuindo para disseminar a cultura voltada às boas práticas de Segurança da Informação, no PJTO;
- Realizar um estudo de caso no âmbito dos Tribunais de Justiça Estaduais para análise, relacionamentos e discussão das origens dos incidentes de Segurança da Informação;
- Apresentar um levantamento e discussão acerca da possibilidade de implantação do plano de conscientização em Segurança da Informação para os demais órgãos e instituições do Estado do Tocantins.

Os assuntos apresentados acima em forma de sugestão, visam aprofundar ainda mais o conhecimento na área de Segurança da Informação, como também fomentar a

conscientização dos usuários de orgãos e instituições do Estado do Tocantins, com o objetivo de disseminar a cultura de boas práticas relacionada à Segurança da Informação.

REFERÊNCIAS BIBLIOGRÁFICAS

ABNT NBR ISO/IEC 17799. **Tecnologia da Informação – Código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2005.

ABNT NBR ISO/IEC 27001. T**ecnologia da Informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos**. Rio de Janeiro, 2006.

ABNT NBR ISO/IEC 27001. **Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação — Requisitos,** 2ª Edição, 2013.

ABNT NBR ISO/IEC 27002: T**ecnologia da informação: técnicas de segurança: código de prática para a gestão da segurança da informação**. Rio de Janeiro, 2013.

ABNT. (2011) Associação Brasileira de Normas Técnicas. NBR 27005:2011: **Tecnologia da Informação - Técnicas de Segurança – Gestão de Riscos de Segurança da Informação**. Rio de Janeiro.

ALENCAR, Gliner Dias; QUEIROZ, Anderson A.L.; DE QUEIROZ, R. J. G. B. **Insiders: Um Fator Ativo na Segurança da Informação**. IX Simpósio Brasileiro de Sistemas de Informação (SBSI 2013), p. 61-72, 2013.

ALEXANDRIA, João Carlos Soares de. **Gestão de segurança da informação - uma proposta para potencializar a efetividade da segurança da informação em ambiente de pesquisa científica**. 2009. Tese (Doutorado em Tecnologia Nuclear - Aplicações) - Instituto de Pesquisas Energéticas e Nucleares, Universidade de São Paulo, São Paulo, 2009. doi:10.11606/T.85.2009.tde-22092011-095831. Acesso em: 2020-04-01.

ARAÚJO, L. G. S; BEZERRA, E. K; COELHO, F. E. S. **Gestão da Segurança da Informação**. Rio de Janeiro: RNP/ESR, 2014.

ARAÚJO, M. T.; FERREIRA, F. N. F.**; Política de segurança da informação: guia prático para a elaboração e implementação**. Rio de Janeiro: Ciência Moderna, 2008.

BEAL, Adriana. **Segurança da Informação: princípios e melhores práticas para a proteção dos ativos de informação nas organizações**. São Paulo: Atlas, 2008.

Bezerra, Edson Kowask. **Gestão de Riscos de TI: NBR 27005**. Rio de Janeiro: RNP/ESR. 2013. 138 p.;28 cm.

CAMPOS, André. **Sistema de Segurança da informação: controlando os riscos**. 2. Ed. Florianópolis: Visual Books, 2007.

DZAZALI, Suhazimah; ZOLAIT, Ali Hussein. **Assessment of information security maturity: An exploration study of Malaysian public servisse organizations**. Journal of Systems and Information Technology. v. 14 No. 1, p. 23-57, 2012.

FERREIRA, Fernando Nicolau Freitas. **Segurança da Informação**. Rio de Janeiro: Ciência Moderna, 2003.

FERREIRA, J. O. **Análise sob a ótica da segurança em sistemas de informação: estudo de caso aplicado ao Sistema de Concessão de Diárias e Passagens (SCDP) no Departamento Contábil da UFPB** / Ferreira. Dissertação de Mestrado em Ciência da Informação - João Pessoa, 2013.

FONTES, E. **Políticas e normas para a segurança da informação**. Rio de Janeiro: Brasport, 2012.

FONTES, Edison. **Segurança da Informação: o usuário faz a diferença**. São Paulo: Saraiva, 2015.

GIL, A. C. **Como elaborar projetos de pesquisa**. 5 ed. São Paulo: Atlas, 2010.

KERMACK, W. O. y MCKENDRICK, A.G. (1927). **Contributions to the Mathematical Theory of Epidemics THE ROYAL SOCIETY. Proceedings of the Royal Society of London A: mathematical, physical and engineering sciences**. [S.l.], 1927. v. 115, n. 772, p. 700–721.

KIM, David; SOLOMON, Michael G. **Fundamentos de segurança de sistemas de informação**. Tradução por Daniel Vieira. Rio de Janeiro: LTC, 2014.

LAKATOS, M.E; MARCONI, M. A. **Metodologia Científica**. 7ª. ed. São Paulo: Atlas, 2017.

LIMA, F. J. **Estudo de Melhorias em Segurança de Informação. Monografia de Pós-Graduação (Especialização) em Configuração e Gerenciamento de Servidores e Equipamentos de Rede**, Universidade Tecnológica Federal do Paraná, Curitiba, 2013.

MITNICK, K. D.; SIMON, W. L. A. **A arte de enganar**: ataque de hackers, controlando o fator humano na segurança da informação. São Paulo: Pearson Education do Brasil, 2003.

MOREIRA, Nilton Stringasci. **Segurança mínima: uma visão corporativa da segurança de informações**. Rio de Janeiro: Axcel Books, 2001.

NASCIMENTO, Janilson Pereira do. **Segurança em Redes de Computadores: "Uma Abordagem sobre o Comprometimento Individual em Benefício da Corporação**". Tecnologias em Projeção, v. 6, n. 1, p. 01-06, 2015.

NIST - National Institute of Standards and Technology - SPECIAL PUBLICATION 800-16. **Computer Security- Information Technology Security Training Requirements: A Role-and Performance-Based Model**, version 1.0, 1998.

OLIVEIRA, G. D. DE; MOURA, R. K. G. DE; ARAÚJO, F. DE A. N. G. DE. **Gestão da Segurança da Informação: Perspectivas Baseadas na Tecnologia da Informação (T.I.)**. Múltiplos Olhares em Ciência da Informação, v. 3, n. 2, 29 maio 2014.

OLIVEIRA, M. S. et al. **Aplicação das Normas ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 em uma média empresa**. Revista Eletrônica de Sistemas de Informação e Gestão Tecnológica. Vol. 06, Nr. 02, p. 37-49, 2015.

Parsons, Kathryn & Young, Elise & Butavicius, Marcus & McCormac, Agata & Pattinson, Malcolm & Jerram, Cate. (2015). **The Influence of Organizational Information Security Culture on Information Security Decision Making**. Journal of Cognitive Engineering and Decision Making. 9. 117-129. 10.1177/1555343415575152.

PINHEIRO, Patricia Peck. **Direito Digital**. 3. Ed. São Paulo: Saraiva, 2009.

PWC. Price Waterhouse Coopers**. Pesquisa Global de Segurança da Informação 2018** - PwC. São Paulo. 2018.

PWC. Price Waterhouse Coopers**. Pesquisa Global de Segurança da Informação 2014** - PwC. São Paulo. 2014.

RAMOS, Anderson; **Conscientização em Segurança da Informação como processo**. In: CABRAL, Carlos (Org.); CAPRINO, Willian (Org.). Trilhas em Segurança da Informação: Caminhos e ideias para a proteção de dados. Rio de Janeiro: Brasport, 2015. p. 39-57.

ROCHA, P. C. C. **Segurança da informação: uma questão não apenas tecnologia**. 2008. Trabalho de Conclusão de Curso (Especialização) – Departamento de Ciência da Computação, Universidade de Brasília, Brasília, 2008.

SÊMOLA, M. **Gestão da Segurança da Informação - Uma Visão Executiva** – 2. ed. São Paulo: Elsevier, 2014.

SÊMOLA, Marcos. **Gestão da Segurança da Informação: uma visão executiva** - Rio de Janeiro: Campus, 2004.

SÊMOLA, Marcos. **Gestão de Segurança da Informação**. Rio de Janeiro: Campus, 2003.

SILVA, A. E. N. da**. Segurança da informação – vazamento de informações – as informações estão realmente seguras em sua empresa?** Rio de Janeiro: Editora Ciência Moderna Ltda, 2012.

SILVA, E. L. DA; MENEZES. E.M. **Metodologia da Pesquisa e Elaboração de Dissertação**. UFSC, 4. Ed. Ver. Atual. Florianópolis 2005.

SILVA, E. L; MENEZES, M. E. **Metodologia da pesquisa e elaboração de dissertação.** Florianópolis: UFSC, 4. Ed. 2005.

WASLAWICK, Raul Sidnei. **Metodologia de Pesquisa para ciência da computação**. 2. Ed. Rio de Janeiro: Elsevier, 2014.

Referências Consultadas

Cert.br. **Cartilha de Segurança para Internet**. Disponível em: https://cartilha.cert.br/. Acesso em: 29 jul. 2019.

CNJ. (2015) Conselho Nacional de Justiça. **Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD)**. 2015. Disponível em: http://www.cnj.jus.br/atos-normativos?documento=2227. Acesso em: 29 jul. 2019.

CNJ. (2015) Conselho Nacional de Justiça. Resolução n. 211, de 15 de dez. de 2015. **Dispõe sobre a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário**. Disponível em: http://www.cnj.jus.br///images/atos_normativos/resolucao/resolucao_211_15122015_18122015173345.pdf . Acesso em: 13 out. 2018.

Cybersecurity Ventures. **Relatório Cybercrime 2017**. Disponível em: https://1c7fab3im83f5gqiow2qqs2k-wpengine.netdna-ssl.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf. Acesso em: 10 nov. 2019.

FOINA, Paulo Rogério. **ESTRATÉGIA E SEGURANÇA DE INFORMAÇÃO**. In: LYRA, Mauricio Rocha (Org.). Governança da Segurança da Informação. Brasília: Edição do Autor, 2015. p. 1-7. Disponível em: http://mauriciolyra.pro.br/site/wp-content/uploads/2016/02/Livro-Completo-v4-para-impress%C3%A3o-com-ISBN.pdf. Acesso em: 03 fev. 2020.

Gartner Group, 2019. **Quadrante Mágico para Treinamento de Conscientização em Segurança por Computador**. ID G00 378818. Disponível em: https://www.gartner.com/doc/reprints?id=1-1OAZDU37&ct=190723&st=sb. Acesso em: 08 dez. 2019.

GRIFFIN, Dan; Network **Security: The Four Pillars of Endpoint Security**. 2018. Disponível em: https://technet.microsoft.com/en-us/library/gg213837.aspx. Acesso em: 28 jun. 2019.

High Security Center – HSC. **Por que ter um plano de conscientização em segurança da informação?** 2018. Disponível em: https://www.hscbrasil.com.br/plano-de-conscientizacao-em-seguranca-da-informacao/. Acesso em: 20 abr. 2020.

NORTON. 2017 **Relatórios do Norton Cyber Security Insights** - Resultados Globais. Disponível em: https://www.symantec.com/content/dam/symantec/docs/about/2017-ncsir-global-results-en.pdf. Acesso em: 02 nov. 2019.

RNP. Rede Nacional de Ensino e Pesquisa - **Mês da Segurança**. Disponível em: http://meseg.rnp.br/. Acesso em: 29 jul. 2018.

SANTOS, Rodrigo Costa dos; SANTOS, Manuela Fernandes dos; CARREIRA, Fernando Spencer. **Campanha de Conscientização em Segurança da Informação**: **Um Estudo de Caso**. XII Simpósio de Excelência em Gestão e Tecnologia. Associação Educacional Dom Bosco. 2014. Disponível em: < http://www.aedb.br/seget/arquivos/artigos16/382440.pdf. Acesso em: 15 out. 2019.

Software Advice, **Golpes de phishing: por que os funcionários clicam e o que fazer sobre isso Industry View** | 2015. Disponivel em: https://www.softwareadvice.com/security/industryview/phishing-scams-report-2015/. Acesso em: 12 nov. 2019.

TJTO, **Política de Segurança da Informação (PSI), no âmbito do Poder Judiciário do Estado do Tocantins e dá outras providências.** 2017. Disponível em http://www.tjto.jus.br/images/tic/PORTARIA_PSI.pdf. Acesso em: 23 jul. 2018.

TJTO - Tribunal de Justiça do Tocantins (2017). Portaria n. 3433, de 26 de jun. de 2017. **Dispõe sobre a Política de Segurança da Informação (PSI).** Disponível em: http://www.tjto.jus.br/tic/index.php/governanca-de-tic/documentos-normativos/send/98-normativas/1147-politica-de-seguranca-da-informacao. Acesso em: 15 jul. 2018.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas Práticas em Segurança da Informação**. 4ª Edição, 2012. Disponível em: https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24D6E86A4014D72AC823F5491&inline=1. Acesso em: 25 out. 2019.

WANDERLEY, Danillo Lustosa; BATELLO, João Carlos Vilela; BARRETO, Marcelo Leal de Araújo; BARBOSA, Gentil Veloso. **Mapping of information technology risks in the Judiciary Tocantinense. International Journal of Development Research**, Vol. 09, Issue 09, pp. 29633-29639, September 2019. Disponível em: http://www.journalijdr.com/sites/default/files/issue-pdf/16815.pdf. Acesso em: 18 out. 2019.

WANDERLEY, Danillo Lustosa; BATELLO, João Carlos Vilela; PRATA, David Nadler; BARBOSA, Gentil Veloso. **Um Estudo Sobre a Epidemia de Vírus Computacionais no Poder Judiciário do Tocantins**. Revista Cereus, v. 10, n. 4, p. 182-197, 2018. Disponível em: http://www.ojs.unirg.edu.br/index.php/1/article/view/2392/740. Acesso em: 18 mar. 2019.

APÊNDICES

APÊNDICE A – Artigos Publicados

1. Um Estudo Sobre a Epidemia de Vírus Computacionais no Poder Judiciário do Tocantins

A Study on the Computer Virus Epidemic in the Judicial Power of Tocantins

Danillo Lustosa Wanderley 1, João Carlos Vilela Batello 2, Davi d Nadler Prata 3, Gentil Veloso Barbosa 4
1,2,3,4 UFT – Universidade Federal do Tocantins

http://ojs.unirg.edu.br/index.php/1/article/view/2392
DOI: 10.18605/2175-7275/cereus.v10n4p182-197

2. Mapping of Information Technology Risks in the Judiciary Tocantinense

Mapeamento de Riscos de Tecnologia da Informação no Judiciário Tocantinense

[1,2]Danillo Lustosa Wanderley, [1,2]João Carlos Vilela Batello, [1,2]Marcelo Leal de Araújo Barreto and [1]Gentil Veloso Barbosa
[1]UFT – Universidade Federal do Tocantins, Brazil
[2]TJTO – Tribunal de Justiça do Estado do Tocantins, Brazil

https://www.journalijdr.com/mapping-information-technology-risks-judiciary-tocantinense
Vol. 09, Issue, 09, pp. 29633-29639, September, 2019.

APÊNDICE B - Norma TIC-09 – Proposta da Minuta do Plano de Conscientização em SI no PJTO

Minuta

O novo conceito deve fazer parte do **MANUAL DE ORGANIZAÇÃO DE CONCEITOS, Anexo I da Portaria nº 3.433**, de 26 de junho de 2017:

1.1. Conscientização em Segurança da Informação: Atividade que tem por finalidade orientar sobre o que é a Segurança da Informação, levando os participantes a obterem um nível adequado de conhecimento sobre o tema, além de um senso apropriado de responsabilidade. O objetivo dessa atividade é proteger o ativo de informações do órgão ou entidade para garantir a continuidade dos negócios, minimizar os danos e reduzir eventuais prejuízos financeiros;

1.2. Plano: Um plano é uma intenção ou um projeto que, por meio de um modelo sistemático, elabora as ações antes de colocar em execução, com o objetivo de trilhar o percurso a ser seguido;

1.3. Elo mais Fraco: Considera-se que as pessoas sejam o elo mais fraco da Segurança da Informação, porque as próprias deficiências naturais do ser humano podem ser exploradas muito mais facilmente que as de um *software*; os engenheiros sociais, sabendo dessa deficiência, exploram as vulnerabilidades humanas para extrair a informação de que necessitam;

1.4. Ciclo PDCA: Método interativo de gestão com quatro etapas, utilizado para o controle e melhoria contínua de processos e produtos. **P**: Planejar (Plan); **D**: Executar (Do); **C**: Checar (Check); **A**: Agir (Action);

1.5. Phishing: Tipo de fraude por meio do envio de mensagens eletrônicas. Um golpista tenta obter dados pessoais e financeiros de um usuário por meio destas, combinando meios técnicos e engenharia social;

1.6. Estrutura Analítica: Tipo de diagrama sistematizado que auxilia a compreensão e a solução de problemas de maneira simples e objetiva;

1.7. Fluxo do Processo: É a agregação de subprocessos e respectivas orquestrações de atividades funcionais num fluxo que mostra o movimento e a ordem em que são executados.

1.8. Ciberataques: É a tentativa de invadir sistemas e computadores para se apoderar de determinadas informações, por meio do uso de criptografia – técnica que transforma informação inteligível em algo que um agente externo seja incapaz de compreender – para capturar dados e fazer com que as empresas tenham de pagar para tê-las de volta. Geralmente, o ciberataque vem associado a um objetivo financeiro, mas também pode ser utilizado apenas para apagar informações existentes.

1.9. Cibersegurança: É a prática que protege computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados de ataques maliciosos. Também chamada de Segurança de Tecnologia da Informação ou Segurança de Informações Eletrônicas. O termo é muito abrangente e se aplica a tudo o que se refere à segurança de computadores, recuperação de desastres e conscientização do usuário final.

1.10. Cultura em Segurança da Informação: Conjunto de valores, de crenças e de conhecimentos existentes em uma organização que leva, direciona e guia as pessoas para laborarem suas atividades de uma forma segura.

2. Acrescentar o capítulo sobre Plano de Conscientização em Segurança da Informação nas disposições finais da PSI e acrescentar a Norma TIC-09.

PLANO DE CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Art. 9. O Poder Judiciário do Tocantins deve adotar um processo que permite identificar as necessidades e implementar um plano de conscientização, divulgação das normas instituídas na Política da Segurança da Informação, e de assuntos voltados a esta, possibilitando incentivar a cultura e as boas praticas em Segurança da Informação para magistrados e servidores.

9. **Norma-TIC-09**: Conscientização em Segurança da Informação: regras de segurança para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação do Poder Judiciário do Tocantins.

9.1. Disposições Iniciais

9.1.1. 9.1.1. O Plano de Conscientização em Segurança da Informação tem como objetivo a divulgação das normas instituídas na Política da Segurança da Informação e de assuntos voltados à Segurança da Informação para magistrados e servidores do Poder Judiciário Tocantinense;

9.1.2. O Plano de Conscientização deve ser implementado no âmbito do Poder Judiciário do Tocantins, visando incentivar a cultura de boas práticas em Segurança da Informação por meio de ações de conscientização;

9.1.3. As Unidades da Diretoria de Tecnologia da Informação deverão indicar e detalhar os assuntos a serem encaminhados para as ações de conscientização;

9.1.4. O Comitê Gestor de Tecnologia da Informação e Comunicação ficará responsável por validar os assuntos e seus conteúdos, validar a diagramação e editoração das matérias e, por fim, validar os registros e *logs*;

9.1.5. O Comitê Gestor de Segurança da Informação será o responsável por coordenar as atividades e as ações de conscientização, validando os assuntos e conteúdos e posteriormente cientificando e divulgando os resultados obtidos;

9.1.6. A Diretoria de Comunicação Social será responsável pelas diagramações e editoração dos materiais, como também responsável pela divulgação das ações de conscientização, e, por fim, ser responsável pelas coletas dos registros e *logs*;

9.1.7. A Diretoria de Gestão de Pessoas deverá ser responsável pela divulgação das Normas contidas na Política de Segurança da Informação para os novos magistrados e servidores por meio do Termo de Ciência;

9.1.8. A Coordenadoria de Gestão Estratégica deverá ser responsável pela tabulação dos indicadores do Macroprocesso de Segurança da Informação;

9.1.9. Os Gabinetes e demais Diretorias, Setores e Comarcas deverão participar das atividades e ações de conscientização, como também conhecer e respeitar as normas existentes na Política de Segurança da Informação, ficando estes e aos demais responsáveis por comunicar a Diretoria de Tecnologia da Informação qualquer incidente de Segurança da Informação.

9.2. Sistematização do Plano de Conscientização em Segurança da Informação

9.2.1. O Plano de Conscientização em Segurança da Informação é composto por 17 processos e foi estruturado nas seguintes etapas:

9.2.1.1. **Planejamento:** Considerando a etapa inicial do fluxo do processo, esta etapa é constituída de 9 processos, que visa à identificação das necessidades, elaboração dos assuntos e conteúdos, editoração e diagramação. É responsabilidade de o Comitê Gestor de Tecnologia da Informação e Comunicação e de o Comitê Gestor de Segurança da Informação coordenarem e validarem todas as ações dessa etapa, antes que o processo passe para a etapa de execução;

9.2.1.2. **Execução:** Fazem parte desta etapa 4 processos contemplando a realização das divulgações das atividades e ações de conscientização pelos meios de comunicações existentes. È nesta etapa que serão divulgadas as normas da Política de Segurança da Informação para os novos magistrados e servidores. Esta etapa de execução visa, ainda, contemplar que todos os magistrados e servidores participem das atividades e ações de conscientização, conheçam e respeitem as normas existentes na Política de Segurança da Informação;

9.2.1.3. **Registros:** Esta etapa visa identificar a participação dos magistrados e servidores nas atividades e ações de conscientização, por meio dos registros ou *logs* coletados das ferramentas de divulgação. Esta etapa possui apenas 2 processos;

9.2.1.4. **Validar**: Etapa possui apenas 1 processo, cuja função é validar e tabular os registros e *logs*;

9.2.1.5. **Resultados:** Considera-se a etapa final do fluxo do processo cujo objetivo é cientificar e divulgar os resultados das ações de conscientização em Segurança da Informação no Poder Judiciário do Tocantins, para serem tabulados nos indicadores do macroprocesso de Gestão de Segurança da Informação, com vista ao acompanhamento dos resultados e melhoria contínua.

9.3. Responsabilidades

9.3.1. Integram a estrutura do Plano de Conscientização em Segurança da Informação do Poder Judiciário do Tocantins:

9.3.1.1. Unidades da Diretoria de Tecnologia da Informação;

9.3.1.2. Comitê Gestor de Tecnologia da Informação e Comunicação;

9.3.1.3. Comitê Gestor de Segurança da Informação;

9.3.1.4. Diretoria de Comunicação Social;

9.3.1.5. Diretoria de Gestão de Pessoas;

9.3.1.6. Gabinetes, demais Diretorias, Setores e Comarcas do PJTO;

9.3.2. São responsabilidades das Unidades da Diretoria de Tecnologia da Informação:

9.3.2.1. Identificar as necessidades;

9.3.2.1. Elaborar e detalhar os assuntos e conteúdos a serem inseridos no Formulário para Conscientização;

9.3.2.1. Realizar ajustes conforme solicitado;

9.3.2.4. Coletar registros ou *logs*;

9.3.3. São responsabilidades do Comitê Gestor de Tecnologia da Informação e Comunicação:

9.3.3.1. Ciência das necessidades;

9.3.3.1. Validar os assuntos e conteúdos;

9.3.3.4. Validar a diagramação e editoração dos assuntos e conteúdos;

9.3.3.5. Validar os registros e *logs*;

9.3.4. São responsabilidades do Comitê Gestor de Segurança da Informação;

9.3.4.1. Coordenar e estar ciente das atividades e ações sobre Segurança da Informação;

9.3.4.1. Dar ciência dos assuntos e conteúdos;

9.3.4.4. Cientificar e divulgar os resultados obtidos com as ações de conscientização;

9.3.5. São responsabilidades da Diretoria de Comunicação Social:

9.3.5.1. Realizar a diagramação e editoração dos assuntos e conteúdos;

9.3.5.1. Divulgar as atividades e ações de conscientização por meio dos meios de comunicação (Zap Justiça, Zimbra *Webmail*, *Spark*, Tv *Indoor*, Portais Intranet e Internet), dentre outros.

9.3.5.4. Coletar registros ou *logs*;

9.3.6. São responsabilidades da Diretoria de Gestão de Pessoas:

9.3.6.1. Realizar a divulgação das Normas da Política de Segurança da Informação para novos magistrados e servidores por meio do Termo de Ciência;

9.3.6. São responsabilidades dos Gabinentes e demais Diretorias, Setores e Comarcas do PJTO:

9.3.6.1. Participar das atividades e ações de conscientização em Segurança da Informação;

9.3.6.1. Conhecer e respeitar as normas contidas na Política de Segurança da Informação do Poder Judiciário do Tocantins.

9.4. **Disposições Finais**

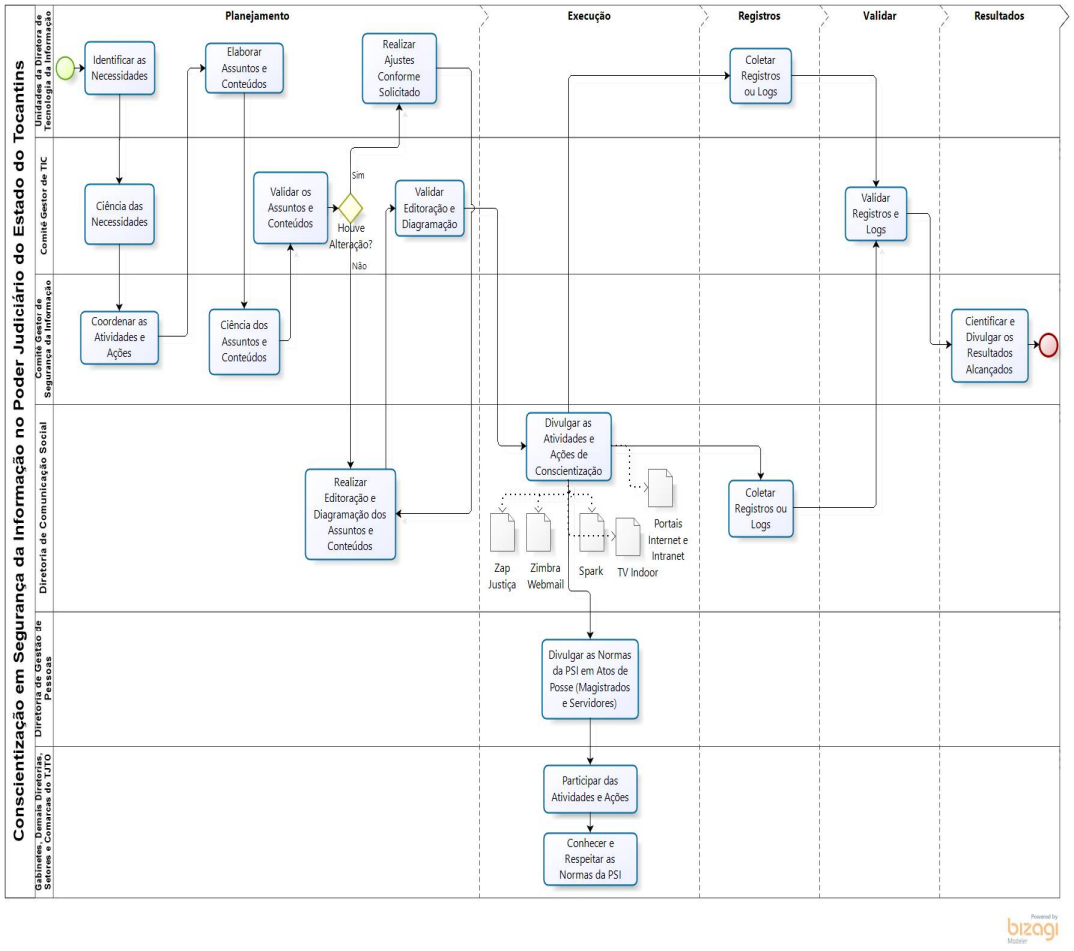
9.4.1. O Comitê Gestor de Segurança da Informação deverá ser comunicado de todas as ações que compõem o plano de conscientização em Segurança da Informação;

9.4.2. O Comitê Gestor de Segurança da Informação indicará um dia do ano, que será destinado como o “Dia da Conscientização em Segurança da Informação do Poder Judiciário Tocantinense”, com ações totalmente voltadas à Segurança da Informação;

9.4.3. A Diretoria de Gestão Estratégica é responsável pela compilação e tabulação dos indicadores do macroprocesso de Gestão de Segurança da Informação;

9.4.4. O Plano de Conscientização deverá ser atualizado periodicamente, no mínimo uma vez por ano, ou quando se fizer necessário.

APÊNDICE C – Fluxo do Processo de Conscientização em SI no PJTO



APÊNDICE D – Formulário para o Plano de Conscientização em SI do PJTO

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação (DTINF)
FÓRMULÁRIO PARA CONSCIENTIZAÇÃO EM SEGURANÇA DA INFORMAÇÃO	
INDICAÇÃO DO PLANO DE AÇÕES E DETALHAMENTOS	**Data:**
Área:	
Responsável:	

1 Indicação do Plano de Ações

<<Nesta Seção, deverão ser descritas as Normas da Política de Segurança da Informação e/ou assuntos relevantes relacionados à Segurança da Informação a serem inseridos no Plano de Conscientização para 2020. >>

Exemplo: O uso de senhas fracas é um exemplo de possíveis falhas de Segurança da Informação; por esse motivo, é um assunto relevante a ser inserido nas ações de conscientização. Para tanto, poderá ser inserido como tema o Uso Correto de Senhas para Acesso aos Serviços e Sistemas do Poder Judiciário do Tocantins.

<<Deverá constar em anexo a esse documento a Indicação dos Assuntos para o Plano de Conscientização em SI. >>

2 Detalhamentos dos Assuntos Indicados

<<Recentes pesquisas mostram que cerca de 80% das brechas de segurança dos dados empresariais se deve à fraqueza das senhas dos usuários. Esses dados evidenciam a importância do uso de padrões mais complexos para garantir uma verdadeira proteção. Outro grande problema em relação ao uso de senhas é o seu compartilhamento indevido entre funcionários da organização.

Assim, para manter que sua senha seja um tanto quanto segura, é de fundamental importância seguir alguns critérios: a) criar o hábito de trocar suas senhas a cada noventa dias; b) utilizar senhas com letras alfanuméricas, letras maiúsculas e minúsculas, além de usar caracteres especiais (# @ $ & !); c) criar senhas que tenham no mínimo 10 caracteres; e d) nunca escrever suas senhas em um papel ou guardá-las perto do computador.>>

<<Deverá constar em anexo a esse documento o Detalhamentos dos Assuntos para o Plano de Conscientização em SI >>

3 Apreciação pelo Comitê Gestor de Tecnologia da Informação e Comunicação

<<Este campo será de preenchimento exclusivamente pelo Comitê Gestor de Tecnologia da Informação e Comunicação, que deve analisar cada assunto e detalhamento inseridos nos Anexos I e II.

O Comitê deverá analisar, aprovar ou reprovar os assuntos inseridos nos anexos abaixo. A apreciação deve ser preenchida conforme tabela abaixo, e, em caso de reprovação, deve ser encaminhada à unidade de origem para correções. Em caso de aprovação deve ser encaminhada para a Cecom para editoração e diagramação dos assuntos propostos. >>

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Comitê Gestor de Tecnologia da Informação e Comunicação** Diretoria de Tecnologia da Informação (DTINF)	**Data:**
Presidente:		

Análise do Plano de Conscientização em SI					
ID	**Assunto/Detalhamento**	**Aprovado**	**Reprovado**	**Encaminhar para**	**Observação**

ANEXO I

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação (DTINF)	**Data:**
Responsável:		**Área:**

Indicação dos Assuntos para o Plano de Conscientização em SI				
ID	**Assunto**	**Prioridade**	**Público**	**Periodicidade**

ANEXO II

PODER JUDICIÁRIO ESTADO DO TOCANTINS	**Unidade Organizacional:** Diretoria de Tecnologia da Informação (DTINF)	**Data:**
Responsável:		**Área:**

Detalhamentos dos Assuntos para o Plano de Conscientização em SI		
ID	**Assunto**	**Detalhamentos e Orientações**

APÊNDICE E – Termo de Ciência da PSI do PJTO

PODER JUDICIÁRIO ESTADO DO TOCANTINS	Diretoria de Tecnologia da Informação (DTINF) Diretoria de Gestão de Pessoas (DIGEP)
TERMO DE CIÊNCIA DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO PODER JUDICIÁRIO DO ESTADO DO TOCANTINS	

Por meio deste instrumento, (nome)_____,
(nacionalidade)_____,(profissão) _____,
Carteira de Identidade (RG) nº_____, expedida por _____,
CPF nº _____, nesta data realizando a posse no cargo público de: _____,
e-mail: _____,
Residente em: _____,

Declaro ter recebido neste ato uma cópia deste Termo, contendo informações relacionadas à Política de Segurança da Informação do Poder Judiciário do Tocantins e que realizarei o acesso ao documento e farei uma leitura minuciosa das Normas estabelecidas na Política de Segurança da Informação deste Poder, conforme orientações abaixo:

Política de Segurança da Informação do Poder Judiciário do Tocantins	
Onde encontrar a PSI-PJTO:	http://www.tjto.jus.br/tic/index.php/governanca-de-tic/documentos-normativos/send/98-normativas/1147-politica-de-seguranca-da-informacao
Dúvidas sobre a PSI-PJTO:	Diretoria de Tecnologia da Informação (DTINF/TJTO) – Telefone: (63) 3218-4410 ou pelo e-mail: dtinf@tjto.jus.br.
Reportar Incidentes de Segurança da Informação:	Diretoria de Tecnologia da Informação (DTINF/TJTO) – Telefone: (63) 3218-4410 ou pelo e-mail: dtinf@tjto.jus.br.

Palmas/TO, _____,_____,20_____.

(Nome e Matrícula do Magistrado ou Servidor Empossado)

APÊNDICE F - Questionário

Para a realização do estudo de caso, foi elaborado um instrumento de pesquisa para coleta de dados, com o objetivo de obter um panorama do conhecimento sobre a Segurança da Informação no Poder Judiciário do Tocantins. O instrumento de pesquisa foi composto por 21 perguntas, sendo todas fechadas e elaboradas tendo por base o estudo desenvolvido por Alexandria (2009) em sua tese de doutorado.

Nessa pesquisa, foram distribuídos 205 questionários via Sistema Eletrônico de Informações (SEI), dos quais 180 foram respondidos no período de 30/4/2020 a 15/0/2020, totalizando 16 dias de disponibilidade.

Dentro do SEI, um departamento, setor, escrivania civel ou criminal, diretorias, gabinetes, dentre outros setores, são representados como sendo uma Unidade Organizacional, que em sua grande maioria possui mais de um servidor (a). Contudo foi solicitada que apenas um magistrado (a) ou servidor (a) de cada Unidade Organizacional respondesse ao questionário, assim a resposta obtida não representa a ideia de todos os demais servidores de tal Unidade Organizacional.

Receberam os questionários as Unidades Organizacionais das áreas meio e fim do Poder Judiciário do Tocantins, obtendo uma representatividade das unidades, sendo possível obter uma opnião de este Poder quase como um todo.

Autorização de envio do Instrumento de Pesquisa

Para que o instrumento de pesquisa fosse encaminhado às Unidades Organizacionais do Poder Judiciário, foi necessário abrir um processo administrativo por meio do Sistema Eletrônico de Informações (SEI), a ser remetido à Diretoria de Tecnologia da Informação (DTINF) para conhecimento e manifestação do envio do instrumento de pesquisa. Nessa mesma solicitação, foi reforçada a informação de que o instrumento de pesquisa tinha apenas finalidades acadêmicas, no intuito de salvaguardar a proteção dos direitos dos respondentes desse instrumento. Informando ainda que os dados obtidos não serão utilizados para outros fins que não aqueles constantes nos objetivos do estudo.

Ao receber o processo, a DTINF acolheu a solicitação e encaminhou os autos à Diretoria Geral para providências necessárias, que manifestou pelo envio dos autos à douta Presidência do TJTO para conhecimento e deliberação, tendo em vista que o

público-alvo da pesquisa envolvia a própria Presidência, Gabinetes dos Desembargadores, Gabinete da Corregedoria Geral de Justiça, Diretoria Geral da Esmat, Diretorias dos Fóruns e Coordenadoria de Gestão Estratégica. Assim, a Presidência acolheu a manifestação da DTINF e autorizou a aplicação do instrumento de coleta de dados (questionário).

Instrumento de Pesquisa

O questionário foi dividido em três dimensões, sendo a primeira composta por perguntas relacionadas ao comportamento do respondente ante a Segurança da Informação, com o propósito de identificar os possíveis comportamentos inadequados dos respondentes sobre o tema apresentado.

A segunda abordou perguntas pertinentes à concordância da implantação do plano de ações de conscientização em Segurança da Informação, bem como o interesse de participação do respondente, com vista à busca pela cultura de boas práticas em Segurança da Informação no Poder Judiciário do Tocantins.

Já a terceira e última dimensão, por sua vez, teve como objetivo identificar o local de ocupação dos servidores lotados nas repartições para onde foram encaminhados os instrumentos, bem como o tempo de serviço e os serviços e sistemas que utilizam ou têm acesso. Nessa dimensão, também consta a escolha de três assuntos, para possíveis prioridades na composição inicial do plano de conscientização em Segurança da Informação no Tribunal de Justiça do Estado do Tocantins, além de identificar se o respondente já havia participado de algum programa voltado à Segurança da Informação.

O instrumento de pesquisa foi baseado por meio da escala Likert, que, de acordo com Dzazali e Zolait (2012), é amplamente utilizado para medição de atitudes, crenças e opiniões. Assim foram definidas cinco categorias de escolha, sendo: na dimensão 1, correspondentes às perguntas de 1 até 7, foram utilizadas como respostas as seguintes representações: 1 (muita frequência), 2 (frequentemente), 3 (ocasionalmente), 4 (raramente) e 5 (nunca). Na dimensão 2, correspondentes às perguntas de 8 até 14, foram utilizadas como respostas as seguintes representações: 1 (concordo totalmente), 2 (concordo), 3 (indeciso), 4 (discordo) e 5 (discordo totalmente).

Quanto à definição do público-alvo do instrumento de pesquisa, esta levou em consideração que a administração do TJTO tivesse o conhecimento e a importância

deste trabalho para o Tribunal de Justiça do Estado do Tocantins. Dessa forma, e em conjunto com o professor orientador, foram definidas como público-alvo deste estudo algumas Unidades Organizacionais do Poder Judiciário do Tocantins, inicialmente compostas por 64 Unidades Organizacionais, a saber: Presidência, Gabinetes dos Desembargadores, Gabinete da Corregedoria Geral de Justiça, Diretoria Geral da Esmat, Diretorias dos Fóruns, Coordenadoria de Gestão Estratégica, Diretoria Geral e demais Diretorias do Poder Judiciário do Tocantins.

Após autorização do envio do instrumento de pesquisa pelo presidente do TJTO, desembargador-presidente em exercício, o processo SEI, com o link para acesso e preenchimento do questionário, foi encaminhado em 30/4/2020, para as 64 Unidades Organizacionais pré-definidas. No envio do instrumento de pesquisa, foi reforçado que era necessário que apenas um (a) magistrado (a) ou servidor (a) de cada Unidade Organizacional respondesse ao questionário.

Contudo, algumas Unidades Organizacionais, ao receberem o Processo SEI, com o questionário, reencaminharam-no para suas Subunidades. O instrumento de pesquisa foi recebido por 205 Unidades Organizacionais, porém respondido por 180 delas, totalizando um percentual de 88,78% respondentes.

Para destacar a seriedade desse estudo, foram inseridas duas informações no Processo SEI tratando da importância do tema "Segurança da Informação para o Tribunal de Justiça do Estado Tocantins", bem como a necessidade de obter o máximo de respostas possíveis a serem analisadas**.**

Para a realização do estudo de caso, foi elaborado um instrumento de pesquisa para coleta de dados, com o objetivo de obter um panorama do conhecimento sobre a Segurança da Informação no Poder Judiciário do Tocantins. O instrumento de pesquisa foi composto por 21 perguntas, sendo todas fechadas. Estas foram elaboradas tendo por base o estudo desenvolvido por Alexandria (2009) em sua tese de doutorado.

Nessa pesquisa, foram distribuídos 205 questionários via Sistema Eletrônico de Informações (SEI), dos quais 180 foram respondidos no período de 30/4/2020 a 15/5/2020, totalizando 16 dias de disponibilidade. As Unidades Organizacionais que receberam o questionário foram às da área-meio e fim do Poder Judiciário do Tocantins, contemplando, dessa forma, todos os prédios da capital e do interior.

Instrumento de Pesquisa

O questionário foi dividido em três dimensões: a primeira, composta por perguntas relacionadas ao comportamento do respondente ante a Segurança da Informação, com o propósito de identificar os possíveis comportamentos inadequados dos respondentes sobre o tema. A segunda abordou perguntas pertinentes à concordância da implantação do plano de ações de conscientização em Segurança da Informação, bem como o interesse de participação do respondente, com vista à busca pela cultura de boas práticas em Segurança da Informação no Poder Judiciário do Tocantins.

Já a terceira e última dimensão, por sua vez, teve como objetivo identificar o local de ocupação dos servidores lotados nas repartições para onde foram encaminhados os instrumentos, bem como o tempo de serviço e os serviços e sistemas que utilizam ou têm acesso. Nessa dimensão, também consta a escolha de três assuntos, para possíveis prioridades na composição inicial do Plano de Conscientização em Segurança da Informação no Tribunal de Justiça do Estado do Tocantins, além de identificar se o respondente já havia participado de algum programa voltado à Segurança da Informação.

O instrumento de pesquisa foi baseado na escala *Likert*, que, de acordo com Dzazali e Zolait (2012), é amplamente utilizado para medição de atitudes, crenças e opiniões. Assim, foram definidas cinco categorias de escolha: na dimensão 1, correspondentes às perguntas de 1 até 7, foram utilizadas como respostas as seguintes representações: 1 (muita frequência), 2 (frequentemente), 3 (ocasionalmente), 4

(raramente) e 5 (nunca). Na dimensão 2, correspondentes às perguntas de 8 até 14, foram utilizadas como respostas as seguintes representações: 1 (concordo totalmente), 2 (concordo), 3 (indeciso), 4 (discordo) e 5 (discordo totalmente).

Quanto à definição do público-alvo do instrumento de pesquisa, esta levou em consideração que a administração do TJTO tivesse o conhecimento e a importância deste trabalho para o Tribunal de Justiça. Dessa forma e em conjunto com o professor orientador, foi definido como sendo o público-alvo deste estudo algumas Unidades Organizacionais do Poder Judiciário do Tocantins, inicialmente compostas por 64, a saber: Presidência, Gabinetes dos (as) Desembargadores (as), Gabinete da Corregedoria Geral de Justiça, Diretoria Geral da Esmat, Diretorias dos Fóruns, Coordenadoria de Gestão Estratégica, Diretoria Geral e demais Diretorias do Poder Judiciário do Tocantins.

Após autorização do envio do instrumento de pesquisa pelo presidente do TJTO, desembargador-presidente em exercício, o processo SEI com o *link* para o acesso e preenchimento do questionário foi encaminhado, em 30/4/2020, para as 64 Unidades Organizacionais pré-definidas. No envio do instrumento de pesquisa, foi reforçado que seria necessário que apenas um (a) magistrado (a) ou servidor (a) de cada Unidade Organizacional respondesse ao questionário.

Contudo, algumas Unidades Organizacionais, ao receberem o Processo SEI com o questionário, reencaminharam-no para suas Subunidades. Portanto, o instrumento de pesquisa foi recebido por 205 Unidades Organizacionais, sendo respondido por 180 delas, totalizando um percentual de 88,78% respondentes.

Para destacar a seriedade desse estudo, foram inseridas duas informações no Processo SEI, tratando da importância do tema "Segurança da Informação para o Tribunal de Justiça do Estado Tocantins", bem como a necessidade de obter o máximo de respostas possíveis a serem analisadas.

Questionário

Senhor (a) Magistrado (a) ou Servidor (a) do Poder Judiciário do Tocantins.

O questionário a seguir é parte integrante de uma pesquisa de campo para uma dissertação de Mestrado cujo tema é "Estudo de Viabilidade para a Implantação do

Plano de Conscientização em Segurança da Informação no Poder Judiciário do Tocantins", e segue sob orientação do professor doutor Gentil Veloso Barbosa.

Responda às questões, marcando a(as) opção(ões) que melhor corresponde(m) ao seu perfil, comportamento e conhecimento, diante das situações apresentadas.

Não é necessário identificar-se. Os dados não serão utilizados para outros fins que não aqueles constantes nos objetivos deste estudo.

Muito obrigado por sua colaboração.

Dimensão 1 – Responda às questões de 1 a 7 sobre o comportamento relacionado à Segurança da Informação. As respostas devem ser de 1 a 5, em que 1 representa (Muita frequência) e 5 (Nunca).

1. Utiliza senhas fáceis de lembrar, compostas por nomes ou suas iniciais, datas de aniversários, sequências de letras ou números?

1 – Muita frequência.
2 – Frequentemente.
3 – Ocasionalmente.
4 – Raramente.
5 - Nunca.

2. Anota suas senhas em agenda ou deixa-as fixadas no monitor, debaixo do teclado ou sobre a mesa de trabalho?

1 – Muita frequência.
2 – Frequentemente.
3 – Ocasionalmente.
4 – Raramente.
5 – Nunca.

3. Compartilha suas senhas com terceiros (colegas de trabalho ou sala/gabinete)?

1 - Muita frequência.
2 - Frequentemente.
3 - Ocasionalmente.
4 - Raramente.
5 - Nunca.

4. Fornece informações pessoais quando solicitadas por meio de correio eletrônico (e-mail) de órgãos públicos ou de empresas conceituadas do mercado (Bancos, Correios, Receita Federal, Justiça Eleitoral, dentre outras)?

1 – Muita frequência.

2 – Frequentemente.
3 – Ocasionalmente.
4 – Raramente.
5 – Nunca.

5. Ao se ausentar do local de trabalho, encerra a sessão aberta no computador (faz *logout*), bloqueia a sessão com uso de senha?

1 – Muita frequência.
2 – Frequentemente.
3 – Ocasionalmente.
4 – Raramente.
5 – Nunca.

6. Consegue identificar um vírus de computador, quando recebido por meio de mensagens de correio eletrônico (e-mail)?

1 – Muita frequência.
2 – Frequentemente.
3 – Ocasionalmente.
4 – Raramente.
5 – Nunca.

7. O Tribunal de Justiça do Estado do Tocantins instituiu pela Portaria nº 3.433, de 26/7/2017, a Política de Segurança da Informação (PSI). Você já teve conhecimento das Normas nela contidas?

1 – Muita frequência.
2 – Frequentemente.
3 – Ocasionalmente.
4 – Raramente.
5 – Nunca.

Dimensão 2 – Responda às questões de 8 a 14 sobre a conscientização em Segurança da Informação. As respostas devem ser de 1 a 5, em que 1 representa (Concordo Totalmente) e 5 (Discordo Totalmente).

8. Em sua opinião, cada magistrado (a) ou servidor (a) deve ter consciência de sua responsabilidade sobre ações que envolvam a Segurança da Informação?

1 – Concordo Totalmente.
2 – Concordo.
3 – Indeciso.
4 – Discordo.

5 – Discordo Totalmente.

9. É interessante que o Tribunal de Justiça do Estado do Tocantins institua um Plano de Conscientização em Segurança da Informação, a ser disponibilizado periodicamente pelos meios de comunicação existentes (exemplos: *Spark*, E-mail, Portais Intranet e Internet, Zap Justiça, Tvs *Indoor*)?

1 – Concordo Totalmente.
2 – Concordo.
3 – Indeciso.
4 – Discordo.
5 – Discordo Totalmente.

10. Caso o Tribunal de Justiça do Estado do Tocantins instituísse um Plano de Conscientização em Segurança da Informação, concordaria em participar das ações de conscientização?

1 – Concordo Totalmente.
2 – Concordo.
3 – Indeciso.
4 – Discordo.
5 – Discordo Totalmente.

11. Considera importante que o Tribunal de Justiça do Estado do Tocantins crie o dia "D", com ações voltadas à conscientização em Segurança da Informação, por meio de palestras, mesas redondas, *workshops*?

1 – Concordo Totalmente.
2 – Concordo.
3 – Indeciso.
4 – Discordo.
5 – Discordo Totalmente.

12. O objetivo das ações de conscientização em Segurança da Informação é munir as pessoas com informações e experiências, a fim de que elas construam uma consciência própria e saibam como agir perante a identificação de uma ameaça?

1 – Concordo Totalmente.
2 – Concordo.
3 – Indeciso.
4 – Discordo.
5 – Discordo Totalmente.

13. A conscientização visa criar uma cultura de boas práticas voltadas à Segurança da Informação no Poder Judiciário do Tocantins?

1 – Concordo Totalmente.

2 – Concordo.
3 – Indeciso.
4 – Discordo.
5 – Discordo Totalmente.

14. O sucesso de um plano de conscientização em Segurança da Informação só terá efeito se houver políticas e práticas de segurança bem definidas, aparatos tecnológicos capazes de identificar e impedir ataques e **principalmente** o engajamento de todos os membros da organização, pois uma equipe desta, se conscientizada, educada e engajada na importância da proteção das informações dificilmente sofrerá prejuízos causados por ciberataques?

1 – Concordo Totalmente.
2 – Concordo.
3 – Indeciso.
4 – Discordo.
5 – Discordo Totalmente.

Dimensão 3 – Por gentileza, forneça agora algumas informações sobre sua ocupação, tempo de serviço, serviços e sistemas que utiliza ou tem acesso, como também a escolha de três assuntos para possíveis prioridades na composição inicial do plano de conscientização em Segurança da Informação no Tribunal de Justiça do Estado do Tocantins. **Estes dados não serão utilizados para a identificação do respondente**.

15. Em qual localidade exerce sua atividade laboral?

( ) Comarcas.
( ) Tribunal de Justiça/Anexos.
( ) Corregedoria Geral de Justiça.
( ) Escola Superior da Magistratura Tocantinense (ESMAT).
( ) Outra.

16. Há quantos anos é magistrado (a) ou servidor (a), no Poder Judiciário do Tocantins?

( ) De 0 a 9 anos.
( ) De 10 a 15 anos.
( ) De 16 a 20 anos.
( ) De 21 a 25 anos.
( ) Mais de 26 anos.

17. Selecione quais serviços e sistemas você utiliza ou tem acesso?

( ) e-Pproc-TJTO.
( ) SEI.
( ) e-Gesp.
( ) Funjuris.
( ) *Login* de Rede.
( ) Malote Digital.

( ) *Assyst (Service Desk*)
( ) *Webmail.*
( ) *Spark.*
( ) Demais Sistemas (outros).

18. Quais das ações listadas abaixo você acredita ser a mais efetiva quando se trata de conscientizar os membros internos do Poder Judiciário do Tocantins?

( ) Comunicação Periódica.
( ) Palestras de Especialistas.
( ) Envio de Notícias.
( ) Simulações de Ataques.
( ) Palestras de Colaboradores.

19. Acredita que as ações de conscientização voltadas à Segurança da Informação irão impactar no seu trabalho?

( ) Positivamente.
( ) Negativamente.

20. Escolha três assuntos dentre os apresentados abaixo, que considere prioritário na composição inicial do Plano de Conscientização em Segurança da Informação do Tribunal de Justiça do Estado do Tocantins.

( ) *Phishing*.
( ) Senhas seguras.
( ) Mesa e Tela limpas.
( ) Engenharia Social.
( ) *Spam*.
( ) Normas da Política de Segurança da Informação do Tribunal de Justiça do Estado do Tocantins.

21. Por fim, selecione abaixo de quais programas voltados à Segurança da Informação já tenha participado:

( ) Treinamento.
( ) Palestra.
( ) Evento.
( ) Videoaulas.
( ) Ações de Conscientização.
( ) Nenhuma das opções.