Primeiros passos da implantação do PPSI no Instituto Federal Catarinense

RESUMO

Este artigo apresenta uma análise inicial da implementação do Programa de Privacidade e Segurança da Informação (PPSI), previsto para início em 2024, em conformidade com as diretrizes estabelecidas no Plano de Desenvolvimento Institucional (PDI) 2024–2028 do Instituto Federal Catarinense, bem como com os normativos vigentes. Trata-se de uma pesquisa qualitativa, fundamentada em análise documental, que objetiva compreender os desafios, os avanços e as perspectivas relacionados à governança de Tecnologia da Informação no contexto da transformação digital e da segurança da informação na administração pública educacional. Os resultados forneceram subsídios teóricos e práticos para futuras iniciativas de implantação.

Palavras-chave: Segurança da Informação; Governança de TI; IFC; PPSI; PDI

1. INTRODUÇÃO

O movimento atual do governo brasileiro em relação à digitalização dos serviços caminha a passos largos, conforme dados do painel de monitoramento dos serviços digitais (BRASIL, 2025), hoje encontram-se a disposição da população brasileira mais de 4500 serviços digitais disponíveis em mais de 226 órgãos diferente do Governo brasileiro. Neste contexto segurança da informação tornou-se um pilar essencial desta estrutura para a Administração Pública Federal (APF).

Neste contexto o artigo apresenta como tema central de pesquisa o processo de implantação do Programa de Privacidade e Segurança da Informação (PPSI) no Instituto Federal Catarinense e os problemas encontrados durante o processo. O PPSI, instituído pela Secretaria de Governo Digital do Ministério da Gestão e da Inovação em Serviços Públicos (SGD/MGI), apresenta-se como um framework estratégico para orientar órgãos e entidades na implementação de controles eficazes de segurança e privacidade para sustentar esta gama de serviços com segurança e resiliência. (Brasil, 2025)

O PPSI foi instituído pela Portaria SGD/MGI nº 852, de 28 de março de 2023, como um conjunto de projetos e processos voltados à privacidade e segurança da informação no âmbito da Administração Pública Federal, especialmente para os órgãos que integram o Sistema de Administração dos Recursos de Tecnologia da Informação (SISP).(Brasil, 2025)

Este conjunto teve sua origem na compilação de boas práticas internacionais reconhecidas, notadamente recomendações do CIS (Center for Internet Security) além de alinhar-se à realidade brasileira através de sua vinculação a diversos normativos ABNT/NBR assim como a Lei Geral de Proteção de Dados (LGPD) – Lei nº 13.709/2018, a Política Nacional de Segurança da Informação (PNSI) – Decreto nº 9.637/2018 e a Estratégia Nacional de Segurança Cibernética - E-Ciber Decreto nº 10.222/2020.

A implantação do Programa de Privacidade e Segurança da Informação no Instituto Federal Catarinense inicia-se com a portaria IFC Nº 1946/2023 - PORT/REIT (11.01.18.56) de 06 de outubro de 2023 que nomeou seu primeiro Gestor de Segurança da Informação com o objetivo de viabilizar a implantação do PPSI em sua estrutura, a partir deste momento foram iniciados os trabalhos de adequação aos controles e

determinações legais, a partir deste marco inicial desenvolveram-se mudanças gradativas com o objetivo de adequar a infraestrutura de pessoal e técnica aos normativos vigentes e aos controles do PPSI.!

A partir deste momento foi traçado um plano para o Instituto Federal Catarinense com o objetivo de atender às demandas do PPSI. O Plano construído inicialmente consistiu em 5 etapas a identificação dos objetivos e metas a serem alcançados, o desenvolvimento dos planos de implantação prioritários para cada controle, a documentação do processo a especificação das entregas esperadas e pôr fim a revisão do processo por ciclos do PPSI conforme Figura 1.

Figura 1- Planejamento de adequação do IFC ao PPSI

Fonte: o Autor

Neste trabalho demonstrasse o processo de implantação do PPSI com foco nas ações executadas, na percepção dos efeitos positivos ou negativos e finalizando com sugestões e propostas. A partir do detalhamento da execução de cada etapa o artigo tem como objetivo principal colaborar com os demais órgãos na disseminação do conhecimento e servindo como linha de base para futuras implantações.

A seguir são detalhados alguns dos momentos-chave de nossa implantação com os respectivos detalhes e processos associados.

O PPSI está alinhado ao plano de desenvolvimento institucional do Instituto Federal catarinense Resolução nº 03/2024 e neste sentido foram definidas como ações prioritárias o alinhamento com a alta gestão e o de diagnóstico estrutural do IFC a partir dos 7 controles iniciais fornecidos pelo PPSI 0.1 a 0.7 respectivamente que correspondem a estrutura básica institucional para a gestão da Segurança da informação.

2. FUNDAMENTAÇÃO TEÓRICA

1.1. O PPSI

O Programa de Privacidade e Segurança da Informação (PPSI) foi instituído por meio da Portaria SGD/MGI nº 852 de autoria do Secretário de governo digital do ministério da gestão e da inovação em serviços públicos Sr. Rogério Souza Mascarenhas, publicada em 28 de março de 2023. No Capítulo IV da referida portaria, é estabelecido o

Framework de Privacidade e Segurança da Informação, que constitui a base conceitual e operacional do PPSI.

O programa é composto por um conjunto estruturado de medidas e controles voltados à elevação da maturidade institucional e da resiliência organizacional no que tange à proteção de dados pessoais e à segurança da informação. Dessa forma, busca-se fortalecer a confiança da sociedade na prestação de serviços públicos digitais.

Desenvolvido pela Secretaria de Governo Digital (SGD), o framework do PPSI incorpora diretrizes fundamentadas em boas práticas nacionais e internacionais, incluindo as normas das famílias ISO/IEC 27000 e 29100, os CIS Controls, bem como os frameworks do National Institute of Standards and Technology (NIST), o Cybersecurity Framework e o Privacy Framework. O modelo também está alinhado à legislação vigente, especialmente à LGPD, e aos normativos do Gabinete de Segurança Institucional (BRASIL, 2024).

A estrutura do PPSI contempla 310 medidas organizadas em 32 controles (BRASIL, 2024; CARVALHO, 2023; ALMEIDA, 2024). A principal referência adotada foi o CIS Controls, cuja estrutura foi incorporada integralmente. Para os demais controles, foram utilizadas normas ISO e os frameworks do NIST, conforme mencionado.

O modelo de implementação do PPSI adota uma abordagem cíclica, inspirada no ciclo PDCA (Plan, Do, Check, Act), o que permite a revisão contínua dos processos e a realização de ajustes conforme necessário. Entre os instrumentos disponibilizados às instituições estão o inventário de dados pessoais, a avaliação de riscos, os relatórios de impacto à proteção de dados (RIPD) e guias específicos para a implementação dos requisitos da LGPD (ALMEIDA, 2024). Tais ferramentas visam identificar lacunas e apoiar a adaptação das entidades às exigências normativas, promovendo um processo contínuo de conformidade.

O framework prevê a realização de autoavaliações periódicas pelas instituições públicas, com base em questionários e ferramentas fornecidos pela SGD. Os resultados dessas avaliações geram indicadores de maturidade em privacidade e segurança da informação, os quais subsidiam a elaboração de planos de ação para a mitigação de deficiências identificadas (ALMEIDA, 2024).

O PPSI abrange hoje 254 entidades da Administração Pública Federal com diferentes portes, finalidades e capacidades institucionais. Essa diversidade demanda constante atualização e adaptação do framework frente às transformações legislativas e tecnológicas, o que pode impactar os níveis de maturidade aferidos em ciclos avaliativos anteriores (CARVALHO, 2023) Nos órgãos finalísticos este é um dos principais desafios enfrentados atém da escassez de recursos financeiros e de pessoal.

3. METODOLOGIA

Esta pesquisa classifica-se como aplicada, uma vez que possui o objetivo de gerar conhecimentos voltados à resolução de problemas concretos, com aplicação prática imediata no contexto das instituições públicas. Segundo Lakatos e Marconi (2003), a pesquisa aplicada objetiva contribuir para o avanço do conhecimento com vistas à sua utilização na realidade, sendo frequentemente direcionada à resolução de questões específicas enfrentadas por organizações ou setores sociais.

Quanto à abordagem, adota-se uma metodologia qualitativa, pois busca-se compreender os fenômenos em profundidade, considerando os significados atribuídos pelos sujeitos envolvidos. A pesquisa qualitativa, conforme Lakatos e Marconi (2003), é apropriada para estudos que envolvem análise interpretativa de dados não numéricos, permitindo uma compreensão mais abrangente dos contextos e das relações sociais. Para tanto, serão utilizados também instrumentos como análise documental, entrevistas semiestruturadas e observação participante.

O delineamento da pesquisa é do tipo exploratório-descritivo. A fase exploratória tem como objetivo proporcionar maior familiaridade com o problema, enquanto a fase descritiva visa caracterizar, de forma sistemática, os elementos observados. De acordo com Lakatos e Marconi (2003), a pesquisa exploratória é indicada quando o tema é pouco conhecido ou carece de estudos aprofundados, e a pesquisa descritiva permite o registro e a análise das características de determinado fenômeno ou população. A combinação dessas abordagens possibilita uma investigação mais robusta e alinhada aos objetivos propostos.

4. CICLO 1 do PPSI - Diagnóstico da Estrutura de Segurança da Informação

O trabalho inicialmente desenvolvido pelo Gestor de Segurança da Informação foi a elaboração do diagnóstico institucional, no levantamento foi identificado que o órgão já possuía em seus quadros designados: a Autoridade máxima de TI conforme portaria nº 33 / 2020 assim como também possuía já nomeados o Gestor de Segurança da Informação e o Responsável pela proteção de dados conforme portaria nº 2151/2023, de 10 de novembro de 2023 ambos vinculados a Diretoria Executiva, unidade máxima na administração da entidade, já atendendo nestes casos às melhores práticas na gestão de Segurança da Informação.

Nesta fase inicial dos trabalhos também foi solicitado ao dirigente máximo da instituição a recondução de servidores ao Comitê Gestor de Segurança da Informação, porém estas ações foram impactadas negativamente pela greve dos servidores assim como pela alteração no organograma institucional o que demandou novas nomeações para diversos cargos incluindo a recomposição do Comitê Gestor de Segurança da Informação (CGSI).

Quanto a entrega relativa ao ciclo 1 determinada para 31 de dezembro de 2023 conforme dados do MGI os trabalhos limitaram-se aos diagnósticos iniciais e elaboração os planos de trabalho para os controles ativos sendo estes em sua maioria previstos para implantação no decorrer do primeiro semestre de 2024 dadas as restrições de tempo e equipe.

5. CICLO 2 do PPSI - Controles e medidas críticos.

Foram identificadas neste primeiro momento como prioritárias as deficiências nos controles 0.3, 0.4, 0.5, 0.6 respectivamente: a definição do responsável pelo controle interno, a recondução de servidores que compunham o comitê gestor de segurança da informação, a instituição de uma Equipe de Tratamento e Resposta a Incidentes Cibernéticos(ETIR) equipe especializada em lidar com incidentes de segurança cibernética, desde a identificação e avaliação até a resposta e recuperação, e a elaboração de uma política de segurança da informação.

Por tratar-se de itens ainda pertinentes ao ciclo 1 foram incluídos como itens prioritários no planejamento, os quais passaram a ser incluídos nos trabalhos para o primeiro semestre de 2024

Como parte do planejamento de execução foram agendadas para acompanhamento do processo reuniões semanais entre o responsável pela Gestão de Segurança da Informação o Diretor de Tecnologia da Informação e o responsável pela proteção de dados. No decorrer das reuniões semanais realizadas durante os ciclos 2 e 3 foram validados semanalmente o andamento dos processos de implantação, documentos e encaminhamentos e reavaliados os riscos atuais do processo assim como possíveis entraves operacionais. A cada reunião foram redefinidas as atividades prioritárias e os responsáveis pelo seu acompanhamento.

Para atendimento ao controle 0.3 do PPSI salientamos que o instituto federal não possuí em sua estrutura unidade nomeada como controle interno assim como diversos outros institutos federais de ensino, para este caso foi designada a figura do Vice-reitor em exercício como responsável pelo controle interno sendo que esta atribuição já era desempenhada à época pela secretaria executiva do órgão, unidade chefiada pelo Vice-reitor.

O controle 0.4 o comitê gestor de Segurança da informação foi definido em reunião conjunta com a diretoria de tecnologia da informação o responsável pela proteção de dados e o gabinete do reitor e foi definida sua composição conforme

Ainda no primeiro semestre de 2024 foram concluídos os trabalhos referentes ao controle 0.5. Nomeação da ETIR, o qual foi atendido através do apoio institucional do Centro Integrado de Segurança Cibernética do Gov.Br (Cisc Govbr) que fornece consultoria para a definição de estrutura e composição da Equipe, os resultados dos trabalhos foram publicados na Portaria Normativa nº 4/2024 de 24 de junho de 2024

No que tange aos controles pertencentes ao ciclo 2, observa-se que as atividades previstas foram significativamente impactadas pela paralisação dos servidores e docentes. Tal ocorrência limitou o desenvolvimento de diversos processos ao longo do primeiro semestre, sendo os seguintes controles os que puderam ser efetivamente abordados:

10.1: O órgão instala e mantém um software antimalware?

Este controle foi atendido através de nota técnica emitida pela DTI do órgão padronizando a ferramenta de software institucionalmente.

10.2: O órgão configura atualizações automáticas de assinatura antimalware?

Este controle foi compreendido em nota técnica que definiu os parãmetros de configuração de devem ser aplicados a todos os ativos da informação institucionais onde o software antimaware for aplicável.

15.1: O órgão cria e gerencia o inventário de provedores de serviços?

O Onventário de provedores de serviços foi providenciado em esforço conjunto entre DTI e Pro-Reitoria administrativa responsável pela gestão de contratos.

17.1: O órgão designa os colaboradores para gerenciar o tratamento de incidentes?

A ETIR do IFC foi modelada com o apoio institucional da CTIR que colaborou na definição do modelo de equipe a ser adotado e também na edição da portaria normativa que a institui no órgão, esta parceria se mostrou altamente produtiva.

17.2: O órgão estabelece e mantém informações de contato para relatar incidentes de segurança?

Foi criado no portal WEB do IFC área exclusiva para a divulgação institucional dos documentos e informações relativas a segurança da informação, também foi criado E-mail exclusivo e seguro para a recepção de informações e o tratamento de incidentes.

17.3: O órgão estabelece e mantém informações do fluxo de tratamento de incidentes de segurança?

O fluxo de tratamento de incidentes foi normatizado e publicado no portal do IFC para amplo acesso a comunidade acadêmica e demais usuários dos sistemas corporativos e institucionais assim como sua publicação foi divulgada por e-mail a todos os servidores e alunos.

21.4: O órgão disponibiliza para o encarregado os recursos necessários para implementação da LGPD e acesso direto à alta administração?

Ao encarregado de dados foi garantido o acesso direto a alta administração inclusive realocando o servidor fisicamente para expediente no gabinete onde possui acesso livre ao reitor, vice reitor e demais gestores.

21.6: O órgão divulga a seus colaboradores internos e externos as políticas e procedimentos operacionais relacionados à proteção de dados pessoais?

Foi criada área exclusiva para divulgação de documentos referências e informações a cerca da proteção de dados no portal institucional do IFC, acessível publicamente e divulgado amplamente a comunidade interna através do E-mail institucional.

22.1: A organização revisou e adequou a Política de Segurança da Informação ou instrumento similar à LGPD?

Foi criado um Grupo de Trabalho que revisou e atualizou a política de Segurança da Informação do IFC segundo as normativas vigentes, o processo foi concluído e encontra-se em tramites finais de publicação.

29.2: O órgão adota meios para disponibilizar a política de privacidade em local de fácil acesso, antes ou no momento do tratamento de dados pessoais, sem a necessidade de o titular ter que solicitá-lo especificamente?

A política de privacidade foi publicada no portal WEB do IFC com amplo acesso e divulgada por E-mail institucional enviado a todos os usuários do IFC.

29.6: A identidade e as informações de contato do encarregado estão divulgadas publicamente, de forma clara e objetiva, preferencialmente no sítio eletrônico do controlador?

As informações de contato do encarregado de dados foram inseridas nos sistemas WEB para publicação no portal público garantindo o pleno acesso e conhecimento das formas de contato.

31.4: A instituição considera o princípio do privilégio mínimo na concessão de direitos de acesso para o processamento de dados pessoais?

Todas as concessões de acesso são baseadas no acesso mínimo necessário e a revogação de acessos foi automatizada nos sistemas institucionais a partir da alteração de locação ou exercício dos servidores.

Devido à falta de recursos técnicos e humanos os demais controles alinhados com a alta administração e com a direção de TI para futura execução no decorrer do biênio 2024/2025 conforme priorização e obtenção de recursos.

Os controles citados acima foram efetivamente aplicados e constados como adotados em maior parte ou totalmente conforme documentação enviada ao MGI.

6. CICLO 3 – Dependências dos Controles e medidas críticos.

Durante o ciclo 3 foram priorizados atos normativos decorrentes da elaboração de documentos e formalização de processos administrativos com o objetivo de padronizar ações e procedimentos no âmbito do Instituto Federal Catarinense. Neste sentido foram elaborados em conjunto com o diretor de TI portarias, notas técnicas e outros documentos norteadores atendendo aos controles:

8.3: O órgão padroniza a sincronização de tempo?

A padronização de tempo no IFC foi normatizada através de nota técnica da DTI vigente para todos os campus.

10.1: O órgão instala e mantém um software antimalware?

O controle foi padronizado através de nota técnica com abrangência para todo o IFC.

10.2: O órgão configura atualizações automáticas de assinatura antimalware?

O controle foi padronizado através de nota técnica com abrangência para todo o IFC.

11.1: O órgão protege os dados de recuperação?

Atendido através de padronização do procedimento de armazenamento dos dados de Backup.

11.2: O órgão estabelece e mantém um processo de recuperação de dados?

O controle foi padronizado através da elaboração de uma política de backup implantada a partir de 31/12/2024 atendendo aos sistemas corporativos e sites do IFC.

11.3: O órgão executa backups automatizados?

O Backup foi automatizado através de ferramenta comercial, com implantação padronizada pela política de backup.

11.4: O órgão estabelece e mantém uma instância isolada de dados de recuperação?

Os dados de backup são mantidos em ambiente fisicamente isolado para atendimento ao controle

11.5: O órgão testa os dados de recuperação?

Foram implantados controles de restauração e teste automatizados na ferramenta de backup para homologação e atendimento ao controle.

16.8: O órgão separa sistemas de produção e não produção?

O órgão possui em sua estrutura ambiente de homologação completamente isolado do ambiente de produção e neste são efetuados o desenvolvimento, testes e homologação de alterações nos sistemas.

22.2: Há uma política vigente ou documento equivalente que dispõe sobre diretrizes de proteção de dados pessoais?

Foi elaborada e publicada a política de proteção de dados do IFC.

25.1: O órgão configura os sistemas para registrar a data em que os dados pessoais são coletados, criados, atualizados, excluídos ou arquivados?

Os sistemas foram configurados para gerar registros de log de atividades de cadastro em que sejam inseridos dados pessoais.

31.6: O acesso físico aos dados e dispositivos é gerenciado?

O acesso físico ao CPD da reitoria foi normatizado com o objetivo de gerenciar o acesso físico ao ambiente controlado.

Foram ainda disparados neste interim o inventário de ativos de TI (relatório inicial confirmado pelo patrimônio) e o inventário de ativos da informação (relatório efetuado pela DTI) para atendimento aos respectivos controles.

7. AVALIAÇÃO DA IMPLEMENTAÇÃO

A trajetória de implantação do Programa de Privacidade e Segurança da Informação (PPSI) no Instituto Federal Catarinense (IFC) revela avanços significativos na estruturação institucional voltada à proteção de dados e à segurança da informação. A adoção progressiva dos controles e medidas previstas no framework do PPSI, especialmente ao longo dos três primeiros ciclos, demonstra o comprometimento da instituição com a conformidade normativa e a maturidade organizacional.

Para isto apresentaremos os indicadores do IFC referentes ao iSeg que mede a eficácia das práticas de segurança aplicadas, e iPriv que analisa as iniciativas para proteger a privacidade e garantir a conformidade com regulamentações como a Lei Geral de Proteção de Dados Pessoais (LGPD) aplicados como referência pelo MGI.

Os indicadores de desempenho do IFC refletem essa evolução.

No Ciclo 1, os índices eram modestos: iSeg 0,33 e iPriv 0,14, com uma estrutura básica de 0,60.

No Ciclo 2, observa-se uma melhora: iSeg passou para 0,39 e iPriv para 0,33, enquanto a estrutura básica avançou para 0,80.

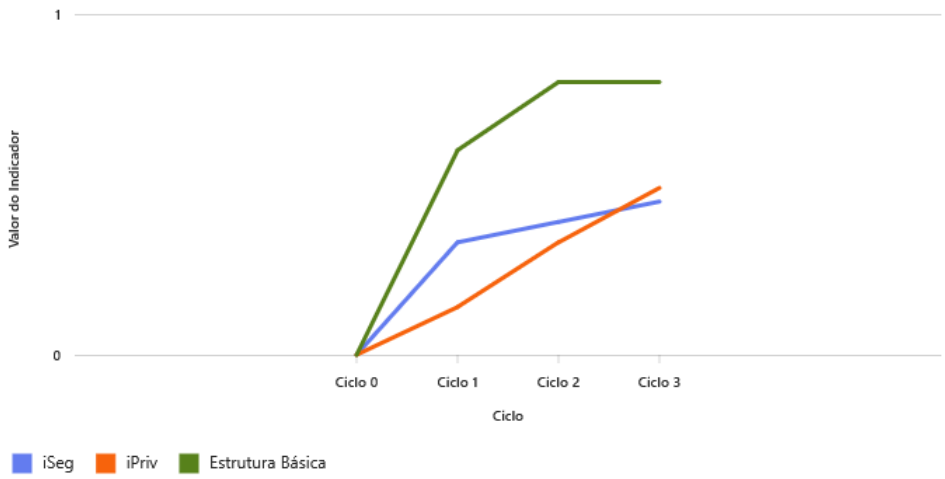
No Ciclo 3, o IFC alcançou uma melhora expressiva: iSeg atingindo 0,45 e iPriv 0,49, enquanto a estrutura básica avançou para 0,80.

Ao final deste processo inicial, ou seja, ao encerrarmos o ciclo 03 em números o indicador iSeg evoluiu significativamente assim como o iPriv , enquanto a estrutura básica manteve-se estável em ainda significativos 0,80. Estes números refletiram na

quantidade de notificações por vazamento de senhas e dados que após o primeiro ano de implantação do PPSI reduziram-se em mais de 80%.

O gráfico 1 mostra a evolução dos indicadores no decorrer desta implantação.

Gráfico 2- Evolução dos Indicadores



Fonte: O autor

Esses números evidenciam o impacto positivo das medidas implementadas, como a nomeação de gestores, a criação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR), a formalização de políticas institucionais e a padronização de procedimentos técnicos.

Apesar das limitações enfrentadas — como escassez de recursos humanos e financeiros, paralisações e mudanças estruturais — o IFC conseguiu avançar de forma estratégica, priorizando ações viáveis e alinhadas à sua realidade institucional. A adoção do ciclo PDCA como metodologia de gestão contribuiu para a organização dos processos e para a melhoria contínua dos indicadores.

A experiência do IFC reforça a importância da adaptação contextual na implementação de programas complexos como o PPSI. A evolução dos indicadores iPriv e iSeg não apenas representa o progresso técnico, mas também simboliza o fortalecimento da cultura organizacional voltada à segurança da informação e à proteção de dados pessoais. Este trabalho, portanto, oferece subsídios valiosos para outras instituições públicas que buscam iniciar ou aprimorar suas práticas de governança digital e segurança da informação.

8. ENTREVISTA

Em consonância com a abordagem metodológica do ciclo PDCA, ao término do ciclo 03 foi conduzida uma entrevista com o Gestor de Tecnologia da Informação do Instituto Federal Catarinense (IFC), com o intuito de coletar subsídios acerca de sua percepção sobre a implantação do Programa de Proteção de Segurança da Informação (PPSI)no IFC. Suas colaborações fazem parte deste artigo com o propósito de fornecer

conhecimento a unidades ou órgãos da APF sobre o resultado do processo aplicado a seguir relatamos as perguntas e respostas da direção de TI.

Pergunta 1: Quais foram os principais desafios enfrentados pela DTI do IFC nos primeiros passos da implantação do PPSI, especialmente em relação à adequação da infraestrutura técnica e de pessoal?

Em relação aos desafios enfrentados pelo IFC quando do início dos trabalhos o DTI afirmou que a implantação da PPSI se iniciou em ano anterior a atual gestão da DTI, ainda no ciclo 1, e que este foi mais tranquilo devido os níveis de controle solicitados. Sobre os demais ciclos, para atender a implementação das medidas foram criadas políticas ou recomendações internamente. Reforçou que o IFC, não possui equipe suficiente e nem recursos financeiros suficientes para implementar de fato boa parte das medidas.

Pergunta 2: Como o senhor avalia o impacto da nomeação do Gestor de Segurança da Informação em outubro de 2023 na condução e no avanço das ações relacionadas ao PPSI?

Sobre a nomeação do Gestor de Segurança da Informação, ocorrida em outubro de 2023 foi reportado pelo DTI que a ação colaborou positivamente para a instituição, e negativamente para a área de TI; por ser o gestor uma pessoa técnica anteriormente lotada na diretoria de tecnologia da informação, na sua opinião, poderia implementar ações de segurança dentro da área, mas infelizmente fica sobrecarregado com a burocracia.

Pergunta 3: Na sua percepção, quais controles ou diretrizes do PPSI trouxeram os efeitos mais positivos até o momento para a governança de TI do IFC?

Sobre sua percepção em relação aos controles do PPSI e sua efetividade e melhorias em relação a SI o DTI informou que através da efetivação dos controles, conseguimos escrever algumas práticas que fazíamos sem formalização porém e outras não realizamos e nem temos previsão para realizar. Algumas ações tímidas avançaram com aquisição de firewall e contratação de serviços da RNP, como o SOC.

Reportou ainda que grande parte dos controles já eram de certa forma efetivos, mas sem a devida documentação e normatização.

Pergunta 4: Houve resistência institucional ou cultural à adoção das práticas propostas pelo PPSI? Se sim, como a DTI lidou com essas barreiras?

Questionado se houve resistência institucional ou cultural à adoção das práticas propostas pelo PPSI? Reportou que poucos tem resistência ao tema, a meu ver, pode parecer que é ignorado, mas não temos força de pessoal e maturidade no momento para olhar verdadeiramente para PPSI. As pessoas na ponta provavelmente não fazem ideia do que é segurança da informação e da importância que isso tem, provavelmente uma falha institucional ainda em não capacitar as pessoas sobre. A única área incomodada de verdade que obrigatoriamente tem que levar isso em consideração é a TI, dentro da TI não podemos chamar de resistência, é questão de não ter como priorizar mesmo.

Pergunta 5: Com base na experiência inicial, que sugestões ou recomendações o senhor daria para outras instituições públicas que estão iniciando a implantação do PPSI?

Apenas desejaria boa sorte, estou atuando como coordenador da comissão de segurança da informação do FORTI e é unânime entre os 41 gestores de TI dos institutos federais que o tema é importante e essencial e que todos estão em um patamar parecido em buscar iniciativas de melhoria. Aqui, nós optamos em olhar ao menos o que podemos atender para mostrar certo avanço, esse é um caminho melhor do que ficar estagnado. Outra dica é, não contar com apoio do órgão responsável por apoiar as instituições, o mesmo não tem noção da realidade das pontas, nem das dificuldades enfrentadas.

9. CONCLUSÕES

A experiência de implantação do Programa de Privacidade e Segurança da Informação (PPSI) no Instituto Federal Catarinense evidenciou que a proximidade entre os principais atores institucionais — alta administração, diretoria de tecnologia da informação e gestor de segurança — é um fator determinante para o sucesso do processo. A articulação direta com o gabinete do reitor, que garantiu respaldo nas decisões mais críticas e impactantes, foi essencial para superar barreiras estruturais e culturais, além de conferir legitimidade às ações implementadas. Essa relação de confiança e apoio institucional permitiu maior agilidade na tomada de decisões e na formalização de políticas e normativas.

Outro aspecto relevante foi a constância das reuniões semanais entre os envolvidos, que se mostraram fundamentais para o acompanhamento contínuo das etapas de implantação. Esses encontros possibilitaram a reavaliação de riscos, a redefinição de prioridades e o alinhamento estratégico entre os setores, promovendo uma gestão colaborativa e responsiva. A dinâmica estabelecida favoreceu a construção de soluções conjuntas, mesmo diante de limitações operacionais, como escassez de recursos humanos e paralisações, demonstrando que a governança integrada é um diferencial competitivo na administração pública.

Portanto, a trajetória do IFC na implementação do PPSI reforça que a governança eficaz em segurança da informação depende não apenas de diretrizes técnicas e normativas, mas também de uma estrutura organizacional que valorize o diálogo intersetorial e a liderança comprometida. A proximidade entre os gestores e a alta administração, aliada à institucionalização de espaços de decisão e acompanhamento, constitui um modelo replicável para outras instituições públicas que buscam fortalecer sua maturidade digital e garantir a conformidade com os marcos regulatórios vigentes.

Com a publicação e defesa deste trabalho esperamos contribuir para futuras implantações do PPSI em outros órgãos da APF nos colocando a disposição para colaborar sempre que necessário.

10. REFERÊNCIAS

ALMEIDA, Willdson Gonçalves de. Implementação de compliance à LGPD em instituições federais de ensino superior: proposta de um processo estruturado para conformidade. 2024. Dissertação (Mestrado em Engenharia de Produção) – Universidade Federal de São Carlos, São Carlos, 2024.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Painel de Monitoramento de Serviços Federais. Disponível em:https://www.gov.br/governodigital/pt-br/estrategias-e-governanca-

digital/transformacao-digital/central-de-qualidade/painel-de-monitoramento-de-servicos-federaisv2. Acesso em: 03 jun. 2025.

BRASIL. Ministério da Gestão e da Inovação em Serviços Públicos. Portaria SGD/MGI nº 852, de 28 de março de 2023. Dispõe sobre o Programa de Privacidade e Segurança da Informação – PPSI. Diário Oficial da União, Brasília, DF, 30 mar. 2023. Seção 1, p. 92. Disponível em: https://www.in.gov.br/web/dou/-/portaria-sgd/mgi-n-852-de-28-de-marco-de-2023-473750908. Acesso em: 01 jun. 2025.

BRASIL. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética. Diário Oficial da União: seção 1, Brasília, DF, 6 fev. 2020. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm. Acesso em: 10 jun. 2025.

BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação. Diário Oficial da União: seção 1, Brasília, DF, 27 dez. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/d9637.htm. Acesso em: 10 jun. 2025.

BRASIL. Instituto Federal Catarinense. Portaria nº 2151/2023, de 10 de novembro de 2023. Dispõe sobre a vinculação do Setor de Dados à Diretoria Executiva. Disponível em: https://protecaodedados.ifc.edu.br/wp-content/uploads/sites/61/2024/05/Portaria-2151.23-Vinculacao-do-Setor-de-Dados-a-Diretoria-Executiva.pdf. Acesso em: 30 jun. 2025.

BRASIL. Instituto Federal Catarinense. Resolução nº 03/2024 – CONSUPER, de 16 de janeiro de 2024. Aprova o Plano de Desenvolvimento Institucional – PDI 2024–2028 do Instituto Federal Catarinense. Disponível em: https://pdi.ifc.edu.br/wp-content/uploads/sites/80/2024/01/Resolucao-03.2024-IFC-Aprova-PDI-2024-2028-Anexo.pdf. Acesso em: 30 jun. 2025.

BRASIL. Instituto Federal Catarinense. Portaria Normativa nº 4/2024 – ASTEC/REIT, de 24 de junho de 2024. Institui a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR/IFC). Disponível em: https://sig.ifc.edu.br/public/documentos/index.jsp. Acesso em: 30 jun. 2025.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da União: seção 1, Brasília, DF, 15 ago. 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10 jun. 2025.

BRASIL. Ministério da Economia. Secretaria de Governo Digital. Guia de implementação do Framework de Políticas de Segurança da Informação (PSI). Disponível em: https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf. Acesso em: 3 nov. 2024.

CARVALHO, Abraão José de. Transformação digital nas organizações públicas: um estudo de caso na Universidade Federal do Cariri. 2023. Dissertação (Mestrado em Gestão Pública) – Universidade Federal do Rio Grande do Norte, Natal, 2023.

LAKATOS, Eva Maria; MARCONI, Marina de Andrade. Fundamentos de metodologia científica. 5. ed. São Paulo: Atlas, 2003.

SILVA, Gustavo Perroni Gomes da et al. Aplicabilidade do ciclo PDCA na gestão escolar e as potencialidades para a melhoria contínua da qualidade. IOSR Journal of Business and Management, v. 26, n. 4, p. 07-11, 2024. Disponível em: https://www.iosrjournals.org/iosr-jbm/papers/Vol26-issue4/Ser-7/B2604070711.pdf. Acesso em: 29 jul. 2025.

TOMAZ, Lídia Bononi P.; OLIVEIRA, Patrícia Araújo de; GUALBERTO, Éder Souza. Investigação da ferramenta Keycloak na mitigação de incidentes cibernéticos: uma abordagem integrada com o Programa de Privacidade e Segurança da Informação (PPSI). Anais Estendidos do SBSeg 2024: WGID, 2024.