MINISTÉRIO DA EDUCAÇÃO
Secretaria de Educação Profissional e Tecnológica
Instituto Federal de Educação, Ciência e Tecnologia do Ceará
Unidade de Auditoria Interna

RELATÓRIO DE AUDITORIA INTERNA Nº 04/2023-13

Senhor Reitor,
Senhores Diretores Gerais dos Campi Acaraú, Baturité e Crato,
Senhor Pró-Reitor de Gestão de Pessoas,
Senhor Diretor da Diretoria de Gestão de Tecnologia da Informação,

Com a finalidade de atender aos trabalhos da Unidade de Auditoria Interna – AUDIN, referente à Ação Nº 13 – PAINT de 2023 – Análise dos riscos relativo ao processo Manutenção da Infraestrutura Física e Lógica, ação esta que se justifica pelo alto risco identificado pela matriz de riscos da Audin, e no anseio de dar suporte a essa gestão, evidenciam-se os mais relevantes achados e, consequentemente, apresentam-se recomendações à luz dos diplomas legais, a fim de que as irregularidades e/ou impropriedades encontradas sejam sanadas e que as boas práticas sejam reconhecidas e tomadas como referências para a Gestão e Governança do Instituto Federal de Educação, Ciência e Tecnologia do Ceará.

I) ESCOPO DOS EXAMES

Os órgãos de controle do governo, a exemplo da Controladoria Geral da União – CGU, pedem cada vez mais aos auditores internos governamentais que ampliem a variedade das auditorias operacionais e incluam trabalhos que tenham foco prospectivo ou ofereçam orientações, informações sobre boas práticas ou, ainda, informações sobre temas que afetem os macroprocessos da instituição. Nesse contexto, a equipe de auditoria realizou um serviço de avaliação, dos tipos conformidade e operacional, o qual se caracteriza pela obtenção e análise de evidências para fornecer opiniões ou conclusões independentes e objetivas sobre um objeto de auditoria.

Dada a importância e complexidade das atividades desenvolvidas pela Diretoria de Gestão de Tecnologia da Informação do IFCE – DGTI para promover a política de uso da Tecnologia da Informação, planejando, coordenando, supervisionando, e por dar assistência aos demais setores do IFCE, o presente trabalho se propõe a apresentar um diagnóstico da gestão de segurança da informação no IFCE, utilizando por base a normatização vigente do Gabinete de Segurança da Informação da Presidência da República, como também as boas práticas de segurança da informação existentes.

Portanto, com base na matriz de controle elaborada após a análise das atividades relevantes para o atingimento das metas do PDI 2019-2023, referente à DGTI, e após o levantamento dos riscos de controle e residual das atividades do processo **Manutenção da Infraestrutura Física e Lógica**, objeto desta ação de auditoria, identificou-se como principais riscos associados: a fragilidade no armazenamento das informações relevantes e na segurança da informação.

Para realizar as análises, a equipe de auditoria realizou reuniões com o Coordenador da Coordenadoria de Infraestrutura e Redes de Computadores – COIR, com o Chefe do Departamento de Governança de TI e com o Diretor da DGTI. Também foram enviadas solicitações de auditoria à DGTI, ao Comitê Gestor de Segurança da Informação do IFCE, à Coordenadoria de Monitoramento das Leis de Acesso à Informação e Proteção de Dados, e, também, aos *campi*.

II) VERIFICAÇÃO

Os objetivos dessa Ação de Auditoria foram:

1) Verificar as deficiências nos controles internos aplicados ao processo de Manutenção da Infraestrutura Física e Lógica;
2) Verificar o atingimento das metas do PDI 2019-2023 quanto aos indicadores "Taxa de tickets gerados em serviços críticos" e "Satisfação do usuário em relação aos serviços ofertados";
3) Analisar a capacidade técnica e operacional das Coordenações de TI nos *campi* do IFCE;
4) Analisar a implantação da Política de Segurança da Informação do IFCE – PSI, bem como a sua adequação aos normativos vigentes;
5) Analisar os mecanismos de gestão da segurança da informação no IFCE à luz dos normativos vigentes;
6) Verificar a adequação dos equipamentos de backup do data center.

III) LIMITAÇÕES

Não houve limitações aos trabalhos da Audin.

IV) CONSTATAÇÕES

Segue relato das constatações identificadas pela equipe de auditoria.

1. ÁREA: Gestão Operacional

1.1 SUBÁREA: Controles da Gestão

1.1.1 ASSUNTO: Gestão da Segurança da Informação

1.1.1.1 CONSTATAÇÃO: Desconhecimento da PSI pelos colaboradores do IFCE.

Em resposta à Solicitação de Auditoria Interna nº 04 – e-Aud 1459941, o Diretor da DGTI informou que a Política de Segurança da Informação – PSI do IFCE é disponibilizada no portal da Instituição, através do link https://ifce.edu.br/dgti/governanca/arquivo/resolucao-posic.pdf/view (Resolução nº 1 Política de Segurança da Informação).

Apesar da PSI estar disponível no site da instituição, isso não garante o seu conhecimento pelos colaboradores, havendo a necessidade de campanhas de divulgação, explicação e conscientização para a efetiva implantação da política. O sucesso na implantação de políticas envolve questões culturais e comportamentais dos servidores, assim a melhor maneira para a institucionalização de uma política de segurança é capacitando os usuários sobre a importância do tema, tanto no ambiente organizacional como no residencial, uma vez que o tele trabalho já é uma realidade da instituição.

Em reunião realizada no dia 23/05/2023, o Diretor da DGTI mostrou preocupação com a segurança da informação em termos que os colaboradores não estão capacitados. Na ocasião, o Diretor apresentou uma possível solução: realizar capacitação dos servidores quanto ao tema segurança da informação na forma de cursos curtos oferecidos pela DGTI. Contudo, ainda não há concretização.

A constatação contraria o disposto na PSI do IFCE:

> Art. 8º As Diretrizes Básicas da Política de Segurança da Informação devem ser divulgadas na Unidade Organizacional, garantindo que todos tenham consciência da política e a pratiquem na organização.
>
> Parágrafo único. Todos os colaboradores devem obedecer ao disposto nas Diretrizes Básicas da Política de Segurança da Informação, recebendo as informações necessárias para o seu adequado cumprimento.

Sobre a capacitação dos colaboradores, a PSI ainda traz:

> Art. 9º Os colaboradores devem ser continuamente capacitados para o uso dos ativos de informação quando da realização de suas atividades.
>
> Art. 10. Programas de conscientização sobre segurança da informação serão implementados através de treinamentos específicos, assegurando que todos os colaboradores sejam informados sobre os potenciais riscos de segurança e o tipo de exposição a que estão submetidos os sistemas de informações e operações do IFCE e suas partes interessadas.

A Instrução Normativa nº 01/2020/GSI/PR estabelece no art. 10, Parágrafo único, que:

> Parágrafo único. Cabe ao Gestor de Segurança da Informação promover, com apoio da alta administração, a ampla divulgação da Política, das normas internas de segurança da informação e de suas atualizações, de forma ampla e acessível, a todos os servidores, aos usuários e aos prestadores de serviço, a fim de que esses tomem conhecimento de tais instrumentos.

Dessa forma, a Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:

"Referente à questão levantada durante a auditoria interna sobre a Manutenção da Infraestrutura Física e Lógica da área de TI do IFCE, gostaria de compartilhar minha concordância com a constatação apresentada. A análise apontou corretamente a existência de um desconhecimento generalizado da Política de Segurança da Informação (PSI) por parte dos colaboradores do IFCE. Embora a PSI esteja disponível no portal da instituição, a mera disponibilidade não garante o seu efetivo conhecimento e prática por parte dos membros da comunidade acadêmica. É evidente que a implementação bem-sucedida de políticas de segurança da informação requer uma abordagem abrangente que vá além da simples divulgação. Concordo com a necessidade de campanhas de conscientização e capacitação para promover a compreensão da importância da segurança da informação. Tais medidas não apenas são fundamentais para o ambiente organizacional, mas também se estendem ao contexto residencial, considerando a realidade do teletrabalho no âmbito da instituição. É compreensível que a institucionalização de uma política de segurança da informação seja um desafio que envolve aspectos culturais e comportamentais dos servidores. A abordagem proposta pelo Diretor da DGTI, que sugere a realização de cursos curtos oferecidos pela DGTI, é uma iniciativa positiva que visa preencher essa lacuna. No entanto, compreendo que a DGTI enfrenta limitações de pessoal para elaborar e ministrar tais treinamentos de forma abrangente. Além disso, concordo com a sua observação de que, mesmo que os treinamentos sejam elaborados, a falta de um mecanismo que obrigue os servidores a participar pode limitar a eficácia dessas ações. A conscientização e adesão à política de segurança da informação devem ser uma responsabilidade compartilhada entre diferentes áreas da instituição. No sentido de abordar esse desafio de maneira mais abrangente, é louvável que a DGTI tenha tomado a iniciativa de enviar ofícios à PROGEP e CREAD para elaborar uma estratégia conjunta de conscientização. Essa abordagem colaborativa e multidisciplinar é um passo importante para garantir que a implementação da política de segurança da informação seja abrangente, eficaz e alinhada às diretrizes institucionais. Acredito que uma abordagem combinada, envolvendo a DGTI, PROGEP, CREAD, Comunicação e outras partes interessadas, seja essencial para promover a conscientização e capacitação necessárias para a segurança da informação. Afinal, a segurança cibernética é uma preocupação global que impacta a todos nós, e a colaboração interdepartamental é fundamental para enfrentar esses desafios de maneira eficaz."

ANÁLISE DA AUDITORIA: A Audin mantém a recomendação 001.

RECOMENDAÇÃO 001 – [DGTI]: Recomenda-se à DGTI que elabore um plano de capacitação (com definição de datas, responsáveis e público alvo) para os colaboradores

da instituição (servidores, estagiários, funcionários terceirizados e outros que de qualquer modo acessem os dados institucionais) sobre o tema segurança da informação. E em paralelo, promova campanhas para divulgar a Política de Segurança da Informação – PSI do IFCE nos campi e Reitoria.

1.1.1.2 CONSTATAÇÃO: Política de Segurança da Informação – PSI não aplicada no IFCE.

Das análises da equipe de auditoria evidenciadas nas respostas às Solicitações de Auditoria nº 04 (e-Aud 1459941) e nº 35 (SEI 5024515), verificou-se que a Política de Segurança da Informação do IFCE não é aplicada na instituição. Constatou-se as seguintes fragilidades: 1. Desconhecimento da PSI pelos colaboradores; 2. Falhas de segurança não são comunicadas ao Comitê Gestor de Segurança da Informação; 3. Os acessos à rede de dados do IFCE não são gerenciados em todos os tipos de Conexão; 4. Nem toda informação veiculada eletronicamente pelo colaborador dentro da instituição é controlada e monitorada; 5. Não há na instituição mecanismos para garantir o uso responsável dos recursos computacionais; 6. Falhas no controle de acesso físico ao datacenter fragilizado; e 7. Ausência de controle de responsabilidade dos colaboradores.

Todas as fragilidades citadas afrontam aos princípios estabelecidos na PSI do IFCE, principalmente, os arts. 9º, 10, 13, 16, 18, 20, 21-I, 21-II.

De acordo com a PSI, § único do art. 13, o Comitê Gestor de Segurança da Informação deve ser comunicado de qualquer violação na segurança da informação, mas não é o que ocorre na prática. Em resposta à Solicitação de Auditoria Interna nº 04 – e-Aud 1459941, o Diretor da DGTI informou que: *"Parte das violações referentes à segurança da informação são registradas na plataforma de atendimento do Centro de Atendimento a Incidentes de Segurança - CAIS, contudo o IFCE não dispõe de plataforma própria, nem de equipe para tratamento em específico. As violações são analisadas periodicamente, porém não são comunicadas a nenhuma unidade posterior."* Verifica-se que não há um processo formal de comunicação e tratamento das violações de segurança. Esse ponto da PSI poderá ser atingido quando da instituição da Equipe de Tratamento e Resposta a Incidentes Cibernéticos, conforme a IN 02/2020/GSI/PR.

Em relação aos acessos à rede wifi não serem gerenciados, em resposta à Solicitação de Auditoria Interna nº 04 – e-Aud 1459941, o Diretor da DGTI informou que: *"O atendimento de identificação é parcial pois em alguns campi o acesso a rede wifi não é autenticado. Acessos remotos à infraestrutura de TI são validados com logins e senha, e o acesso de todos os sistemas são autenticados pelo AD Único da Instituição."*

Frisa-se que há vulnerabilidade nas conexões wifi não autenticadas, assim, o ideal é que os acessos à rede wifi sejam autenticados por usuário, caso seja inviável, que seja criada

senha de acesso. Uma política de gestão de senhas e controle de acessos também possibilitam maior segurança da rede.

Para garantir a segurança do ambiente digital, é importante implementar uma estratégia robusta de cibersegurança que inclua autenticação de dois fatores, bem como outras medidas seguras. Mesmo que haja certa complexidade no uso dessas ferramentas e tecnologias, as vantagens que elas proporcionam quanto à prevenção de ataques e acessos indevidos são inúmeras.

Também foi informado pelo Diretor da DGTI, em resposta à Solicitação de Auditoria Interna nº 04 – e-Aud 1459941, que: *"Não existem atualmente controles para servidores, no entanto, durante os processos de contratações é previsto assinatura do aceite das cláusulas de confidencialidade presentes no termo de referência."*

Ante o exposto, verifica-se o não cumprimento da PSI quanto à existência de controle de responsabilidade dos colaboradores, embora a PSI traga anexo de responsabilidade, este não é aplicado na instituição.

Dessa forma, a Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:
"Em resposta às recomendações apresentadas pela auditoria, queremos informar que a Diretoria de Gestão de Tecnologia da Informação (DGTI) do IFCE acata plenamente as recomendações e está empenhada em garantir a segurança e a integridade dos recursos de tecnologia da informação da instituição. Recomendação 002 - Comunicação de Violações de Segurança: A DGTI reconhece a importância de uma comunicação eficaz das violações de segurança da informação. Estamos comprometidos em estabelecer um fluxograma claro para a comunicação dessas violações ao Comitê de Segurança da Informação do IFCE, conforme a Política de Segurança da Informação (PSI) vigente. Recomendação 003 - Normas para Autenticação de Conexões Wifi: Entendemos a necessidade de padronizar a autenticação de conexões wifi em toda a rede do IFCE, incluindo Reitoria e campi. Estamos dedicados a desenvolver normas internas que estabeleçam diretrizes claras para a autenticação de conexões wifi, visando aprimorar a segurança e a acessibilidade em toda a rede. A DGTI pretende implementar esta funcionalidade na rede sem fio da Reitoria (com a estrutura atual de equipamentos), normatizar o serviço junto aos campi, repassar e divulgar esse processo (e normativo) aos servidores. Ressalto ainda que a RNP possui um serviço chamado EDUROAM (https://www.rnp.br/servicos/eduroam) que visa justamente prover uma conexão de rede sem fio, segura e transparente. Necessário criar documento normativo. Recomendação 004 - Política de Gestão de Senhas e Controle de Acessos: A colaboração entre a DGTI e o Comitê de Segurança da Informação é fundamental para estabelecer uma Política de Gestão de Senhas e Controle de Acessos abrangente e

eficaz. Estamos comprometidos em trabalhar em conjunto para criar essa política, visando aprimorar a segurança do IFCE em relação às práticas de autenticação e controle de acesso. Ressaltamos que todas as recomendações serão cuidadosamente endereçadas à Comissão de Segurança Digital do IFCE para elaboração, revisão, aprovação e implementação adequada. A DGTI irá elaborar um documento normativo definindo controle de acessos físicos e política de gestão de senhas. RECOMENDAÇÃO 005 – [DGTI]: Em relação à recomendação apresentada pela auditoria, a Diretoria de Gestão de Tecnologia da Informação (DGTI) do IFCE agradece pelo feedback valioso e compartilha o compromisso de fortalecer a segurança da informação em toda a instituição. Recomendação 005 - Implantação do Termo de Responsabilidade: Reconhecemos a importância de estabelecer um Termo de Responsabilidade como documento obrigatório para os colaboradores do IFCE. Esse termo garantirá o uso responsável dos recursos computacionais, alinhando-se à Política de Segurança da Informação (PSI) e promovendo a conscientização sobre as boas práticas de segurança. Gostaríamos de informar que já iniciamos um processo de colaboração com a Pró-Reitoria de Gestão de Pessoas (PROGEP) para explorar maneiras de envolver ainda mais os servidores na política de segurança da informação. A integração das ações de TI e recursos humanos é fundamental para alcançar os melhores resultados. Nesse contexto, a sugestão de implantação do Termo de Responsabilidade será discutida e acrescentada à pauta de nossas próximas reuniões conjuntas. Estamos comprometidos em trabalhar de forma proativa para implementar essa medida em conjunto com a PROGEP, buscando o envolvimento efetivo de todos os colaboradores na promoção de um ambiente seguro e consciente em relação à segurança da informação. Agradecemos mais uma vez pela contribuição da auditoria e estamos ansiosos para avançar em direção a um ambiente digital seguro e colaborativo."

ANÁLISE DA AUDITORIA: A Audin mantêm as recomendações 002, 003, 004 e 005.

RECOMENDAÇÃO 002 – [DGTI]: Recomenda-se à DGTI estabelecer fluxograma para a comunicação das violações de segurança da informação ao Comitê de Segurança da Informação do IFCE, em atendimento à PSI do IFCE.

RECOMENDAÇÃO 003 – [DGTI]: Recomenda-se à DGTI criar normas internas para normatizar a autenticação de conexões wifi em toda rede do IFCE, Reitoria e campi.

RECOMENDAÇÃO 004 – [DGTI]: Recomenda-se à DGTI em colaboração com o Comitê de Segurança da Informação criar Política de Gestão de Senhas e Controle de Acessos no âmbito do IFCE.

RECOMENDAÇÃO 005 – [DGTI]: Recomenda-se à DGTI, com o apoio da PROGEP, implantar o Termo de Responsabilidade, Anexo da PSI, como documento obrigatório a ser respondido pelos colaboradores do IFCE, no ato da assinatura do termo de posse, termo contratual ou outro instrumento que regulamente o vínculo do

colaborador com a instituição, para garantir o uso responsável dos recursos computacionais na instituição.

1.1.1.3 CONSTATAÇÃO: Ausência de normas internas de TI que viabilizem a implantação da PSI.

Em resposta à Solicitação de Auditoria Interna nº 04 – e-Aud 1459941, o Diretor da DGTI informou que não há normas internas de TI que viabilizem a implantação da PSI. A constatação contraria ao disposto na PSI do IFCE:

> Art. 31. Fica a DGTI autorizada a regulamentar, e submeter à Reitoria do IFCE para aprovação, os procedimentos necessários para a aplicação das disposições estabelecidas nesta Norma que estarão consubstanciadas na norma interna que regulamenta o uso de equipamentos de informática, de sistemas de informação, da rede de comunicações e de continuidade do negócio do IFCE.

A Instrução Normativa nº 01/2020/GSI/PR afirma que:

> § 2º A Política de Segurança da Informação, quando necessário, deve ser complementada por normas, metodologias e procedimentos.

Esta Unidade de Auditoria Interna entende que a PSI do IFCE não é completa havendo, portanto, a necessidade da edição de normas internas para a concretização dos procedimentos e dos controles necessários para o alcance das diretrizes presentes na PSI, a exemplo do Plano de Continuidade do Negócio, Política de Backup, Acordos de Nível de Serviço e inventário atualizado dos ativos de informação.

Dessa forma, a Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:
"Concordo plenamente com as observações apresentadas na auditoria interna quanto à insuficiência da equipe de TI para a adequada implantação da Política de Segurança da Informação (PSI) no âmbito do IFCE. Reconheço que, apesar dos conhecimentos técnicos presentes na equipe, a falta de recursos humanos dedicados especificamente às demandas de segurança da informação é um desafio substancial. A equipe da Coordenação de Infraestrutura e Redes (COIR) possui um conhecimento valioso na área de segurança da informação. No entanto, as diversas prioridades, incluindo Infraestrutura de TI, Comunicação e Suporte, tornam difícil concentrar esforços suficientes nas atividades de segurança. O volume de notificações do Centro de Atendimento a Incidentes de Segurança (CAIS), notificações externas, a necessidade de capacitações na comunidade acadêmica e a administração de serviços de segurança, como firewall e IDS, evidenciam a importância de contar com uma equipe de segurança dedicada. A situação fica ainda mais desafiadora devido à falta de uma

Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) instituída no âmbito do IFCE, o que está em discordância com as orientações normativas federais. Isso enfraquece a área de segurança da informação da instituição, aumentando a vulnerabilidade a incidentes cibernéticos. Dada a natureza das circunstâncias, é essencial que se busque uma solução adequada para atender às exigências da PSI e às diretrizes normativas. Reconhecendo o déficit de recursos humanos especializados e considerando a realidade operacional da DGTI, estamos empenhados em adotar medidas para mitigar essa deficiência. Uma estratégia que estamos explorando é a realização de um edital de trabalho remoto (ETR) para atrair profissionais qualificados na área de segurança da informação. Esse passo é vital para compor uma equipe dedicada às demandas de segurança e, assim, cumprir as diretrizes da PSI e da normativa federal. Porém, é importante ressaltar que mesmo com essa iniciativa, o déficit de recursos humanos especializados é um desafio persistente. Estamos comprometidos em implementar a solução mais viável, considerando as limitações atuais, e continuaremos a advogar por recursos adicionais para compor uma equipe de segurança da informação competente e eficaz, que possa garantir a proteção e integridade dos sistemas e dados institucionais."

ANÁLISE DA AUDITORIA: A Audin mantém a recomendação 006.

RECOMENDAÇÃO 006 – [DGTI]: Recomenda-se à DGTI editar normas internas que visem a implantação das diretrizes estabelecidas na Política de Segurança da Informação do IFCE.

1.1.1.4 Equipe de TI insuficiente para implantação da PSI.

Em resposta à Solicitação de Auditoria Interna nº 04 – e-Aud 1459941, o Diretor da DGTI informou que: *"A Diretoria tem servidores com conhecimento na área de segurança, mas os recursos humanos são insuficientes para que se dediquem com o mínimo necessário para as demandas de segurança existentes. O ideal seria que existisse um setor específico para tratar dos aspectos de segurança. Não possuímos servidores focados em ações operacionais de segurança, nem a nível operacional, nem de gestão. Considerando o volume de notificações que recebemos do Centro de Atendimento a Incidentes de Segurança - CAIS, notificações externas, capacitações a serem realizadas na comunidade acadêmica, serviços de segurança que precisam ser administrados, tais como, firewall, IDS, etc, seria necessário pelo menos 5 (cinco) servidores focados na área de segurança."*

Questionado sobre as ações de capacitação na área de segurança da informação realizadas pelos servidores de TI, o Diretor da DGTI informou que foram realizados cursos de formação na Escola Nacional de Redes por 4 (quatro) servidores da Coordenação de Infraestrutura e Redes – COIR em 2022 e que há 2 (dois) servidores matriculados para 2023, conforme abaixo:

Cursos Realizados em 2022:

Valber Jones de Castro - 23255.003588/2022-81 – Curso: Correlacionamento de eventos com Graylog: 30/05/2022 a 10/07/2022 (Modalidade EaD) - ESR EaD;

Antonio Alexandre Barboza de Paula - 23255.003588/2022-81 – Curso: Segurança de Redes e Sistemas (EaD): 31/10/2022 a 18/12/2022 (Modalidade EaD) - ESR EaD;

Alexandre Magno Cavalcante Sucupira - 23255.007947/2022-79 – Curso: Hardening em Linux (EaD): 07/11/2022 a 18/12/2022 (Modalidade EaD) - ESR EaD;

Mário César de Oliveira Luz - 23255.007947/2022-79 – Curso: Cibersegurança EaD (parceria oficial Ascend): 17/10/2022 a 04/12/2022 (Modalidade EaD) - ESR EaD.

Cursos a serem realizados em 2023:

Larissa Kelly Santos Carvalho – Curso: Fundamentos de Segurança da Informação EaD (parceria oficial Ascend): 17/07/2023 a 27/08/2023 (Modalidade EaD) - ESR EaD;

Aldísio Gonçalves Medeiros – Curso: PenTest EaD (parceria oficial Ascend): 25/09/2023 a 12/11/2023 (Modalidade EaD) - ESR EaD.

Constata-se que a equipe da Coordenação de Infraestrutura e Redes – COIR, apesar de possuir conhecimento técnico na área de segurança da informação, não consegue se dedicar especificamente aos assuntos de segurança, pois há outras demandas que são priorizadas, como Infraestrutura de TI, Comunicação e Suporte, uma vez que refletem diretamente na continuidade dos serviços.

Contudo, a segurança da informação fica fragilizada quando não há equipe para cuidar da pauta. A COIR conta com 5 (cinco) servidores, número esse que atende a todos os serviços de Infraestrutura de TI, Comunicação e Suporte, portanto, verifica-se uma necessidade de ampliação da força de trabalho para compor uma equipe de segurança da informação.

A Instrução Normativa nº 01/2020/GSI/PR, atualizada pela IN nº 02/2020/GSI/PR estabelece a instituição de equipe de tratamento de incidentes no âmbito dos órgãos da Administração Pública Federal:

> Art. 15. Além das obrigações já dispostas nesta Instrução Normativa, compete aos órgãos e às entidades da administração pública federal, direta e indireta, em seu âmbito de atuação:
>
> IV - instituir e implementar Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos - ETIR, que constituirá a rede de equipes, integrada pelos órgãos e pelas entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo do Gabinete de Segurança Institucional da Presidência da República; " (NR)

Em resposta à Solicitação de Auditoria Interna nº 05 – e-Aud 1459941 foi informado pelo Chefe do Departamento de Governança de TI que não existe Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR instituída no âmbito do IFCE.

A constatação apresenta a discordância com orientações normativas federais, fragilizando a área de segurança da informação da instituição.

Dessa forma, a Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que: [Mesma manifestação da recomendação 006].

ANÁLISE DA AUDITORIA: A Audin mantêm as recomendações 007 e 008.

RECOMENDAÇÃO 007 – [DGTI]: Recomenda-se à DGTI designar servidores de TI para constituir setor específico para tratar da segurança da informação no âmbito do IFCE.

RECOMENDAÇÃO 008 – [DGTI]: Recomenda-se à DGTI instituir e implantar Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR nos termos da IN nº 01/2020/GSI/PR e da IN nº 02/2020/GSI/PR.

1.1.1.5 CONSTATAÇÃO: Desconformidade da Política de Segurança da Informação – PSI com a IN 01/2020/GSI.

Foi realizado pela equipe de auditoria o cotejamento entre a Política de Segurança da Informação do IFCE e os requisitos mínimos que devem ser observados na política, conforme dispõe o art. 12 da Instrução Normativa nº 01/2020/GSI/PR. Das análises, identificou-se algumas fragilidades na PSI, principalmente, quanto aos requisitos:

Segurança Física e do Ambiente – O Art. 21 da PSI afirma apenas que serão criados controles para prevenir acesso físico indevido e para que os colaboradores entendam suas responsabilidades. No entanto, a IN 01/2020, art. 12, frisa que é necessário definir as diretrizes para a implementação da segurança física e de ambiente. Portanto, é necessária uma melhor definição dessas diretrizes, como por exemplo, a definição dos ambientes que requerem controles de restrição de acesso.

Gestão do Uso dos Recursos Operacionais e de Comunicações – Art.17, Art. 20, Anexo I – Termo de Responsabilidade. A PSI traz em anexo um termo de responsabilidade para assinatura do colaborador e do representante de recursos humanos, mas não traz quando e como esse termo será cobrado dos colaboradores. Verificou-se que a PSI não aborda o tema computação em nuvem, entretanto, grande

parte dos dados e informações institucionais estão na computação em nuvem. Portanto, a PSI deverá ser atualizada para incluir diretrizes quanto a esse tema.

Controles de Acesso – O art. 18 da PSI traz que os acessos à rede de dados do IFCE são gerenciados e os colaboradores devem ser identificados e ter acesso apenas às informações e aos recursos tecnológicos necessários ao desempenho de suas atividades. O Art. 21, I, afirma apenas que serão criados controles para prevenir acesso físico indevido e sem autorização. Contudo, a PSI não traz diretrizes sobre controles de acesso aos sistemas (autenticação, autorização e auditoria).

Gestão de Riscos – Não há dispositivos na PSI sobre Gestão de Riscos.

Gestão de Continuidade – O Art. 22 da PSI traz que os procedimentos que garantam a continuidade e a recuperação do fluxo de informações devem ser mantidos, mas não define que procedimentos são esses, ou quando e onde serão definidos. A PSI também não aborda sobre a elaboração do Plano de continuidade do negócio, do Plano de Contingências e da Política de Backup, instrumentos que correspondem à gestão de continuidade.

Política de atualização – Art. 36 – O artigo diz que a PSI será revisada periodicamente, mas não definiu o prazo como determina a IN 01/2020/GSI/PR: art. 12, VII, "§ 1º A periodicidade para a revisão da Política de Segurança da Informação não deve exceder 4 (quatro) anos." Considerando que a data da PSI do IFCE é de 14 de janeiro de 2020, conforme Resolução nº 01/CONSUP, já se faz necessária à sua revisão, pois aproxima-se o prazo de 4 anos estabelecido na IN 01/2020/GSI/PR.

Dessa forma, a Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:
"Concordamos com as observações apontadas pela equipe de auditoria em relação à Política de Segurança da Informação (PSI) do IFCE, especialmente no que diz respeito às inconformidades identificadas em relação aos requisitos estabelecidos na Instrução Normativa nº 01/2020/GSI/PR. É essencial garantir que a PSI esteja em total conformidade com as diretrizes estabelecidas pela normativa federal para assegurar a integridade, confidencialidade e disponibilidade das informações institucionais. As fragilidades apontadas, tais como a ausência de diretrizes claras sobre segurança física e de ambiente, gestão do uso de recursos operacionais e de comunicações, controles de acesso, gestão de riscos, gestão de continuidade e política de atualização, requerem uma ação imediata para aprimorar e fortalecer nossa abordagem de segurança da informação. Comprometo-me a encaminhar essas questões ao Comitê de Segurança da Informação, que foi responsável pela elaboração da PSI. O comitê será convocado a revisar as observações apresentadas pela auditoria, a fim de propor as medidas corretivas necessárias para alinhar a PSI às diretrizes da Instrução Normativa

nº 01/2020/GSI/PR. A revisão da PSI será conduzida com a máxima prioridade, e todos os pontos mencionados pela equipe de auditoria serão abordados para garantir que a política atenda plenamente aos requisitos estabelecidos. Além disso, considerando a proximidade do prazo de quatro anos para a revisão, conforme estabelecido na normativa federal, nos comprometemos a concluir a atualização da PSI dentro desse período."

ANÁLISE DA AUDITORIA: A Audin mantém a recomendação 009.

RECOMENDAÇÃO 009 – [DGTI]: Recomenda-se à DGTI em colaboração com o Comitê de Tecnologia da Informação do IFCE que atualizem a Política de Segurança da Informação do IFCE em observância aos requisitos mínimos exigidos pela IN 01/2020/GSI/PR (art. 12), principalmente, nos seguintes tópicos: 1. Segurança Física e do Ambiente – definir controles de segurança física e lógica e definir os ambientes que requerem controles de restrição de acesso; 2. Gestão do Uso dos Recursos Operacionais e de Comunicações – definir diretrizes sobre computação em nuvem; 3. Controles de Acesso – definir diretrizes sobre controles de acesso aos sistemas (autenticação, autorização e auditoria); 4. Gestão de Riscos – definir diretrizes sobre a gestão de riscos; 5. Gestão de Continuidade – definir diretrizes para a elaboração do Plano de continuidade do negócio, do Plano de Contingências e da Política de Backup; e 6. Política de atualização – definir a periodicidade de atualização da PSI, não superior à 4 (quatro) anos.

1.1.1.6 CONSTATAÇÃO: Desconformidade entre a gestão de segurança da informação do IFCE e a Instrução Normativa nº 03/2021/GSI.

Além das fragilidades nos requisitos mínimos da Política de Segurança da Informação, constata-se que o IFCE não possui Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR. Em resposta à Solicitação de Auditoria Interna nº 05 – e-Aud 1459941, foi informado pelo Chefe do Departamento de Governança de TI que não existe a equipe supracitada instituída no âmbito do IFCE.

Ainda em resposta à Solicitação de Auditoria Interna nº 05 – e-Aud 1459941, foi informado pelo Chefe do Departamento de Governança de TI que não há, no âmbito do IFCE, processos estabelecidos sobre mapeamento de ativos de informação, gestão de riscos de segurança da informação, gestão de continuidade de negócios em segurança da informação, gestão de mudanças nos aspectos de segurança da informação e avaliação de conformidade de segurança da informação.

Esses processos são tratados na Instrução Normativa nº 03/2021/GSI/PR e são de observância obrigatória pelos órgãos e entidades da administração pública federal. Portanto, conforme o art. 3º da referida IN:

> Art. 3º A gestão de segurança da informação será constituída pelos seguintes processos de realização obrigatória pelos órgãos e pelas entidades da administração pública federal:
> I - mapeamento de ativos de informação;
> II - gestão de riscos de segurança da informação;
> III - gestão de continuidade de negócios em segurança da informação;
> IV - gestão de mudanças nos aspectos de segurança da informação; e
> V - avaliação de conformidade de segurança da informação.

A constatação apresenta a discordância com orientações normativas federais, fragilizando a área de segurança da informação da instituição.

Dessa forma, a Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Não houve manifestação do gestor para essa constatação.

ANÁLISE DA AUDITORIA: A Audin mantém a recomendação 010.

RECOMENDAÇÃO 010 – [DGTI]: Recomenda-se à DGTI em colaboração com o Comitê de Segurança da Informação do IFCE e com o Gestor de Segurança da Informação do IFCE que instituam a gestão de segurança da informação no âmbito da instituição por meio da constituição dos processos de mapeamento de ativos de informação, de gestão de riscos de segurança da informação, de gestão de continuidade de negócios em segurança da informação, de gestão de mudanças nos aspectos de segurança da informação e de avaliação de conformidade de segurança da informação, de acordo com a IN 03/2021/GSI/PR.

1.1.2 ASSUNTO: Gestão da computação em nuvem

1.1.2.1 CONSTATAÇÃO: Ausência de ato normativo interno sobre o uso seguro de computação em nuvem.

Em resposta à Solicitação de Auditoria Interna nº 05 – e-Aud 1459941 foi informado pelo Chefe do Departamento de Governança de TI que não há ato normativo interno do IFCE sobre o uso seguro de computação em nuvem, mas que vem sendo realizada diversas análises quanto aos atuais ambientes de infraestrutura em uso para migração ou não dos mesmos para plataformas de nuvem (conforme pede a IN Nº 5, DE 30 DE AGOSTO DE 2021), porém sem nenhum registro formal dessa ação.

Verifica-se com essa situação o não atendimento ao disposto na Instrução Normativa n º 05/2021/GSI/PR:

> Art. 4º Todos os órgãos ou as entidades, que desejarem utilizar computação em nuvem, deverão editar, obrigatoriamente, um ato normativo sobre o uso seguro de computação em nuvem.

> Art. 5º O ato normativo sobre o uso seguro de computação em nuvem deverá, no mínimo:
> I - ser elaborado com base na política de segurança da informação do órgão ou da entidade;
> II - ser homologado pela alta administração e divulgado a todas as partes interessadas;
> III - relacionar as metas a serem alcançadas e os objetivos que regem o serviço de computação em nuvem;
> IV - definir as funções e as responsabilidades dos agentes designados para o gerenciamento dos serviços de computação em nuvem; e
> V - estabelecer a periodicidade para sua revisão, a qual não deve exceder dois anos.
> Parágrafo único. A revisão do ato normativo previsto no caput poderá ocorrer a qualquer tempo, quando houver mudanças significativas nos requisitos de segurança da informação que influenciem o uso seguro de computação em nuvem, de forma a assegurar sua continuidade, sustentabilidade, adequação e efetividade.
> Art. 6º O órgão ou a entidade deverá instituir uma equipe para elaboração e revisões do ato normativo sobre o uso seguro de computação em nuvem.

Portanto, a Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:

"Compreendemos a recomendação apresentada pela Auditoria Interna referente à instituição da gestão de segurança da informação no âmbito do IFCE, especialmente no que diz respeito à utilização segura da computação em nuvem, de acordo com a Instrução Normativa nº 05/2021/GSI/PR. Após uma avaliação detalhada da situação e considerando a atual realidade operacional da Diretoria de Gestão de Tecnologia da Informação (DGTI), gostaríamos de compartilhar nossa visão a respeito dessa recomendação. Embora compreendamos a importância teórica da criação de um ato normativo interno sobre o uso seguro da computação em nuvem, acreditamos que, do ponto de vista prático, a implementação dessa medida poderia ter impactos limitados no processo geral de segurança da informação da instituição. A nossa equipe da Coordenação de Infraestrutura e Redes (COIR), responsável pela gestão dos recursos de computação em nuvem, é composta por apenas 4 servidores, os quais já enfrentam um volume significativo de demandas relacionadas ao uso desses recursos. Cada um desses servidores passou por treinamentos abrangentes nas melhores práticas de segurança e recebe assessoria contínua de especialistas da empresa fornecedora dos serviços de nuvem. Além disso, a COIR é diretamente responsável por assegurar a segurança e eficácia dos ambientes de nuvem em uso pela instituição. Dado o contexto operacional atual, acreditamos que a criação do ato normativo interno demandaria recursos humanos consideráveis, recursos estes que são limitados e já estão comprometidos com as tarefas operacionais de gestão da infraestrutura e segurança existentes. A equipe atual da COIR já trabalha arduamente para assegurar que todas as práticas e procedimentos estejam em conformidade com as diretrizes de segurança

da informação. Nesse sentido, considerando que nossa equipe de especialistas já possui um alto nível de treinamento e está constantemente assessorada por profissionais da empresa de serviços de nuvem, acreditamos que a criação desse ato normativo interno poderia não ter um impacto significativo na qualidade do processo, podendo até mesmo consumir recursos que atualmente são escassos. Portanto, nossa visão é de que, dada a situação descrita, a implementação dessa recomendação poderia ser considerada não produtiva e, em última análise, não agregaria um valor substancial ao processo existente."

ANÁLISE DA AUDITORIA: A Audin compreende a realidade de escassez de pessoal na DGTI do IFCE, tornando desafiador para os servidores o desenvolvimento das atividades diárias e o cumprimento de determinações dos órgãos de controle. Contudo, considerando que a edição de normativo interno sobre a computação em nuvem não é apenas uma boa prática, mas uma obrigação normativa, a Audin mantém a recomendação 011.

RECOMENDAÇÃO 011 – [DGTI]: Recomenda-se à DGTI em colaboração com o Comitê Gestor de Segurança da Informação, editar ato normativo sobre o uso seguro de computação em nuvem no IFCE, nos termos da Instrução Normativa n º 05/2021/GSI/PR.

1.1.2.2 CONSTATAÇÃO: Contratação de serviço de computação em nuvem decorrente de pregão anterior à IN 05/2021/GSI/PR.

Em análise ao Contrato nº 02/2022 – IFCE Maracanaú (SEI 3394877) - Processo SEI 23255.000003 /2022-71, assinado em fevereiro de 2022, decorrente de uma Adesão à Ata de Registro de Preços nº 11/2021 (Pregão por Sistema de Registro de Preços nº 18/2020 do Ministério da Economia), com a EXTREME DIGITAL CONSULTORIA E REPRESENTAÇÕES LTDA. inscrito(a) no CNPJ/MF sob o nº 00.489.828/0051-14, compreende-se que a contratação vigente não foi realizada em observância à IN 05/2021/GSI/PR uma vez que o procedimento licitatório ocorreu em 2020, portanto, ano anterior à emissão da IN 05/2021/GSI/PR.

A supracitada IN traz a obrigatoriedade de os instrumentos contratuais firmados com provedor de serviço de nuvem, para prestação do serviço de computação em nuvem, terem cláusulas que tratem dos requisitos mínimos para a adoção segura de computação em nuvem. Tais requisitos estão dispostos nos arts. 10 ao 18. Além dos requitos mínimos, os contratos também devem conter os procedimentos de segurança previstos no art. 19 da IN 05/2021/GSI/PR.

No caso do órgão ou entidade da administração pública federal já possuir contratação de serviço de computação em nuvem, caso do IFCE, este deverá adequar à referida IN os contratos vigentes:

> Art. 26. Os órgãos ou as entidades da administração pública federal que já estiverem utilizando os serviços de provedor de serviço de nuvem terão um prazo de doze meses, após a entrada em vigor desta Instrução Normativa, para adequação de seus contratos.

Ante o exposto, faz-se necessário que o IFCE promova a adequada contratação de serviço de computação em nuvem com base nas diretrizes da IN 05/2021/GSI/PR.

A Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:
"Em atendimento à recomendação em questão, informamos que o processo de contratação em análise foi construído pelo Ministério da Economia em conjunto com outros órgãos como o GSI da Presidência da República, onde o mesmo colaborou com as considerações que posteriormente vieram a formar a IN nº 05/2021/GSI/PR. Realizamos ainda nova consulta ao SISP por meio do protocolo 308803.2861645/2023 onde o mesmo reforça que o processo de contratação segue sim a IN nº 05/2021/GSI/PR."

ANÁLISE DA AUDITORIA: Considerando que o documento referente a consulta ao SISP, citado na manifestação do gestor, não foi encaminhado para análise da equipe de auditoria, a Audin mantém a recomendação 012.

RECOMENDAÇÃO 012 – [DGTI]: Considerando que a vigência do contrato de serviço de nuvem nº 02/2022 - Maracanaú é até 02/2024, recomenda-se à DGTI que seja realizada nova contratação de serviço de nuvem com observância à IN nº 05/2021/GSI/PR, quando do fim da vigência do contrato nº 02/2022.

1.1.3 ASSUNTO: Gestão de Backup

1.1.3.1 CONSTATAÇÃO: Inexistência de Política de Backup.

Em resposta à Solicitação de Auditoria Interna nº 05 – e-Aud 1459941 foi informado pelo Chefe do Departamento de Governança de TI que não há a política de backup como documento institucionalizado no IFCE. Tal fato está em desacordo com os normativos vigentes e as boas práticas relacionadas à privacidade e à segurança da informação.

De acordo com a Lei Geral de Proteção de Dados, Lei nº 13.709/2018:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não

> autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

O Controle 11 do Guia do Framework de Privacidade e Segurança da Informação (p. 49) estabelece: *"Recuperação de Dados – Criar e manter práticas de recuperação de dados que sejam capazes de restaurar os ativos da organização para um estado pré-incidente ou o estado mais confiável possível."*

O Modelo de Política de Backup do Ministério da Gestão e da Inovação em Serviços Públicos orienta que a Política de Backup objetiva instituir diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelas unidades de tecnologia da informação (TI) e formalmente definidos como de necessária salvaguarda na Organização, para se manter a continuidade do negócio. No sentido de assegurar sua missão é fundamental estabelecer mecanismos que permitam a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças.

Sobre o tema, o Tribunal de Contas da União já emitiu acórdão sobre a obrigatoriedade dos órgãos públicos emitirem sua Política de Backup, conforme segue:

> ACÓRDÃO 1109/2021 - PLENÁRIO
> 9.1 recomendar ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) , ao Conselho Nacional de Justiça (CNJ) e ao Conselho Nacional do Ministério Público (CNMP) , com fundamento no art. 11 da Resolução - TCU 315/2020, que editem normativos para, cada um no seu âmbito de governança, **orientar os gestores e regulamentar a obrigatoriedade de que as entidades e órgãos públicos aprovem formalmente e mantenham atualizadas políticas gerais e planos específicos de backup** (para suas bases de dados e sistemas críticos, por exemplo) , contemplando requisitos mínimos para endereçar os cinco subcontroles do controle 10 (Data Recovery Capabilities) do framework preconizado pelo Center for Internet Security (CIS) , em especial quanto à definição do escopo dos dados a serem copiados, suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança; (grifo nosso)

Nesse contexto, frisa-se a importância da gestão da tecnologia da informação no âmbito do IFCE elaborar a Política de Backup, não só para atender aos normativos vigentes como também às boas práticas de gestão da tecnologia da informação a exemplo do Guia do Framework de Privacidade e Segurança da Informação e da ABNT NBR ISO/IEC 27002.

A Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:

"Reconhecemos a importância crítica de estabelecer uma Política de Backup que esteja em conformidade com as regulamentações vigentes, as boas práticas de segurança da informação e os princípios de proteção de dados. Diante disso, gostaríamos de confirmar nosso total comprometimento com a recomendação feita. Iniciaremos um processo interno para desenvolver a Política de Backup para o IFCE. Nesse processo, trabalharemos em colaboração estreita com o Comitê de Segurança da Informação, com o objetivo de assegurar que as diretrizes estabelecidas estejam alinhadas com os padrões da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos. Para posterior submissão dessa política para aprovação do Comitê de Governança Digital e pelo Colegiado de Diretores (COLDIR). Embora não exista uma formalização da política de backup, a gestão de backup é considerada uma atividade prioritária na COIR, sendo a atividade que mais consome os escassos recursos humanos."

ANÁLISE DA AUDITORIA: A Audin mantém a recomendação 013.

RECOMENDAÇÃO 013 – [DGTI]: Recomenda-se à DGTI em colaboração com o Comitê de Segurança da Informação editar Política de Backup para o IFCE, tendo como base o Modelo de Política de Backup da Secretaria de Governo Digital (SGD) do Ministério da Gestão e da Inovação em Serviços Públicos.

1.1.3.2 CONSTATAÇÃO: Ausência de equipamentos adequados para realização de backup do data center.

Em resposta à Solicitação de Auditoria Interna nº 05 – e-Aud 1459941, sobre a existência de equipamentos adequados para a realização de backups eficientes e seguros do data center do IFCE, foi informado pelo Chefe do Departamento de Governança de TI que: *"Parcialmente. São utilizadas ferramentas de backup (softwares e hardwares) nas instalações do IFCE e nas plataformas de computação em nuvem, contudo no último mês de maio o equipamento do IFCE apresentou problemas e no momento encontra-se em avaliação as possíveis soluções para o mesmo. Como solução de contorno, estamos realizando os backups em nuvem e executando processos manuais de backup nas instalações do IFCE."*

Em reunião realizada no dia 25/05/2023 como o Coordenador da Coordenação de Infraestrutura e Redes – COIR, foi informado pelo coordenador que atualmente, o IFCE está operando com um backup modesto, sendo necessário renovar a extensão da garantia de um backup mais robusto, o qual não está funcionando por falta da garantia da máquina. Segundo o coordenador, é importante e necessário que o IFCE tenha uma política de gestão de dados, pois não cabe à COIR definir, por exemplo, a temporalidade de disponibilidade dos dados armazenados. Além de realizar o backup, também é necessária a validação desse backup, o que significa verificar a sua integridade, ou seja, se contém todos os arquivos e nada foi corrompido. Para o coordenador, a atividade de backup deveria ter um servidor exclusivo, pois é uma área crítica, contudo a realidade de pessoal da coordenação não permite que isso seja possível.

A constatação apresenta uma fragilidade nas cópias de segurança dos dados, dos softwares e das informações relevantes da instituição. Todos esses registros devem ser protegidos contra perda, destruição, falsificação, acesso não autorizado e liberação não autorizada. Ressalta-se que o sistema Q-Acadêmico está com sua base de dados toda no data center da instituição, pois a sua migração para a nuvem seria inviável economicamente. Portanto, a instituição deve investir em equipamentos que proporcionem o backup adequado e eficiente de acordo com os requisitos do negócio.

A Audin solicita uma manifestação do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:
"Como o equipamento que constitui a solução de backup (software e hardware) apresentou defeito no último mês de maio de 2023, não sendo possível a recuperação do mesmo pela equipe interna do IFCE, foi aberto um processo (23255.005569/2023-70) para contratação de empresa que forneça os serviços de manutenção e suporte do referido equipamento. O processo encontra-se em sua fase interna de construção do documento Estudo Técnico Preliminar."

ANÁLISE DA AUDITORIA: A Audin mantém a recomendação 014 até a concretização da contratação.

RECOMENDAÇÃO 014 – [DGTI]: Recomenda-se à DGTI realizar a contratação de garantia do equipamento de backup do data center.

1.1.4 ASSUNTO: Gestão de TI nos campi

1.1.4.1 CONSTATAÇÃO: Designação de servidor para função de coordenador sem que se observassem os requisitos de qualificação profissional e técnica para o exercício do cargo.

A Audin realizou consulta ao Suap, nos dias 29 e 30/06/2023, para verificar a qualificação profissional e técnica dos servidores que são coordenadores nas unidades de tecnologia da informação nos campi do IFCE. Da análise das respostas apresentadas e das consultas realizadas ao Suap, compreende-se que os servidores Coordenadores dos campi Acaraú, Baturité e Crato não possuem qualificação profissional e técnica em Tecnologia da Informação para desempenharem as atribuições definidas no Regimento dos campi.

Em consulta ao Regimento dos campi destaca-se os arts. 11 e 12:

> DA COODENADORIA DE TECNOLOGIA DA INFORMAÇÃO
> Art. 11. A Coordenadoria de Tecnologia da Informação é o órgão responsável por promover a política de uso da Tecnologia da Informação planejando, coordenando, supervisionando, e por dar assistência, aos demais setores do campus.
> Art.12. São atribuições da Coordenadoria de Tecnologia da Informação:
> I. Promover políticas na área da tecnologia da informação para o Campus;
> II. Identificar as necessidades nas áreas de informática e comunicação e propor alternativas de solução;
> III. **Planejar, coordenar e controlar o desenvolvimento de sistemas de informação e comunicação do campus;**
> IV. Fornecer apoio operacional a infraestrutura necessária para o desenvolvimento do ensino a distância;
> V. Fornecer apoio operacional a infraestrutura necessária para o desenvolvimento do ensino a distância;
> VI. Promover a difusão e bom uso dos aplicativos, equipamentos, sistemas e ambientes virtuais de ensino e pesquisa;
> VII. Apoiar e coordenar a melhor distribuição dos recursos de informática e comunicação, bem como, o atendimento das requisições de serviços;
> **VIII. Acompanhar e/ou realizar o desenvolvimento e manutenção de sistemas computacionais de interesse das Unidades de Ensino;**
> IX. Propor e desenvolver treinamento local ou à distância, visando à melhor utilização da rede, sistemas e aplicativos instalados;
> X. Gerenciar recursos das redes de computadores, no que concerne, a infraestrutura de acesso e aos aplicativos que se utilizam dessa rede;
> XI. Zelar pela integridade e segurança da informação;
> XII. Prestar suporte e manutenção aos equipamentos de informática (hardwares) e comunicação da rede de computadores nas formas preventiva e corretiva. (grifo nosso)

Tal constatação pode ocasionar fragilidade na coordenação das atividades do setor de TI do campus, como também desestimular os demais servidores que possuem competência técnica e profissional para ocupar o cargo de gestor.

Além da constatação supracitada, verificou-se a existência de quatro cargos de Analista de TI na composição da força de trabalho dos campi Crato, Fortaleza, Limoeiro e Tianguá. A Audin entende que os cargos de Analista de TI devem ser concentrados na DGTI/Reitoria, pois esta é responsável pela gestão de todos os componentes de criticidade do negócio da instituição relacionados à tecnologia da informação. Além do fato de que a capacidade operacional da DGTI é deficitária para gerir todas as responsabilidades da diretoria.

Destaca-se as atribuições de um Analista de TI e de um Técnico de TI, extraído do Edital nº 1, de 6 de setembro de 2021 - Concurso Público IFCE:

> 2.2.2. ANALISTA DE TECNOLOGIA DA INFORMAÇÃO
> DESCRIÇÃO SUMÁRIA DAS ATIVIDADES: Desenvolver e implantar sistemas informatizados dimensionando requisitos e funcionalidade do sistema, especificando sua arquitetura, escolhendo ferramentas de desenvolvimento, especificando programas, codificando aplicativos. Administrar ambientes informatizados, prestar suporte técnico ao usuário e o treinamento, elaborar documentação técnica. Estabelecer padrões, coordenar projetos e oferecer soluções para ambientes informatizados e pesquisar

tecnologias em informática. Assessorar nas atividades de ensino, pesquisa e extensão.

2.2.21. TÉCNICO EM TECNOLOGIA DA INFORMAÇÃO:
DESCRIÇÃO SUMÁRIA DAS ATIVIDADES: Desenvolver sistemas e aplicações, determinando interface gráfica, critérios ergonômicos de navegação, montagem da estrutura de banco de dados e codificação de programas; projetar, implantar e realizar manutenção de sistemas e aplicações; selecionar recursos de trabalho, tais como metodologias de desenvolvimento de sistemas, linguagem de programação e ferramentas de desenvolvimento. Assessorar nas atividades de ensino, pesquisa e extensão.

A Audin solicita uma manifestação dos Diretores Gerais dos campi Acaraú, Baturité e Crato, bem como do Pró-Reitor de Gestão de Pessoas quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA – [BATURITÉ]: Não houve manifestação do gestor.

MANIFESTAÇÃO DA ÁREA AUDITADA – [PROGEP]: Não houve manifestação do gestor.

ANÁLISE DA AUDITORIA – [BATURITÉ / PROGEP]: Considerando a ausência de manifestação dos gestores do Campus Baturité e da PROGEP, conclui-se pela concordância tácita da constatação e recomendações apresentadas. Assim, a Audin mantém as recomendações 015 e 016.

ANÁLISE DA AUDITORIA – [ACARAÚ / CRATO]: A análise consta no item V) Informação.

RECOMENDAÇÃO 015 – [BATURITÉ]: Recomenda-se à Diretoria Geral do Campus Baturité designar para ocupação do cargo de Coordenador de TI servidor com qualificação técnica e profissional para o exerício do cargo.

RECOMENDAÇÃO 016 – [PROGEP]: Considerando os cargos vagos e as futuras vacâncias, recomenda-se à PROGEP concentrar as vagas de analista de TI na Reitoria do IFCE.

RECOMENDAÇÃO 017 – [DGTI]: Recomenda-se à DGTI emitir atestado de capacidade técnica indicando se os Coordenadores de TI dos campi Acaraú, Baturité e Crato estão aptos para a função ocupada.

1.2 SUBÁREA: Programação dos objetivos e metas

1.2.1 ASSUNTO: Consistência das metas

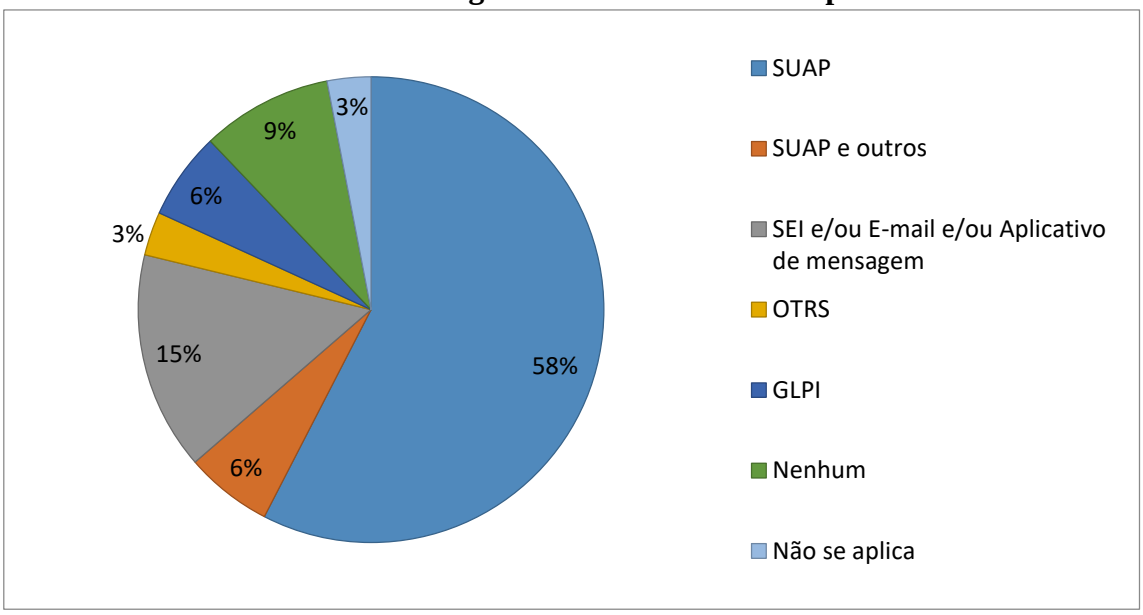
1.2.1.1 CONSTATAÇÃO: Ausência de acompanhamento das metas do PDI 2019-2023. Utilização de sistemas diversos não institucionalizados.

O indicador "Taxa de tickets atendidos" possui como meta o alcance de no mínimo 90% de atendimento. Conforme o catálogo de objetivos ajustado em abril de 2022, esse indicador *"é uma meta progressiva, ou seja, o campus deverá a cada ano do PDI aumentar o atendimento dos tickets, até atingir ou ultrapassar o patamar de 90% de atendimento. Desta forma, ao final do PDI, terá cumprido a meta, o campus que encerrar o exercício de 2023, com no mínimo, 90% dos tickets sendo devidamente atendidos".* O indicador possui periodicidade de acompanhamento trimestral e é um indicador desdobrável, portanto, seu alcance é de responsabilidade da Reitoria e dos Campi.

Com o objetivo de verificar se há acompanhamento das metas do PDI 2019-2023, a Audin questionou às 33 unidades do IFCE, por meio da Solicitação de Auditoria nº 30/2023 (SEI 4955235), qual o sistema utilizado para o controle de registro de tickets das solicitações dos usuários dos serviços de TI.

Da análise das respostas apresentadas, conforme exposto no Gráfico 1, constata-se que há uma despadronização no controle utilizado para o registro dos tickets gerados para solucionar algum problema identificado nos serviços de tecnologia da informação e comunicação na Reitoria e nos campi.

Gráfico 1 - Meios de registro dos tickets nos Campi do IFCE



Fonte: Campi do IFCE.

Quando solicitado relatórios de tickets gerados de janeiro a maio de 2023, parte das informações não foi disponibilizada por alguns campi, pois não havia o controle dos registros em um sistema de chamados, mas por outros meios, como, por exemplo, SEI, e-mail e aplicativos de mensagens. Outros apresentaram relatórios analíticos que não

apresentam informações concisas e de fácil compreensão para o controle e para a tomada de decisão pelos gestores. Tal situação impossibilita o controle dos serviços realizados e, dessa forma, impossibilita a verificação do alcance da meta estabelecida no PDI 2019-2023.

Tendo em vista a recomendação da DGTI, por meio do Ofício-Circular nº 4/2023/DGTI/REITORIA-IFCE, de 5 de junho de 2023 (SEI 4968414), *"Recomendamos o uso do SUAP, como central de atendimento, para a abertura de chamados e demais demandas de tecnologia da informação"*, a Audin recomenda a utilização do SUAP como sistema único para registro dos tickets, devido à necessidade da gestão em informações confiáveis, disponíveis e tempestivas para o acompanhamento das metas estabelecidas no PDI.

Dessa forma, a Audin solicita uma manifestação do Reitor e do Diretor da Diretoria de Gestão de Tecnologia da Informação quanto às providências que serão tomadas.

MANIFESTAÇÃO DA ÁREA AUDITADA: Em resposta enviada pelo Sistema e-Aud (Id 1500068), o Diretor da Diretoria de Gestão de Tecnologia da Informação informou que:
"A DGTI já promoveu essa ação com diversos campus e se dispõe a fazê-lo novamente. No entanto, não consideramos pertinente essa recomendação para DGTI, pois a mesma já realizou essa ação, no entanto, nem todos os campi aderiram a solicitação da DGTI."

ANÁLISE DA AUDITORIA: Considerando a Portaria Normativa nº 88/GABR/REITORIA, de 18 de agosto de 2023, a Audin mantém a recomendação 020 para que a DGTI realize capacitações com os campi que, até a emissão da citada portaria, não faziam o uso do Sistema Suap – central de serviços. Frisa-se a importância de haver uma sensibilização junto aos campi que utilizam outros sistemas para que o processo de migração para o Suap – Central de Serviços seja eficaz.

RECOMENDAÇÃO 018 – [DGTI]: Considerando a Portaria Normativa nº 88/GABR/REITORIA, de 18 de agosto de 2023, recomenda-se à DGTI promover a realização de capacitação no Sistema Suap - central de serviços - para os responsáveis pelo recebimento das demandas e para os usuários solicitantes dos serviços de TI nos campi que não fazem uso desse sistema. E promova apoio aos campi durante o processo de migração dos sistemas.

V) INFORMAÇÃO

1. Recomendações retiradas do relatório preliminar:

A seguir apresenta-se as recomendações que foram retiradas após a manifestação dos gestores sobre o Relatório Preliminar.

Recomendação 006 – [DGTI]: No dia 30/08/2023 a equipe de auditoria realizou uma nova vistoria nas instalações do data center da reitoria para confirmar se os controles de acesso ao equipamento foram alterados. Verificou-se que o acesso ao data center foi automatizado por reconhecimento facial e o acesso ao nobreak também foi alterado para reconhecimento biométrico. Considerando a nova situação encontrada, a Audin retirou a recomendação 006 deste relatório.

Recomendação 011 – [GABR]: O Gabinete do Reitor emitiu a Portaria Normativa nº 87/GABR/REITORIA, de 18 de agosto de 2023, a qual dispõe sobre a designação do gestor de segurança da informação no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Ceará – IFCE.

Recomendação 017 – [ACARAÚ]: O Diretor Geral do Campus Acaraú apresentou os certificados de cursos realizados pelo Coordenador de TI do campus, verificou-se cursos realizados em Tecnologias de Rede sem Fio, Gerenciamento de Serviços de TI, ITIL – Information Technology Infrastructure Library, Administração de Sistemas Linux e Fundamentos de Scrum, todos certificados pela Escola Superior de Redes RNP, realizados no período de 2011 a 2019. Dessa forma, a Audin compreende que não possui expertise para afirmar a capacidade técnica do Coordenador de TI do Campus Acaraú para a função ocupada. Por esse motivo, a equipe de auditoria incluiu a RECOMENDAÇÃO 019 neste relatório.

Recomendação 019 – [CRATO]: O Diretor Geral do Campus Crato apresentou os certificados de cursos realizados pelo Coordenador de TI do campus, verificou-se cursos realizados em Data Cabling System, Roteamento, Gestão da Segurança da Informação, Ferramentas de Segurança, Planejamento de TI, Planejamento de Contratações de TI, e Gestão de Riscos nas Contratações. Os cursos foram certificados pela Escola Superior de Redes RNP, pelo Núcleo de Informação e Coordenação do Ponto BR e pela Escola Nacional de Administração Pública, realizados no período de 2011 a 2023. Dessa forma, a Audin compreende que não possui expertise para afirmar a capacidade técnica do Coordenador de TI do Campus Crato para a função ocupada. Por esse motivo, a equipe de auditoria incluiu a RECOMENDAÇÃO 019 neste relatório.

Recomendação 021 – [GABR]: O Gabinete do Reitor emitiu a Portaria Normativa nº 88/GABR/REITORIA, de 18 de agosto de 2023, a qual dispõe sobre os registros de demandas por serviços de TI, no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Ceará – IFCE. A citada portaria determina que os registros de demandas

por serviços de TI sejam realizados exclusivamente no sistema SUAP, módulo central de serviços.

Recomendação 023 – [DGTI]: O próximo PDI do IFCE, para os anos 2024 a 2028, conterá objetivos estratégicos, indicadores e metas apenas para os macroprocessos finalísticos da instituição, sendo elas ensino, pesquisa, extensão e inovação, conforme informado pelo Chefe do Departamento de Planejamento e Políticas Institucionais, via e-mail no dia 30/08/2023. Portanto, a DGTI como área de apoio à instituição não terá objetivos estratégicos no PDI. Contudo, destaca-se que a DGTI tem instrumento próprio de planejamento, o Plano Diretor de Tecnologia da Informação – PDTI, o qual deve conter os objetivos estratégicos de TI alinhados às necessidades da instituição e, portanto, com os objetivos institucionais.

2. Coaduna com as recomendações deste relatório o Acordão nº 1.688/2023 – TCU – Plenário, de 16/08/2023:

O Tribunal de Contas da União – TCU realizou levantamento em quatro temas relativos à Rede Federal de Educação Profissional, Científica e Tecnológica (Institutos Federais de Educação, Ciência e Tecnologia; Centros Federais de Educação Tecnológica; e Colégio Pedro II) – IFEs, dentre eles a Governança de Tecnologia da Informação e Comunicação (TIC). O trabalho resultou no Acordão nº 1.688/2023 – TCU – Plenário e mostra que as IFEs estão no estágio inicial de implementação das políticas de segurança da informação.

O supracitado acordão traz como determinação:

> 9.1. dar ciência às 41 instituições de ensino que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica, com fundamento no art. 9º, inciso II, da Resolução-TCU 315/2020, no sentido de que:
> 9.1.3. a não implementação da Estrutura de Segurança de Informação e Comunicação, mais especificamente, o Comitê Gestor de Segurança da Informação, bem como a designação formal de um Gestor de Segurança da Informação e Comunicação, constitui afronta ao previsto no art. 16 da IN-GSI 01/2020;
> 9.1.4. a elaboração de Políticas de Segurança da Informação e Comunicação que não contemplam as diretrizes mínimas representam afronta ao previsto no inciso IV do art. 12 da IN-GSI 01/2020.

Nesse contexto, é notória a relevância e pertinência do objeto desta ação de auditoria no IFCE para que a instituição se adeque aos normativos vigentes e atenda as determinações dos órgãos de controle.

VI) CONCLUSÃO

Por meio das técnicas utilizadas e das evidenciações colhidas, encorajamos que a observância às recomendações desta unidade de auditoria seja uma prática constante das unidades auditadas, a fim de que as irregularidades e/ou impropriedades encontradas sejam resolvidas, bem como as boas práticas da Administração Pública estejam incorporadas ao cotidiano.

Isso posto, elucidamos que a atividade da Auditoria Interna está estruturada em procedimentos, com enfoque técnico, objetivo, sistemático e disciplinado, e tem por finalidade agregar valor ao resultado da organização, apresentando subsídios para o aperfeiçoamento dos processos da gestão e dos controles internos, por meio da recomendação de soluções para as não-conformidades apontadas nos relatórios. Nessa perspectiva, continuaremos monitorando as recomendações exaradas pela Auditoria Interna, a fim de cotejar o antes e o depois da presente auditoria e, sobretudo, a aderência da DGTI aos seus objetivos estratégicos presentes no Plano de Desenvolvimento Institucional – PDI.

Encaminha-se este relatório ao Reitor, ao Diretor da Diretoria de Gestão de Tecnologia da Informação, ao Pró-Reitor de Gestão de Pessoas e aos Diretores Gerais dos Campi Acaraú, Baturité e Crato para conhecimento e providências.

Fortaleza, 30 de Agosto de 2023.

Equipe Responsável:
Milena Mendes da Costa – Auditora-Chefe da AUDIN/IFCE
Antonia Karina Barroso Gouveia Cunha – Auditora
Dirlândia de Oliveira Marques – Auditora