

RELATÓRIO Final de Auditoria Operacional n.º 09/2024 - AUDIT
PROCESSO: 00111-00002291/2024-44
INTERESSADO: AUDIT/CONAD/TERRACAP
ASSUNTO: Análise dos controles primários na Governança de TI no âmbito da TERRACAP.

Senhor Chefe da Auditoria Interna,

Apresenta-se o relatório final de auditoria operacional que trata da análise dos controles primários na **Governança de TI** no âmbito da TERRACAP, instaurada pela Ordem de Serviço n.º 002/2024- AUDIT, documento SEI (134913923), prorrogadas pelas n.ºs 06, 10 e 14 (152026664, 152985975 e 156325798), respectivamente, em cumprimento ao Plano Anual de Atividades de Auditoria Interna - PAINT/2024 (134913042), aprovado pelo Conselho de Administração por meio da Decisão n.º 01/2024 (134913550), constante no processo 00111-00008904/2023-76.

Ressaltamos que o PAINT/2024 aborda as ações que a Auditoria Interna da Terracap considera relevantes para o fortalecimento e aprimoramento da gestão, assim como o adequado relacionamento com parceiros e instituições externas. Ademais, este trabalho leva em consideração pontos de auditoria independente levantados nos últimos três anos, especialmente para a Governança de TI.

I – CONTEXTUALIZAÇÃO

A auditoria operacional objeto do presente plano de trabalho tem como propósito avaliar os controles primários na Governança de TI no âmbito da Terracap.

A auditoria busca promover a análise dos fluxos de trabalho no âmbito da Tecnologia da Informação, identificando todas as fases dos processos e avaliar a possibilidade de possíveis riscos e formas de monitoramento, o que pode gerar oportunidades de aprimoramento dos controles da organização.

A Governança de TI de uma empresa é responsável por definir e gerenciar o orçamento da área de tecnologia, o que envolve pessoas e infraestrutura. Ela é responsável por fazer a aquisição e gestão de recursos, monitorar fornecedores externos e criar programas de treinamento e desenvolvimento pessoal.

Em específico nesta Companhia, a Governança alcança de forma geral todas as unidades e com o objetivo de tornar mais eficiente e eficaz todos os processos com a devida segurança e além disso, monitorar toda parte informatizada da empresa.

Durante o exercício de 2023 iniciou-se a implementação do sistema ERP/BENNER, visando a integralização quase que total de todas as áreas da empresa, com isso, tanto a rotina atual necessitou de uma remodelação afim de atender os módulos existentes no sistema BENNER, para a grande virada de chave que deverá ocorrer em fevereiro de 2024.

A recente transferência da estrutura da ASINF - área de informática da TERRACAP, que passa a ser denominada Coordenação de Tecnologia e Inovação (COTIN) - para a Controladoria Interna, objetivou auxiliar na integração das ações de tecnologia e promover eficiência e aderência dos projetos às diretrizes de Governança do alto comando da Companhia, além de aprimorar as competências e modernizar a forma de atuação, notadamente nos aspectos de segurança da informação.

A reestruturação em referência tem como contexto a **necessidade de aprimoramento da governança de TI, bem como o fortalecimento dos mecanismos de segurança da informação da Companhia, (Cibersegurança)**, de forma a proteger a organização contra ameaças cibernéticas e ataques maliciosos.

Ademais, a necessidade verificada em promover um aprimoramento do alinhamento estratégico entre negócios e tecnologia, com vistas a estabelecer uma governança de TI que busque garantir que o uso da TI agregue valor ao negócio com riscos aceitáveis.

Nesse sentido, vale mencionar que a definição da estratégia de TI para que este objetivo seja atingido não considera apenas a tecnologia, mas, também, a criação de ambientes integrados que liberem as competências pessoais dos gestores, processos de negócios, estruturas organizacionais, e tecnologias para transformar a posição competitiva dos negócios.

A governança de TI, parte da governança corporativa, localiza-se no âmbito das decisões estratégicas de uma organização e vem se mostrando essencial para o alcance dos objetivos corporativos e o atendimento das necessidades dos *stakeholders*. Dentre as suas preocupações centrais, destaca-se: (1) agregar valor ao negócio, por meio do alinhamento entre este e a TI, e (2) mitigar riscos, com a incorporação da *accountability* na organização.

Nesse aspecto que surge a necessidade de integração entre a área de informática da empresa e as áreas de gestão da TERRACAP, para desenvolver iniciativas voltadas à governança de tecnologia da informação.

Não há dúvidas de que a tecnologia da informação tem desempenhado função cada vez mais estratégica nas instituições, por isso é necessário um **mecanismo para sua governança que permita sua organização bem como seu controle, direcionamento e monitoramento**. Justamente nesse contexto entra em cena, uma visão completa e sistêmica da Companhia, promovendo esse alinhamento com a missão, a estratégia, os valores e a cultura da empresa, bem como as ferramentas necessárias para a implementação da Governança de TI.

Além disso, a tecnologia da informação é um fator importante para as metas de uma organização, de forma que as decisões sobre investimentos em TI devem ser criteriosas, a fim de favorecer o alinhamento entre a TI e os objetivos organizacionais.

Partindo de todas as premissas delineadas acima, quais sejam, a necessidade de aperfeiçoamento da área da tecnologia da empresa nos aspectos de governança, aperfeiçoamento de processos de TI, com a aprovação de processos de trabalho e de documentos normatizadores, otimização do modelo de gestão e mitigação de riscos, a Companhia vislumbra na parceria com a Fundação de Amparo à Pesquisa e Extensão Universitária - FAPEU uma oportunidade de enfrentar os pontos explicitados até aqui.

A parceria em questão se encontra estruturada em três agendas, quais sejam:

- 1) Estruturação de um Ambiente de Inteligência de Gestão;
- 2) Desenvolvimento de Roadmap de Cibersegurança; e,
- 3) Construção de Modelo de Governança de TIC.

A agenda **Estruturação de um Ambiente de Inteligência de Gestão** compreende uma plataforma, física e/ou digital, que agrupa e disponibiliza, em tempo real e em formato dinâmico, um conjunto de dados para a tomada de decisão, estruturada.

A de **Desenvolvimento de Roadmap de Cibersegurança** visa proteger a organização contra ameaças cibernéticas e ataques maliciosos, com o Desenvolvimento de Roadmap de Cibersegurança, a partir do mapeamento das vulnerabilidades, identificação das oportunidades de sofisticação dos processos chaves, e proposição de soluções às

vulnerabilidades e falhas identificadas.

Por fim, a última agenda prevê a **Construção de Modelo de Governança de Tecnologia da Informação e Comunicação (TIC)**, que consiste em um sistema pelo qual o uso atual e futuro de TIC é dirigido e controlado, mediante avaliação e direcionamento, para atender às necessidades prioritárias e estratégicas da organização e monitorar sua efetividade por meio de planos, incluída a estratégia e as políticas de uso de TIC no âmbito da empresa.

Importante mencionar que a base de dados para construção dos produtos de inteligência será mantida dentro do ambiente da Terracap, que serão atualizados em tempo real de acordo com as bases de dados originárias das informações.

Assim, este trabalho de auditoria será conduzido com vistas a avaliar a execução, eficácia e eficiência dos controles internos relacionados à governança de TI, garantindo que existam procedimentos adequados para todo o ambiente que inclui segurança, integração, comunicação, capacitação, ciência de dados, que recaem sobre a Terracap, bem como em relação ao monitoramento de mudanças de acordo com a necessidade do cenário.

Ressalta-se que devido a classificação da atividade econômica principal explorada pela Terracap e compreender a gestão e administração da propriedade imobiliária, é salutar monitorar a Governança de TI como um todo, visando tornar tanto internamente como externamente o ambiente tecnológico que garante segurança e prudência tanto para os clientes como para a empresa.

Isto posto, e considerando a relevância do tema, em especial quanto ao acompanhamento do gerenciamento das rotinas e procedimentos relativos à governança de TI no âmbito da Terracap, este assunto foi inserido no PAINTE/2024.

Por fim, esta análise se baseia nas informações apresentadas, normativos vigentes disponíveis, relatórios de atividades, cronogramas de execução, plano de ação da área responsável, dentre outros elementos constantemente verificados pelo corpo funcional desta Empresa, pela Auditoria Independente contratada, assim como órgãos de Controle Externo. Visa-se diagnosticar o atual cenário no âmbito da Tecnologia, abrangendo integração entre sistemas e segurança que resguardam a empresa.

II – ESCOPO DO TRABALHO

Os trabalhos de auditoria foram realizados na sede da Terracap, voltados para a avaliação dos processos, providências e ações referentes à Governança de TI no âmbito da TERRACAP, incluindo segurança, interação entre as unidades, integração de sistemas e principalmente o mapeamento dos riscos para a empresa.

Para a análise pretendida, houve a necessidade de pesquisar todos os aspectos do tema, em especial, no quesito Governança e segurança cibernética, devido à classificação da atividade econômica principal explorada pela Terracap e compreender a gestão e administração da propriedade imobiliária, portanto, é salutar monitorar a Governança de TI como um todo, visando tornar tanto internamente como externamente o ambiente tecnológico que garante segurança e prudência tanto para os clientes como para a empresa.

Dessa forma, por esses e outros motivos, se faz cada vez mais indispensável ter uma gestão de eficiente, pois além de mitigar os riscos, gera valor agregado para a empresa. Salienta-se que a gestão eficaz das ações com vistas à Governança de TI, pode evitar prejuízos de curto e longo prazo, garantindo a padronização de processos, rotinas e setores envolvidos na entrega.

Portanto, esta auditoria operacional teve como escopo analisar como um todo o atual cenário, as ações em desenvolvimento e as possíveis dificuldades existentes nos controles primários tanto nas instruções processuais, como na rotina praticada pela mão-de-obra para o feito, seu desempenho na tomada de decisão e iniciativa de ações corretivas visando identificar os possíveis gargalos das falhas.

Destaca-se como OBJETIVO GERAL:

Examinar os controles primários referentes à Governança de TI, visando avaliar a conformidade na realização das tarefas que abrangem a governança como um todo que inclui segurança, interação entre as unidades, integração de sistemas e riscos, com o objetivo de avaliar e identificar possíveis situações que possam ser implementadas para mitigar riscos no âmbito da Terracap.

Cumprir destacar ainda, que o presente trabalho fez uso dos trabalhos realizados pela Auditoria Independente nos últimos 3 anos, o Plano Diretor de TI, Relatório de atividades de TI, Convênio nº 170/2023 com a Fundação de Amparo à Pesquisa e Extensão Universitária - FAPEU, a Lei nº 13.303/2016, Regimento Interno, estatuto jurídico da empresa pública, outros documentos disponibilizados pelas áreas responsáveis.

Nessa cenário, a presente auditoria operacional visou realizar análise nas rotinas, bem como em processos por amostragem, com o objetivo de detectar o plano de ação da área de TI, visando o atingimento do objetivo final.

Os trabalhos de auditoria foram realizados somente no âmbito da Companhia Imobiliária de Brasília – TERRACAP no período de março a outubro de 2024. Além da coleta e análise de documentos, foram realizados cruzamento de informações a partir da revisão dos controles internos, entrevistas considerando as unidades orgânicas, mediante demandas e solicitações direcionadas à área relacionada com o objeto da presente Auditoria Operacional, predominantemente de forma formal e virtual, tendo em vista a consolidação do teletrabalho no âmbito desta Empresa Pública, em consonância com as diretrizes aplicadas na Administração Pública Distrital.

III – PLANEJAMENTO DA AUDITORIA

Conforme o Plano de Auditoria Interna -PAINTE/2024 (134913042), aprovado pelo Conselho de Administração por meio da Decisão nº 01/2024 (134913550), constante no processo 00111-00008904/2023-76, foi prevista a realização da presente Auditoria Operacional.

Neste sentido, foi iniciado o presente Processo Sei nº 00111-00002291/2024-44, expedida a Ordem de Serviço nº 02/2024 - AUDIT (113268050), e por meio do Memorando nº 05/2024 - TERRACAP/CONAD/AUDIT (135166477), comunicou-se a todas as unidades o início da presente auditoria.

Na fase preliminar, foi elaborado o Plano de Trabalho 4 - TERRACAP/CONAD/AUDIT, (137946254), contendo os assuntos considerados críticos quanto do trabalho em campo. Para tanto, o referido planejamento incluiu estratégias e procedimentos de auditoria que consideramos apropriados neste momento para testar de forma amostral os mecanismos de controles internos afetos à cadeia em análise, a fim de otimizar a gestão, sem, contudo, emitir uma conclusão estanque sobre os controles internos desta empresa pública.

Ressalta-se que a Administração da Terracap possui liberdade para conduzir os controles internos necessários à governança de TI, porém sempre após autorização em DIRET, de forma a evidenciar adequadamente a realidade empresarial da Empresa, no que tange à escrituração/registro. Há, portanto, espaço para avaliação acerca da conveniência e oportunidade para determinar providências no que tange à adoção de novos controles administrativos e operacionais, considerando as recomendações emanadas ao final deste trabalho, ou seja o item - VII - RECOMENDAÇÕES.

Cabe à gestão fazer constantemente avaliações no sentido de determinar a profundidade, extensão e relevância dos mecanismos de controles internos a serem implementados pelas unidades orgânicas responsáveis, de acordo com as atribuições regimentais, considerando aspectos como: relação custo-benefício; estabelecimento de responsabilidades; segregação de funções; acesso a ativos; estabelecimento de comprovações; testagens autônomas; ferramentas e métodos de processamento de dados; capacidade instalada de pessoal, dentre outros critérios não estáticos. O conceito de custo-benefício reconhece que o custo de um controle não deve exceder os benefícios que ele possa proporcionar. Portanto, há que se avaliar se determinadas recomendações merecem ou não prosperar, ao momento de sua proposição, considerando aspectos técnicos e situacionais, sob a ótica da Administração.

Neste trabalho estão contemplados os resultados obtidos em decorrência da análise prévia sobre os processos e procedimentos voltados para avaliação dos controles internos relativos à Governança de TI no âmbito da TERRACAP, após contato com áreas diretamente relacionadas ao tema, com posterior avaliação do grau de adequabilidade dos controles primários das unidades orgânicas analisadas no âmbito desta Empresa Pública.

Faz-se mister, inicialmente, trazeremos à baila o **Decreto Distrital nº 40.015 de 14 de agosto de 2019**, que dispõe sobre a obrigatoriedade de elaboração e publicação dos Planos Diretores de Tecnologia da Informação e Comunicação e sobre a centralização e utilização da rede GDFNet, da infraestrutura do Centro de Tecnologia da Informação e Comunicação do Distrito Federal - CeTIC-DF e dos sistemas de informação no âmbito da Administração Direta e Indireta do Distrito Federal, e dá outras providências

O GOVERNADOR DO DISTRITO FEDERAL, no uso das atribuições que lhe confere o artigo 100, incisos VII, XXI e XXVI da Lei Orgânica do Distrito Federal, DECRETA:

Art. 1º Compete aos órgãos e entidades que compõem a Administração Direta e Indireta do Distrito Federal a elaboração e a publicação dos seus respectivos Planos Diretores de Tecnologia da Informação e Comunicação - PDTIC como condição para as aquisições e contratações de bens, soluções e serviços de tecnologia da informação e comunicação.

§ 1º Os setores dos órgãos e entidades responsáveis pelas aquisições e contratações de bens, soluções e serviços de tecnologia da informação e comunicação, e pela ordenação de despesa, somente devem autorizar o prosseguimento da aquisição e contratação e a realização de despesa se a demanda estiver prevista no PDTIC do respectivo órgão ou entidade, comprovada por meio de declaração expressa, emitida pela autoridade máxima do órgão ou entidade.

§ 2º O PDTIC de cada órgão ou entidade deve ser publicado em até 180 (cento e oitenta dias), a contar da publicação deste decreto, e ser revisto anualmente, ou antes deste prazo, caso necessário.

Art. 2º Ficam instituídos o CeTIC-DF como datacenter e a rede GDFnet como rede metropolitana corporativa oficiais, privados e exclusivos do Distrito Federal.

§ 1º O CeTIC-DF é o centro de dados corporativo privado do Distrito Federal, ambiente com soluções integradas de hardware e software, que provê serviços de nuvem corporativa privada, armazenamento de dados, hospedagem de aplicações e sistemas a todos os órgãos e entidades da Administração Direta e Indireta do Distrito Federal, compreendendo os sistemas estruturantes, bases de dados e os serviços corporativos de tecnologia da informação e comunicação.

§ 2º A GDFNet é a rede corporativa metropolitana privada de comunicação de alta velocidade dos órgãos e entidades da Administração Direta e Indireta do Distrito Federal, que interliga as unidades administrativas e unidades operacionais, permitindo a comunicação e a troca de informações seguras entre si e com o CeTIC-DF e acesso aos sistemas corporativos e à rede mundial de computadores.

§ 3º Fica vedada a aquisição e contratação direcionada à construção de redes metropolitanas paralelas ou apartadas da rede GDFNet, devendo o órgão ou entidade, caso tenha interesse, estabelecer acordo formal com a Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal, desde que a infraestrutura seja integrada à rede GDFNet e a gestão esteja a cargo da Subsecretaria de Tecnologia da Informação e Comunicação, da Secretaria Adjunta de Gestão Administrativa, da Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal.

§ 4º A centralização e obrigatoriedade de utilização da rede GDFNet, da infraestrutura do Centro de Tecnologia da Informação e Comunicação do Distrito Federal - CeTIC-DF, prevista no presente Decreto, não se aplica à Polícia Civil do Distrito Federal. [\(Acrescido\(a\) pelo\(a\) Decreto 41435 de 09/11/2020\)](#)

Art. 3º A Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal, por meio da Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria Adjunta de Gestão Administrativa, fica responsável direta e exclusivamente pela gestão, sustentação e operação do CeTIC-DF e da rede GDFNet.

§ 1º À Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria Adjunta de Gestão Administrativa compete as ações voltadas à sustentação, operação e modernização dos serviços de Tecnologia da Informação e Comunicação corporativos e administrativos dos órgãos e entidades da Administração Direta e Indireta do Distrito Federal, com foco na melhoria da gestão tecnológica e no atendimento da população com serviços eletrônicos de governo, excetuando-se os serviços e iniciativas de caráter de inclusão social, pesquisa e desenvolvimento, em relação aos quais prestará apenas apoio técnico e operacional.

§ 2º A Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria Adjunta de Gestão Administrativa deve zelar pela manutenção e atualização tecnológica do CeTIC-DF e da rede GDFNet, de forma que atendam às necessidades dos órgãos e entidades da Administração Direta e Indireta do Distrito Federal, usuários destas infraestruturas, sendo vedada, por questões de gestão, sigilo e segurança da informação, a cessão, a transferência, a utilização, a integração ou a interconexão de qualquer natureza, de suas infraestruturas físicas e lógicas, por qualquer entidade ou instituição que não faça parte da Administração Pública Distrital.

§ 3º As atividades de gestão e governança do CeTIC e da rede GDFNet devem ser realizadas por equipe técnica integrante de quadro próprio e permanente do Distrito Federal.

§ 4º Os órgãos e entidades da Administração Direta e Indireta do Distrito Federal devem disponibilizar à Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal, para fins de planejamento de capacidade e disponibilidade do CeTIC-DF, os seus respectivos Planos Diretores de Tecnologia da Informação e Comunicação, os sistemas e os requisitos, aplicáveis às ações a que se refere o artigo 4º deste Decreto, conforme cronograma a ser definido entre as partes.

§ 5º Na condição de unidade gestora do CeTIC-DF e da rede GDFNet, a Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal pode incorporar ao seu respectivo Plano Diretor de Tecnologia da Informação e Comunicação, após análise técnica e aprovação, as demandas de cunho corporativo do Distrito Federal constantes dos Planos Diretores de Tecnologia da Informação e Comunicação dos órgãos e entidades da Administração Direta e Indireta do Distrito Federal.

Art. 4º A gestão, a sustentação e a operação do CeTIC e da rede GDFNet compreende as seguintes atividades:

I - estruturar e prover os serviços de datacenter corporativo, inclusive nuvem, a todos os órgãos e entidades da Administração Direta e Indireta do Distrito Federal;

II - estruturar, gerir, operar e manter a rede GDFNet;

III - prestar serviços corporativos de tecnologia da informação e comunicação aos órgãos e entidades da Administração Direta e Indireta do Distrito Federal;

IV - formular a política de unificação, hospedagem e sustentação dos sistemas, dos serviços e das informações, de acordo com requisitos de segurança da informação e continuidade de negócios;

V - prover os serviços de internet administrativa e publicação de serviços web hospedados no CeTIC no âmbito do Distrito Federal;

VI - gerenciar o domínio df.gov.br;

VII - responder tecnicamente junto ao Gabinete de Segurança Institucional da Presidência da República - GSI-PR acerca da segurança da informação e integridade do domínio df.gov.br;

VIII - acompanhar, apoiar e desenvolver junto às áreas de negócios, os projetos voltados à melhoria e aperfeiçoamento dos sistemas corporativos estruturantes dos órgãos e entidades da Administração Direta e Indireta do Distrito Federal.

IX - zelar pela segurança da informação no âmbito do CeTIC-DF e da rede GDFNet;

X - zelar pelo sigilo e segurança física e lógica dos ambientes do CeTIC-DF e da rede GDFNet, inclusive os cadastros, projetos, mapas e diagramas.

Parágrafo único. As ações a que se refere este artigo devem observar os princípios:

- a) da autonomia em gestão de Tecnologia da Informação e Comunicação;
- b) da economicidade na racionalização das aquisições de Tecnologia da Informação e Comunicação;
- c) da eficiência do planejamento de Tecnologia da Informação e Comunicação;
- d) do sigilo de matérias definidas em lei;
- e) da segurança institucional;
- f) da segurança da informação.

Art. 5º A rede GDFNet, os sistemas estruturantes e os serviços corporativos de tecnologia da informação e comunicação de interesse do Distrito Federal deverão ser integrados, hospedados e sustentados no ambiente seguro do CeTIC-DF, ou onde a Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal indicar, por intermédio da Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria Adjunta de Gestão Administrativa.

§ 1º Consideram-se sistemas estruturantes aqueles que oferecem apoio informatizado às atividades de organização administrativa do Distrito Federal, tais como execução financeira e orçamentária, administração de pessoal, contabilidade, auditoria, serviços gerais e aquelas descritas no parágrafo único do art. 7º deste Decreto.

§ 2º Consideram-se serviços corporativos de tecnologia da informação e comunicação todos aqueles providos aos órgãos e entidades da Administração Direta e Indireta do Distrito Federal pelo CeTICDF e pela rede GDFNet, na forma do art. 2º deste Decreto.

Art. 6º Os órgãos e entidades da Administração Direta e Indireta do Distrito Federal devem formalizar comunicação e consulta prévia à Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal nas seguintes hipóteses:

I - Contratações que tenham como objeto enlaces (links) de comunicação de dados de qualquer natureza, mesmo os de simples acesso à internet, necessários aos órgãos e entidades da Administração Direta e Indireta do Distrito Federal, para análise técnica e verificação da possibilidade de compartilhamento da infraestrutura existente na rede GDFNet;

II - Aquisições de servidores, storages, racks, salas cofres, salas seguras, contêineres modulares e quaisquer itens de infraestrutura de Datacenter e/ou Processamento de Dados em Tecnologia da Informação e Comunicação, para análise técnica e verificação da possibilidade de compartilhamento da infraestrutura existente no CeTIC-DF;

III - Ações na área de desenvolvimento ou implantação de sistemas voltados ao Governo do Distrito Federal, para fins de verificação da viabilidade técnica de hospedagem no CeTIC-DF, da existência de sistemas similares já em desenvolvimento ou produção, ou da possibilidade de compartilhamento da solução com os demais órgãos e entidades da Administração Direta e Indireta do Distrito Federal.

§ 1º As disposições do caput deste artigo não se aplicam às atividades de modelagem de processos de negócios, desenvolvimento de softwares departamentais

próprios, aquisição de licenças de uso de software para estações de trabalho, aquisição de itens de computação pessoal e demais recursos tecnológicos departamentais, que continuam sob responsabilidade do próprio órgão e entidade da Administração Direta ou Indireta do Distrito Federal, sem necessidade de consulta à Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal.

§ 2º O domínio e a autorização para utilização de sistemas, dados e informações corporativas por terceiros continuam sob a responsabilidade dos órgãos gestores, da entidade dependente gestora dos sistemas e serviços corporativos, e da Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal.

Art. 7º Compete exclusivamente à Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal realizar as seguintes contratações:

I - a hospedagem de serviços eletrônicos de interesse do Governo do Distrito Federal em datacenters de terceiros ou a contratação de serviços de nuvem pública ou privada, salvo expressa anuência, justificada em processo, do órgão gestor do CeTIC-DF;

II - os circuitos e enlaces de comunicação de dados para interligação de suas unidades ou para acesso à internet, salvo expressa anuência, justificada em processo, do órgão gestor da rede GDFNet; e

III - os serviços voltados ao desenvolvimento de softwares de atividades de área meio, salvo expressa anuência da Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal, por intermédio da Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria Adjunta de Gestão Administrativa, ou do órgão gestor do respectivo sistema estruturante.

Parágrafo único. Consideram-se softwares de atividades de área meio os utilizados para apoio de atividades de gestão ou administração operacional, tais como softwares de gestão de recursos humanos, almoxarifado, patrimônio, contratos, gestão eletrônica de documentos, agendamento eletrônico de serviços ao cidadão, plataforma de voluntariado, execução orçamentária e financeira, e aqueles que não possuem o objetivo de atender as áreas finalísticas para a consecução de políticas públicas ou programas temáticos dos órgãos ou entidades.

Art. 8º Para serem atendidos pelos serviços providos pelo CeTIC-DF e rede GDFNet, os órgãos e entidades da Administração Direta e Indireta do Distrito Federal devem observar os requisitos e os procedimentos técnicos estabelecidos pela Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal mediante regulamentação específica.

Parágrafo único. Observado o procedimento estabelecido no caput, será instituída, por intermédio do instrumento legal adequado, comissão para a elaboração de projeto voltado à finalidade a que se destina, firmando-se cooperação técnica e estabelecendo-se cronograma para desenvolvimento de ações e soluções.

Art. 9º As disposições previstas neste Decreto aplicam-se às aquisições em curso, sem prejuízo da continuidade da prestação do serviço público.

§ 1º As aquisições de que trata o caput devem observar as disposições contratuais e de garantia.

§ 2º As partes envolvidas na operação de migração devem promover os ajustes contratuais e operacionais que se fizerem necessários.

§ 3º Os investimentos necessários à expansão do parque tecnológico do CeTIC visando receber os sistemas e aplicações a serem migrados devem ser negociados conjuntamente entre a Secretaria de Estado de Fazenda, Planejamento, Orçamento e Gestão do Distrito Federal, por meio da Subsecretaria de Tecnologia da Informação e Comunicação da Secretaria Adjunta de Gestão Administrativa, e a entidade responsável pela gestão da aquisição dos bens, soluções, serviços ou dados.

Art. 10. Este Decreto entra em vigor na data de sua publicação.

Art. 11. Ficam revogados os [Decretos nº 30.034, de 06 de fevereiro de 2009](#), [nº 30.762, de 31 de agosto de 2009](#) e [nº 35.974, de 05 de novembro de 2014](#).

Há também a **Portaria nº 484, de 25 de outubro de 2018** que Institui os procedimentos básicos a serem observados pelos órgãos do complexo administrativo do Distrito Federal para solicitação dos serviços providos pelo Data Center Corporativo do GDF e pela Rede Corporativa Metropolitana de Comunicação do Distrito Federal - Rede GDFNet:

O SECRETÁRIO DE PLANEJAMENTO, ORÇAMENTO E GESTÃO DO DISTRITO FEDERAL, com base no disposto no Decreto nº 30.034, de 6 de fevereiro de 2009, no Decreto nº 37.574, de 26 de agosto de 2016 e no uso das atribuições regimentais conferidas pelo Decreto nº 35.837, de 22 de setembro de 2014, em seus arts. 1º, I e IX, e 16, I e II, resolve:

Art. 1º Ficam instituídos os procedimentos básicos a serem observados pelos órgãos do complexo administrativo do Distrito Federal para solicitação dos serviços providos pelo Data Center Corporativo do GDF e pela Rede Corporativa Metropolitana de Comunicação do Distrito Federal - Rede GDFNet.

Art. 2º Para solicitar os serviços fornecidos pelo Data Center Corporativo do GDF e pela Rede Corporativa Metropolitana de Comunicação do GDF - Rede GDFNet, os órgãos do complexo administrativo distrital deverão encaminhar requerimento eletrônico, por meio do Sistema Eletrônico de Informações - SEI, em modelo previamente definido e disponível naquele sistema, à Secretaria de Estado de Planejamento, Orçamento e Gestão. Os órgãos que ainda não disponham do Sistema SEI implantado deverão solicitar por meio de Ofício.

Parágrafo Único. Para que a solicitação seja analisada é necessária declaração expressa da autoridade competente do órgão solicitante, garantindo que o serviço requerido esteja contemplado no Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC do órgão demandante ou do órgão ao qual o solicitante seja vinculado.

Art. 3º Cabe à Subsecretaria de Tecnologia da Informação e Comunicação - SUTIC, da Secretaria de Estado de Planejamento, Orçamento e Gestão - SEPLAG elaborar, atualizar e disponibilizar os modelos de requerimento específicos para os serviços, contendo os requisitos necessários à análise técnica das demandas.

Parágrafo Único. Os modelos de requerimento a serem utilizados para solicitação de hospedagem de sistemas no Data Center Corporativo do GDF e para solicitação de conexão à Rede Corporativa GDFNet serão disponibilizados por meio de Ordens de Serviço específicas, a serem publicadas em até 30 (trinta) dias após a publicação desta Portaria.

Art. 4º Cabe à Subsecretaria de Tecnologia da Informação e Comunicação - SUTIC, da Secretaria de Estado de Planejamento, Orçamento e Gestão - SEPLAG avaliar tecnicamente a solicitação e, caso não seja possível o atendimento no prazo e condições solicitados, apontar as ações e medidas necessárias, assim como condições e previsão de prazo para atendimento, se for o caso.

Art. 5º Cabe ao Secretário de Estado de Planejamento, Orçamento e Gestão decidir acerca dos casos omissos e as situações excepcionais.

Art. 6º Esta Portaria entra em vigor na data de sua publicação.

Além disso os termos do **Regimento Interno** da TERRACAP, em especial o artigo 20 e subsequentes traz:

Art. 20. À Coordenação de Tecnologia da Informação e Inovação - COTIN, unidade orgânica diretamente subordinada à COINT, compete:

I - planejar, coordenar e controlar as atividades das divisões Governança e Processos de TI; Segurança da Informação;

II - sistemas e Gestão de Dados; e Infraestrutura de Redes e Atendimento ao Usuário;

III - coordenar as ações de governança em tecnologia, de modo a promover a sua integração alinhamento à estratégia e plano de negócios da Companhia;

IV - coordenar a elaboração do orçamento e planejamento anual e plurianual da Coordenação e de suas unidades subordinadas, segundo as diretrizes definidas pela Direção da Companhia, bem como acompanhar e monitorar sua execução; e

V - realizar outras tarefas que sejam demandadas pela COINT no exercício de sua competência institucional.

Art. 21. Divisão de Governança e Processos de TI - DIGTI, unidade orgânica diretamente subordinada à COTIN, compete:

I - estabelecer e apoiar a implantação da Governança de TI;

II - atuar no planejamento, execução e controle de políticas relativas à Governança de Tecnologia da Informação;

III - apoiar a elaboração e acompanhar o Plano Estratégico de TI e o Plano Diretor de TI da Terracap, em alinhamento com a estratégia da organização e as políticas governamentais;

IV - estabelecer e apoiar a criação e a manutenção do portfólio, do catálogo de serviços de TI e dos processos de TI;

V - acompanhar e apoiar a gestão dos projetos e dos contratos de soluções de TI;

VI - apoiar a gestão de riscos e segurança da informação de TI;

VII - acompanhar as atividades e a avaliação dos resultados da TI; e

VIII - implementar, acompanhar e fiscalizar o cumprimento das ações de TI em consonância aos apontamentos feitos pelos órgãos de controle visando o amadurecimento da TI da Terracap.

Art. 22. À Divisão de Segurança da Informação - DISEG, unidade orgânica diretamente subordinada à COTIN, compete:

I - planejar e executar a atividade de segurança da informação, no âmbito da Terracap, incluídos a segurança cibernética, a gestão de incidentes computacionais, a proteção de dados, o credenciamento de segurança e o tratamento de informações sigilosas;

<ul style="list-style-type: none"> - Compromisso com resultados - Criatividade e inovação - Satisfação dos clientes - Transparência na Gestão - Comportamento ético - Responsabilidade socioambiental - Respeito nas relações interpessoais
--

Os objetivos estratégicos almejados pela Terracap são os seguintes:

[OBJ01]	ATUAR PARA O ORDENAMENTO DA OCUPAÇÃO E USO DO SOLO
[OBJ02]	ENTREGAR AÇÕES CONCRETAS DE ESG (GOVERNANÇA AMBIENTAL, SOCIAL E CORPORATIVA)
[OBJ03]	ESTIMULAR O DESEMPENHO ECONÔMICO DO DF
[OBJ04]	CONTRIBUIR PARA A MELHORIA DA INFRAESTRUTURA URBANA DO DF
[OBJ05]	APERFEIÇOAR O RELACIONAMENTO COM O CLIENTE
[OBJ06]	GARANTIR A REGULARIDADE DO PATRIMÔNIO FUNDIÁRIO
[OBJ07]	DESENVOLVER NOVOS MODELOS DE NEGÓCIOS QUE GEREM RECEITAS CONTÍNUAS
[OBJ08]	APRIMORAR OS PROCESSOS DE PLANEJAMENTO E ORÇAMENTO
[OBJ09]	APERFEIÇOAR A GESTÃO DOS ATIVOS DE FORMA EFETIVA
[OBJ10]	FORTALECER A TRANSPARÊNCIA NA GESTÃO DA INFORMAÇÃO
[OBJ11]	INOVAR EM PROL DA GESTÃO ORIENTADA PARA RESULTADOS
[OBJ12]	ESTIMULAR A GESTÃO DE PESSOAS COM FOCO EM QUALIDADE DE VIDA E EM COMPETÊNCIAS ESTRATÉGICAS
[OBJ13]	PROVER SOLUÇÕES TECNOLÓGICAS INTEGRADAS

OBJETIVOS ESTRATÉGICOS DA TI

PERSPECTIVA ESTRATÉGICA
Garantir execução mínima de 70% das necessidades previstas no presente PDTI.
PERSPECTIVA DE PESSOAL
Promover a valorização dos seus colaboradores por meio de capacitação contínua, alinhadas aos objetivos estratégicos a serem atingidos.
PERSPECTIVA DE PROCESSOS INTERNOS
Melhorar processos de controle de práticas de gestão do portfólio de TI.
PERSPECTIVA TECNOLÓGICA
Prover soluções tecnológicas estratégicas, previstas no Plano Estratégico da Terracap.

ANÁLISE SWOT

INTERNOS

FORÇAS <ul style="list-style-type: none"> - Engajamento e comprometimento para a resolução de problemas; - Bom relacionamento com as áreas de negócio; - Capacitação adequada para a execução dos trabalhos rotineiros; - Equipe motivada com ações que demonstram a existência de uma liderança interna; - Ambiente de trabalho saudável. 	FRAQUEZAS <ul style="list-style-type: none"> - Falta de envolvimento do setor de TI nos debates estratégicos; - Critérios de priorização de demandas inexistente, ineficaz ou ineficiente; - Sistemas de apoio ineficientes; - Infraestrutura de TI (redes, armazenamento, internet, computadores, sistemas operacionais etc.) desatualizada; - Organização deficiente (hierarquia, quantidade de profissionais etc.).
OPORTUNIDADES <ul style="list-style-type: none"> - Decisão do TCDF (5093/2018) com a finalidade de dar preferência à criação de serviços ao cidadão de forma online; - Desenvolvimento de gestão de riscos setoriais; 	AMEAÇAS <ul style="list-style-type: none"> - Indefinição sobre a manutenção do home office; - Indisponibilidade de infraestrutura de servidores da Terracap;

<ul style="list-style-type: none"> - Diminuição do custo de contratação de serviços em nuvem; - Necessidade de criação de sistemas internos para uso em campo; - Aprimorar/evoluir plataformas tecnológicas envolvidas na venda e no atendimento ao cliente. 	<ul style="list-style-type: none"> - Indisponibilidade dos serviços da Terracap (seja por ataques externos, internos, exploração de vulnerabilidades ou questões contratuais); - Orçamento limitado ou inadequado às metas estratégicas da TI; - Não reposição do quadro de funcionários da ASINF.
---	---

BOLSÃO DE DESENVOLVIMENTO

PROJETOS DE DESENVOLVIMENTO		
ID	DESCRIÇÃO	STATUS
#PDEV033	ERP - Contabilidade e Patrimônio - Implantação de sistema de Contabilidade e Patrimônio em substituição aos sistemas legados atuais que se encontram defasados [OBJ13]	EM ANDAMENTO
#PDEV034	ERP - Financeiro e Tributário - Implantação de sistema de Financeiro e Tributário em substituição aos sistemas legados atuais que se encontram defasados [OBJ13]	EM ANDAMENTO
#PDEV035	ERP - Orçamentário e Gestão Estratégica - Implantação de sistema de Orçamento e Gestão Estratégica em substituição aos sistemas legados atuais que se encontram defasados [OBJ13]	EM ANDAMENTO
#PDEV036	ERP - Suprimentos (Compras e Contratos) - Implantação de sistema de Suprimentos (Compras e Contratos) em substituição aos sistemas legados atuais que se encontram defasados [OBJ13]	EM ANDAMENTO
#PDEV018	Desenvolvimento de projeto de sistema que permita integração entre alienação fiduciária e permita um leilão automatizado. [OBJ13]	SUSPENSO
#PDEV042	Gestão de Estoque Rural - Estabelecer procedimentos informatizados na gestão do estoque rural bem como mecanismos de controles e procedimentos. [OBJ09]	EM ANDAMENTO
#PDEV003	Projeto de atualização dos sistemas GAI, GIU, GIR e GPZ para garantir uma gestão de recebíveis unificada de alienações providas de imóveis rurais ou urbanos. [OBJ08]	SUSPENSO
#PDEV009	Evolução arquitetural do sistema GAI. [OBJ13]	SUSPENSO
#PDEV047	Atualização das tecnologias e arquiteturas de sistemas para acompanhar as melhores práticas do mercado [OBJ13]	A INICIAR

BOLSÃO DE AQUISIÇÕES/RENOVAÇÕES 2024

PROJETOS DE AQUISIÇÃO/CONTRATAÇÃO		
ID	DESCRIÇÃO	STATUS
#PACR028	Aquisição de ferramentas de reunião, comunicação, gestão de equipes e colaboração online.	EM ANDAMENTO
#PACR008	Aquisição de computadores.	EM ANDAMENTO
#PACR036	Serviço de envio de e-mails automatizados (SMTP) na nuvem	A INICIAR
#PACR038	Aquisição de equipamentos de comunicação de rede (<i>switches</i>)	A INICIAR
#PACR039	Solução antivírus para terminais (<i>endpoints</i>)	A INICIAR
#PACR040	Reestruturação de salas técnicas dos escritórios descentralizados da Terracap (508, ETR, Biotic, Garagem)	A INICIAR
#PACR041	Serviços especializados de avaliação e assessoramento em segurança cibernética (<i>pentests</i>)	A INICIAR
#PACR042	Solução tecnológica de Gestão de Acesso Privilegiado (PAM)	A INICIAR
#PACR043	Serviço de gateway antispam	A INICIAR
#PACR044	Suporte e Garantia Storage	A INICIAR
#PACR045	Contratação/Renovação de contrato de fábrica de software.	A INICIAR
#PACR046	Aquisição/Renovação de contrato de link de internet.	A INICIAR
#PACR047	Aquisição de equipamentos profissionais para salas de videoconferência.	A INICIAR
#PACR048	Aquisição de projetores	A INICIAR

ORÇAMENTO TI 2024

Esfera Orçamentária	Despesa Prevista
2024	
Dispêndio	R\$ 11.291.191,00
Investimento	R\$ 7.662.045,00
Total para 2024	R\$ 18.953.236,00

ANÁLISE DE RISCOS

FATORES CRÍTICOS DE SUCESSO

- Disponibilidade Orçamentária;
- Disponibilidade de recursos humanos;
- Respeito à cronologia de execução e prioridades estabelecidas neste Plano Diretor;
- Evolução dos processos internos acerca da gestão de portfólio de metas, projetos e ações previstas neste PDTI;
- Controle e acompanhamento das metas, projetos e ações derivadas do PDTI pelo Comitê de Tecnologia da Informação;
- Acompanhamento dos riscos extraídos do PDTI;
- Envolvimento efetivo das áreas de negócio da Terracap.

MAPA DE RISCOS TI - VIDE 154431988

MATRIZ DE RISCOS DE TI

- 34 (trinta e quatro) riscos podendo conter mais de um fator de causa associado, divididos entre os níveis extremo, alto e moderado.
- Apetite de Risco: Médio
- Fase 1: 09 riscos -> Execução Imediata
- Fase 2: 25 riscos -> Início no 4º Trimestre
- Aprovada em 18/07/2024 -> Decisão DIRET 540/2024
- SEI: 00111-00010136/2023-11

RELATÓRIOS AUDITORIA INDEPENDENTE - AMBIENTE DE TI

EXERCÍCIO	Pontos de Atenção	STATUS
2022(00111-00001290/2022-11)	2.1 - Política de Privacidade de Dados Pessoais 2.2. Fragilidade em controles no ambiente de alocação dos servidores 2.3. Ausência de formalização dos procedimentos de testes de contingências	2.1 - ATENDIDA 2.2 - ATENDIDA 2.3 - ATENDIDA **Monitoramento extinto
2023(00111-00002824/2023-15)	2.1. Parâmetros de senha na rede corporativa 2.2. Ausência de formalização de concessão de acesso 2.3. Ausência de metodologia formal de gerenciamento de mudanças sistêmicas 2.4. Revisão de políticas internas 2.5. Implementar políticas para mapeamento de transações conflitantes 2.6. Uso de contas de acesso genéricas	2.1 - ATENDIDA 2.2 <i>PARCIALMENTE ATENDIDA</i> 2.3 - <i>PARCIALMENTE ATENDIDA</i> 2.4 - <i>EM ATENDIMENTO</i> 2.5 - <i>A SER IMPLEMENTADA</i> 2.6 - ATENDIDA *Em monitoramento pela AUDIT
2024(00111-00006247/2024-11)	2.1 - Ausência de parâmetros de segurança aplicáveis a complexibilidade das senhas de acessos 2.2 - Ausência de formalização de usuários administradores genéricos 2.3 - Ausência de um plano de contingência	2.1 - ATENDIDA 2.2 - A VERIFICAR 2.3 - A VERIFICAR *Em monitoramento pela AUDIT

Ressalta-se mais uma vez que o objetivo geral da presente auditoria consiste em verificar os controles primários referentes governança de TI no âmbito da Terracap, por amostragem, relativos à confecção, gerenciamento, acompanhamento, atingimento de metas e modificações ao longo dos resultados.

Durante o planejamento, é importante frisar os **objetivos específicos** que nortearam o escopo:

1. Verificar as ações e planos para a execução da Governança de TI;
2. Verificar as ferramentas e rotinas referentes à Cibersegurança;
3. Identificar os mecanismos e rotinas relacionados à ciência de dados;
4. Avaliação da implementação do sistema integrado de gestão (BENNER);
5. Verificar a integração entre a área de informática da empresa e as áreas de gestão da TERRACAP;
6. Analisar as ações para mitigação dos pontos de atenção da auditoria independente;
7. Verificar a existência e utilização do TIC (Tecnologia da Informação e Comunicação);
8. Verificar os riscos diretos na gestão de riscos.

IV – SOLICITAÇÕES DE AUDITORIA

Considerando o contexto, no decorrer dos trabalhos foram expedidas as seguintes Solicitações de Auditoria:

Nº SOLICITAÇÃO	DESTINO	PEDIDO
96 (143303747)	COTIN	Reunião com o titular da COTIN e os respectivos Chefes de Núcleos, de forma presencial, na sala da COTIN, no dia 21/06/2024, às 10h , visando apresentar a missão, estrutura e rotinas
98 (122529443)	COTIN	Pedidos: a) Apresentação referente à reunião realizada no último dia 21/06/2024; b) Informar quais normativos a COTIN utiliza nas suas atribuições; c) Apresentar lista de todos os contratos e convênios ativos que a COTIN executa/fiscaliza; d) Os projetos pertencentes ao PDTI/2021/2024 (144184291) com o status: "SUSPENSO" possuem previsão de retomada?; e) Os projetos pertencentes ao PDTI/2021/2024 (144184291) com o status: "A INICIAR" possuem previsão para o exercício de 2024?; f) Apresentar o relatório de atividades dessa Coordenação referente ao 1º trimestre de 2024; g) Existe alguma ferramenta de controle para gerenciamento das atividades?; h) Enumere, se for o caso, os principais gargalos/dificuldades dessa Coordenação para realização de suas atividades.
102 (144689415)	DIGER	1. Informar detalhadamente sobre a matriz de risco de TI, informando inclusive o atual estágio e número de processo com acesso, se houver.
112 (147748674)	COINT e COTIN	COTIN: cronograma de implementação do sistema BENNER, com previsão de entregas, em especial até 31/12/2024; - Informar se houve no exercício de 2024 alguma tentativa de invasão aos sistemas corporativos da TERRACAP, e outras tentativas virtuais maliciosas (se sim, detalhar), e se houve algum dano no(s) sistema (s), e quais ações realizadas pela COTIN para mitigação. COTIN e Gestoras do do Convênio nº 170/2023: Relatar, de acordo com o plano de trabalho estabelecido, se houve entregas, o que está em desenvolvimento (detalhar), e as possíveis entregas/produtos previstos até 31/12/2024.

No que se refere aos métodos e técnicas empregados na auditoria os trabalhos seguiram as práticas usuais de auditoria. Quanto aos procedimentos de auditoria foram analisados documentos, manuais, legislação, processos, observações e esclarecimentos diversos.

V – DESENVOLVIMENTO DA AUDITORIA

O presente relatório contempla os resultados obtidos em decorrência das informações prestadas pelas áreas responsáveis, análise de normas e manuais VIGENTES, análise amostral dos processos que englobam várias frentes relacionadas à governança de TI.

Utilizou-se de revisões analíticas nas declarações e controles apresentados pela Coordenação de Tecnologia da Informação e Inovação - COTIN, visando obter algum grau de confiabilidade acerca dos principais desdobramentos das ações em desenvolvimento.

Observa-se que, no que tange ao relacionamento intersetorial dos envolvidos no processo, esta auditoria interna não pôde verificar a uniformização ou padronização na instrução processual, impossibilitando que a verificação das sequências da condução dos procedimentos internos fosse observada em sua completude, fato observado no corpo deste trabalho.

Para as análises foram considerados:

- Regimento Interno da Companhia Imobiliária de Brasília;
- Norma NBC TA 265 (Comunicação de Deficiências de Controle Interno);
- Plano Diretor de TI (144184291);
- Mapa de riscos de TI 2023 e atualizado (154427883 e 154431988);
- Convênio 170/2023 (137785000);
- Norma de Serviço RIS 03 - Norma de Segurança da Informação (154448174);
- Norma de Serviço TIS 04 - Política de Privacidade de Dados Pessoais (154443324);
- Relatórios de auditoria independente que avaliaram o ambiente e segurança de TI - 2022, 2023 e 2024 (154439967, 137839477 e 154448407);
- Fluxo de rotina da COTIN;
- Relatórios de Atividades da COTIN - 1º, 2º e 3º Trimestres de 2024 (144690468, 154453266 e 154453508);
- Dados oficiais da TI (144666624);
- Projeto de Governança e Cyber Segurança (144666624).

Algumas das informações acima foram apresentadas quando provocadas por meio da Solicitação de Auditoria nº 98 (144175544). Além disso, informaram:

a) Apresentação referente à reunião realizada no último dia 21/06/2024;

Ver Doc. SEI 144666624.

b) Informar quais normativos a COTIN utiliza nas suas atribuições;

Atualmente a tecnologia da informação da Terracap (TI organizacional) está amparada pelos seguintes normativos internos:

- Plano Diretor de Tecnologia (PDTI)
- Política de Segurança da Informação (POSIC) [00111-00004374/2020-44];
- Norma de Segurança da Informação (TIS 03) [00111-00004374/2020-44]
- Política de Privacidade de Dados Pessoais (TIS 04) [00111-00007646/2022-20]
- Regimento Interno do Comitê de Tecnologia e Segurança da Informação [0111-001514/2012; 00111-00014542/2017-12]
- RILC - Regulamento Interno de Licitações e Contratações da Companhia Imobiliária de Brasília – TERRACAP
- DECRETO Nº 40.015, DE 14 DE AGOSTO DE 2019
- Dispõe sobre a obrigatoriedade de elaboração e publicação dos Planos Diretores de Tecnologia da Informação e Comunicação e sobre a centralização e utilização da rede GDFNet, da infraestrutura do Centro de Tecnologia da Informação e Comunicação do Distrito Federal - CeTIC-DF e dos sistemas de informação no âmbito da Administração Direta e Indireta do Distrito Federal, e dá outras providências.
- PORTARIA Nº 484, DE 25 DE OUTUBRO DE 2018
Institui os procedimentos básicos a serem observados pelos órgãos do complexo administrativo do Distrito Federal para solicitação dos serviços providos pelo Data

c) Apresentar lista de todos os contratos e convênios ativos que a COTIN executa/fiscaliza;

Ver Doc. SEI 144671592.

d) Os projetos pertencentes ao PDTI/2021/2024 (144184291) com o status: "SUSPENSO" possuem previsão de retomada?

ID	PROJETOS COM STATUS "SUSPENSO" NO PDTI 2024	MANIFESTAÇÃO COTIN
#PDEV018	Desenvolvimento de projeto de sistema que permita integração entre alienação fiduciária e permita um leilão automatizado	Previsto para o exercício atual, porém dependerá de conclusão de etapas de integração financeira do ERP com sistemas GAI, Controle de Operação, GIR, GGR e Certidão de Crédito
#PDEV003	Projeto de atualização dos sistemas GAI, GIU, GIR e GPZ para garantir uma gestão de recebíveis unificada de alienações providas de imóveis rurais ou urbanos	Previsto para o exercício atual, porém dependerá de conclusão de etapas de integração financeira do ERP com sistemas GAI, Controle de Operação, GIR, GGR e Certidão de Crédito
#PDEV009	Evolução arquitetural do sistema GAI	Previsto para o exercício atual, porém dependerá de conclusão de etapas de integração financeira do ERP com sistemas GAI, Controle de Operação, GIR, GGR e Certidão de Crédito

e) Os projetos pertencentes ao PDTI/2021/2024 (144184291) com o status: "A INICIAR" possuem previsão para o exercício de 2024?

ID	PROJETOS COM STATUS "A INICIAR" NO PDTI 2024	MANIFESTAÇÃO COTIN
#PDEV047	Atualização das tecnologias e arquiteturas de sistemas para acompanhar as melhores práticas do mercado	<p>Não se trata de um projeto único, mas de ações evolutivas de diversos sistemas. Atualmente está em andamento e já foram executadas atualizações tecnológicas nos sistemas legados visando sua adequação aos perfis das tecnologias de mercado, tais quais: adoção de ferramentas para gestão de dependências, ajustes para execução em ambiente baseado em contêineres e evolução em versões de linguagem de programação.</p> <p>Além disso, temos trabalhado no desenvolvimento e aprimoramento de bibliotecas de código-fonte que contém componentes reutilizáveis referentes a autenticação/autorização, padronização de interface de usuário e interface swagger API para outros sistemas, artefatos para enquadramento das aplicações nas esteiras DevOps em ambientes baseados em contêineres, dentre outros.</p> <p>Sistemas legados migrados para PHP 8.1 e que receberam a adição do gerenciador de dependências "composer" (já em produção)</p> <ul style="list-style-type: none"> - Contracheque Internet - Compras On-line - Proposta - Autenticador de Documentos - GPZ Externo (Gestão de Prazos) - Portal do Servidor - Consulta de Ocupação* - Notificação de Licitações* - Autenciador de Documentos <p>Sistemas já migrados para Docker para adequação à nova esteira DevOps (em fase final de homologação)</p> <ul style="list-style-type: none"> - GLA (Licitações Ambientais) - GLI (Licitações e Instrumentos) - gai-api (API de Alienações) <p>Sistemas novos já concebidos sob a nova arquitetura e infraestrutura DevOps (em fase de homologação)</p> <ul style="list-style-type: none"> - PII Redactor (Tarjamento de Documentos) - homologação - Portal Aldeias do Cerrado - Venda Direta - Consulta de Ocupação* - Notificação de Licitações* <p>*Primeiramente migrados para PHP 8 e posteriormente movidos para a nova esteira</p>
#PACR036	Serviço de envio de e-mails automatizados (SMTP) na nuvem	Não iniciado. Término previsto até o fim do exercício atual.
#PACR038	Aquisição de equipamentos de comunicação de rede (switches)	Em andamento. Término previsto para 2025.
#PACR039	Solução antivírus para terminais (endpoints)	Em andamento. Término previsto até o fim do exercício atual.
#PACR040	Reestruturação de salas técnicas dos escritórios descentralizados da Terracap (508, ETR, Biotic, Garagem)	Em andamento. Término previsto até o fim do exercício atual.
#PACR041	Serviços especializados de avaliação e assessoramento em segurança cibernética (pentests)	Não iniciado. Término previsto até o fim do exercício atual.

#PACR042	Solução tecnológica de Gestão de Acesso Privilegiado (PAM)	Não iniciado. Término previsto para 2025.
#PACR043	Serviço de gateway antispam	Em andamento. Término previsto até o fim do exercício atual.
#PACR044	Suporte e Garantia Storage	Em andamento. Término previsto até o fim do exercício atual.
#PACR045	Contratação/Renovação de contrato de fábrica de software	Em andamento. Término previsto até o fim do exercício atual.
#PACR046	Aquisição/Renovação de contrato de link de internet.	Não iniciado. Término previsto até o fim do exercício atual.
#PACR047	Aquisição de equipamentos profissionais para salas de videoconferência	Concluído.
#PACR048	Aquisição de projetores	Concluído.

f) Apresentar o relatório de atividades dessa Coordenação referente ao 1º trimestre de 2024;

Ver Doc. 144690468.

g) Existe alguma ferramenta de controle para gerenciamento das atividades?

Sim. A COTIN e suas unidades usam como ferramenta de gestão e acompanhamento de projetos e tarefas o sistema Redmine (redmine.terracap.df.gov.br). Dessa maneira, tanto os projetos planejados no PDTI, quanto outras ações internas necessárias para a manutenção e evolução do ambiente de tecnologia são cadastrados pelos responsáveis e acompanhados pelos gestores.

h) Enumere, se for o caso, os principais gargalos/dificuldades dessa Coordenação para realização de suas atividades.

- Ausência de programa continuado de capacitação/atualização da equipe, o que leva a defasagem do conhecimento interno e dificuldade de acompanhar as melhores práticas de tecnologia do mercado;
- Dependência de terceiros acima do desejável no que se refere a equipe técnica especializada de infraestrutura de tecnologia, o que gera um alto risco de continuidade e segurança, além de baixa capacidade na execução de projetos de tecnologia de interesse da Terracap.
- Equipes de governança e segurança de TI subdimensionadas para o trabalho de médio e longo prazo que deve ser realizado, ou seja, suporte para melhoria da maturidade de TI de acordo com as melhores práticas.
- Com a mudança de plataforma principal de sistemas corporativos para ERP, será necessário ter no quadro profissionais que dominem a tecnologia e funcionamento do sistema para garantir o bom andamento dos processos de trabalhos e possíveis futuras novas implantações, como Biotic, ETR e outras demais empresas que venham surgir.
- Baixa quantidade de normativos e políticas para suportar a governança de tecnologia.

Já na Solicitação de Auditoria nº 102 (144689415) a Divisão de Gestão de Riscos informou que:

"foi apresentada minuta da Matriz de riscos de Governança de TI (142481359) com a proposição dos respectivos planos de resposta (142481687), bem como foi elaborado o Relatório Final (141902817) dos trabalhos contemplando todas as etapas desenvolvidas."

MATRIZ DE RISCOS DE TI

- 34 (trinta e quatro) riscos podendo conter mais de um fator de causa associado, divididos entre os níveis extremo, alto e moderado.
- Apetite de Risco: Médio
- Fase 1: 09 riscos -> Execução Imediata
- Fase 2: 25 riscos -> Início no 4º Trimestre
- Aprovada em 18/07/2024 -> Decisão DIRET 540/2024
- SEI: 00111-00010136/2023-11

Fonte: Diger - Relatório 2º Trimestre 2024

A Solicitação de Auditoria nº 112 (147748674), a COTIN foi indagada acerca do cronograma de execução do sistema BENNER (ERP) e sobre tentativas de invasão ao sítio da TERRACAP, a qual se manifestou da seguinte forma:

" Em atenção ao pedido de informações da Solicitação SEI 147748674, seguem as manifestações da Coordenação de Tecnologia da Informação e Inovação (COTIN). O cronograma de implementação dos módulos remanescentes do sistema BENNER atual está previsto para seguir a tabela abaixo.

MÓDULO/ PRAZO	ago/24			set/24	out/24	nov/24	dez/24
ORÇAMENTO	Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados			Preparar informações e sistemas para virada de chave
FINANCEIRO		Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados		Preparar informações e sistemas para virada de chave
CONTÁBIL			Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados	Preparar informações e sistemas para virada de chave
TRIBUTOS			Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados	Preparar informações e sistemas para virada de chave
COMPRAS				Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados
CONTRATOS				Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados
INTEGRAÇÃO FINANCEIRA	Configuração contábil das operações			Parametrizção do ERP		Validação das operações implementadas	
				Implementação das operações entre sistemas			

Cronograma ERP Benner até o fim de 2024

Quanto a tentativas de invasão, destaca-se que, mensalmente, a Terracap registra **milhares de tentativas (ou suspeita de tentativas) de exploração ou ataques. O Relatório SEI 148789414 traz mais detalhes sobre esse cenário de ameaças que pode resultar em invasão ou outros tipos de crimes cibernéticos, caso as barreiras de segurança não sejam suficientes.**" (g.n.)

Extrato de tentativas de invasões 2024 - Janeiro a julho

Tipos de Ataques	Non Compliant HTTP, Non Compliant DNS, FTP Bounce, Sequence Verifier, Spoofed Reset, Packet Sanity, HTTP Format Sizer, HTTP Methods, Non Compliant CIFS, Command Injection, Cross-Site Scripting (XSS), SQL Injection, Microsoft Windows NT Null - centenas de milhares por mês - 257 mil requisições suspeitas só em junho 2024. Média de 8.586 p/dia.
SPAM por destinatário	SPAM por destinatário - 102.688(até agosto de 2024)

Já as executoras do Convênio nº 170/2023 informaram sobre a execução do Convênio nº 170/2023 FAPEU e TERRACAP que tem por objeto a construção de Ambiente de Inteligência de Gestão, Roadmap de Cibersegurança e Modelo de Governança de TIC para a TERRACAP, em consonância com o Plano de Trabalho e cronograma acostados aos autos do Processo SEI/GDF nº 00111-00005622/2023-17:

" Em resposta à solicitação da Auditoria Interna, apresentamos o status atual das atividades relacionadas à Governança de TI no âmbito da Terracap, conforme o plano de trabalho estabelecido no Convênio nº 170/2023 - Processo SEI nº 00111-00005622/2023-17.

Este relatório inclui informações sobre as entregas realizadas, os projetos em desenvolvimento e as previsões de entregas até 31/12/2024.

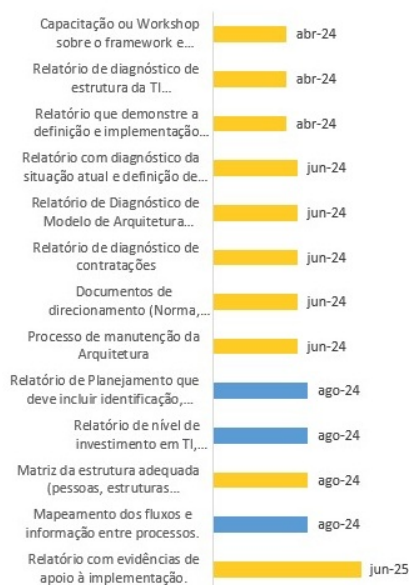
Até o momento, temos o seguinte **panorama envolvendo as atividades entregues e em desenvolvimento do referido convênio - separado por agenda:**

Legenda: os itens em **amarelo** foram validados informalmente pelos executores, ou seja, já estão prontos para faturamento. Os itens em **verde** já fizeram parte da primeiro pagamento. Os itens em **azul** são os que faltam entregar.

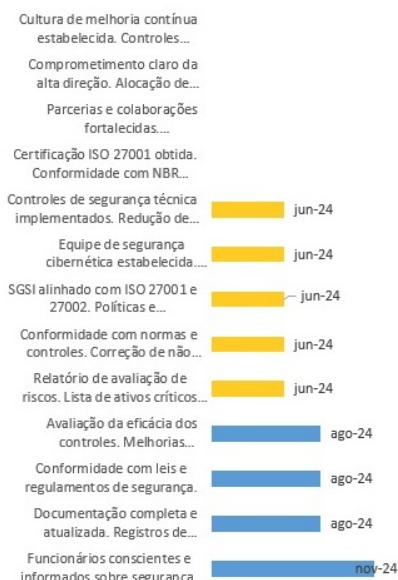
Cronograma de Entregas Previstas Agenda_01



Cronograma de Entregas Previstas Agenda_02



Cronograma de Entregas Previstas Agenda_03



7. Com relação à **Agenda 1**, apresenta-se o seguinte panorama: até o momento, **62 (sessenta e dois) painéis estão em produção**, abrangendo os temas detalhados na abaixo:

Área	Fase de Implementação	Qtd Painéis	Processo de Trabalho
	100%	0	
PRESI/DIPLA	75%	7	Orçamento/Financeiro
PRESI/DIMOG	75%	5	Estratégia
COINT/DIGER	75%	2	Riscos
DITEC/GEREN	75%	8	Gestão de Contratos e execução de obras
DITEC/GEPRO	75%	1	Projetos Urbanísticos
DITEC/GEFIS	50%	2	Fiscalização do Patrimônio
DITEC/GEMAM	25%	3	Licenciamento Ambiental
DIRAF	50%	9	Gestão Financeira/ Recebíveis/ Gestão de Contratos/ Gestão de Certidão de Créditos / Recursos Humanos
DIRAF/GEPEs	50%	2	Recursos Humanos
DICOM	50%	3	Gestão de vendas/Gestão de Concessões
DIRES	50%	5	Progr. Desenvolvimento / Regularização Especial
DINEG	50%	8	Gestão de Contratos de Parceria/ Gestão de Contratos/ Gerenciamento de Projetos/ Prospecção de Novos Negócios
DIJUR	50%	4	Gestão Jurídica
ETR/DIRAD	50%	3	Recursos Humanos
TOTAL		62	

Adicionalmente, acostamos aos autos o **cronograma de entregas originalmente pactuado** (148408464), bem como o **cronograma das entregas realizadas**

e previstas (148481190), para conhecimento.

Este relatório reflete o progresso contínuo na implementação da Governança de TI na Terracap. Todas as frentes estão empenhadas em cumprir os prazos estabelecidos, assegurando que as atividades sejam conduzidas com o mais alto padrão de qualidade e conformidade. Permanecemos à disposição para esclarecimentos adicionais e para acompanhar as próximas etapas da auditoria."

Por fim, foram objeto de consulta desta Auditoria os seguintes processos:

Processo	Objeto	Observação
00111-00004374/2020-44	Política de Segurança da Informação	Ativo
00111-00004374/2020-44	Norma de Segurança da Informação	Ativo
00111-00007646/2022-20	Política de Privacidade de Dados Pessoais	Ativo
00111-00014542/2017-12	Regimento Interno do Comitê de Tecnologia e Segurança da Informação	Ativo
00111-00005622/2023-17	Convênio nº 170/2023 - TERRACAP e FAPEU	Em execução
00111-00001290/2022-11	Auditoria Independente 0 ambiente e segurança de TI - 2022	concluído
00111-00002824/2023-15	Auditoria Independente 0 ambiente e segurança de TI - 2023	Em monitoramento
00111-00006247/2024-11	Auditoria Independente 0 ambiente e segurança de TI - 2024	Em monitoramento

VI - ANÁLISE

De todas as informações disponibilizadas para esta Auditoria Interna em resposta às solicitações de Auditoria, identificou-se:

Inicialmente, com relação a atual estrutura da Coordenação de Tecnologia da Informação e Inovação, atualmente subordinada à Controladoria Interna, esta passou por uma reestrutura robusta em relação a anterior que conta com 26 funcionários de TI para aproximadamente 1.000(mil) usuários, para atendimento em 4 (quatro) locais: TERRACAP, BIOTIC, ETR, 508 sul e ALDEIAS.

Ativamente operacionalizam 76 (setenta e seis) sistemas de informação, 1 (um) aplicativo móvel, 251 (duzentos e cinquenta e um) servidores virtuais e 26 contratos ativos.

Em síntese:



Com relação aos normativos em utilização pela área tecnológica, detectou-se-se a utilização dos seguintes principais normativos:

- Política de Segurança da Informação (POSIC);

- Norma de Segurança da Informação (TIS 03);
- Política de Privacidade de Dados Pessoais (TIS 04);
- Regimento Interno do Comitê de Tecnologia e Segurança da Informação.

Já no que diz respeito aos projetos para 2024, temos:

Projetos *suspensos*, porém com previsão de retomada para 2024:

- Desenvolvimento de projeto de sistema que permita integração entre alienação fiduciária e permita um leilão automatizado

De acordo com a COTIN, há a previsão para o exercício atual, porém dependerá de conclusão de etapas de integração financeira do ERP com sistemas GAI, Controle de Operação, GIR, GGR e Certidão de Crédito;

- Projeto de atualização dos sistemas GAI, GIU, GIR e GPZ para garantir uma gestão de recebíveis unificada de alienações providas de imóveis rurais ou urbanos

De acordo com a COTIN, há a previsão para o exercício atual, porém dependerá de conclusão de etapas de integração financeira do ERP com sistemas GAI, Controle de Operação, GIR, GGR e Certidão de Crédito;

- Evolução arquitetural do sistema GAI

De acordo com a COTIN, há a previsão para o exercício atual, porém dependerá de conclusão de etapas de integração financeira do ERP com sistemas GAI, Controle de Operação, GIR, GGR e Certidão de Crédito.

Para os projetos previstos, há 7 *em andamento*:

- 1) **Aquisição de equipamentos de comunicação de rede (switches) - Término previsto para 2025;**
- 2) **Solução antivírus para terminais (endpoints) - Término previsto até o fim do exercício atual;**
- 3) **Reestruturação de salas técnicas dos escritórios descentralizados da Terracap (508, ETR, Biotic, Garagem) - Término previsto até o fim do exercício atual;**
- 4) **Serviço de gateway antispam - Término previsto até o fim do exercício atual;**
- 5) **Suporte e Garantia Storage - Término previsto até o fim do exercício atual;**
- 6) **Contratação/Renovação de contrato de fábrica de software - Término previsto até o fim do exercício atual;**
- 7) **Reestruturação de salas técnicas dos escritórios descentralizados da Terracap (508, ETR, Biotic, Garagem) - Término previsto até o fim do exercício atual;**

2 Projetos **concluídos**:

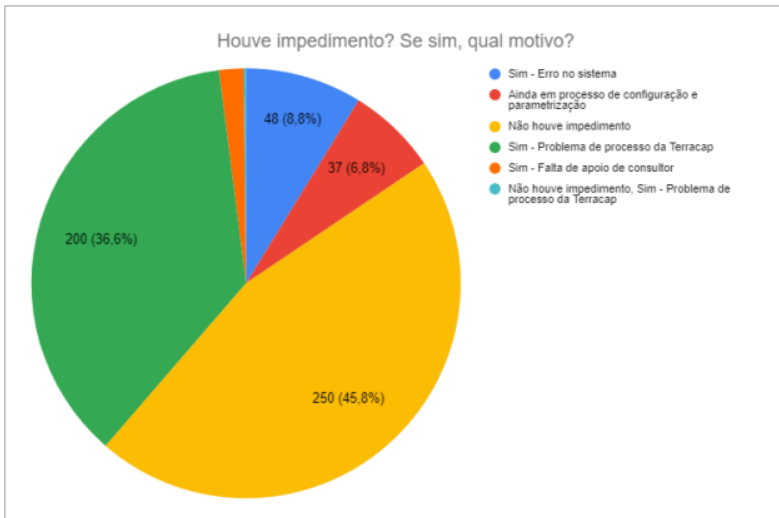
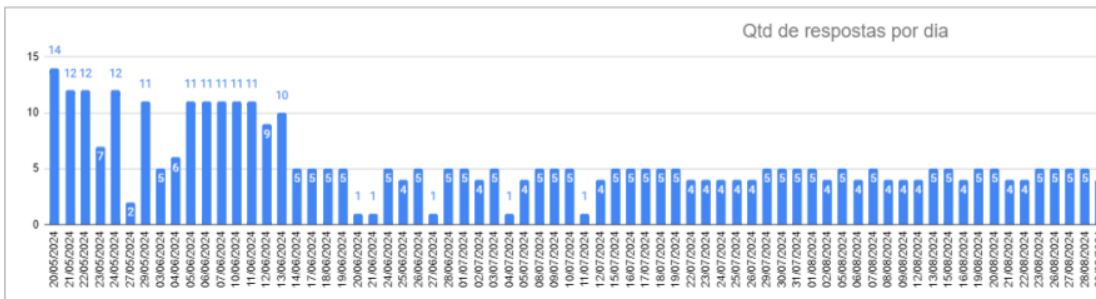
- **Aquisição de equipamentos profissionais para salas de videoconferência - concluído;**
- **Aquisição de projetores - concluído.**

-Sistema BENNER - cronograma de execução - 08/2024:

MÓDULO/ PRAZO	ago/24		set/24	out/24	nov/24	dez/24		
ORÇAMENTO	Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados			Preparar informações e sistemas para virada de chave	
FINANCEIRO		Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados		Preparar informações e sistemas para virada de chave	
CONTÁBIL			Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados	Preparar informações e sistemas para virada de chave	
TRIBUTOS			Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados	Preparar informações e sistemas para virada de chave	
COMPRAS				Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados	Preparar informações e sistemas para virada de chave
CONTRATOS				Adequação do processo de trabalho ao sistema	Corrigir erros blocantes de sistema	Atualizar informações	Fechamento paralelo com sistemas legados	Preparar informações e sistemas para virada de chave
INTEGRAÇÃO FINANCEIRA	Configuração contábil das operações			Parametrização do ERP		Validação das operações implementadas		
				Implementação das operações entre sistemas				

Cronograma ERP Benner até o fim de 2024

-Sistema BENNER - cronograma de execução - 10/2024:



- Financeiro * F
- Contabil * Contabilidade e Patrimonio - Conta
- Contabil * Contabilidade e Patrimonio - Fisr
- Contabil * Contabilidade e Patrim
- Contabil * Contabilidade e Patrimonio - Conta
- Contabil * Contabilidade
- Compras * Suprimentos
- Compras * Suprimentos
- Compras * S
- Compras * Supriment
- Materiais * Inventari

O cronograma apresentado mostra o monitoramento diário das fases de implementação, bem como suas repactuações quando necessárias. É um sistema robusto, grande que envolve ao mesmo tempo diversas áreas que precisam integrar juntas, pois do caso contrário o módulo não avança. Há uma previsão de "virada de chave" em 01/2025.

O Convênio com a Fundação de Amparo à Pesquisa e Extensão Universitária - FAPEU que tem por objeto desenvolvimento de Ambiente de Inteligência de Gestão, Roadmap de Cibersegurança e Modelo de Governança de TIC para TERRACAP, está sendo executado dentro do previsto (plano de trabalho original), onde foram já entregues 18 itens, data-base junho de 2024, e as demais em curso normal:

Área	Fase de Implementação	Qtd Painéis	Processo de Trabalho
	100%	0	
PRESI/DIPLA	75%	7	Orçamento/Financeiro
PRESI/DIMOG	75%	5	Estratégia
COINT/DIGER	75%	2	Riscos
DITEC/GEREN	75%	8	Gestão de Contratos e execução de obras
DITEC/GEPRO	75%	1	Projetos Urbanísticos
DITEC/GEFIS	50%	2	Fiscalização do Patrimônio
DITEC/GEMAM	25%	3	Licenciamento Ambiental
DIRAF	50%	9	Gestão Financeira/ Recebíveis/ Gestão de Contratos/ Gestão de Certidão de Créditos / Recursos Humanos
DIRAF/GEPEs	50%	2	Recursos Humanos
DICOM	50%	3	Gestão de vendas/Gestão de Concessões
DIRES	50%	5	Progr. Desenvolvimento / Regularização Especial
DINEG	50%	8	Gestão de Contratos de Parceria/ Gestão de Contratos/ Gerenciamento de Projetos/ Prospeção de Novos Negócios
DIJUR	50%	4	Gestão Jurídica
ETR/DIRAD	50%	3	Recursos Humanos
TOTAL		62	

A FAPEU NÃO CONTABILIZA OS STATUS:

- Ambiente de engenharia
- Encaminhado para executores
- Ambiente de decisão
- Cancelado
- Em Branco

Data	Fluxo Financeiro Acumulado
Jun/24	0
Jul/24	141
Ago/24	288
Sep/24	428
Out/24	568
Nov/24	708
Dez/24	848
Jan/25	988
Fev/25	1128
Mar/25	1268
Abr/25	1408
Mai/25	1548
Jun/25	1688
Jul/25	1828
Ago/25	1968
Sep/25	2108
Out/25	2248
Nov/25	2388
Dez/25	2528
Jan/26	2668
Fev/26	2808
Mar/26	2948
Abr/26	3088
Mai/26	3228
Jun/26	3368
Jul/26	3508
Ago/26	3648
Sep/26	3788
Out/26	3928
Nov/26	4068
Dez/26	4208
Jan/27	4348
Fev/27	4488
Mar/27	4628
Abr/27	4768
Mai/27	4908
Jun/27	5048
Jul/27	5188
Ago/27	5328
Sep/27	5468
Out/27	5608
Nov/27	5748
Dez/27	5888
Jan/28	6028
Fev/28	6168
Mar/28	6308
Abr/28	6448
Mai/28	6588
Jun/28	6728
Jul/28	6868
Ago/28	7008
Sep/28	7148
Out/28	7288
Nov/28	7428
Dez/28	7568
Jan/29	7708
Fev/29	7848
Mar/29	7988
Abr/29	8128
Mai/29	8268
Jun/29	8408
Jul/29	8548
Ago/29	8688
Sep/29	8828
Out/29	8968
Nov/29	9108
Dez/29	9248
Jan/30	9388
Fev/30	9528
Mar/30	9668
Abr/30	9808
Mai/30	9948
Jun/30	10088
Jul/30	10228
Ago/30	10368
Sep/30	10508
Out/30	10648
Nov/30	10788
Dez/30	10928
Jan/31	11068
Fev/31	11208
Mar/31	11348
Abr/31	11488
Mai/31	11628
Jun/31	11768
Jul/31	11908
Ago/31	12048
Sep/31	12188
Out/31	12328
Nov/31	12468
Dez/31	12608
Jan/32	12748
Fev/32	12888
Mar/32	13028
Abr/32	13168
Mai/32	13308
Jun/32	13448
Jul/32	13588
Ago/32	13728
Sep/32	13868
Out/32	14008
Nov/32	14148
Dez/32	14288
Jan/33	14428
Fev/33	14568
Mar/33	14708
Abr/33	14848
Mai/33	14988
Jun/33	15128
Jul/33	15268
Ago/33	15408
Sep/33	15548
Out/33	15688
Nov/33	15828
Dez/33	15968
Jan/34	16108
Fev/34	16248
Mar/34	16388
Abr/34	16528
Mai/34	16668
Jun/34	16808
Jul/34	16948
Ago/34	17088
Sep/34	17228
Out/34	17368
Nov/34	17508
Dez/34	17648
Jan/35	17788
Fev/35	17928
Mar/35	18068
Abr/35	18208
Mai/35	18348
Jun/35	18488
Jul/35	18628
Ago/35	18768
Sep/35	18908
Out/35	19048
Nov/35	19188
Dez/35	19328
Jan/36	19468
Fev/36	19608
Mar/36	19748
Abr/36	19888
Mai/36	20028
Jun/36	20168
Jul/36	20308
Ago/36	20448
Sep/36	20588
Out/36	20728
Nov/36	20868
Dez/36	21008
Jan/37	21148
Fev/37	21288
Mar/37	21428
Abr/37	21568
Mai/37	21708
Jun/37	21848
Jul/37	21988
Ago/37	22128
Sep/37	22268
Out/37	22408
Nov/37	22548
Dez/37	22688
Jan/38	22828
Fev/38	22968
Mar/38	23108
Abr/38	23248
Mai/38	23388
Jun/38	23528
Jul/38	23668
Ago/38	23808
Sep/38	23948
Out/38	24088
Nov/38	24228
Dez/38	24368
Jan/39	24508
Fev/39	24648
Mar/39	24788
Abr/39	24928
Mai/39	25068
Jun/39	25208
Jul/39	25348
Ago/39	25488
Sep/39	25628
Out/39	25768
Nov/39	25908
Dez/39	26048
Jan/40	26188
Fev/40	26328
Mar/40	26468
Abr/40	26608
Mai/40	26748
Jun/40	26888
Jul/40	27028
Ago/40	27168
Sep/40	27308
Out/40	27448
Nov/40	27588
Dez/40	27728
Jan/41	27868
Fev/41	28008
Mar/41	28148
Abr/41	28288
Mai/41	28428
Jun/41	28568
Jul/41	28708
Ago/41	28848
Sep/41	28988
Out/41	29128
Nov/41	29268
Dez/41	29408
Jan/42	29548
Fev/42	29688
Mar/42	29828
Abr/42	29968
Mai/42	30108
Jun/42	30248
Jul/42	30388
Ago/42	30528
Sep/42	30668
Out/42	30808
Nov/42	30948
Dez/42	31088
Jan/43	31228
Fev/43	31368
Mar/43	31508
Abr/43	31648
Mai/43	31788
Jun/43	31928
Jul/43	32068
Ago/43	32208
Sep/43	32348
Out/43	32488
Nov/43	32628
Dez/43	32768
Jan/44	32908
Fev/44	33048
Mar/44	33188
Abr/44	33328
Mai/44	33468
Jun/44	33608
Jul/44	33748
Ago/44	33888
Sep/44	34028
Out/44	34168
Nov/44	34308
Dez/44	34448
Jan/45	34588
Fev/45	34728
Mar/45	34868
Abr/45	35008
Mai/45	35148
Jun/45	35288
Jul/45	35428
Ago/45	35568
Sep/45	35708
Out/45	35848
Nov/45	35988
Dez/45	36128
Jan/46	36268
Fev/46	36408
Mar/46	36548
Abr/46	36688
Mai/46	36828
Jun/46	36968
Jul/46	37108
Ago/46	37248
Sep/46	37388
Out/46	37528
Nov/46	37668
Dez/46	37808
Jan/47	37948
Fev/47	38088
Mar/47	38228
Abr/47	38368
Mai/47	38508
Jun/47	38648
Jul/47	38788
Ago/47	38928
Sep/47	39068
Out/47	39208
Nov/47	39348
Dez/47	39488
Jan/48	39628
Fev/48	39768
Mar/48	39908
Abr/48	40048
Mai/48	40188
Jun/48	40328
Jul/48	40468
Ago/48	40608
Sep/48	40748
Out/48	40888
Nov/48	41028
Dez/48	41168
Jan/49	41308
Fev/49	41448
Mar/49	41588
Abr/49	41728
Mai/49	41868
Jun/49	42008
Jul/49	42148
Ago/49	42288
Sep/49	42428
Out/49	42568
Nov/49	42708
Dez/49	42848
Jan/50	42988
Fev/50	43128
Mar/50	43268
Abr/50	43408
Mai/50	43548
Jun/50	43688
Jul/50	43828
Ago/50	43968
Sep/50	44108
Out/50	44248
Nov/50	44388
Dez/50	44528
Jan/51	44668
Fev/51	44808
Mar/51	44948
Abr/51	45088
Mai/51	45228
Jun/	

- Ausência de formalização de usuários administradores genéricos;
- Ausência de um plano de contingência.

Sendo assim, cumpre frisar que as análises foram realizadas por amostragem, levando em consideração a fase de cada processo.

De todo o material referente ao tema, incluindo a documentação, esclarecimentos e análise por amostragem dos processos, e é importante ressaltar a legislação atende a missão a ser desenvolvida pela COTIN.

Além disso, é importante ressaltar que todo o cenário atual está em desenvolvimento, com uma estrutura compatível com as várias frentes de ações, e concomitantemente, a implementação do sistema ERP - BENNER, novidade para a empresa, seus usuários e técnicos, tornando o desafio ainda maior, contudo, observou-se os seguintes **achados**:

1) INFRAESTRUTURA DE TI (redes, armazenamento, internet, computadores e sistemas operacionais) desatualizados;

Apesar do incremento recente na parte de investimento, ainda há a necessidade de modernização dos mesmos.

2) INDISPONIBILIDADE DOS SERVIÇOS DA TERRACAP (SEJA POR ATAQUES EXTERNOS, INTERNOS, VULNERABILIDADES, ETC) COM ALGUMA FREQUÊNCIA;

Conforme informado e constatado, A indisponibilidade de serviços internos ainda acontece com alguma frequência, atrasando as rotinas diárias e direcionando a alguma insegurança no ambiente virtual.

3) AUSÊNCIA DE CAPACITAÇÃO/ATUALIZAÇÃO CONTINUADA DE EQUIPE

Não foi detectado nenhuma informação ou processo sobre capacitação/atualização de equipe continuada, no entanto, há o convênio vigente que prevê o "know-how" visando a Governança em TI.

4) DEPENDÊNCIA EXTERNA TÉCNICA ESPECIALIZADA EM INFRAESTRUTURA DE TECNOLOGIA

Apesar da observância da recente reestrutura da equipe, ainda é possível detectar que a técnica não é autosuficiente, em consonância com o item 3.

5) POUCOS NORMATIVOS E POLÍTICAS PARA A ÁREA DE TI

Apesar da constatação de normas para a área, observou-se um número mínimo de normativos que possam desenhar a rotina tecnológica em sua totalidade.

6) REANÁLISE E READEQUAÇÃO DAS PRIORIDADES DO PDTI (ATUALIZAÇÃO)

Com o passar do tempo, o cenário vai se modificando e há a necessidade de revisitação na escala de prioridades para o bom desempenho da empresa, em especial para sua atividade principal. Observou-se em especial, que os sistemas " suspensos" como o GAI e HOPE ainda não são prioridades de melhorias (abrangendo integração), devendo ser avaliado.

7) GRANDE NÚMERO DE RISCOS COM GRAU ALTO E CRÍTICO

Apesar do mapeamento detalhado dos riscos na área de TI, observou-se uma grande número de riscos com grau "alto" e crítico", exigindo um monitoramento permanente e com ações e entregas pactuadas com previsões reais.

8) GRANDE NÚMERO DE ENTREGAS REFERENTES AO CONVÊNIO Nº 170/2023 COM A FUNDAÇÃO DE AMPARO À PESQUISA E EXTENSÃO UNIVERSITÁRIA - FAPEU

Foi detectado um grande número de entregas previstas no convênio e com temas bem específicos na área de tecnologia, com 1 gestor e 3 executores..

Achado de conformidade:

1) REFORÇO DE PROFISSIONAIS ESPECIALIZADOS PARA A EXECUÇÃO DO SISTEMA BENNER

É importante registrar a relevância e a necessidade do sistema de integração para uma empresa de grande porte como a TERRACAP.

Com a implementação completa do citado sistema, e operacionalização, sem o auxílio de terceirizada, haverá a necessidade de profissionais especializados na plataforma para que seja garantida seu uso ideal. Devendo portanto, haver um plano de ação para a implementação completa com os profissionais especializados, visando a utilização ideal, minimizando riscos futuros.

VII- RECOMENDAÇÕES

De acordo com cada achado descrito no item VI, recomenda-se:

R.1 - Recomendar à PRESI e COINT/COTIN que estude possibilidade de incremento na infraestrutura de TI, incluindo redes, armazenamento, internet, computadores e sistemas operacionais (modernização);

R.2 - Recomendar à COINT/COTIN que promova o reforço seja de ações, prevenções, ferramentas que mitiguem a ocorrência de indisponibilidades nos sistemas da Companhia, visando não atingir a rotina diária da empresa e fortalecendo a *cybersegurança*;

R.3 - Recomendar à DIRAF/GEPES e COINT/COTIN que em conjunto confeccionem um plano de capacitação para o exercício de 2025, visando capacitar e atualizar a equipe de TI, com foco principal em Construção de Modelo de Governança de TIC, e posteriormente de modo continuado, visando as reciclagem periódica que a tecnologia sofre;

R.4 - Recomendar à COINT/COTIN que confeccione um plano de ação com o objetivo de mitigar a dependência externa técnica especializada em infraestrutura de tecnologia, consequentemente a robustez da equipe interna;

R.5 - Recomendar à COINT/COTIN e Comitê de Tecnologia e Segurança da Informação que promovam estudo visando fortalecer e atualizar os normativos para executar a Governança de TI, com celeridade;

R.6 - Recomendar à COINT/COTIN e Comitê de Tecnologia e Segurança da Informação que promovam a reanálise e atualização do Plano Diretor de Tecnologia da Informação - PDTI, em tempos programados, visando especialmente readequar as prioridades dos projetos que envolvam diretamente a atividade principal da empresa, como por exemplo o sistema GAI, HOPE e a possibilidade de integração, etc;

R.7 - Recomendar à COINT/DIGER e COINT/COTIN, que exerçam esforços para um monitoramento permanente com data programada para os riscos, em especial os que possuem grau "alto" e crítico", visando a minimização dos graus de riscos e com entregas pactuadas reais e comunicação a esta AUDIT trimestralmente;

R.8 - Recomendar à COINT e COINT/COTIN, que designem uma comissão integrada para acompanhamento do Convênio nº 170/2023 - com a FAPEU, com a participação de no mínimo 5 executores oficiais da área de TI e um gestor, visando o acompanhamento, fiscalização e validação das inúmeras entregas previstas;

R.9 - Recomendar à COINT/COTIN, que envie esforços visando o atendimento integral das recomendações apresentadas pela Auditoria Independente, nos anos de 2023 (2.2. Ausência de formalização de concessão de acesso, 2.3. Ausência de metodologia formal de gerenciamento de mudanças sistêmicas, 2.4. Revisão de políticas internas, 2.5. Implementar políticas para mapeamento de transações conflitantes) e 2024 (2.2 - Ausência de formalização de usuários administradores genéricos e 2.3 -

Ausência de um plano de contingência), conforme processos Sei nºs 00111-00002824/2023-15 e 00111-00006247/2024-11, respectivamente;

R.10 - Recomendar à AUDIT que inclua em seu portfólio de monitoramento permanente a presente auditoria até que o sistema Benner seja totalmente implementado, todas as entregas previstas no Convênio nº 170/2023 seja finalizado e o mapeamento de riscos seja mitigado em pelo menos 80%.

VIII - MANIFESTAÇÃO DAS ÁREAS APÓS RELATÓRIO PRELIMINAR Nº 05/2024 - AUDIT (154408858)

Após o envio do Relatório preliminar nº 05/2023-AUDIT (127204909), várias áreas deram publicidade aos empregados, conforme volumes VI e VII do presente processo, e algumas responderam de forma pontual às recomendações, conforme segue:

À respeito das recomendações, a GEPES, COINT, DIGER e COTIN - 155903961, 156413497, 155681214, e 156150326, respectivamente, manifestaram-se:

A GEPES se colocou à disposição da COTIN, para atendimento da Recomendação 3;

A COINT se manifestou por meio da Gestora do Convênio nº 170/2023, firmado com a FAPEU, em relação à recomendação nº 8, informando que a atual composição da comissão executora é suficiente;

A DIGER por sua vez, em relação à R.7, trouxe a informação "que a Matriz de Riscos de TI teve seus planos de tratamentos priorizados em fases, conforme Decisão DIRET nº 540/2024 (146129668). Na oportunidade, a DIRET indicou para a Fase 1 os riscos tidos como prioritários. Aproveita-se para dar conhecimentos os riscos a serem desenvolvidos na Fase 1, com seu respectivo grau de severidade:

MATRIZ	ID GPP	FATOR DE RISCO	SEVERIDADE	PRODUTO A SER ENTREGUE - PLANO ORIGINAL
TECNOLOGIA DA INFORMAÇÃO	TI0034	- Não há procedimento para que o titular dos dados concorde com os termos de uso dos dados coletados. Inclusive para fins comerciais e estratégia de marketing	Extremo	Evidência de inclusão dos termos de privacidade e de uso na etapa de cadastro dos serviços online
TECNOLOGIA DA INFORMAÇÃO	TI002	- Arquivos armazenados em sistemas de arquivos de rede (NFS) sem criptografia e sem controle de acesso por credenciais	Extremo	Relatório de implementação de solução que permite a criptografia e descriptografia por credenciais/tokens no nível de armazenamento dos arquivos
TECNOLOGIA DA INFORMAÇÃO	TI0027	- Ausência de práticas de atualização periódica de todos os sistemas	Extremo	Plano de atualização dos sistemas, detalhando cronograma e procedimentos para atualizações baseadas em planejamento ou identificação de vulnerabilidades
TECNOLOGIA DA INFORMAÇÃO	TI0019	- Ausência de suporte tecnológico para gerenciamento e execução dos processos de TI	Extremo	Documentação da definição, implantação e manutenção de uma ferramenta para gerenciamento e execução de processos via workflows
TECNOLOGIA DA INFORMAÇÃO	TI0034	- Utilização de dados reais dos titulares dos dados para o desenvolvimento, teste ou homologação de Software	Extremo	Normativo de adequação de processos e métodos para evitar o uso de dados de produção em ambientes não produção ou garantir segurança equivalente
TECNOLOGIA DA INFORMAÇÃO	TI002	- Nem todas as tabelas de dados importantes possuem logs para auditoria	Extremo	Relatório de logs de auditoria em sistemas gerenciadores de banco de dados habilitados
TECNOLOGIA DA INFORMAÇÃO	TI0027	- Comunicações sem uso de protocolo seguro	Alto	Relatório de verificação dos protocolos de comunicação nas auditorias periódicas de segurança
TECNOLOGIA DA INFORMAÇÃO	TI002	- Ausência de bloqueio de tela de estações de trabalho com base em período de inatividade	Alto	Relatório de implementação do bloqueio de tela, detalhando o tempo de inatividade configurado e o processo de ativação do bloqueio
TECNOLOGIA DA INFORMAÇÃO	TI002	- Ausência de justificativa no sistema de gestão de identidade e acesso (GIA) para concessão/recusa/manutenção de acesso	Alto	Documentação do recurso de justificativa de concessão de acesso desenvolvido para o sistema GIA, incluindo guias de uso para auditorias futuras
TECNOLOGIA DA INFORMAÇÃO	TI002	- Sistema de gestão de identidade e acesso só permite conceder acessos por prazo indeterminado	Alto	Relatório de evolução do sistema GIA, detalhando a eliminação da concessão de acesso por tempo indeterminado para sistemas críticos
TECNOLOGIA DA INFORMAÇÃO	TI0013	- Ausência de documentação e validação periódica do escopo dos controles de cibersegurança e privacidade de dados	Alto	Processo estabelecido para a manutenção contínua dos framework(s) de segurança, garantindo sua atualização e eficácia
TECNOLOGIA DA INFORMAÇÃO	TI009	- Ausência de documento descritivo do modelo de arquitetura corporativa	Alto	Relatórios de Modelo de Arquitetura Corporativa (AS IS e TO BE) baseados no TOGAF, incluindo visualizações Archimate
TECNOLOGIA DA INFORMAÇÃO	TI0013	- Ausência de framework institucional de cibersegurança e privacidade de dados	Alto	Framework(s) criado(s) para cibersegurança e privacidade de dados, personalizado(s) para atender às necessidades específicas da organização

MATRIZ	ID GPP	FATOR DE RISCO	SEVERIDADE	PRODUTO A SER ENTREGUE - PLANO ORIGINAL
TECNOLOGIA DA INFORMAÇÃO	TI0027	- Diagramas de rede e diagramas de fluxo de dados incompletos ou desatualizados	Alto	Diagrama lógico de rede confeccionado, detalhando a estrutura e conexões da rede
TECNOLOGIA DA INFORMAÇÃO	TI0016	- Ambiente de execução de aplicações de alta disponibilidade (contêinerizado) não implantado para produção	Alto	Documentação da implantação de clusters kubernetes, detalhando a conformidade com a arquitetura de infraestrutura aprovada
TECNOLOGIA DA INFORMAÇÃO	TI0016	- Ambiente de execução de aplicações de alta disponibilidade (contêinerizado) não implantado para produção	Alto	Playbook desenvolvido com baseline de configuração para clusters kubernetes, incluindo padrões e procedimentos de implementação
TECNOLOGIA DA INFORMAÇÃO	TI0011	- Baixa maturidade em monitoramento contínuo dos ativos de TIC	Alto	Manual de processos e procedimentos para o monitoramento contínuo das operações de TIC
TECNOLOGIA DA INFORMAÇÃO	TI0011	- Baixa maturidade em monitoramento contínuo dos ativos de TIC	Alto	Procedimentos para a detecção e resposta a atividades suspeitas ou maliciosas na rede de TIC
TECNOLOGIA DA INFORMAÇÃO	TI0011	- Baixa maturidade em monitoramento contínuo dos ativos de TIC	Alto	Relatório de implementação e configuração do sistema centralizador de logs
TECNOLOGIA DA INFORMAÇÃO	TI002	- Ausência de criptografia de disco das estações de trabalho sicas dos usuários	Alto	Relatório de habilitação da criptografia de disco nas estações de trabalho, incluindo procedimentos técnicos e políticas de segurança
TECNOLOGIA DA INFORMAÇÃO	TI002	- Compartilhamento de credenciais de ativos críticos de TI nos processos de implantação de sistemas	Alto	Relatório de implantação e uso da solução de tecnologia para gerenciamento, armazenamento e distribuição de dados confidenciais, incluindo segredos, certificados e chaves
TECNOLOGIA DA INFORMAÇÃO	TI0027	- Uso desnecessário de usuários de alto privilégio para execução de aplicações	Alto	Relatório de revisão da infraestrutura como código (Dockerfile, manifestos, arquivos de configuração etc.) antes da implantação de versão de aplicação
TECNOLOGIA DA INFORMAÇÃO	TI002	- Compartilhamento de credenciais de ativos críticos de TI nos processos de implantação de sistemas	Alto	Normativo detalhando os procedimentos para gerenciamento, armazenamento e distribuição de dados confidenciais em pipelines e automações de infraestrutura
TECNOLOGIA DA INFORMAÇÃO	TI002	- Compartilhamento de certificado digital de pessoa jurídica	Alto	Relatório de concessão de procurações eletrônicas, detalhando sistemas abrangidos e níveis de acesso concedidos
TECNOLOGIA DA INFORMAÇÃO	TI008	- A organização não realiza uma revisão independente do design do Software para confirmar que todos os requisitos de segurança cibernética e privacidade de dados são atendidos e que quaisquer riscos identificados são abordados de forma satisfatória	Alto	Normativo com a definição e implementação de práticas DevSecOps e GitOps, incluindo fluxos de trabalho e políticas de segurança integradas
TECNOLOGIA DA INFORMAÇÃO	TI0027	- Ausência de implementação de práticas de segurança cibernética e privacidade de dados reconhecidas pela indústria na especificação, concepção, desenvolvimento, implementação e modificação de sistemas e serviços; organização não adota práticas do Ciclo de Vida do Desenvolvimento Seguro	Alto	Evidências de revisão da infraestrutura como código (Dockerfile, manifestos, arquivos de configuração etc.) a cada implantação de versão de aplicação

Ainda, os demais planos de tratamento terão previsão de início no 4º Trimestre do corrente ano, conforme Decisão ora citada: " *aprovar, também, a implementação da fase 2, dos demais riscos para iniciar no 4º trimestre do corrente ano;*"

Esta DIGER/COINT expõe que realiza o monitoramento do desenvolvimento dos planos de tratamento junto à COTIN e que será enviado trimestralmente à AUDIT - quando é enviado ao COAUD e ao CONFI - o relatório com o *status* das ações adotadas."

A COTIN se manifestou acerca das recomendações conforme a seguir:

"R.1 - Recomendar à PRESI e COINT/COTIN que estude possibilidade de incremento na infraestrutura de TI, incluindo redes, armazenamento, internet, computadores e sistemas operacionais (modernização);

A Terracap realizou as seguintes aquisições recentes (ou está realizando), no que se refere a infraestrutura de TI:

1. Compra de computadores e notebooks, com contrato assinado que irá atualizar todo o parque computacional da Terracap no curto prazo, com parte dos itens já entregues (00111-00004124/2023-57); 2. Compra de estações de trabalho de configurações mais avançadas (para trabalhos técnicos e de arquitetura/engenharia), processo de aquisição 00111-00010139/2023-54; 3. Renovação de suporte e atualização do servidor de armazenamento de dados ("storage") - licitação homologada (155167061); 4. Compra de equipamentos de rede "switches", em que o termo de referência já foi aprovado pelo presidente (00111-00002503/2024-93); 5. Aquisição dos servidores de rede e software de virtualização VMWARE, que constituem o ambiente operacional onde os sistemas corporativos da Terracap são executados e servidos aos clientes

(00111-00007329/2021-22); 6. Atualização da infraestrutura de rede sem fio corporativa (wifi) do edifício sede da Terracap (00111-00000736/2022-90).

Cabe dizer que atualização da infraestrutura tecnológica é uma constante e ocorre praticamente em todos os anos, em maior ou menor grau.

R.2 - Recomendar à COINT/COTIN que promova o reforço seja de ações, prevenções, ferramentas que mitiguem a ocorrência de indisponibilidades nos sistemas da Companhia, visando não atingir a rotina diária da empresa e fortalecendo a cyberssegurança;

A Terracap realiza/realizou as seguintes ações, no que se refere a segurança da informação:

1. Compra de licenças de subscrição de solução de proteção de endpoints (antivírus) para as estações de trabalho (e outros dispositivos) da Terracap (em contratação por meio do processo 00111-00005492/2024-01); 2. Compra de licença de solução de antispam, em procedimento de compra, processo 00111-00005488/2024-35; 3. Implantação de novas soluções de segurança de firewall, firewall de aplicação (WAF) e serviço de Centro de Operações de Segurança (SOC) para proteção do datacenter e do edifício sede da Terracap (00111-00001860/2023-53); 4. Implantação de dispositivos firewall em cada uma das unidades externas (508 Sul, Biotic, ETR, Garagem), com gestão centralizada (00111-00004344/2024-61); 5. Além de todas essas ações, o projeto por meio da colaboração da FAPEU está elaborando um roadmap de ações de segurança e aprimoramento de processos (00111-00005622/2023-17), com boa parte das entregas validadas (156094678) e, em tempo, informa-se ainda que o indicador estratégico para 2025 sugerido pela COTIN refere-se à "*Conscientização dos colaboradores da TERRACAP em Segurança da Informação, devendo ocorrer, minimamente, 4 ações durante o ano de 2025.*" constante no processo 00111-00014160/2024-18.

R.3 - Recomendar à DIRAF/GEPES e COINT/COTIN que em conjunto confeccionem um plano de capacitação para o exercício de 2025, visando capacitar e atualizar a equipe de TI, com foco principal em Construção de Modelo de Governança de TIC, e posteriormente de modo continuado, visando as reciclagem periódica que a tecnologia sofre;

Estão previstos no Convênio com a FAPEU workshop de cyberssegurança e repasses de conhecimento em processos de governança. O Plano de Trabalho 151087025 prevê a realização de workshops de governança (este já realizado) e de cibersegurança; além disso apoio à implementação do modelo de governança e dos principais processos.

Ainda, a COTIN deverá encaminhar no início de 2025 para a GEPES relação de necessidades de capacitação/atualização para o ano, abrangendo assuntos correlatos a governança e cibersegurança aplicáveis ao ambiente da Terracap.

R.4 - Recomendar à COINT/COTIN que confeccione um plano de ação com o objetivo de mitigar a dependência externa técnica especializada em infraestrutura de tecnologia, consequentemente a robustez da equipe interna;

A TI está tomando medidas de documentação das operações críticas realizadas pela equipe terceira, como exemplo, backup e restauração - evitando-se assim que o conhecimento técnico de atividades essenciais para a continuidade do negócio estejam completamente sob posse de fornecedores externos. Contudo, para resolver a questão de fato, faz-se necessária que a TERRACAP contrate profissionais que possuam formação técnica para suportar tais atividades.

Além do risco de continuidade, a terceirização da equipe especializada de suporte atualmente é um dos principais gargalos no que se refere a projetos de melhoria ou implantação de novos serviços e processos na TI, pois a gestão dos profissionais dos fornecedores de serviços não passa pela Terracap, o que prejudica bastante a agilidade e eficiência da empresa. A Terracap está restrita a avaliar o serviço sob os termos rígidos do instrumento de contratação, prejudicando a agilidade da organização, especialmente no contexto de tecnologia que se atualiza muito rapidamente.

R.5 - Recomendar à COINT/COTIN e Comitê de Tecnologia e Segurança da Informação que promovam estudo visando fortalecer e atualizar os normativos para executar a Governança de TI, com celeridade;

Por meio de parceria formada pelo convênio com a FAPEU, foram realizados estudos que resultaram em uma proposta de modelo de governança de TI. Esse estudo contém avaliação do nível de maturidade que a TI da Terracap se encontra, bem como, sugestão de diversos novos processos de trabalho que fortalecerão a governança e segurança da informação (ver 156094678). Ademais, a COTIN trabalha atualmente para apresentar uma proposta de Estruturação de Arcabouço Normativo de Governança e Gestão de TI com previsão de conclusão até janeiro de 2025.

R.6 - Recomendar à COINT/COTIN e Comitê de Tecnologia e Segurança da Informação que promovam a reanálise e atualização do Plano Diretor de Tecnologia da Informação - PDTI, em tempos programados, visando especialmente readequar as prioridades dos projetos que envolvam diretamente a atividade principal da empresa, como por exemplo o sistema GAL, HOPE e a possibilidade de integração, etc;

Anualmente o PDTI é revisado e a minuta do novo Plano Diretor de TI já está sendo confeccionada e será encaminhada para aprovação até o início de 2025, com ações focadas principalmente na estabilização do sistema de gestão ERP e sistemas de apoio a processos principais, e na implementação das ações de governança de TI e do roadmap de segurança da informação.

R.7 - Recomendar à COINT/DIGER e COINT/COTIN, que exerçam esforços para um monitoramento permanente com data programada para os riscos, em especial os que possuem grau "alto" e "crítico", visando a minimização dos graus de riscos e com entregas pactuadas reais e comunicação a esta AUDIT trimestralmente;

A respeito do gerenciamento de riscos de tecnologia da informação, a Terracap instituiu um grupo de trabalho (processo 00111-00010136/2023-11) para identificação, análise e proposição de plano de tratamento dos riscos de tecnologia da informação. Para melhorar a capacidade de gestão desses riscos e ações, a COTIN recentemente instituiu o uso da ferramenta GRC "Simplerisk", a qual permite registrar, atualizar, estabelecer períodos de revisão, gerar relatórios etc. sobre os riscos de TI

A implantação da ferramenta ainda está em andamento e esta COTIN prevê a sua conclusão e pleno uso durante o primeiro trimestre de 2025.

R.8 - Recomendar à COINT e COINT/COTIN, que designem uma comissão integrada para acompanhamento do Convênio nº 170/2023 - com a FAPEU, com a participação de no mínimo 5 executores oficiais da área de TI e um gestor, visando o acompanhamento, fiscalização e validação das inúmeras entregas previstas;

Já existe uma comissão composta por dois gestores do convênio, mais dois fiscais para cada uma das três agendas (Portarias (143719464) e 154713147), totalizando assim oito pessoas na equipe de fiscalização que participam ativamente do projeto. Esta COTIN não vislumbra necessidade de alteração dessa composição no momento.

R.9 - Recomendar à COINT/COTIN, que envie esforços visando o atendimento integral das recomendações apresentadas pela Auditoria Independente, nos anos de 2023 (2.2. Ausência de formalização de concessão de acesso, 2.3. Ausência de metodologia formal de gerenciamento de mudanças sistêmicas, 2.4. Revisão de políticas internas, 2.5. Implementar políticas para mapeamento de transações conflitantes) e 2024 (2.2 - Ausência de formalização de usuários administradores genéricos e 2.3 - Ausência de um plano de contingência), conforme processos Sei nºs 00111-00002824/2023-15 e 00111-00006247/2024-11, respectivamente;

Processo 00111-00002824/2023-15

Item 2.1 - ATENDIDA, Item 2.2 - ATENDIDA - Item 3 do Relatório 152494635. Foram feitas correções no GIA e evoluções para suportar uma nova metodologia de acesso em que o usuário é permitido por um período pré-determinado, substituindo a maneira antiga em que o prazo era indeterminado; Item 2.3 - Já há uma gestão de mudanças na prática, faltando apenas a formalização. Com o início da implementação do modelo de governança, esse processo será submetido à aprovação como norma, podendo ser então ser monitorada periodicamente a conformidade e o desempenho; Item 2.4 - Trata-se de ação contínua/periódica. Novas revisões dos documentos Política de Segurança e da Norma de Segurança já está sendo feitas e serão submetidas à aprovação até dezembro de 2024; Item 2.5 - Ação sob gestão da COINT; aguardando estabilização do ERP para definição dos requisitos e posterior implementação; Item 2.6 - ATENDIDA."

Por fim, o Comitê de Tecnologia e Segurança da Informação se manifestou por meio do despacho - 157337235:

"Informo que, como Presidente do Comitê de Tecnologia e Segurança da Informação, estou ciente das recomendações constantes do Relatório de Auditoria nº 5/2024 - TERRACAP/CONAD/AUDIT (154408858), em especial **às recomendações R.5 e R.6**, que serão avaliadas e discutidas no âmbito do Comitê, com vistas ao seu atendimento."

IX - ANÁLISE DA AUDITORIA INTERNA

Após a análise das manifestações apresentadas é possível identificar que as áreas responsáveis já iniciaram as ações visando ao atendimento das recomendações, contudo todas em desenvolvimento.

As compras visando a modernização dos equipamentos foram demonstradas, porém o universo tecnológico é muito dinâmico, e exige investimentos frequentes. Já com relação o uso de ferramentas que mitiguem a ocorrência de indisponibilidades nos sistemas da Companhia, foram iniciados investimentos para aquisição de licenças, antivírus, entre outras ações que fortaleçam o ambiente tecnológico, porém trata-se de ações constantes devido à alta dinamicidade da área de TI.

Com relação ao plano de ação com o objetivo de mitigar a dependência externa técnica, capacitação para treinamentos foi informado que várias ações foram iniciadas como criação de arquivo documental crítica entre outras ações.

Há também a tratativa da revisão do Plano Diretor de TI em andamento, e ainda com relação as recomendações apontadas pela Auditoria Independente(R.9), foi esclarecido que avançaram, porém há a necessidade de avaliação pela auditoria externa.

E quanto ao Comitê de Tecnologia e Segurança da Informação, foi informado que as recomendações serão avaliadas e discutidas no âmbito do Comitê, com vistas ao seu atendimento.

Portanto, há várias ações em andamento, muitas em estágio inicial, permanecendo assim, a necessidade da permanências das recomendações.

X - CONCLUSÃO

A presente auditoria operacional referente aos controles primários referentes à Governança de TI é uma forte ferramenta visando a melhoria dos controles internos, bem como o aumento da eficiência e eficácia das rotinas, além de colaborar para elevar o nível de entendimento na complexa função do contexto dos controles, externo e interno.

É imperioso registrar que a recente alteração de subordinação e reestrutura da TI insidiram em uma reorganização interna e principalmente da missão e ações visando implementar a Governança de TI.

Foi transparente nas análises as frentes de ações desenhadas para a modernização e implementação da Governança de TI, e é notório que há a necessidade de um cronograma a ser seguido, exigindo um tempo para maturação para cada entrega.

Além disso, o ajuste firmado com a Fundação de Amparo à Pesquisa e Extensão Universitária - FAPUEU trará além da implementação, a *expertise* para utilização da equipe de TI desta empresa, onde serão implementados : Estruturação de um Ambiente de Inteligência de Gestão; Desenvolvimento de Roadmap de Cibersegurança; e Construção de Modelo de Governança de TIC, podendo ser um divisor de águas para a Companhia.

Na análise de toda a documentação disponibilizada e dos processos definidos na amostra, verificou-se que, em linhas gerais, a Governança de TI foi iniciada, está sendo executada, porém com um longo caminho e desafio pela frente, sendo imperioso a prioridade para o tema, pois interfere diretamente nas atividades da empresa e de seus empregados.

Outro registro importante é a implementação do sistema ERP - BENNER, onde além da integração em grande maioria dos sistemas da empresa, trará segurança , eficácia e eficiência nos processos e rotinas da empresa, em especial quando da sua implementação integral prevista para o início do próximo exercício.

A manifestação das áreas envolvidas no tema acerca do Relatório Preliminar nº 05/2024 - AUDIT (154408858) comprovou que as ações visando o atingimento das recomendações foram iniciadas, devendo ser acompanhadas regularmente.

Em linhas gerais, observou-se na presente auditoria que a Governança de TI está em direção congruente com o planejado, porém é possível melhorar tanto a rotina o mapeamento de ações e tarefas para atingimento do planejado, inclusive no que diz respeito a capacitação e atualização de normativos para exercer as rotinas, conforme detalhamento no presente relatório.

Além disso, e levando em consideração as justificativas apresentadas e visando a melhoria nos controles internos da gestão da Governança de TI, **conclui-se** que os controles primários na Governança de TI está em plena execução, com planejamento e ferramentas compatíveis, para médio e longo prazo, com tudo há possibilidades de melhorias, conforme o teor do presente relatório e, desde que atendidas as recomendações elencadas no item VII - RECOMENDAÇÕES, recomendando ainda, que as unidades orgânicas da TERRACAP implementem medidas tendentes a garantir a desejável missão definida, corroborando para melhoria da eficiência e eficácia dos trabalhos e com prioridade no monitoramento permanente até o atingimento de todas as frentes em desenvolvimento.

Além disso, e levando em consideração as justificativas apresentadas e visando a melhoria nos controles internos da gestão da Governança de TI, **conclui-se esta auditoria operacional com as recomendações de melhorias nas rotinas e gestão, devidamente recepcionadas pelas áreas envolvidas no processo, ratificando as seguintes recomendações:**

R.1 - Recomendar à PRESI e COINT/COTIN que estude possibilidade de incremento na infraestrutura de TI, incluindo redes, armazenamento, internet, computadores e sistemas operacionais (modernização);

R.2 - Recomendar à COINT/COTIN que promova o reforço seja de ações, prevenções, ferramentas que mitiguem a ocorrência de indisponibilidades nos sistemas da Companhia, visando não atingir a rotina diária da empresa e fortalecendo a *cybersegurança*;

R.3 - Recomendar à DIRAF/GEPES e COINT/COTIN que em conjunto confeccionem um plano de capacitação para o exercício de 2025, visando capacitar e atualizar a equipe de TI, com foco principal em Construção de Modelo de Governança de TIC, e posteriormente de modo continuado, visando as reciclagem periódica que a tecnologia sofre;

R.4 - Recomendar à COINT/COTIN que confeccione um plano de ação com o objetivo de mitigar a dependência externa técnica especializada em infraestrutura de tecnologia, consequentemente a robustez da equipe interna;

R.5 - Recomendar à COINT/COTIN e Comitê de Tecnologia e Segurança da Informação que promovam estudo visando fortalecer e atualizar os normativos para executar a Governança de TI, com celeridade;

R.6 - Recomendar à COINT/COTIN e Comitê de Tecnologia e Segurança da Informação que promovam a reanálise e atualização do Plano Diretor de Tecnologia da Informação - PDTI, em tempos programados, visando especialmente readequar as prioridades dos projetos que envolvam diretamente a atividade principal da empresa, como por exemplo o sistema GAL, HOPE e a possibilidade de integração, etc;

R.7 - Recomendar à COINT/DIGER e COINT/COTIN, que exerçam esforços para um monitoramento permanente com data programada para os riscos, em especial os que possuem grau "alto" e crítico", visando a minimização dos graus de riscos e com entregas pactuadas reais e comunicação a esta AUDIT trimestralmente;

R.8 - Recomendar à COINT e COINT/COTIN, que designem uma comissão integrada para acompanhamento do Convênio nº 170/2023 - com a FAPUEU, com a participação de no mínimo 5 executores oficiais da área de TI e um gestor, visando o acompanhamento, fiscalização e validação das inúmeras entregas previstas;

R.9 - Recomendar à COINT/COTIN, que envide esforços visando o atendimento integral das recomendações apresentadas pela Auditoria Independente, nos anos de 2023 (2.2. Ausência de formalização de concessão de acesso, 2.3. Ausência de metodologia formal de gerenciamento de mudanças sistêmicas, 2.4. Revisão de políticas internas, 2.5. Implementar políticas para mapeamento de transações conflitantes) e 2024 (2.2 - Ausência de formalização de usuários administradores genéricos e 2.3 - Ausência de um plano de contingência), conforme processos Sei nºs 00111-00002824/2023-15 e 00111-00006247/2024-11, respectivamente;

R.10 - Recomendar à AUDIT que inclua em seu portfólio de monitoramento permanente a presente auditoria até que o sistema Benner seja totalmente implementado, todas as entregas previstas no Convênio nº 170/2023 seja finalizado e o mapeamento de riscos seja mitigado em pelo menos 80%.

QUADRO-RESUMO

Unidade	Recomendação
COINT/GESTOR CONVÊNIO	R.8
COINT/DIGER	R.7

COINT/COTIN	R.1, R.2, R.3, R.4, R.5, R.6, R.7, R.8, R.9.
COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO	R.5 e R.6
DIRAF/GEPES	R.3
PRESI	R.1

DIVULGAÇÃO DOS RESULTADOS DA AUDITORIA

A divulgação dos resultados da auditoria é medida de transparência ativa privilegiada pelos Artigos 3º, I e II; 7º, VII, “b”; 8º, §2º, todos da Lei nº 12.527/2011 e deve ter lugar após a aprovação do Relatório Final, incorporando-se eventuais correções e acréscimos.

À superior consideração.

CLAUDIA TOLENTINO

Assessora

1. **Aprovo** a íntegra do presente Relatório Final de Auditoria Operacional de nº **09/2024-AUDIT**.
2. **Encaminhe-se** o presente Relatório Final nº 09/2024-AUDIT à **PRESI, DINEG, DIJUR, DITEC, DICOM e DIREs**, para conhecimento e ciência.
2. **Encaminhe-se** o presente Relatório Final nº 09/2024 - AUDIT ao **GABIN, com vistas ao Comitê de Tecnologia e Segurança da Informação**, à **COINT**, com vistas à **COTIN e DIGER**, e à **DIRAF**, com vistas à **GEPES**, para conhecimento, ciência e manifestação no prazo de 4 meses, a saber: **03/04/2025**, a contar do envio do presente relatório, nos termos da IS nº 03/2021 - PRESI.

DENI AUGUSTO P F E SILVA

Chefe da Auditoria Interna



Documento assinado eletronicamente por **CLAUDIA THEREZA ROCHA TOLENTINO BARROS - Matr. 0002819-3, Assessor(a)**, em 02/12/2024, às 14:39, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



Documento assinado eletronicamente por **DENI AUGUSTO PEREIRA FERREIRA E SILVA - Matr.0002060-5, Chefe da Auditoria Interna**, em 02/12/2024, às 15:07, conforme art. 6º do Decreto nº 36.756, de 16 de setembro de 2015, publicado no Diário Oficial do Distrito Federal nº 180, quinta-feira, 17 de setembro de 2015.



A autenticidade do documento pode ser conferida no site:
[http://sei.df.gov.br/sei/controlador_externo.php?](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
[acao=documento_conferir&id_orgao_acesso_externo=0](http://sei.df.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0)
verificador= **157096054** código CRC= **835E8078**.

"Brasília - Patrimônio Cultural da Humanidade"
SAM BLOCO F EDIFICIO SEDE - Bairro Brasília - CEP 70620-000 - DF
Telefone(s): 33421819
Site - www.terracap.df.gov.br