2022

UNIVERSIDADE FEDERAL DE CAMPINA GRANDE

Relatório Final de Auditoria Interna nº 01/2022

Ação nº 08 – Avaliação da gestão de Tecnologia da Informação e Comunicação (TIC) da Universidade Federal de Campina Grande (UFCG) com base no Índice de Gestão de TI (iGestTI) do Índice Integrado de Governança e Gestão Pública (IGG) de 2021.

Unidade auditada:

Secretaria de Planejamento e Orçamento – SEPLAN.

Coordenação de Controle Interno – CCI/UFCG.
Av. Aprígio Veloso, 882 - Bodocongó - Bloco BQ - CEP: 58.509.970
Campina Grande – PB.
Telefone: (83) 2101.1555 - e-mail: cci@reitoria.ufcg.edu.br

Número: 01/2022	**RELATÓRIO FINAL DE AUDITORIA**

Unidade Auditada:	Secretaria de Planejamento e Orçamento - SEPLAN
Responsável:	Vinicius Farias Moreira
Objeto:	Avaliar a gestão de Tecnologia da Informação e Comunicação (TIC) da Universidade Federal de Campina Grande (UFCG) com base no Índice de Gestão de TI (iGestTI) do Índice Integrado de Governança e Gestão Pública (IGG) de 2021.
Motivação:	PAINT 2022

Prezado Senhor,

Em cumprimento à **Ordem de Serviço nº 03/2022** da Coordenação de Controle Interno (CCI/UFCG), exarada no **processo SEI 23096.005762/2022-08**, e em consonância com o Plano Anual de Atividades de Auditoria Interna - PAINT/2022, apresenta-se o relatório final dos trabalhos de auditoria realizados entre fevereiro e junho de 2022, no *campus* de Campina Grande desta instituição, referentes à **avaliação da Gestão de Tecnologia da Informação e Comunicação (TIC) da Universidade Federal de Campina Grande (UFCG)**.

I. INTRODUÇÃO

A presente auditoria, em cumprimento ao PAINT 2022, se debruçou sobre os resultados dos exames da gestão de TIC da UFCG, oriundos da matriz de análise de criticidade dos indicadores e subindicadores do Índice de Gestão de TI (iGestTI). Este índice, por sua vez, faz parte do Índice Integrado de Governança e Gestão Pública (IGG) de 2021 desta Instituição Federal de Ensino Superior (IFES).

O IGG - Índice Integrado de Governança e Gestão Pública - foi estabelecido pelo Tribunal de Contas da União (TCU) através do Acórdão nº 588/2018 - Plenário, e constitui um levantamento, via questionário, realizado periodicamente pela referida Corte junto a órgãos e entidades da Administração Pública federal, para fins de averiguação da governança e da gestão de tais entes, a fim de identificar possíveis riscos sistêmicos e, a partir de análises comparativas (*benchmarking*), estimular a adoção de boas práticas.

O referido questionário foi estruturado de forma que as instituições avaliadas (381 órgãos e entidades) o respondessem eletronicamente, com o intuito de averiguar informações referentes ao seu nível de maturidade de governança e a sua capacidade de gestão a partir de perguntas agrupadas pelos seguintes temas:

- *Governança pública* (Índice de Governança Pública - iGovPub);
- *Gestão de pessoas* (Índice de Governança e Gestão de pessoas - iGovPessoas);

- *Gestão de tecnologia e da segurança da informação* (Índice de Governança e Gestão de TI - iGovTI);
- *Gestão de contratações* (Índice de Governança e Gestão de Contratações - iGovContrat);
- *Gestão orçamentária* (Índice de governança e gestão orçamentárias - iGovOrcament).

Assim, para cada pergunta, o questionário apresentava quatro opções de resposta - e cada uma dessas opções correspondia a um intervalo que refletia o nível de governança ou gestão para determinado indicador, como pode-se ver nas tabelas abaixo:

Nível de Governança		
Estágios		**Intervalos**
Inicial	Inexpressivo	0% - 14,99%
	Iniciando	15% - 39,99%
Intermediário		40% - 70%
Aprimorado		70,01% - 100%

Fonte: Acórdão 588/2018-TCU-Plenário

Descrição
[Inicial: Inexpressivo] A organização ainda não adota a prática, bem como não iniciou planejamento para adotá-la.
[Inicial: Iniciando] A organização ainda não adota a prática, mas iniciou ou concluiu planejamento visando adotá-la, o que se evidencia por meio de documentos formais (planos, atas de reunião, estudos preliminares etc).
[Intermediário] A organização iniciou a adoção da prática, que ainda não está completamente implementada, conforme planejamento realizado; ou a prática não é executada uniformemente em toda a organização.
[Aprimorado] A organização adota integralmente a prática apresentada, de modo uniforme, o que se evidencia em documentação específica ou por meio do(s) produto(s) ou artefato(s) resultante(s) de sua execução.

Fonte: Elaborado pela AUDI - IFPE. Adaptado da AUDIN - UNIPAMPA.

Como afirmado acima, entre os temas avaliados pelo IGG está a gestão de tecnologia e segurança da informação, ou seja, o iGovTI, que é o índice geral relativo à TI.

Este, por sua vez, é composto por dois subíndices: Índice de Governança de TI (GovernançaTI) e Índice de Gestão de TI (iGestTI), os quais são formados, respectivamente, pelos seguintes indicadores e subindicadores:

<u>Componentes do Índice de Governança de TI - GovernançaTI:</u>

- *Capacidade em estabelecer modelo de gestão de TI;*
- *Capacidade em monitorar o desempenho da gestão de TI:*

    - *A liderança monitora o desempenho da gestão de tecnologia da informação?*
    - *Os serviços de auditoria interna prestados anualmente para a organização contemplam avaliação da gestão de tecnologia da informação?*
    - *Os serviços de auditoria interna prestados anualmente para a organização contemplam avaliação da gestão de segurança da informação?*
- *Capacidade em prestar serviços públicos com qualidade:*
    - *A organização definiu metas para a simplificação do atendimento prestado aos usuários dos serviços públicos?*
    - *A organização assegura que os serviços acessíveis via internet atendam aos padrões de interoperabilidade, usabilidade e acessibilidade, e que as informações pessoais utilizadas nesses serviços sejam adequadamente protegidas?*
    - *A organização promove a participação dos usuários com vistas à melhoria da qualidade dos serviços públicos prestados?*

Componentes do Índice de Gestão de TI - iGestTI:

- *Capacidade em realizar planejamento de TI:*
    - *A organização executa processo de planejamento de tecnologia da informação?*
    - *A organização possui plano de tecnologia da informação vigente?*
- *Capacidade em gestão de pessoal de TI:*
    - *Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de colaboradores da organização estão definidos e documentados?*
    - *Há definição do quantitativo necessário de pessoal por unidade organizacional ou por processo de trabalho?*
    - *A escolha dos gestores ocorre segundo perfis profissionais previamente definidos e documentados?*
    - *As lacunas de competências dos colaboradores e gestores da organização são identificadas e documentadas?*
    - *A organização realiza, formalmente, avaliação de desempenho individual, com atribuição de nota ou conceito, tendo como critério de avaliação o alcance das metas previstas?*
- *Capacidade em processos de TI:*
    - *Capacidade em Gerir Serviços de TI:*
        - *A organização elabora um catálogo de serviços de tecnologia da informação?*
        - *A organização executa processo de gestão de mudanças?*
        - *A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)?*
        - *A organização executa processo de gestão de incidentes de serviços de tecnologia da informação?*
    - *Capacidade em gerir nível de serviço de TI*
    - *Capacidade em gerir riscos de TI:*
        - *A estrutura da gestão de riscos está definida?*

        - *Atividades típicas de segunda linha de defesa estão estabelecidas?*
        - *O processo de gestão de riscos da organização está implantado?*
        - *Os riscos considerados críticos para a organização são geridos?*
        - *A organização executa processo de gestão de continuidade do negócio?*
        - *A organização executa processo de gestão dos riscos de tecnologia da informação relativos a processos de negócio?*
        - *A organização executa processo de gestão de continuidade de serviços de tecnologia da informação?*
    - *Índice de Gestão da Segurança da Informação:*
        - *Capacidade em definir políticas de responsabilidades para a gestão da TI:*
            - *A organização dispõe de uma política de segurança da informação?*
            - *A organização dispõe de comitê de segurança da informação?*
            - *A organização possui um gestor institucional de segurança da informação?*
        - *Capacidade em estabelecer processos e atividades para a gestão da TI:*
            - *A organização executa processo de gestão de riscos de segurança da informação?*
            - *A organização executa processo de controle de acesso à informação e aos ativos associados à informação?*
            - *A organização executa processo de gestão de ativos associados à informação?*
            - *A organização executa processo para classificação e tratamento de informações?*
            - *A organização executa processo de gestão de incidentes de segurança da informação?*
            - *A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem?*
    - *Capacidade em executar processo de software:*
        - *A organização executa um processo de software?*

Segundo o TCU, no ano de 2021, a nível nacional, a adoção de boas práticas de governança e gestão de TI citados anteriormente não se apresentou em níveis ideais, mas ainda assim, de modo geral, o resultado foi positivo. Trinta e um por cento (31%) das instituições avaliadas encontravam-se no estágio “Iniciando” (de 15% a 39,99%), 51% estavam no estágio “Intermediário” (de 40% a 70%) e 19% ficaram no estágio “Aprimorado” (de 70% a 100%) do iGovTI.

Ao fazer um comparativo do **iGovTI** de 2018 com o de 2021, o TCU também constatou uma melhoria no nível de aplicação das práticas analisadas, ou seja, uma movimentação dos estágios iniciais para “Intermediário” e “Aprimorado”. O reflexo da referida melhoria foi que os entes avaliados que estavam no estágio “Inicial” diminuíram de 41% para 30%, e os que estavam em estágio “Aprimorado” aumentaram de 14% para 19%.

Tal fato surpreendeu o TCU, pois ocorreu mesmo com o aumento da complexidade da referida avaliação, ou seja, uma maior quantidade de itens analisados. Entretanto, em uma análise mais criteriosa dos componentes do iGovTI, a mesma Corte de Contas identificou uma série de práticas aquém do desejado, ou seja, em nível "Inexpressivo", merecendo maior atenção.

Todavia, no caso da UFCG, a tendência não se repetiu, pois o seu iGovTI subiu pouco (5,44%) e permaneceu no nível "Inicial". Entretanto, o objetivo deste trabalho é analisar apenas uma parte deste, qual seja, o **Índice de Gestão de TI (iGestTI)**, juntamente com seus respectivos indicadores e subindicadores, deixando de lado o Índice de Governança de TI (GovernançaTI).

Com relação ao **iGestTI**, o TCU também identificou uma evolução positiva a nível nacional, ou seja, como visto anteriormente, uma movimentação do estágio "Inicial" para os estágios "Intermediário" e "Aprimorado". A referida evolução resultou, entre 2018 e 2021, em um percentual menor de instituições avaliadas no estágio "Inicial" (de 39% para 29%) e um percentual maior no estágio "Aprimorado" (de 15% para 19%).

Entretanto, mais uma vez, a UFCG não acompanhou essa tendência e teve um decréscimo (6,66%) no referido indicador, permanecendo no nível "Inicial".

Com relação aos componentes do iGestTI, este é um índice que se subdivide nos seguintes indicadores, que serão analisados nos próximos parágrafos:

- *planejamento de TI (PlanejamentoTI);*
- *gestão de pessoas em TI (PessoasTI); e*
- *gestão de processos de TI (ProcessosTI).*

Entre os referidos indicadores, o que mais progrediu nas instituições avaliadas foi o PessoasTI: em 2018, contava com 67% dos avaliados em estágio "Inicial", e em 2021 possuía 46% na mesma situação.

Entretanto, **no caso da UFCG, nenhum indicador do iGestTI apresentou evolução**; o PlanejamentoTI permaneceu estável, e os outros dois caíram: ProcessosTI teve queda de 4,84% e PessoasTI 18,47%.

Assim, em síntese, o resultado do iGestTI na UFCG mostra-se contrário à evolução das boas práticas de gestão de TI vista em outras entidades brasileiras, entre 2018 e 2021, o que indica que a referida instituição não vem respondendo positivamente à necessidade de mudança na sua gestão de Tecnologia da Informação.

Após toda esta exposição e diante do cenário contextual, conceitual e legal exposto, o presente trabalho de auditoria buscou evidenciar se a UFCG atende satisfatoriamente a legislação pertinente e se adota boas práticas no que diz respeito aos mecanismos de gestão de Tecnologia da Informação e Comunicação (TIC), principalmente quanto aos controles relacionados à segurança da informação, a partir da análise do seu iGestTI.

II. ESCOPO DO TRABALHO

O foco desta auditoria foi determinado através da seleção dos indicadores considerados mais críticos no Índice de Gestão de TI (iGestTI) do IGG 2021 da UFCG. Assim, o presente trabalho teve como escopo a verificação e a análise dos procedimentos, fluxos e mecanismos de gestão e controle utilizados pela área de TI institucional, concernentes ao planejamento, serviço, riscos e segurança da informação e comunicações, por meio da criticidade dos referidos indicadores, e respectivos subindicadores, do iGestTI desta IFES.

Planejou-se realizar os trabalhos de análise documental na modalidade à distância (*home-office*) no período de fevereiro a março de 2022 e de análise presencial no período de abril a junho de 2022, com estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal e à legislação que disciplina a matéria examinada, destacando-se:

- Boletim de Serviço nº 44/2021, de 16 de novembro de 2021, o qual aprovou o regulamento da Política de Segurança da Informação e Comunicações (PoSIC) da UFCG
- Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) da UFCG;
- Plano de Desenvolvimento Institucional (PDI) da UFCG;
- *Control Objectives for Information and Related Technology* (COBIT) - é um guia de boas práticas apresentado como *framework*, dirigido para a gestão de tecnologia da informação (TI);

Os trabalhos foram feitos junto ao Serviço de Tecnologia da Informação (STI), setor ligado à Secretaria de Planejamento e Orçamento (SEPLAN) da Universidade Federal de Campina Grande, responsável por garantir o funcionamento eficiente, confiável e atualizado da estrutura de tecnologia da informação e comunicação da UFCG.

Destaca-se ainda que nenhuma restrição foi imposta à execução dos trabalhos de auditoria por parte da unidade auditada.

III. OBJETIVOS

Como dito anteriormente, esta ação de auditoria foi realizada com o **objetivo principal de avaliar a Gestão de TIC da UFCG com base no Índice de Gestão de TI do IGG de 2021**, nas legislações vigentes e orientações do TCU e Controladoria Geral da União (CGU), sugerindo possíveis melhorias nos processos.

No intuito de alcançar o objetivo principal deste trabalho, foram traçados também objetivos específicos baseados em indicadores e subindicadores selecionados pela equipe, relativos à verificação da capacidade de:

- Realização do planejamento de TI:
    - Execução do processo de planejamento;
    - Posse de plano vigente.
- Processos de TI:
    - Gestão de serviços:

        - Elaboração de catálogo de serviços;
        - Execução do processo de gestão de configuração e ativos (de serviços);
        - Execução do processo de gestão de incidentes de serviços.
    - Gestão de nível de serviço de TI;
    - Gestão de riscos:
        - Execução do processo de gestão de continuidade de serviços;
        - Definição da estrutura da gestão de riscos;
        - Estabelecimento de atividades típicas de segunda linha;
        - Implantação do processo de gestão de riscos;
        - Execução do processo de gestão de continuidade do negócio.
    - Índice de Gestão da Segurança da Informação:
        - Definição de políticas de responsabilidades para a gestão:
            - Disposição de comitê de segurança da informação;
            - Posse de gestor de segurança da informação.
        - Estabelecimento de processos e atividades para a gestão:
            - Execução do processo de gestão de riscos de segurança da informação;
            - Execução do processo de controle de acesso à informação e aos ativos associados à informação;
            - Execução do processo para classificação e tratamento de informações;
            - Execução do processo de gestão de incidentes de segurança da informação;
            - Execução de atividades de gestão da segurança dos recursos de processamento da informação.
    - Execução de processo de software

Com isto, aplicou-se neste trabalho a seguinte metodologia: fez-se um levantamento do "score" de todos os indicadores e subindicadores do Índice de Gestão de TI da UFCG apresentados em 2018 e 2021 (anos nos quais ocorreu levantamento de IGG) e então os valores referentes a cada ano foram comparados entre si, para se ter uma melhor noção de eventuais evoluções ou regressões. Em seguida, passou-se à seleção da amostra: foram considerados "críticos" pela equipe e, portanto, inseridos na amostra, os componentes de 2021 que apresentaram valor em 15% ou menos, ou seja, todos os componentes do nível "inexpressivo" (que vai de 0% até 14,99%), bem como uma pequena parcela dos componentes do grupo "Iniciando" (i.e., que pontuaram exatamente em 15,0%).

Em seguida, o questionário que embasa os referidos indicadores e subindicadores críticos foi enviado para a área responsável pela gestão da TI na UFCG, ou seja, o STI, que está vinculado à Secretaria de Planejamento e Orçamento (SEPLAN). As referidas perguntas foram enviadas através da Solicitação de Auditoria (SA) nº 18, anexada ao processo SEI nº. 23096.005762/2022-08.

Assim, a partir das questões utilizadas pelo TCU no levantamento do iGestTI dos pontos críticos já citados, e a fim de avaliar a eficiência e eficácia da gestão de TI na UFCG, realizou-se a presente auditoria.

IV. RESULTADO DOS EXAMES - ACHADOS DE AUDITORIA

Constatação 1: Insuficiência no indicador PlanejamentoTI (Capacidade em Planejamento de TI)

Fato:

No que concerne ao indicador PlanejamentoTI, o TCU considerou que este já estava em situação aceitável em 2018, com 60% das organizações avaliadas no estágio "Aprimorado" e apenas 21% nos estágios iniciais ("Inexpressivo" ou "Inicial"). Em 2021, não houve variação expressiva nesses resultados.

A UFCG, porém, tem apresentado um nível muito baixo ("Inexpressivo") no referido indicador, de apenas 5%, o qual não sofreu variação entre 2018 e 2021.

Com relação aos subindicadores do PlanejamentoTI desta IFES, verificou-se que pouco menos da metade das questões (46%) referentes ao assunto receberam respostas afirmativas ("sim") porém insuficientes; é dizer, foram dadas respostas afirmativas, contudo, estas necessitam ser complementadas para melhor compreensão da real situação relativa ao ponto indagado. As respostas afirmativas que foram consideradas insuficientes estão dispostas na tabela abaixo.

Subindicador	Pergunta	Resposta do STI 2022	Comentário da auditoria
EXECUÇÃO DO PROCESSO DE PLANEJAMENTO	d) análises de benefícios, de custos e de riscos subsidiam as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações)?	"Sim, conforme item c." *(Resposta do item c: "Sim").*	Não mencionou qualquer informação sobre a análise de custo-benefício feita para escolha de iniciativas.
	e) o processo de planejamento de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Não. As ações de planejamento de TIC são geridas pelo Comitê de Governança Digital – CGD a partir de sua criação em agosto/2021. Link da portaria: https://sti.ufcg.edu.br/normas.html?download=45:portaria-n-65-de-11-de-agosto-de-2021"	Não deu nenhuma previsão para a formalização do processo de planejamento.
POSSE DE PLANO VIGENTE	e) a seleção de iniciativas de TI (projetos e ações) para compor o plano de TI considera estimativas fundamentadas em dados históricos ou em estudos técnicos sobre a capacidade e a disponibilidade dos recursos de TI da organização (financeiros,	"Os projetos de TIC são avaliados com estudo técnico e priorização da administração orientados pelo PDTIC."	Não informou nada sobre nenhum estudo técnico sobre disponibilidade de recursos realizado anteriormente.

	humanos, materiais, equipamentos etc.)?		
	f) ao elaborar o Plano de TI, a organização avalia iniciativas estratégicas que têm por objetivo ampliar ou melhorar o uso de TI como instrumento de transformação do negócio em benefício da sociedade (transformação digital), especialmente quanto aos riscos de adoção, adoção tardia ou não adoção de tais iniciativas?	"Todas as soluções de TIC afetam diretamente a sociedade, seja comunidade interna ou externa da UFCG (futuros alunos, docentes, etc). Segundo o PDTIC, a missão do Serviço de Tecnologia da Informação (STI) é "planejar e prover soluções de Tecnologia da Informação e Comunicação (TIC) para a comunidade acadêmica e a sociedade"..	Não fez qualquer menção a qualquer avaliação de iniciativa estratégica de transformação digital feita previamente.
	g) é feito acompanhamento concomitante à execução do plano de TI, com vistas a assegurar sua observância e possibilitar a realização de ajustes que se fizerem necessário?	"Sim. Objetivos Estratégicos de TI, conforme PDTIC 2021-2024. Para concretizar a visão estratégica pretendida, o STI atuará para concretizar os seguintes objetivos estratégicos: OE5- Promover e solidificar a Governança de TIC na UFCG; Participar ativamente das atividades de planejamento de TI (PDTIC) e propostas orçamentárias para investimentos necessários em TI; Acompanhar os indicadores das metas do PDTIC; Implementar ações que envolvam o mapeamento e a automatização de processos relacionados à governança de TIC."	Não informou se é feito (em caso negativo é preciso dar uma previsão para a sua realização) e nem como é feito o acompanhamento concomitante da execução do plano.

Manifestação da Unidade Auditada:

As respostas dadas pela Unidade Auditada (Seplan) foram tabeladas e classificadas pelas sua situação (suficiente ou insuficiente), como pode ser visto a seguir.

Subindicador	Pergunta	Resposta do STI ao Relatório Preliminar	Situação
EXECUÇÃO DO PROCESSO DE PLANEJAMENTO	d) análises de benefícios, de custos e de riscos subsidiam as decisões relacionadas à seleção e à priorização das iniciativas de TI (projetos e ações)?	A priorização foi realizada no PDTIC-2021-2024 , itens 9, 13 e 14, publicado em: https://portal.ufcg.edu.br/phocadownload/userupload/Boletim_de_servico/boletim%20de%20servio%20-%202021%2045.pdf	Insuficiente

	e) o processo de planejamento de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	O planejamento de TIC na instituição é realizado por meio do PDTIC (https://portal.ufcg.edu.br/phocadownload/userupload/Boletim_de_servico/boletim%20de%20servio%20-%202021%2045.pdf)	Insuficiente
POSSE DE PLANO VIGENTE	e) a seleção de iniciativas de TI (projetos e ações) para compor o plano de TI considera estimativas fundamentadas em dados históricos ou em estudos técnicos sobre a capacidade e a disponibilidade dos recursos de TI da organização (financeiros, humanos, materiais, equipamentos etc.)?	Os estudos técnicos de viabilidade de contratação são realizados pela equipe de contratação designada em cada processo de aquisição. Os processos estão disponíveis no link: http://metabase.sti.ufcg.edu.br/public/dashboard/2d282375-0a97-4717-a777-d9cfb95b993b	Suficiente
	f) ao elaborar o Plano de TI, a organização avalia iniciativas estratégicas que têm por objetivo ampliar ou melhorar o uso de TI como instrumento de transformação do negócio em benefício da sociedade (transformação digital), especialmente quanto aos riscos de adoção, adoção tardia ou não adoção de tais iniciativas?	As iniciativas foram pactuadas com o Ministério de Economia por meio do Plano de Gestão Estratégica e Transformação Institucional da UFCG (TransformaGov), disponibilizado em: https://sei.economia.gov.br/sei/controlador_externo.php?acao=documento_conferir&codigo_verificador=18682446&codigo_crc=CBE09B7A&hash_download=a2cd5497ae1a1981390f51d0ca70e2c8dbb115d423fc4630fe26826dced8b05945feffd12983122e53da0b68d48d3b5b486242dd9bfd4cfb4ed2f0de429dff90&visualizacao=1&id_orga	Suficiente

		o_acesso_externo=0	
	g) é feito acompanhamento concomitante à execução do plano de TI, com vistas a assegurar sua observância e possibilitar a realização de ajustes que se fizerem necessário?	O PDTIC será cadastrado no sistema ForPDI do MEC, disponível em: https://ufcg.plataformafor.mec.gov.br/ Prazo: OUT/2022	Insuficiente

Análise da Auditoria:

Com relação aos subindicadores do PlanejamentoTI, algumas respostas afirmativas consideradas insuficientes permaneceram nesta situação e foram transformadas em recomendações, descritas a seguir.

Recomendação 1: Utilizar análise de custo-benefício no processo decisório (seleção e priorização) relativo às escolhas das iniciativas de TI (projetos e ações)

Recomendação 2: Formalizar o processo de planejamento de TI

Recomendação 3: Apresentar comprovação do cadastramento do PDTIC no ForPDI até o final de 2022

Constatação 2: Insuficiência no indicador ProcessosTI (Capacidade em Gestão de Processo de TI).

Fato:

As práticas analisadas através dos componentes de ProcessosTI são de fundamental importância para a boa gestão de TI organizacional, conforme preconizam as referências internacionais de boas práticas contidas no COBIT (*Control Objectives for Information and Related Technology*). No modelo COBIT, estas práticas dizem respeito a uma série de objetivos de controle:

- *Estabelecimento e Manutenção da Estrutura de Governança;*
- *Estrutura de Gestão de TI Gerenciada;*
- *Orçamento e Custos Gerenciados;*
- *Acordos de Serviço Gerenciados;*
- *Fornecedores e Contratações Gerenciados;*
- *Riscos Gerenciados;*
- *Segurança Gerenciada;*
- *Identificação e Construção de Soluções de TI Gerenciadas;*
- *Mudanças de TI Gerenciadas;*

- *Projetos Gerenciados;*
- *Requisições de Serviços e Incidentes Gerenciados;*
- *Serviços de Segurança Gerenciados.*

Ainda assim, em geral, segundo o TCU, o componente do iGestTI que teve o pior resultado a nível nacional foi justamente o de gestão de processos de TI (ProcessosTI), pois quase a metade (48%) das instituições avaliadas ainda apresenta este indicador nos níveis iniciais.

No caso da UFCG, este também foi o de menor "score" (14,36%), mas em contrapartida, com o menor decréscimo (-4,84%) de 2018 a 2021.

Ainda assim, analisando mais a fundo o indicador ProcessosTI, identificaram-se algumas melhorias ao longo do tempo (2018 a 2021), como pode ser constatado nos seguintes subindicadores: gestão de riscos de TI (iGestRiscosTI), processo de *software* (ProcessoSoftware), gestão de projetos de TI (iGestProjetosTI) e gestão de contratações de TI (iGestContratosTI).

Apesar da evolução na capacidade processual geral de aplicação das práticas de gestão de riscos de TI, está ainda assim é baixa, com 55% das organizações avaliadas ainda em seus estágios iniciais.

Vale acrescentar que, apesar de não aparecer no rol de subindicadores com evolução positiva, a nível nacional, o índice de gestão de segurança da informação (iGestSegInfo) deve ser citado pelo fato de ter passado por mudanças expressivas nos seus critérios avaliativos entre 2018 e 2021. No referido iGestSegInfo, ocorreu o acréscimo das seguintes práticas:

- *gestão de continuidade do negócio institucional;*
- *gestão de continuidade de serviços de TI;*
- *gestão da segurança da informação no processo de software; e*
- *auditoria da gestão da segurança da informação.*

Ainda assim, apesar das referidas mudanças, as práticas que foram cobradas em ambos os anos de 2018 e 2021 (EstruturaSegInfo e ProcessoSegInfo) não apresentaram grande variação, permanecendo com resultados ruins, o que demonstra que a variação no referido subindicador (iGestSegInfo) decorreu da adição de novos critérios avaliativos em 2021.

No caso da UFCG, os únicos subindicadores do ProcessosTI com evolução foram: gestão de níveis de serviço de TI (iGestNiveisServicoTI), com acréscimo de 15%, e gestão de riscos de TI (iGestRiscosTI), com aumento de 8%.

Apesar de o iGestRiscosTI da UFCG não ter alcançado um grande crescimento, este apareceu entre os maiores "scores" no ano de 2021, no patamar de 14,90%. Assim, o destaque para o subindicador iGestRiscosTI na UFCG ficou evidente; as causas para isso podem ser um ou mais dos motivos elencados pelo TCU no Relatório de Acompanhamento do IGG 2021:

- "a natural e paulatina implementação, pelas instituições avaliadas, de diretrizes já existentes sobre o tema, como a Instrução Normativa Conjunta 1/2016, do então Ministério do Planejamento, Orçamento e Gestão e da Controladoria-Geral da União, que dispõe sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo federal";
- "ações do TCU com objetivos educativos sobre esse assunto, a exemplo da publicação, em 2018, dos guias 'Referencial Básico de Gestão de Riscos' e '10 Passos para a Gestão de Riscos', disponíveis no Portal do TCU no seguinte endereço: https://portal.tcu.gov.br/governanca/governancapublica/gestao-de-riscos;" e
- "a Portaria 277/2019, do Conselho Nacional de Justiça, que instituiu um 'Manual de Gestão de Riscos'".

Contrariamente, em escala nacional, dentre os subindicadores que pioraram, citam-se: gestão de serviços de TI (iGestServicosTI), gestão de níveis de serviço de TI (iGestNiveisServicoTI) e gestão de segurança da informação (iGestSegInfo). Presume-se que tais pioras ocorreram em parte em decorrência das mudanças no questionário aplicado em 2021, que teve novas práticas incluídas, as quais se apresentaram deficientes na maioria das instituições avaliadas. Com relação às práticas que já constavam no questionário de 2018 e foram novamente cobradas em 2021, a variação foi pequena.

No caso da UFCG, os únicos subindicadores do ProcessosTI com regressão foram:

- processo de software (ProcessoSoftware): -51%;
- gestão de segurança da informação (iGestSegInfo) -1%;
- estrutura de segurança da informação (EstruturaSegInfo) -3%;
- processo de segurança da informação (ProcessoSegInfo) -2%; e
- gestão de serviços (iGestServicosTI): -9%.

Vale ressaltar que a queda no desempenho do iGestSegInfo – de forma geral, e não apenas para a UFCG – se torna ainda mais séria, não apenas pelo fato de ser considerada prática essencial, mas também por ter ganhado ainda mais importância após a plena vigência da Lei Geral de Proteção de Dados (LGPD), pois falhas nas políticas, estruturas e processos relativos à segurança da informação podem ter sérias repercussões no cumprimento da referida norma.

Com relação aos mencionados subindicadores deste indicador, no âmbito da UFCG, notou-se que as respostas da unidade auditada podem ser divididas em três categorias: resposta negativa ("não"); resposta afirmativa e suficiente; e resposta afirmativa, mas insuficiente.

Assim, constatou-se que pouco menos da metade (48%) das questões associadas ao tema tiveram resposta negativa ("não") ou similar (ex.: "não há processo de gestão de ativos").

É importante salientar que também houve uma pequena quantidade de questionamentos que não foram respondidos (referentes ao assunto estrutura da gestão de riscos) porque acabaram não sendo entregues à unidade auditada. Isso aconteceu devido a um equívoco da equipe de auditoria, que enviou outros quesitos no lugar. Tais perguntas estão com o

seguinte comentário desta equipe: “Não houve resposta porque a questão não chegou à unidade auditada.”

Sub-Indicadores		Pergunta	Resposta do STI (2022)
CAPACIDADE EM GERIR SERVIÇOS DE TI	A ORGANIZAÇÃO ELABORA UM CATÁLOGO DE SERVIÇOS DE TI?	b) o catálogo está atualizado e as informações que nele constam são compatíveis com os Acordos de Níveis de Serviço (ANS) estabelecidos pela área de TI e as áreas de negócio da organização?	"Não."
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE CONFIGURAÇÃO E ATIVOS (DE SERVIÇOS DE TI)?	b) a base de dados de configurações permite à organização conhecer o histórico da situação dos serviços e ativos de TI e do relacionamento entre eles ao longo do tempo?	"Não."
		d) a base de dados de configurações é utilizada como insumo para o planejamento e o acompanhamento das mudanças?	"Não."
		e) o processo de gestão de configuração e ativos está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Não."
		f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de configuração e ativos e promove eventuais ajustes necessários?	"Não."
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE INCIDENTES DE SERVIÇOS DE TI?	a) a organização definiu regras para a priorização e o escalonamento de incidentes?	"Não."
		b) a resolução de incidentes considera os níveis de serviços especificados em acordos com as áreas clientes?	"Não."

		d) o processo de gestão de incidentes está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Não."
		e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de incidentes de serviços de TI e promove eventuais ajustes necessários?	"Não."
CAPACIDADE EM GERIR RISCOS DE TI	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE CONTINUIDADE DE SERVIÇOS DE TI?	a) a organização elabora um plano de continuidade de serviços de TI?	"Não."
		b) as ações e os prazos definidos no plano de continuidade de serviços de TI fundamentam-se em análises de impacto no negócio realizadas sobre os processos organizacionais críticos?	"Não."
		c) o plano de continuidade de serviços de TI é testado e revisado periodicamente?	"Não."
		d) o processo de gestão de continuidade de serviços de TI integra o processo institucional de gestão de continuidade do negócio?	"Não."
		e) o processo de gestão de continuidade de serviços de TI está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Não."
		f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de continuidade de serviços de TI e promove eventuais ajustes necessários?	"Não."

	A ESTRUTURA DA GESTÃO DE RISCOS ESTÁ DEFINIDA?	a) há política institucional de gestão de riscos aprovada pelo conselho ou colegiado superior ou pela alta administração?	*Não houve resposta porque a questão não chegou à unidade auditada.*
		b) foram definidas as instâncias responsáveis pelo sistema de gestão de riscos e respectivas competências (p. ex. alta administração, gestores operacionais, gestores de riscos, instância de supervisão da gestão de riscos, instância colegiada de assessoramento, outras funções de segunda linha , auditoria interna)?	*Não houve resposta porque a questão não chegou à unidade auditada.*
		c) foram definidas as diretrizes da integração do processo de gestão de riscos aos processos organizacionais?	*Não houve resposta porque a questão não chegou à unidade auditada.*
		d) foram definidos os critérios de análise e avaliação de riscos (orientações para determinação de níveis de risco, classificação e priorização dos riscos, e ainda para seleção das medidas de tratamento)?	*Não houve resposta porque a questão não chegou à unidade auditada.*
		e) foram definidos os fluxos de comunicação para compartilhar informações e decisões acerca de gestão de riscos?	*Não houve resposta porque a questão não chegou à unidade auditada.*
		f) o processo de gestão de riscos está formalizado?	*Não houve resposta porque a questão não chegou à unidade auditada.*
		g) limites para exposição ao risco estão definidos?	*Não houve resposta porque a questão não chegou à unidade auditada.*
	ATIVIDADES TÍPICAS DE SEGUNDA LINHA ESTÃO ESTABELECIDAS?	a) foram definidas e atribuídas atividades típicas de segunda linha de defesa: supervisão, suporte e coordenação de atividades de gestão de	"Não."

		riscos, monitoramento da adequação e eficácia dos controles internos adotados pela gestão?	
		b) foi definido fluxo de comunicação sobre riscos e controles entre os agentes que executam atividades de segunda linha de defesa, os gerentes de áreas (primeira linha de defesa) e a alta administração?	"Não."
		c) as atividades da segunda linha de defesa incluem o monitoramento da integridade e precisão dos reportes de gestão de riscos?	"Não."
		d) as atividades da segunda linha de defesa incluem o fornecimento de metodologias, ferramentas e orientações em geral para que os gestores (1ª linha de defesa) identifiquem e avaliem riscos?	"Não."
		e) as atividades da segunda linha de defesa incluem o suporte aos gestores (1ª linha de defesa) na implementação e monitoramento contínuo dos controles internos destinados a mitigar os riscos identificados?	"Não."
		g) as atividades da segunda linha de defesa incluem alertar a gerência operacional (1ª linha de defesa) para questões emergentes e para as mudanças no cenário regulatório e de riscos?	"Não."
	O PROCESSO DE GESTÃO DE RISCOS DA ORGANIZAÇÃO ESTÁ IMPLANTADO?	a) objetivos e elementos (processos, produtos, atividades, ativos) críticos da organização estão identificados?	"Não."
		b) há lista integrada de riscos, incluindo causas, fontes, efeitos?	"Não."
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE CONTINUIDADE DO NEGÓCIO?	a) há política institucional de gestão de continuidade do negócio (PGCN) aprovada pela alta administração?	"Não."

			b) o processo de gestão de continuidade do negócio está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Não."
			c) há plano de continuidade do negócio (PCN) aprovado pela alta administração?	"Não."
			d) as ações e os prazos definidos no PCN fundamentam-se em análises de impacto no negócio (Business Impact Analysis – BIA) realizadas sobre os processos organizacionais críticos?	"Não."
			e) o PCN é testado e revisado periodicamente?	"Não."
ÍNDICE DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO	CAPACIDADE EM DEFINIR POLÍTICAS DE RESPONSABILIDADE PARA GESTÃO DA TI	A ORGANIZAÇÃO DISPÕE DE COMITÊ DE SEGURANÇA DA INFORMAÇÃO?	a) o comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo?	"Não."
			b) o comitê formula diretrizes para a segurança da informação?	"Não."
			c) o comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação?	"Não."
			d) o comitê é composto por representantes de áreas relevantes da organização?	"Não."
		A ORGANIZAÇÃO POSSUI UM GESTOR INSTITUCIONAL DE SEGURANÇA DA INFORMAÇÃO?	a) o gestor institucional de segurança da informação foi designado formalmente pela alta administração?	"Não."
			b) o gestor institucional de segurança da informação reporta-se diretamente à alta administração?	"Não."
			c) o gestor institucional de segurança da informação coordena o processo de gestão de riscos de segurança da informação em âmbito institucional?	"Não."

			d) o gestor institucional de segurança da informação coordena ações de segurança da informação em âmbito institucional?	"Não."
			e) o gestor institucional de segurança da informação fomenta e coordena ações periódicas de conscientização e de treinamento em segurança da informação para todas as partes interessadas, incluindo autoridades, servidores e colaboradores?	"Não."
			f) o gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências?	"Não."
	CAPACIDADE EM ESTABELECER PROCESSOS E ATIVIDADES PARA GESTÃO DA TI	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO?	b) a organização trata riscos de segurança da informação com base em um plano de tratamento de riscos?	
			c) a organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação?	
			d) o processo de gestão de riscos de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	
			e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de segurança da informação e promove eventuais ajustes necessários?	

		A ORGANIZAÇÃO EXECUTA PROCESSO DE CONTROLE DE ACESSO À INFORMAÇÃO E AOS ATIVOS ASSOCIADOS À INFORMAÇÃO?	a) a organização implementa controles de acesso físicos e lógicos à informação e aos ativos associados à informação que são por ela gerenciados ou custodiados, com vistas a proteger adequadamente a confidencialidade das informações não públicas e a integridade e a disponibilidade das informações consideradas críticas para o negócio?	"Não."
			b) os controles de acesso implementados na organização aplicam o princípio "necessidade de conhecer", o qual prescreve que deve haver necessidade legítima que justifique o acesso à informação por pessoa, sistema ou entidade, bem como o princípio "privilégio mínimo", o qual estabelece que o perfil de acesso concedido deve incluir tão somente os poderes necessários para o atendimento das legítimas necessidades?	"Não."
			c) há controles de acesso lógicos na organização que utilizam autenticação com certificado digital ICP-Brasil, a fim de prover identificação inequívoca de pessoas físicas e jurídicas e comprovação de autoria em transações digitais?	"Não."
			d) a organização analisa criticamente, a intervalos regulares, os direitos de acesso lógicos e físicos existentes, com vistas à remoção de direitos que deixaram de ser necessários e para assegurar que privilégios indevidos não foram obtidos?	"Não."
			e) a organização instituiu uma Política de Controle de Acesso (PCA), a qual estabelece princípios, objetivos,	"Não."

			diretrizes, principais atividades e responsabilidades relativos ao processo de controle de acesso?	
			f) a organização avalia periodicamente o desempenho e a conformidade do processo de controle de acesso e promove eventuais ajustes necessários?	"Não."
		GESTÃO DE ATIVOS ASSOCIADOS À INFORMAÇÃO	b) a organização definiu responsabilidades pelos ativos associados à informação?	"Não."
			d) o processo de gestão de ativos associados à informação subsidia a implantação de controles e ações com vistas a assegurar a adequada proteção dos ativos e das informações que armazenam, processam ou transmitem?	"Não há Processo de Gestão de Ativos."
			e) o processo de gestão de ativos associados à informação subsidia a implantação de ações mitigatórias aplicáveis no caso de ocorrência de evento catastrófico que inviabilize a utilização de ativos?	"Não há Processo de Gestão de Ativos."
			f) o processo de gestão de ativos associados à informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Não há Processo de Gestão de Ativos."
			g) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de ativos associados à informação e promove eventuais ajustes necessários?	"Não há Processo de Gestão de Ativos."
		A ORGANIZAÇÃO EXECUTA PROCESSO DE	e) o processo de gestão de incidentes de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento	"Não."

		GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO?	similar com orientações quanto à execução do processo e definição de responsabilidades)?	
			f) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de incidentes de segurança da informação e promove eventuais ajustes necessários?	"Não."
		A ORGANIZAÇÃO EXECUTA ATIVIDADES DE GESTÃO DA SEGURANÇA DOS RECURSOS DE PROCESSAMENTO DA INFORMAÇÃO, INCLUSIVE DOS RECURSOS DE COMPUTAÇÃO EM NUVEM?	b) a organização gerencia (inventaria e controla) os softwares instalados nos dispositivos conctados em sua rede?	"Não."
	O PROCESSO DE SOFTWARE		f) o processo de software da organização promove a identificação precoce de requisitos de segurança da informação e a gestão permanente desses requisitos durante todo o ciclo de vida do software?	"Não."

Ademais, esta equipe considerou que, dentre todas as respostas dadas para esse indicador, 35% (trinta e cinco por cento) foram afirmativas porém insuficientes, i.e., precisam de complementação para uma melhor compreensão da real situação, como poderá ser visto a seguir:

Subindicadores		Pergunta	Resposta do STI 2022	Comentário da auditoria
CAPACIDADE DE GERIR SERVIÇOS DE TI	A ORGANIZAÇÃO ELABORA UM CATÁLOGO DE SERVIÇOS DE TI?	a) o catálogo contém as metas definidas para cada serviço (p. ex. prazos de entrega, horários de serviço e de suporte, bem como pontos de contato para solicitação do serviço, envio de sugestões, esclarecimento de dúvidas e reporte de incidentes)?	"Há um catálogo em produção para publicação no site do STI, entretanto o OSTicket apresenta o tempo para atendimento da demanda, também nele, após a finalização do ticket, há o envio de um formulário para avaliação/sugestões etc. No site do STI há orientações sobre horário de atendimento e pontos de contato."	Não deu previsão para conclusão do catálogo e nem se este conterá metas para cada serviço.
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE INCIDENTES DE SERVIÇOS DE TI?	c) bases de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes?	"Sim."	Não informou onde é mantida a base de conhecimento sobre erros conhecidos e problemas.
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE MUDANÇAS?	a) a organização estabeleceu critérios para orientar a aprovação de mudanças, inclusive quanto ao tratamento de casos de exceção (mudanças emergenciais)?	"Sim, no processo de desenvolvimento de software."	Não determinou se há critérios para orientar e aprovar mudanças além do processo de desenvolvimento de software.

		c) identificam-se os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados?	"Sim, tanto nos ativos, quanto nos serviços."	Não informou como os serviços e ativos afetados pela mudança são identificados.
		d) a realização de cada mudança é precedida de planejamento e testes?	"Sim, as alterações são realizadas em ambiente de testes e depois de concluídas seguem para o ambiente de produção."	Não disse se os planejamento e testes das mudanças existem além do processo de desenvolvimento de software.
		e) mudanças executadas são rastreáveis e monitoradas, com vistas à avaliação de sua efetividade e para permitir ações corretivas, no caso de ocorrência de efeitos não identificados nas fases de planejamento e testes?	"Sim, há o controle de versão de cada alteração implementada nos sistemas."	Não fez qualquer referência a forma como as mudanças são rastreadas e monitoradas nos sistemas e nem como estas são realizadas fora do processo de desenvolvimento de software.
		f) lições aprendidas com as mudanças são compartilhadas, com vistas ao aprimoramento do processo (ex: Wiki)?	"Sim, são compartilhada via Base de Conhecimento (OsTicket) e também nas ferramentas de gerenciamento de projetos."	Esta não definiu onde as lições aprendidas com as mudanças são compartilhadas.

		g) o processo de gestão de mudanças está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Sim, no processo de desenvolvimento de software."	Apesar da existência da formalização do processo de gestão de mudanças no desenvolvimento de software, este não se encontra acessível on-line e nem há menção deste além do processo de software.
		h) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de mudanças e promove eventuais ajustes necessários?	"Sim, quando necessário."	Não informou como o desempenho e a conformidade do processo de gestão de mudanças é avaliado.
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE CONFIGURAÇÃO E ATIVOS (DE SERVIÇOS DE TI)?	a) a organização mantém uma base de dados consolidada com as configurações dos serviços e ativos de TI e o relacionamento entre eles?	"Sim, para os ativos gerenciados pelo STI."	Não informou onde é mantida a base de dados consolidada com as configurações dos serviços e ativos e o relacionamento entre elas.
		c) a base de dados de configurações é mantida atualizada?	"Sim."	Não determinou onde é mantida a referida base de dados e nem diz a frequência que esta é atualizada.
CAPACIDADE EM GERIR RISCOS DE TI	O PROCESSO DE GESTÃO DE RISCOS DA ORGANIZAÇÃO ESTÁ IMPLANTADO?	d) o tratamento dos riscos está documentado?	"Não. Será elaborado pelo CGD."	Não deu previsão para a formalização do tratamento dos riscos.

			f) os riscos críticos identificados são informados aos membros das instâncias superiores de governança?	"Sim. Os incidentes de segurança são notificados via e-mail."	Não informou se há algum e-mail notificando a CGD sobre os riscos críticos.
ÍNDICE DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO	CAPACIDADE EM DEFINIR POLÍTICAS DE RESPONSABILIDADE PARA GESTÃO DA TI	A ORGANIZAÇÃO DISPÕE DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO?	b) a política (ou norma interna complementar) contempla diretrizes sobre gestão de riscos de segurança da informação?	"Não, pois ainda não foi publicado o plano de gerenciamento de riscos. A STI apresentará planos de gerenciamento de riscos e da ação de resposta a incidentes, a serem aprovados pelo Comitê de Governança Digital e executados pela STI e seus núcleos de tecnologia locais."	Não deu previsão para publicação do plano de gerenciamento de riscos.
			e) a política é mantida atualizada, por meio de revisões periódicas?	"Sim, a revisão é realizada sempre que se fizer necessária não excedendo o período de um ano."	Na POSIC Temos: "Ao Comitê Gestor de Segurança da Informação compete: elaborar e revisar periodicamente a Política de Segurança da Informação e Comunicações (POSIC) e normas relacionadas, submetendo a aprovação do Comitê de Governança Digital ou órgão equivalente;"

	CAPACIDADE EM ESTABELECER PROCESSO E ATIVIDADES PARA GESTÃO DA TI	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO?	a) a organização identifica e avalia riscos de segurança da informação?	"Não, ainda serão elaborados planos de gerenciamento de riscos e da ação de resposta a incidentes, a serem aprovados pelo Comitê de Governança Digital e executados pela STI e seus núcleos de tecnologia locais."	Não deu previsão para a elaboração dos planos de gerenciamento de riscos e ação de resposta à incidentes.
		A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE ATIVOS ASSOCIADOS À INFORMAÇÃO?	a) a organização mantém um inventário dos ativos associados à informação?	"Parcialmente. Há o inventário dos ativos do STI."	Não informou onde é mantido o inventário dos ativos associados à informação do STI. Também não dá previsão para realização do inventário dos ativos associados à informação da UFCG.
			c) o inventário identifica as informações críticas que os ativos armazenam, processam ou transmitem?	"Parcialmente. Há o inventário dos ativos do STI com a descrição dos serviços hospedados."	Não determinou onde é mantido o inventário dos ativos do STI. Também não dá previsão para realização do inventário dos ativos da UFCG e nem diz quais as informações críticas do inventário dos ativos do STI.

		A ORGANIZAÇÃO EXECUTA PROCESSO PARA CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÃO?	a) informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção?	"Parcialmente. Está em adequação no ambiente SEI, processo nº 23096.014700/2022-89. Não existe rotulação e identificação de informações pessoais armazenadas no ambiente do STI."	Não caracteriza como solução parcial se não há identificação e rotulação de informações pessoais.
			b) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item "a" em conformidade com os requisitos legais e de negócio?	"Parcialmente. Está em adequação no ambiente SEI, processo nº 23096.014700/2022-89. Não existe rotulação e identificação de informações pessoais armazenadas no ambiente do STI."	Não caracteriza como solução parcial se não há tratamento e proteção das informações pessoais.
			c) informações sigilosas em razão de sua imprescindibilidade à segurança da sociedade ou do Estado são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção?	"Há uma comissão formada para elaboração do Plano de Dados Abertos (PDA/UFCG) - Processo SEI/UFCG - 23096.076955/2021-54."	Não há referência ao tratamento (identificação e rotulação) e proteção das informações sigilosas no PDA da UFCG.

			d) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item "c" em conformidade com os requisitos legais e de negócio?	"Há uma comissão formada para elaboração do Plano de Dados Abertos (PDA/UFCG) - Processo SEI/UFCG - 23096.076955/2021 -54."	Não há referência ao tratamento e proteção das informações sigilosas no PDA da UFCG.
			e) informações sigilosas em função de outras hipóteses legais de sigilo ou segredo são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção?	"Parcialmente. Está em adequação no ambiente SEI, processo nº 23096.014700/2022 -89. Não existe rotulação e identificação de informações pessoais armazenadas no ambiente do STI."	Não caracteriza como solução parcial se não há tratamento e proteção das informações sigilosas.
			g) informações críticas para a organização em razão de necessidades do negócio (p. ex. requisitos associados à integridade, disponibilidade, autenticidade ou a outros atributos da informação) são identificadas e rotuladas, com vistas a viabilizar adequado	"Há uma comissão formada para elaboração do Plano de Dados Abertos (PDA/UFCG) - Processo SEI/UFCG - 23096.076955/2021-54."	Não há referência ao tratamento (identificação e rotulação) e proteção das informações críticas (em razão de necessidade do negócio) no PDA da UFCG.

			tratamento e proteção?		
			h) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item "g" em conformidade com os requisitos legais e de negócio?	"Há uma comissão formada para elaboração do Plano de Dados Abertos (PDA/UFCG) - Processo SEI/UFCG - 23096.076955/2021-54"	Não há referência ao tratamento e proteção das informações críticas (em razão de necessidade do negócio) no PDA da UFCG.
			j) a organização avalia periodicamente o desempenho e a conformidade do processo de classificação e tratamento de informações e promove eventuais ajustes necessários?	"Há uma comissão formada para elaboração do Plano de Dados Abertos (PDA/UFCG) - Processo SEI/UFCG - 23096.076955/2021-54"	Não há referência a avaliação periódica do desempenho e conformidade da classificação e tratamento das informações no PDA da UFCG.
		A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO?	f) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item "e" em conformidade com os requisitos legais e de negócio?	"Parcialmente. Está em adequação no ambiente SEI, processo nº 23096.014700/2022-89. Não existe rotulação e identificação de informações pessoais armazenadas no ambiente do STI."	Não caracteriza como solução parcial se não há tratamento e proteção das informações sigilosas.

			i) o processo de classificação e tratamento de informações está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Parcialmente. Está em adequação no ambiente SEI, processo nº 23096.014700/2022-89."	Não caracteriza como solução parcial se não há formalização da classificação e tratamento das informações.
			b) a organização definiu procedimentos e responsabilidades quanto ao tratamento das notificações de incidentes de segurança da informação, adoção de ações emergenciais e diretrizes para escalamento e comunicação interna e externa?	"Realizado de maneira não formal, no âmbito do STI."	Não informou previsão para formalização da referida ação.
		A ORGANIZAÇÃO EXECUTA ATIVIDADES DE GESTÃO DA SEGURANÇA DOS RECURSOS DE PROCESSAMENTO DA INFORMAÇÃO, INCLUSIVE DOS RECURSOS DE	c) a organização definiu procedimentos e responsabilidades quanto à análise de incidentes de segurança da informação, identificação de causas raízes e planejamento e implementação de ações corretivas?	"Realizado de maneira não formal, no âmbito do STI."	Não informou previsão para formalização da referida ação.

		COMPUTAÇÃO EM NUVEM?	d) a organização instituiu equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) ou estrutura equivalente?	"Realizado de maneira não formal, no âmbito do STI."	Não informou previsão para formalização da referida ação.
			a) a organização gerencia (inventaria e controla) os dispositivos conectados em sua rede?	"Sim, no âmbito do STI e UFCGNet."	Não informou onde o inventário e o controle dos dispositivos conectados à rede do STI e UFCGNET é mantido. Também não dá previsão para a realização do mesmo no restante da UFCG.
			c) a organização gerencia vulnerabilidades técnicas em seus ativos de software, de hardware e de rede críticos para o negócio?	"Sim, no âmbito do STI e UFCGNet."	Não determinou como é feito o gerenciamento de vulnerabilidades técnicas dos ativos de TI críticos para STI e UFCGNET. Também não dá previsão para realização do referido gerenciamento no restante da UFCG.
			d) a organização implementa configurações seguras em seus ativos de software, de hardware e de	"Sim, no âmbito do STI e UFCGNet."	Não informou como é feita a configuração segura dos ativos críticos de TI do STI e UFCGNET. Também não dá previsão para

			rede críticos para o negócio?		implementação da referida ação no restante da UFCG.
			e) a organização mantém, monitora e analisa logs de auditoria dos ativos de software, de hardware e de rede críticos para o negócio?	"Sim, é realizado sob demanda, no âmbito do STI e UFCGNet."	Não disse como é feito o monitoramento e análise de logs de auditoria dos ativos críticos de TI do STI e UFCGNET. Também não dá previsão para implementação da referida ação no restante da UFCG.
			f) A organização aplica controles compensatórios para o uso de privilégios administrativos em seus ativos de software, de hardware e de rede críticos para o negócio?	"Sim, no âmbito do STI e UFCGNet."	Não determinou como é feito o controle compensatório para uso de privilégios administrativos nos ativos críticos de TI do STI e UFCGNET. Também não dá previsão para implementação da referida ação no restante da UFCG.
			g) a organização implementa defesas contra malware (ex: vírus) e outras ameaças cibernéticas (ex: phishing)?	"Sim, com uso de firewall."	Não deu previsão para o uso de outras defesas contra malware e similares.
			h) a organização limita e controla o uso de portas, protocolos e serviços de rede	"Sim, com uso de firewall."	Não deu previsão para o uso de outras limitações e controle de portas, protocolos e

			nas conexões de sua rede interna com a internet e outras redes externas?		serviços de rede na conexão de rede.
			i) a organização implementa defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas?	"Sim, com uso de firewall"	Não deu previsão para implementação de outras defesas de conexão de rede.
			j) a organização implementa cópias regulares de segurança (backup) das informações em meio digital, conforme as melhores práticas e as necessidades de negócio, incluindo a realização periódica de testes de recuperação das informações?	"Parcialmente, uma vez que não há solução corporativa de backup."	Não determinou qual a frequência do back-up e nem onde é mantido o mesmo. Também não diz quais as práticas de back-up adotadas ou qual a frequência dos testes de recuperação de informações.
	O PROCESSO DE SOFTWARE (DA ORGANIZAÇÃO PROMOVE A IDENTIFICAÇÃO PRECOCE DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E A GESTÃO PERMANENTE DESSES REQUISITOS DURANTE TODO O CICLO DE VIDA DO SOFTWARE)?		b) a organização avalia as soluções existentes no mercado antes de decidir pelo desenvolvimento de software (análise do tipo	"Sim. É realizado análise de soluções existentes no mercado que atendam as necessidades da instituição."	Não determinou onde há avaliações de soluções existentes.

		"construir ou adquirir")?		
		c) na etapa de planejamento das contratações de soluções de software, a organização realiza estudos para identificar e mitigar o risco de dependência tecnológica, com vistas a viabilizar a substituição de fabricante/fornecedor quando tecnicamente viável e economicamente vantajoso?	"Sim, realizado no Estudo Técnico Preliminar na fase de planejamento da contratação."	Não informou onde há estudo técnico preliminar de contratação.
		k) a organização executa regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração)?	"Sim, realizado via CAIS/RNP"	Não disse qual a frequência dos testes de segurança de TI e nem quais os testes de segurança de TI são realizados.

Por último, no caso das respostas afirmativas ("sim") consideradas suficientes, que representaram 16% do total de respostas para esta categoria, estão serão colocadas em um anexo para não deixar este relatório tão extenso.

Manifestação da Unidade Auditada:

As respostas dadas pela Unidade Auditada (Seplan) foram tabeladas e classificadas pelas sua situação (suficiente ou insuficiente), como pode ser visto a seguir.

Subindicadores		Pergunta	Resposta do STI ao Relatório Preliminar	Situação
CAPACIDADE DE GERIR SERVIÇOS DE TI	A ORGANIZAÇÃO ELABORA UM CATÁLOGO DE SERVIÇOS DE TI?	a) o catálogo contém as metas definidas para cada serviço (p. ex. prazos de entrega, horários de serviço e de suporte, bem como pontos de contato para solicitação do serviço, envio de sugestões, esclarecimento de dúvidas e reporte de incidentes)?	O catálogo de serviços já foi avaliado na 30ª Reunião de Infraestrutura e Governança do STI, conforme ata disponível em: https://sei.ufcg.edu.br/sei/publicacoes/controlador_publicacoes.php?acao=publicacao_visualizar&id_documento=2629484&id_orgao_publicacao=0 Status: aguardando próxima reunião do CGD para apreciação e aprovação, a ser realizada em agosto de 2022.	Insuficiente
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE INCIDENTES DE SERVIÇOS DE TI?	c) bases de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes?	É realizado via acessos periódicos ao https://nvd.nist.gov/ e notificações do Centro de Atendimento a Incidentes de Segurança - CAIS/RNP	Suficiente

			(https://www.rnp.br/sistema-rnp/cais). O CAIS reporta incidentes para toda faixa de rede da instituição, porém o tratamento é dificultado pela descentralazição dos entes de TI (pessoal) da UFCG.	
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE MUDANÇAS?	a) a organização estabeleceu critérios para orientar a aprovação de mudanças, inclusive quanto ao tratamento de casos de exceção (mudanças emergenciais)?	Processo de Desenvolvimento disponível em https://sti.ufcg.edu.br/normas.html?download=50:processo-de-desenvolvimento	Insuficiente
		c) identificam-se os serviços e ativos de TI que possam ser afetados pela mudança, de modo a avaliar impactos em níveis de serviços acordados?	https://www.sti.ufcg.edu.br/normas.html?download=50:processo-de-desenvolvimento	Insuficiente
		d) a realização de cada mudança é precedida de planejamento e testes?	https://www.sti.ufcg.edu.br/normas.html?download=50:processo-de-desenvolvimento	Insuficiente

		e) mudanças executadas são rastreáveis e monitoradas, com vistas à avaliação de sua efetividade e para permitir ações corretivas, no caso de ocorrência de efeitos não identificados nas fases de planejamento e testes?	https://www.sti.ufcg.edu.br/normas.html?download=50:processo-de-desenvolvimento	Insuficiente
		f) lições aprendidas com as mudanças são compartilhadas, com vistas ao aprimoramento do processo (ex: Wiki)?	https://suporte.sti.ufcg.edu.br/osticket/kb/index.php	Suficiente
		g) o processo de gestão de mudanças está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	https://www.sti.ufcg.edu.br/normas.html?download=50:processo-de-desenvolvimento	Insuficiente

		h) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de mudanças e promove eventuais ajustes necessários?	https://www.sti.ufcg.edu.br/normas.html?download=50:processo-de-desenvolvimento	Insuficiente
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE CONFIGURAÇÃO E ATIVOS (DE SERVIÇOS DE TI)?	a) a organização mantém uma base de dados consolidada com as configurações dos serviços e ativos de TI e o relacionamento entre eles?	Por questões de segurança a base não é divulgada publicamente por conter dados sensíveis dos ativos de tic.	Suficiente
		c) a base de dados de configurações é mantida atualizada?	Fica armazenada em servidor local, não disponibilizado publicamente por questões de segurança	Suficiente
CAPACIDADE EM GERIR RISCOS DE TI	A ESTRUTURA DA GESTÃO DE RISCOS ESTÁ DEFINIDA?	a) há política institucional de gestão de riscos aprovada pelo conselho ou colegiado superior ou pela alta administração?	Não há Política de Gestão de Risco Institucional	Insuficiente
		b) foram definidas as instâncias responsáveis pelo sistema de gestão de riscos	Não há Política de Gestão de Risco Institucional	Insuficiente

		e respectivas competências (p. ex. alta administração, gestores operacionais, gestores de riscos, instância de supervisão da gestão de riscos, instância colegiada de assessoramento, outras funções de segunda linha , auditoria interna)?		
		c) foram definidas as diretrizes da integração do processo de gestão de riscos aos processos organizacionais ?	Não há Política de Gestão de Risco Institucional	Insuficiente
		d) foram definidos os critérios de análise e avaliação de riscos (orientações para determinação de níveis de	Não há Política de Gestão de Risco Institucional	Insuficiente

		risco, classificação e priorização dos riscos, e ainda para seleção das medidas de tratamento)?		
		e) foram definidos os fluxos de comunicação para compartilhar informações e decisões acerca de gestão de riscos?	Não há Política de Gestão de Risco Institucional	Insuficiente
		f) o processo de gestão de riscos está formalizado?	Não há Política de Gestão de Risco Institucional	Insuficiente
		g) limites para exposição ao risco estão definidos?	Não há Política de Gestão de Risco Institucional	Insuficiente
	O PROCESSO DE GESTÃO DE RISCOS DA ORGANIZAÇÃO ESTÁ IMPLANTADO?	a) objetivos e elementos (processos, produtos, atividades, ativos) críticos da organização estão identificados?	Não há Política de Gestão de Risco Institucional	Insuficiente
		b) há lista integrada de riscos, incluindo	Não há Política de Gestão de Risco Institucional	Insuficiente

			causas, fontes, efeitos?		
	O PROCESSO DE GESTÃO DE RISCOS DA ORGANIZAÇÃO ESTÁ IMPLANTADO?		d) o tratamento dos riscos está documentado?	Não há Política de Gestão de Risco Institucional	Insuficiente
			f) os riscos críticos identificados são informados aos membros das instâncias superiores de governança?	Não há Política de Gestão de Risco Institucional	Insuficiente
ÍNDICE DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO	CAPACIDADE EM DEFINIR POLÍTICAS DE RESPONSABILIDADE PARA GESTÃO DA TI	A ORGANIZAÇÃO DISPÕE DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO?	b) a política (ou norma interna complementar) contempla diretrizes sobre gestão de riscos de segurança da informação?	Há previsão para discussão na próxima reunião do CGD, a ser realizada em agosto de 2022.	Insuficiente
			e) a política é mantida atualizada, por meio de revisões periódicas?	Há previsão para discussão na próxima reunião do CGD, a ser realizada em agosto de 2022.	Insuficiente
	CAPACIDADE EM ESTABELECER PROCESSO E ATIVIDADES PARA GESTÃO DA TI	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO?	a) a organização identifica e avalia riscos de segurança da informação?	Há previsão para discussão na próxima reunião do CGD, a ser realizada em agosto de 2022.	Insuficiente

			b) a organização trata riscos de segurança da informação com base em um plano de tratamento de riscos?	Não há Política de Gestão de Risco Institucional	Insuficiente
			c) a organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação?	Não há Política de Gestão de Risco Institucional	Insuficiente
			d) o processo de gestão de riscos de segurança da informação está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	Não há Política de Gestão de Risco Institucional	Insuficiente

			e) a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de segurança da informação e promove eventuais ajustes necessários?	Não há Política de Gestão de Risco Institucional	Insuficiente
		A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE ATIVOS ASSOCIADOS À INFORMAÇÃO?	a) a organização mantém um inventário dos ativos associados à informação?	É mantido no sistema de Patrimônio SapWeb, disponível em: http://150.165.111.246:8080/Patrimonio, porém não é plucizado, o acesso aos relatórios é feito via processo SEI encaminhado ao setor do Patrimônio Geral.	Suficiente
			c) o inventário identifica as informações críticas que os ativos armazenam, processam ou transmitem?	É mantido no sistema de Patrimônio SapWeb, disponível em: http://150.165.111.246:8080/Patrimonio, porém não é plucizado, o acesso aos relatórios é feito via processo SEI encaminhado ao setor do Patrimônio Geral.	Insuficiente

		A ORGANIZAÇÃO EXECUTA PROCESSO PARA CLASSIFICAÇÃO E TRATAMENTO DE INFORMAÇÃO?	a) informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção?	Cabe ao Comitê Gestor do SEI definir os prazos. Ao STI compete a hospedagem e manutenção do sistema. No processo citado (23096.014700/2022-89) a PRGAF deu o prazo até 22 de julho, conforme documento SEI 2208947 do processo supra.	Suficiente
			b) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item "a" em conformidade com os requisitos legais e de negócio?	O PDA será apreciado e aprovado na próxima reunião do CGD (23096.044820/2022-19)	Insuficiente
			c) informações sigilosas em razão de sua imprescindibilidade à segurança da sociedade ou do Estado são identificadas e rotuladas, com	O PDA será apreciado e aprovado na próxima reunião do CGD (23096.044820/2022-19)	Suficiente

			vistas a viabilizar adequado tratamento e proteção?		
			d) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item "c" em conformidade com os requisitos legais e de negócio?	O PDA será apreciado e aprovado na próxima reunião do CGD (23096.044820/2022-19)	Insuficiente
			e) informações sigilosas em função de outras hipóteses legais de sigilo ou segredo são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção?	No SEI essa função está implementada.	Insuficiente
			g) informações críticas para a organização em razão de necessidades do negócio (p. ex. requisitos associados à integridade, disponibilidade,	O PDA será apreciado e aprovado na próxima reunião do CGD (23096.044820/2022-19)	Insuficiente

			autenticidade ou a outros atributos da informação) são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção?		
			h) a organização adota procedimentos para tratamento e proteção das informações identificadas na forma do item "g" em conformidade com os requisitos legais e de negócio?	O PDA será apreciado e aprovado na próxima reunião do CGD (23096.044820/2022-19)	Insuficiente
			j) a organização avalia periodicamente o desempenho e a conformidade do processo de classificação e tratamento de informações e promove eventuais ajustes necessários?	O PDA será apreciado e aprovado na próxima reunião do CGD (23096.044820/2022-19)	Insuficiente
		A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA	f) a organização adota procedimentos para tratamento e proteção das informações identificadas na	No SEI essa função está implementada.	Insuficiente

		DA INFORMAÇÃO?	forma do item "e" em conformidade com os requisitos legais e de negócio?		
			i) o processo de classificação e tratamento de informações está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	Cabe ao Comitê Gestor do SEI definir os prazos. Ao STI compete a hospedagem e manutenção do sistema. No processo citado (23096.014700/2022-89) a PRGAF deu o prazo até 22 de julho, conforme documento SEI 2208947 do processo supra.	Insuficiente
			b) a organização definiu procedimentos e responsabilidades quanto ao tratamento das notificações de incidentes de segurança da informação, adoção de ações emergenciais e diretrizes para escalamento e comunicação interna e externa?	Não.	Insuficiente

		A ORGANIZAÇÃO EXECUTA ATIVIDADES DE GESTÃO DA SEGURANÇA DOS RECURSOS DE PROCESSAMENTO DA INFORMAÇÃO, INCLUSIVE DOS RECURSOS DE COMPUTAÇÃO EM NUVEM?	c) a organização definiu procedimentos e responsabilidades quanto à análise de incidentes de segurança da informação, identificação de causas raízes e planejamento e implementação de ações corretivas?	É realizado via acessos periódicos ao https://nvd.nist.gov/ e notificações do Centro de Atendimento a Incidentes de Segurança - CAIS/RNP (https://www.rnp.br/sistema-rnp/cais). O CAIS reporta incidentes para toda faixa de rede da instituição, porém o tratamento é dificultado pela descentralização dos entes de TI (pessoal) da UFCG. Não há previsão para o gerenciamento ser realizado no âmbito de toda UFCG, pois depende de orçamento para aquisição de infraestrutura, capacitação e contratação de servidores com perfil de segurança da informação.	Insuficiente
			d) a organização instituiu equipe de tratamento e resposta a	É realizado pela equipe de infraestrutura do STI, porém por falta de servidores	Insuficiente

			incidentes em redes computacionais (ETIR) ou estrutura equivalente?	na área para serem dedicados a esta atribuição.	
			a) a organização gerencia (inventaria e controla) os dispositivos conectados em sua rede?	Os ativos de TIC (rede e servidores) são mantidos em http://webmngr.ufcg.edu.br/cpv/!STI.html , monitor.sti.ufcg.edu.br e planilha interna que por questões de segurança não é divulgada publicamente. Não há previsão para o gerenciamento ser realizado no âmbito de toda UFCG, pois depende de orçamento para aquisição de infraestrutura, capacitação e contratação de servidores com perfil de segurança da informação, além das equipes de TIC da instituição serem descentralizadas não subordinadas ao STI.	Insuficiente
			c) a organização gerencia vulnerabilidades técnicas em seus ativos de software, de	É realizado via acessos periódicos ao https://nvd.nist.gov/ e notificações do Centro de Atendimento a Incidentes de Segurança -	Insuficiente

			hardware e de rede críticos para o negócio?	CAIS/RNP (https://www.rnp.br/sistema-rnp/cais). O CAIS reporta incidentes para toda faixa de rede da instituição, porém o tratamento é dificultado pela descentralazição dos entes de TI (pessoal) da UFCG. Não há previsão para o gerenciamento ser realizado no âmbito de toda UFCG, pois depende de orçamento para aquisição de infraestrutura, capacitação e contratação de servidores com perfil de segurança da informação.	
			d) a organização implementa configurações seguras em seus ativos de software, de hardware e de rede críticos para o negócio?	É feito um hardening do ativos e serviços, aplicação de regras de firewall/ACL e controle de acesso para permitir acesso administrativo apenas a partir da faixa de rede do STI.	Suficiente
			e) a organização mantém, monitora e analisa logs de auditoria dos ativos de software, de	O monitoramento prévio não é realizado. Já a análise de logs de auditoria dos ativos críticos de ti do STI é realizada conforme o tipo de	Insuficiente

			hardware e de rede críticos para o negócio?	ativo e natureza da informação, sendo feita por meio de inspeção manual de logs. Ressalta-se que não há análise proativa de logs de auditoria.	
			f) A organização aplica controles compensatórios para o uso de privilégios administrativos em seus ativos de software, de hardware e de rede críticos para o negócio?	É feito através da restrição de acesso administrativo apenas a partir de algumas faixas de rede para estes fins, a exemplo da rede do STI e da rede de gerência da UFCGnet, bem como o bloqueio de acesso externo à rede da UFCG. As credenciais administrativas no âmbito do STI são compartilhadas apenas entre servidores efetivos do quadro do setor, mediante autorização da gerência do STI.	Suficiente
			g) a organização implementa defesas contra malware (ex: vírus) e outras ameaças cibernéticas (ex: phishing)?	Há interesse por parte do STI em adotar tecnologias e soluções corporativas de segurança da informação. Entretanto, depende de investimentos e contratações de TIC para estes fins.	Insuficiente

			h) a organização limita e controla o uso de portas, protocolos e serviços de rede nas conexões de sua rede interna com a internet e outras redes externas?	Há interesse por parte do STI em adotar tecnologias e soluções corporativas de segurança da informação. Entretanto, depende de investimentos e contratações de TIC para estes fins.	Insuficiente
			i) a organização implementa defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas?	Há interesse por parte do STI em adotar tecnologias e soluções corporativas de segurança da informação. Entretanto, depende de investimentos e contratações de TIC para estes fins.	Insuficiente
			j) a organização implementa cópias regulares de segurança (backup) das informações em meio digital, conforme as melhores práticas e as necessidades de	Devido a falta de infraestruta corporativa de TIC para estes fins o backup é realizado do tipo "melhor esforço" que consiste na utlização de ferramentas open source e ou gratuitas a exemplo do rsync,	Suficiente

			negócio, incluindo a realização periódica de testes de recuperação das informações?	mysqldump, ghettovcb e scripts próprios. A frequencia de backup, por padrão, é diária. Entretanto, devido a nossa limitação de infraestrutura de TIC, alguns backups são feitos a cada 3 dias ou uma vez por semana, ou uma vez por mês. Eles são mantidos em um servidor configurado com FREENAS, nas depedências do STI. Não há frequência pré-definia de recuperação, sendo realizada sob demanda. Ressalta-se que a capacidade computacional dos nossos servidores está próxima do limite, não sendo possível realizar testes de restores.	

	O PROCESSO DE SOFTWARE (DA ORGANIZAÇÃO PROMOVE A IDENTIFICAÇÃO PRECOCE DE REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E A GESTÃO PERMANENTE DESSES REQUISITOS DURANTE TODO O CICLO DE VIDA DO SOFTWARE)?	b) a organização avalia as soluções existentes no mercado antes de decidir pelo desenvolvimento de software (análise do tipo "construir ou adquirir")?	Por meio de pesquisa no site do Software Público Brasileiro, https://www.gov.br/governodigital/pt-br/software-publico, bem como nos sites de outras instituições federais de ensino.	Suficiente
		c) na etapa de planejamento das contratações de soluções de software, a organização realiza estudos para identificar e mitigar o risco de dependência tecnológica, com vistas a viabilizar a substituição de fabricante/fornecedor quando tecnicamente viável e economicamente vantajoso?	Não. O Estudo é realizado pela equipe de contratação na fase de planejamento da contratação	Suficiente
		k) a organização executa regularmente	A frequência da realização dos testes é desconhecida, bem	Insuficiente

		testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração)?	como os tipos de testes.	

Análise da Auditoria:

Com relação aos subindicadores do ProcessosTI, algumas respostas positivas consideradas insuficientes ainda permaneceram nesta situação e foram transformadas em recomendações, descritas a seguir.

Recomendação 4: Comprovar a aprovação do Catálogo de Serviços de TIC para verificar se este tem metas definidas.

Recomendação 5: Formalizar as Políticas de Gestão de Riscos de TI e de Segurança da Informação para, com base nestas, definir os procedimentos da Estrutura da Gestão de Riscos de TI, implantar o Processo de Gestão de Riscos de TI e executar processo de Gestão de Riscos de Segurança da Informação.

Recomendação 6: Implantar a gestão de incidentes de segurança da informação definindo procedimentos e responsabilidades quanto ao tratamento das notificações e análise de incidentes de segurança da informação, identificação de causas raízes, planejamento e implementação de ações corretivas, adoção de ações emergenciais e diretrizes para escalamento e comunicação.

Recomendação 7: Criar uma rotina de revisão e atualização das políticas institucionais de TI.

Recomendação 8: O inventário de ativos de software, hardware e rede de TI associados à informação e / ou conectados na rede de toda a UFCG, e não apenas do STI, precisa identificar as informações críticas armazenadas, processadas ou transmitidas e proporcionar à Coordenação de Controle Interno – CCI/UFCG gerenciamento de vulnerabilidades técnicas dos ativos críticos. Desta forma, o referido controle poderia ir além da demonstração de desempenho, mostrando também detalhes como a identificação do equipamento (com descrição e patrimônio) e de seu responsável. Uma possibilidade para a concretização deste inventário seria a utilização de um servidor DHCP, que poderia conceder automaticamente endereços IP a todos os computadores, impressoras e dispositivos conectados à rede ou internet.

Recomendação 9: Formalizar o processo de classificação, tratamento e proteção de informações (pessoais, sigilosos e críticas) e avaliar o desempenho e a conformidade do mesmo periodicamente.

Recomendação 10: Instituir equipe de tratamento e resposta a incidentes na rede ou estrutura equivalente.

Recomendação 11: Implantar e formalizar protocolos de gestão de mudanças, além do desenvolvimento de software, e avaliar periodicamente o desempenho e a conformidade deste para permitir ações corretivas.

Recomendação 12: Implantar protocolos de teste de segurança de ambiente de TI, como a detecção de vulnerabilidade e teste de penetração a partir do uso de software.

Recomendação 13: Implantar protocolos para o monitoramento prévio e proativo dos logs de auditoria dos ativos críticos de software, hardware e rede.

Recomendação 14: Limitar e controlar o uso de portas, protocolos e serviços de rede nas conexões da rede interna com a internet e outras redes externas com medidas como os firewall de borda e a solução de wi-fi corporativo (Air Defense). Sendo o primeiro um controle de tráfego ou filtro de dados indesejados entre redes - interna e externa (como blogs, redes sociais, aplicativos de mensagens instantâneas) capaz de prevenir ataques por vírus e outras ameaças cibernéticas. Enquanto que o segundo é para o controle de acessos de dispositivos móveis, como está sendo feito na Reitoria.

Recomendação 15: Implantar defesa de perímetro das conexões da rede interna com a internet e outras redes externas, também com a utilização do firewall de borda para proteger a rede da UFCG de ameaças externas.

Recomendação 16: Implantar defesas contra malware e outras ameaças cibernéticas, com ações além do firewall de borda, como a utilização de antivírus institucional.

Recomendação 17: Implantar back-up (cópia de segurança) das informações em meio digital de forma mais compatível com as melhores práticas, com a definição da estratégia de redundância, com maior frequência e a utilização do Data Center que foi recentemente licitado.

Recomendação 18: Implantar redundâncias no backbone da rede para proporcionar maior segurança e estabilidade à rede interna. (considerando a importância do tema e / ou a sua interrelação com as outras recomendações, fizemos esta recomendação adicional).

CONCLUSÃO:

Concluídos os exames de auditoria, identificou-se que a Seplan está se esforçando para melhorar a gestão de TI na UFCG, apesar do atual "score" da referida instituição neste quesito no IGG de 2021. Entretanto, entende-se que muitos itens aqui avaliados são alheios ao controle da Seplan, com exceção daqueles associados à formalização ou normatização, pois estão atrelados à necessidade de maiores investimentos em infraestrutura (backbone da rede, computadores, servidores, hubs, roteadores e comutadores) e pessoal (analistas de segurança da informação, administradores e técnicos administrativos) de TI.

Assim, como as recomendações exaradas por esta Unidade de Auditoria Interna Governamental serão objeto de monitoramento (ou acompanhamento)
posterior, as questões aqui apontadas poderão ser revisitadas com o objetivo de verificar a sua implementação.

Por fim, enfatiza-se que este relatório não tem a intenção de esgotar as possibilidades de melhoria da gestão de TI na UFCG passíveis de implementação, mas sim de servir como orientação para a observância dos aspectos legais, normativos e técnicos para a adequada utilização dos recursos públicos na gestão da Tecnologia da Informação desta IFES. Assim, como consequência, espera-se um aumento da eficiência da UFCG no uso dos seus recursos de TI, reforçando mais uma vez a credibilidade desta IFES perante a sociedade civil.

Técnicos Responsáveis pelo Relatório:

Coordenador: Marcelo Moura Nóbrega
Equipe de apoio: Gustavo Barbosa de Carvalho Almeida
Equipe de apoio: Ibrahim Madruga Cavalcanti

Coordenador de Controle Interno Substituto: Telmo da Rocha Petrucci

Campina Grande - PB, 09 de setembro de 2022

V. ANEXO (RESPOSTAS AFIRMATIVAS CONSIDERADAS SUFICIENTES)

Subindicadores			Pergunta	Resposta do STI 2022
CAPACIDADE DE GERIR SERVIÇOS DE TI	A ORGANIZAÇÃO ELABORA UM CATÁLOGO DE SERVIÇOS DE TI?		c) o catálogo é de fácil acesso e está amplamente disponível a seus usuários e às equipes de suporte?	"Sim, pois pode ser encontrado na página principal do STI. Link: https://sti.ufcg.edu.br/catalogo-de-servicos.html".
	A ORGANIZAÇÃO EXECUTA PROCESSO DE GESTÃO DE MUDANÇAS?		b) mudanças são previamente comunicadas a todas as partes que possam ser afetadas?	"Sim. Mudanças nos sistemas que o STI realiza suporte são comunicadas no site do STI e por e-mail, como também as manutenções de infraestrutura".
CAPACIDADE EM GERIR RISCOS DE TI	O PROCESSO DE GESTÃO DE RISCOS DA ORGANIZAÇÃO ESTÁ IMPLANTADO?		c) os riscos constantes da lista integrada foram analisados e avaliados?	"Sim, pelo fato de ter sido definida com base na probabilidade da ocorrência e do impacto (alto, médio ou baixo)".
			e) os responsáveis pelo tratamento dos riscos participam do processo de escolha das respostas aos riscos	"Devem participar, quando o Plano de Gestão de Risco for elaborado".
	ATIVIDADES TÍPICAS DE SEGUNDA LINHA ESTÃO ESTABELECIDOS?		f) as atividades da segunda linha de defesa incluem o apoio às atividades de auditoria interna (3ª linha de defesa), no acompanhamento e auxílio da interlocução com as áreas auditadas?	"Sim".
ÍNDICE DE GESTÃO DA SEGURANÇA DA INFORMAÇÃO	CAPACIDADE EM DEFINIR POLÍTICAS DE RESPONSABILIDADE PARA GESTÃO DA TI	A ORGANIZAÇÃO DISPÕE DE UMA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO?	a) a política declara o comprometimento da alta administração e estabelece princípios, diretrizes, objetivos, estruturas e responsabilidades relativos à segurança da informação?	"Sim. POSIC publicada em: (link: https://sti.ufcg.edu.br/normas.html)".
			c) a política abrange diretrizes para conscientização, treinamento e educação em segurança da informação?	"Sim".
			d) a política é amplamente comunicada a empregados, servidores, colaboradores e partes externas relevantes?	"Incluído no Portal da UFCG, na seção Documentos, pasta: Governança de TIC".
	O PROCESSO DE SOFTWARE (DA ORGANIZAÇÃO PROMOVE A IDENTIFICAÇÃO PRECOCE DE		a) a organização possui pessoal próprio capacitado para gerir o processo de software?	"Sim. Há metodologia de desenvolvimento de software".

	REQUISITOS DE SEGURANÇA DA INFORMAÇÃO E A GESTÃO PERMANENTE DESSES REQUISITOS DURANTE TODO O CICLO DE VIDA DO SOFTWARE)?	d) a organização utiliza prioritariamente arquiteturas de software que promovem o desacoplamento de soluções, sistemas e componentes, inclusive nos casos de software adquirido e desenvolvimento realizado mediante contratação, com vistas a facilitar a realização de manutenções e otimizar custos?	"Sim".
		e) o processo de software utilizado pela organização promove a participação de representante da área de negócio como integrante da equipe de desenvolvimento ou aquisição de software, desde sua concepção até a aceitação final?	"Sim, definido no processo de desenvolvimento de software do STI".
		g) o processo de software da organização promove a identificação precoce de requisitos de interoperabilidade e a gestão permanente desses requisitos durante todo o ciclo de vida do software?	"Sim".
		h) o processo de software da organização promove a identificação precoce de requisitos de acessibilidade e de usabilidade, bem como a gestão permanente desses requisitos durante todo o ciclo de vida do software?	"Parcialmente, no processo de desenvolvimento, somente a usabilidade é gerida durante o ciclo de vida do software."
		i) a organização assegura os seus direitos autorais, de propriedade e de uso relativamente ao software que desenvolve por meio de contratação?	"Não participamos de contratação de desenvolvimento de software".
		j) organização avalia, por meio de mensurações, indicadores e metas, a qualidade do software desenvolvido ou adquirido?	"Parcialmente, os planos de testes são contemplados dentro da metodologia de desenvolvimento de software."
		k) o processo de software está formalizado (a organização instituiu norma interna, guia ou instrumento similar com orientações quanto à execução do processo e definição de responsabilidades)?	"Sim, a metologia de desenvolvimento de software do STI foi criada e implantada em 2010, formalizada internamente".
		l) a organização avalia periodicamente o desempenho e a conformidade do processo de software e promove eventuais ajustes necessários?	"Sim".