Universidade Federal do Espírito Santo
Auditoria Interna

RELATÓRIO DE AVALIAÇÃO 2023005

Superintendência de Tecnologia da Informação - STI

2023

26 de dezembro de 2024

Universidade Federal do Espírito Santo (Ufes)
Auditoria Interna (Audin)

RELATÓRIO DE AVALIAÇÃO 2023005
Órgão: **Universidade Federal do Espírito Santo**
Unidade Auditada: **STI**
Município/UF: **Vitória/ES**
Relatório de Avaliação: **Ação nº 14 do Paint 2023**

Missão

Assessorar e fortalecer a gestão no desempenho das suas funções e responsabilidades, avaliando e aprimorando a governança pública (controles internos e gestão de riscos).

Avaliação

O trabalho de avaliação, como parte da atividade de auditoria interna, consiste na obtenção e na análise de evidências com o objetivo de fornecer opiniões ou conclusões independentes sobre um objeto de auditoria. Objetiva também avaliar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos relativos ao objeto e à Unidade Auditada, e contribuir para o seu aprimoramento.

QUAL FOI O TRABALHO REALIZADO PELA AUDIN?

Avaliação da regularidade da gestão da tecnologia da informação, visando garantir o planejamento estratégico alinhado ao Plano de Desenvolvimento Institucional (PDI) e a LDO/LOA 2023.9.2

Verificação da estrutura de governança, controles internos e risco organizacional.

POR QUE A AUDIN REALIZOU ESSE TRABALHO?

O trabalho realizado está previsto no Plano Anual da Auditoria Interna (Paint 2023), ação nº 14, decorrente do processo de seleção baseado na avaliação de riscos.

QUAIS AS CONCLUSÕES ALCANÇADAS PELA AUDIN? QUAIS AS RECOMENDAÇÕES DEVERÃO SER ADOTADAS?

Por meio dos testes de auditoria para a avaliação das questões que compuseram o escopo de trabalho, foi possível constatar que a unidade possui razoáveis controles das atividades de suporte ao usuário e de acompanhamento das ações do PDTIC. Contudo, necessita de melhorias no que tange à indicadores das atividades, mapeamento dos riscos e processos, monitoramento das ações do PDTIC e atendimento das metas do PDI. Há também a necessidade de melhoria de recursos humanos para suprir as demandas crescentes. As recomendações, detalhadas em tópico específico do presente Relatório de Auditoria, buscaram propor aos gestores maior formalização dos processos de trabalho, correção de impropriedades constatadas e melhorias nos controles internos e na governança.

LISTA DE SIGLAS E ABREVIATURAS

Audin - Auditoria Interna

Conama – Conselho Nacional de Meio Ambiente

CGU - Controladoria Geral da União

DMP - Diretoria de Materiais e Patrimônio

IGovTI - Índice de governança e gestão de TI

Ibama - Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis

IN - Instrução Normativa

LDO - Lei de Diretrizes Orçamentárias

LOA - Lei Orçamentária Anual

OS - Ordem de Serviço

OEG - Objetivos Estratégicos da Gestão

Paint - Plano Anual de Atividades de Auditoria Interna

PDI - Plano de Desenvolvimento Institucional

PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação

Posati - Política de Sustentabilidade ambiental em Tecnologia da Informação

Posin - Política de Segurança de Informação

Proad – Pró-Reitoria de Administração

SA - Solicitação de Auditoria

STI - Superintendência de Tecnologia da Informação

TCU - Tribunal de Contas da União

TI – Tecnologia da Informação

UAG - Unidade de Auditoria Governamental

Ufes - Universidade Federal do Espírito Santo

SUMÁRIO

INTRODUÇÃO

A Unidade de Auditoria Governamental (UAIG), Auditoria Interna (Audin) da Universidade Federal do Espírito Santo (Ufes), cumprindo as atribuições estabelecidas no Decreto nº 3.591 de 06.09.2000, alterado pelo Decreto nº 4.304, de 16.07.2002, e em observância ao Plano Anual de Atividades de Auditoria Interna (Paint) para o exercício de 2023, aprovado pela Resolução CUN/UFES/Nº 34/2022, pelo Conselho Universitário, em 22 de dezembro de 2022, e em atendimento à Ordem de Serviço (OS) nº 05/2023, realizou o presente trabalho com o objetivo de avaliar a regularidade da gestão da tecnologia da informação, visando garantir o planejamento estratégico alinhado ao Plano de Desenvolvimento Institucional (PDI) e a LDO/LOA 2023.9.2. Junto a isso, também verificou a estrutura de governança, controles internos e risco organizacional.

Os trabalhos realizados decorreram da ação nº 14 prevista no Paint 2023 da Audin que, por sua vez, foram resultado da avaliação baseada em risco dos macroprocessos da Universidade.

As ações de auditoria estão alinhadas com os objetivos e metas constantes no PDI 2021-2030 da Ufes, aprovado pela Resolução nº 5/2021-CUn. Contribui especialmente para os Objetivos Estratégicos da Gestão (OEG) de fortalecer mecanismos de governança (OEG1) e de assegurar uma gestão ética, democrática, transparente, participativa e efetiva (OEG2).

Dessa forma, foram propostas as seguintes questões que nortearam a avaliação da auditoria:

Quadro 01 - Questões de Auditoria

Questão	Subquestão
Q2. As manutenções nos equipamentos de TI da universidade são realizadas de forma satisfatória?	SQ 2.1 Há cronograma de manutenção preventiva de equipamentos de TI?
	SQ 2.2 O suporte ao usuário atende/suporta as demandas da universidade?
	SQ 2.3 A unidade realiza gestão de risco de vazamento de dados/informações?
Q3. Há planejamento de recursos humanos com dimensionamento da força de trabalho necessária?	SQ 3.1 A unidade faz gestão de recursos humanos com dimensionamento da força de trabalho necessária para atender satisfatoriamente às demandas?
Q4. Como é realizado o descarte de equipamentos de TI?	SQ 4.1 O descarte de equipamentos é realizado conforme recomenda o POSATI?
Q5. A implementação da governança digital está ocorrendo de forma satisfatória e dentro do planejado?	SQ 5.1 O planejamento da implementação da governança digital está sendo atendido?
Q6. Há ações em curso com o objetivo de atingir a faixa intermediária do IGovTI e elas são satisfatórias?	SQ 6.1 Foram planejadas e estão sendo executadas ações para atingimento da meta do PDI?

Fonte: Elaboração própria

As metodologias de trabalho compreenderam as técnicas de indagação escrita e exame documental.

O escopo da auditoria abrangeu os controles gerenciais, os mecanismos de monitoramento das atividades, a aderência das atividades ao atendimento das metas constantes no PDI relacionadas à tecnologia da informação e a governança.

Nenhuma restrição foi imposta à realização dos exames, mas houve alguma morosidade na obtenção de respostas às Solicitações de Auditoria devido à implementação do novo Data Center da Ufes e férias de servidores.

Realizadas as análises, foram expedidas solicitações de auditoria para as unidades a fim de que estas tomassem ciência dos pontos verificados e apresentassem as justificativas. Os trabalhos foram realizados em estrita observância às normas de auditoria aplicáveis ao Serviço Público Federal.

RESULTADOS DOS EXAMES

1. Fragilidades nos controles gerenciais de suporte ao usuário

Por meio da subquestão de auditoria SQ.2.2, buscou-se analisar se há controle e gerenciamento dos atendimentos aos usuários dos serviços de TI, a fim de buscar entender as demandas e melhorar o atendimento e tempo de resposta.

Verificou-se que a unidade possui um sistema de *helpdesk, o Osticket*, (www.atendimento.ufes.br) onde são registradas as solicitações de suporte. Conta com 3 servidores e 2 estagiários para realizar os atendimentos. Os chamados são atendidos considerando os critérios de impacto, complexidade e ordem de abertura.

A unidade possui um painel de acompanhamento dos atendimentos aos usuários, conforme figura 01.

Figura 01 - Painel de acompanhamento do atendimento ao usuário do STI

O painel permite a categorização e melhor visualização dos chamados atendidos pelo STI, proporcionando informações para gerenciamento. Entretanto, é possível observar inconsistências no controle de classificação das informações, em que há uma atribuição de classificação “em branco” (destacado de vermelho na figura 1) na classificação de “Chamados por Tópico”, onde 1.769 chamados não foram atribuídos a uma categoria.

Em resposta à Solicitação de Auditoria nº 67/2023 a unidade informou que “os chamados com tópico “em branco” são originados por meio de solicitação por *e-mail*, impossibilitando a catalogação do tópico de serviço (setor destinado à solução do problema)”

Contudo, um controle onde quase metade (42,56%) dos chamados abertos não podem ser classificados distorce o entendimento dos tópicos de fato mais demandados e prejudica um

possível planejamento de alocação de recursos (material e humano) em tópicos mais demandados, assim como o planejamento de ações para tratar as demandas mais críticas.

Para melhor controle, confiabilidade e transparência das informações, é necessária a adoção de mecanismo que permita a classificação de todos os chamados, como a possibilidade de classificação do chamado pelo requisitante quando de sua abertura ou a categorização do chamado pelo atendente já no momento inicial.

Ainda, não são utilizados indicadores de gerenciamento, tais como indicadores dos atendimentos realizados aos usuários, por exemplo: tempo de atendimento do chamado, tempo de resposta e índice de resolução no primeiro chamado *(First Call, Resolution).*

O Referencial[1] básico de governança aplicável às organizações públicas e outros entes jurisdicionados ao TCU assinala como mecanismo de estratégia a prática de monitoramento do desempenho das funções de gestão para "proporcionar a tomada de decisão com base em evidências, corrigindo desvios, identificando oportunidades de melhoria e casos de sucesso e promovendo o aprendizado". Para tanto, elucida que implica em: "a) estabelecimento das rotinas para o levantamento das informações necessárias ao monitoramento; b) implantação dos indicadores de desempenho [...]"

Portanto, para melhorar a governança do suporte ao usuário, promovendo informações mais fidedignas e indicadores para o monitoramento e tomada de decisões, é importante a categorização correta de todos os atendimentos realizados, bem como a instituição de indicadores de desempenho.

2. Mapeamento de riscos incompleto e ausência de mapeamento dos processos

Conforme a subquestão de auditoria SQ. 2.3, foi verificado se a unidade realiza gestão de riscos, em especial de vazamento de dados/informações, elaborando o mapeamento dos processos e de riscos da unidade.

A universidade possui uma Política de Segurança de Informação, POSIN 2022-2024[2], aprovada pelo Comitê de Governança Digital (CGD), que tem o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da Segurança da Informação, além de normas complementares[3] estabelecidas por Instruções Normativas específicas.

O STI possui sistemas de gerenciamento da rede e acessos, bem como *Firewall.* A rede e os sistemas da Ufes são acessados por meio de login e senha únicos (ou gov.br) a fim de garantir confidencialidade, considerando o princípio da segurança da informação, o qual assegura que somente indivíduos autorizados pelo proprietário da informação tenham

[1] Referencial básico de governança aplicável a organizações públicas e outros entes jurisdicionados ao TCU. Disponível em https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881F7AB5B041017BABE767F6467E

[2] POSIN 2022-2024. disponível em https://sti.ufes.br/politicas-e-diretrizes

[3] Normas complementares à Política de Segurança da Informação (POSIN) e aprovadas pelo CGD da Ufes. Disponível em https://sti.ufes.br/instrucoes-normativas.

acesso a ela, bem como a autenticidade, princípio que assegura a veracidade do autor da informação.

Entretanto, o STI não possui os principais processos mapeados e o mapeamento de riscos apresentado está incompleto. Foi apresentado como processo mapeado apenas um procedimento[4] geral disponível na página do gov.br para contratações de bens e serviços de tecnologia da informação e comunicação. A unidade também apresentou uma planilha de gestão de riscos onde consta uma relação de macroprocessos/processos como: Tratamento da Informação, Segurança Física e do Ambiente, Gestão de Incidentes em Segurança da Informação, Gestão de Ativos, Controle de Acesso Lógico, Cópias de Segurança *(Backup)*, dentre outros, mas não apresentou o mapeamento deles.

Ainda no mapeamento de riscos, na planilha apresentada há eventos de riscos em que não constam como avaliados os Efeitos / Consequências (coluna D), não foram identificados os Controles Existentes (colunas F, G e H) e nem como será implementada a resposta ao risco.

A Política de Gestão de Integridade, Riscos e Controles Internos da Gestão da Ufes, instituída pela Portaria nº 1072 de 11 de maio de 2017, dentre outros objetivos, busca suportar a missão, a continuidade e a sustentabilidade institucional, pela garantia razoável de atingimento dos objetivos estratégicos, e proporcionar a eficiência, a eficácia e a efetividade institucional, mediante uma execução ordenada, ética e econômica dos processos de trabalho.

O mapeamento dos macroprocessos, por sua vez, busca agregar valor às atividades fins da Ufes, desenvolvendo para isso as atividades suporte, a exemplo do gerenciamento da governança e infraestrutura. A formalização do mapeamento dos processos e dos riscos das atividades executadas pela unidade proporciona a padronização do processo e a mitigação dos riscos, bem como uma resposta rápida em caso de sua ocorrência. Também auxilia os servidores que ingressam no setor a entenderem os processos e os riscos inerentes às atividades que serão por eles desenvolvidas.

3. Recursos humanos insuficientes para as atividades da unidade

A subquestão de auditoria SQ.3.1 teve por objetivo verificar se a unidade faz gestão de recurso humanos, possuindo um dimensionamento da força de trabalho necessária para atender satisfatoriamente às demandas.

A unidade não possuiu o dimensionamento da força de trabalho, mas, em resposta à Solicitação de Auditoria nº 67/2023, informou que pretende elaborar um estudo adequado do número de profissionais de TIC para a STI e os Centros de Ensino para dimensionamento da força de trabalho junto a Gestão da Ufes. Informou, ainda, que não foi possível fazer devido à priorização de outras atividades.

A Lei nº 14.129/2021, chamada de lei do governo digital, busca promover a digitalização da Administração Pública e a prestação digital de serviços públicos. Expõe princípios e diretrizes a serem observados pelas entidades públicas, dentre eles:

[4] Contratações de Bens e Serviços de Tecnologia da Informação e Comunicação. Disponível em https://sti.ufes.br/contratacoes

- A desburocratização, a modernização, o fortalecimento e a simplificação da relação do poder público com a sociedade, mediante serviços digitais, acessíveis;
- A disponibilização em plataforma única do acesso às informações e aos serviços públicos;
- A interoperabilidade de sistemas e a promoção de dados abertos;
- A possibilidade aos cidadãos, às pessoas jurídicas e aos outros entes públicos de demandar e de acessar serviços públicos por meio digital, sem necessidade de solicitação presencial.

A referida Lei também aborda que "A administração pública utilizará soluções digitais para a gestão de suas políticas finalísticas e administrativas e para o trâmite de processos administrativos eletrônicos." (Art. 5º)

Nesse sentido, existe uma demanda crescente por serviços e recursos de tecnologia da informação para tornar digital a gestão das políticas da universidade e os serviços prestados à sociedade, além da transparência por meio digital. Portanto, há a necessidade de aprimorar a capacidade de atendimento por parte do setor de TI, tanto de recursos humanos quanto de infraestrutura.

Diante dessa realidade é imperioso dimensionar a força de trabalho para fazer frente a esse desafio, a fim de suprir as necessidades de recursos humanos do STI, observando a qualificação necessária para atender às demandas existentes.

4. Desatualização e inconsistência na Política de Sustentabilidade Ambiental em Tecnologia de Informação.

Com a subquestão SQ. 4.1 o objetivo foi verificar se o descarte de equipamentos é realizado seguindo a Política de Sustentabilidade Ambiental em Tecnologia da Informação – POSATI.

Conforme manifestado pela unidade na SA nª 68/2023, a responsabilidade do descarte dos equipamentos é da Diretoria de Materiais e Patrimônio - DMP. O STI envia os equipamentos à DMP utilizando o sistema de patrimônio e este efetua o descarte, sendo imprescindível seguir com as recomendações de descarte presentes na Política de Sustentabilidade. O STI apenas disponibiliza a Política de Sustentabilidade Ambiental em Tecnologia da Informação e Comunicação (POSATI), a qual contém regulamentos e práticas que são implementadas pelas organizações com o intuito de gerir o impacto humano no meio ambiente.

O POSATI[5] explicita a Política de Sustentabilidade Ambiental para a área de Tecnologia da Informação e Comunicação e estabelece critérios a serem usados nos processos de contratações. Entretanto, verificamos inconsistência acerca do descarte de equipamentos e produtos eletrônicos, que é abordado no item 5.5 daquele documento.

Na referida Política de Sustentabilidade Ambiental, há a previsão de que "no caso de computadores e outros equipamentos que armazenam informações devem ser seguidos os procedimentos recomendados no item 5.3 (Descarte de mídias)". Contudo, o item 5.3 aborda critérios de aquisições de equipamentos e não de descarte de mídias, havendo uma

[5] Política de Sustentabilidade Ambiental em Tecnologia da Informação e Comunicação, disponível em https://npd.ufes.br/sites/npd.ufes.br/files/Politica_Sustentabilidade_Ambiental.pdf, acesso em 29.04.2024.

incoerência entre os itens. Além disso, os procedimentos de descarte de mídias não foram identificados em nenhum outro tópico do citado documento.

Soma-se a isso, o fato de a POSATI ter sido elaborada e aprovada no ano de 2011, não sendo verificada nenhuma atualização posterior. Fato corroborado pela legislação de referência citada no item 3 do documento, onde constam legislações já revogadas como: IN IBAMA nº 03/2010 (revogada pela IN IBAMA nº 08/2012), Decreto nº 4.059 (revogado pelo Decreto 9.864/2019), Decreto 7.404 (Revogado pelo Decreto nº 10.936/2022), e mais recentemente a Lei 8.666/93 (revogada em 2024). Tendo ocorrido, ainda, no ano de 2013, a revisão da Resolução CONAMA nº 340/2003.

Assim, é necessário reavaliar a POSATI para sanar as inconsistências e atualizá-la em conformidade com a legislação vigente, criando uma sistemática de atualização periódica a fim de acompanhar as mudanças nos normativos regulamentadores.

5. Inconsistências no gerenciamento de ações do Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC

A subquestão de auditoria 5.1 buscou verificar as ações e seu monitoramento, a fim de atender o Plano Diretor de Tecnologia da Informação e Comunicação – PDTIC e, consequentemente, a implementação da governança digital.

A unidade possui um painel[6] de acompanhamento das ações do Plano Diretor de Tecnologia da Informação e Comunicação - PDTIC onde constam o andamento das ações e o atendimento das metas.

Constatamos que no painel de monitoramento de ações há informações desatualizadas e incompletas, por exemplo, ações com datas de início e de conclusão em atraso, conclusão com datas futuras e ações sem data de conclusão.

Figura 02 – Quantitativo de ações e progressão de conclusão das metas

Fonte: Monitoramento das ações planejadas - PDTIC 2022 a 2025 (STI)

Conforme figura 02, até a emissão deste relatório foram concluídos 17,05% das metas propostas para o ano de 2022 a 2025. O painel apresenta um total de 316 ações, mas somando as quantidades de ações apresentadas nos anos, totalizam 86.

[6] Monitoramento das ações planejadas - PDTIC 2022 a 2025. Disponível em https://lookerstudio.google.com/u/0/reporting/7edb3013-73c2-4c91-98f8-bcc728161fea/page/hieoC, acesso em 29.04.2024.

Considerando os anos de 2022 e 2023, que já se encerraram, foram concluídas apenas metade das metas (52,53%) previstas para serem concluídas nesses anos, conforme figura 03.

Figura 03 – Progresso de conclusão das metas dos anos 2022 e 2023

Fonte: Monitoramento das ações planejadas - PDTIC 2022 a 2025 (STI)

Na figura 04 verifica-se que 39,7% das ações previstas para 2022 e 2023 foram concluídas no prazo e 15,1% estão com a conclusão em atraso, tendo vencido o prazo para conclusão, 26% ainda estão em andamento, 9,6% estão com o início em atraso, ou seja, era para terem sido iniciadas em 2022 ou 2023 e outros 9,6% foram concluídas em atraso.

Figura 04 - Situação das ações dos anos de 2022 e 2023

Fonte: Monitoramento das ações planejadas - PDTIC 2022 a 2025 (STI)

Assim, os atrasos nas conclusões das ações podem acarretar o não cumprimento das metas previstas no PDTIC 2022 - 2025, sendo necessário verificar a causa dos atrasos e possíveis soluções para o atendimento do PDTIC.

Na figura 05 é possível observar algumas inconsistências nas informações e ausência de outras. Por exemplo, as ações A3.01.06, A3.01.01 e A1.04.01 possuem como prazo para conclusão o ano de 2025 e a conclusão real também em 2025 (ano futuro), contudo, nota-se que tais ações já foram concluídas no corrente ano, então a conclusão real é 2024 e não 2025, conforme consta no painel informativo. Também se verifica que nas ações A1.04.05 e

A1.04.04, cujo prazo para conclusão é 2025, a conclusão real foi informada em 2023, ou seja, há dois critérios de baixa de conclusão para a mesma situação.

Figura 05 - Monitoramento de execução das ações PDTIC

Lista de ações do PDTIC

Metas	Ações	Responsável	Status	Execução (%)	Prazo Conclusão	Conclusão Real
M4.02: Sustentar o sistema de banco de dados institucional integrado	A4.02.01 Aquisição de banco de dados e servidores específicos e atualização de licenças	DTI	Concluída	100	2022	2022
M4.02: Sustentar o sistema de banco de dados institucional integrado	A4.02.05 Contratação de suporte e garantia para o banco de dados	DTI	Concluída	100	2022	2022
M3.11: Aumentar a quantidade de páginas Web com conteúdo atualizado automaticamente	A3.11.01 Levantamento das demandas	DPW	Início em atraso	0	2023	
M3.07: Expandir sistemas de repositórios e documentação	A3.07.03 Contratação/desenvolvimento da(s) solução(ões)	DPW	Conclusão em atraso	0.3	2022	
M3.07: Expandir sistemas de repositórios e documentação	A3.07.04 Implantação da(s) solução(ões)	DPW	Conclusão em atraso	0.1	2023	
M3.01: Implementar um sistema de controle de acesso à rede com rastreamento de usuários	A3.01.06 Divulgação do sistema	DIS	Concluída	100	2025	2025
M3.01: Implementar um sistema de controle de acesso à rede com rastreamento de usuários	A3.01.01 Levantamento de requisitos	DIS	Concluída	100	2025	2025
M3.01: Implementar um sistema de controle de acesso à rede com rastreamento de usuários	A3.01.04 Implantação	DTI	Em andamento			
M3.01: Implementar um sistema de controle de acesso à rede com rastreamento de usuários	A3.01.02 Definição da solução	DIS	Em andamento			
M2.12: Inventariar e gerenciar os ativos (hardware e software) da Universidade	A2.12.01 Análise das recomendações do SISP e demais referências	DIS	Em andamento			
M1.04: Viabilizar velocidades e alta disponibilidade das conexões, mantendo-as compatíveis com a demanda em todos os campi	A1.04.01 Levantamento da demanda	DIS	Concluída	100	2025	2025
M1.04: Viabilizar velocidades e alta disponibilidade das conexões, mantendo-as compatíveis com a demanda em todos os campi	A1.04.05 Contratação de garantia de equipamentos	STI	Concluída	100	2025	2023
M1.04: Viabilizar velocidades e alta disponibilidade das conexões, mantendo-as compatíveis com a demanda em todos os campi	A1.04.04 Implantação dos equipamentos de otimização	DTI	Concluída	100	2025	2023
M1.03: Implementar e manter a estrutura de datacenter da universidade	A1.03.05 Implantação de sistema elétrico e de refrigeração de acordo com as melhores práticas	DIS	Concluída em atraso	100	2023	2024
M1.03: Implementar e manter a estrutura de datacenter da universidade	A1.03.04 Implantação do sistema de combate a incêndio e invasão/ocupação	DIS	Em andamento	50	2025	2024
M1.03: Implementar e manter a estrutura de datacenter da universidade	A1.03.03 Implantação de controle de acesso	DTI	Em andamento	50	2025	2024

A1.04.04 Implantação dos equipamentos de otimização

Fonte: Monitoramento das ações planejadas - PDTIC 2022 a 2025 (STI)

Também há a ausência de prazo de conclusão para diversas ações, como é o caso das ações A3.01.04, A3.01.02 e A2.12.01, que possuem o status de “Em andamento”, mas sem prazo para conclusão.

Outra inconsistência é observada nas ações A1.03.03 e A1.03.04, em que foi executado 50% das ações e consta conclusão real em 2024, sendo que não foram concluídas. Há ações que foram executadas 20%, outras 50%, algumas com informação de ano de conclusão real e outra não.

Conforme manifestação da unidade em resposta a SA nº 68/2023, o acompanhamento do PDTIC encontra-se desatualizado devido à necessidade de reavaliação pelo Comitê de Governança Digital, que foi aprovada no final de 2023. Também informou que a equipe que faz o acompanhamento ficou dedicada à conclusão da meta M1.03 de implementar e manter a estrutura de datacenter da Universidade, demandando concentração de esforços e impactando as demais demandas do PDTIC.

O painel de Monitoramento das ações planejadas - PDTIC 2022 a 2025 é uma ferramenta de controle de execução das ações do PDTIC, não só da gestão, mas também um instrumento de transparência ativa e de controle social sobre o atendimento das metas do plano. Dessa forma, é necessário manter as informações atualizadas e confiáveis, fidedignas à real situação das ações.

6. Questões do IGovTi em fase inicial

O objetivo na subquestão 6.1 foi verificar se há questões que compõem o IGovTI que estão em fase anterior à faixa intermediária e se estão sendo tratadas, a fim de atender à meta do PDI de atingir a faixa intermediária do IGovTI.

O Índice de Governança de TI - IGovTI é um índice que é calculado periodicamente pelo Tribunal de Contas da União - TCU para averiguar a situação da Governança na Administração Pública Federal, em relação à tecnologia da informação, com o objetivo estimular as organizações a adotarem boas práticas de governança.

Na avaliação, aplica-se ao órgão público um questionário com diversas questões, agrupadas em categorias que é composto pelo Índice de Governança de TI (GovernançaTI), que por sua vez avalia o Modelo de gestão de TI (ModeloTI), a capacidade em monitorar o desempenho da gestão de TI (MonitorAvaliaTI) e a capacidade em prestar serviços públicos com qualidade (resultadoTI). Compõe o iGovTI também, o índice de Gestão de TI (iGestTI), que por sua vez analisa a capacidade em processos de TI (processosTI), capacidade de realização do planejamento de TI (planejamentoTI) e da gestão de pessoal de TI (pessoasTI).

A pontuação do iGovTI varia de 0 a 100%, sendo que o enquadramento de classificação é realizado conforme o quadro abaixo:

Quadro 02 – Classificação do IGovTI

Classificação	Pontuação
Inexpressivo	0 a 14,9%
Iniciando	15% a 39,9%
Intermediário	40% a 69,9%
Aprimorado	70% a 100%

Fonte: TCU[7]

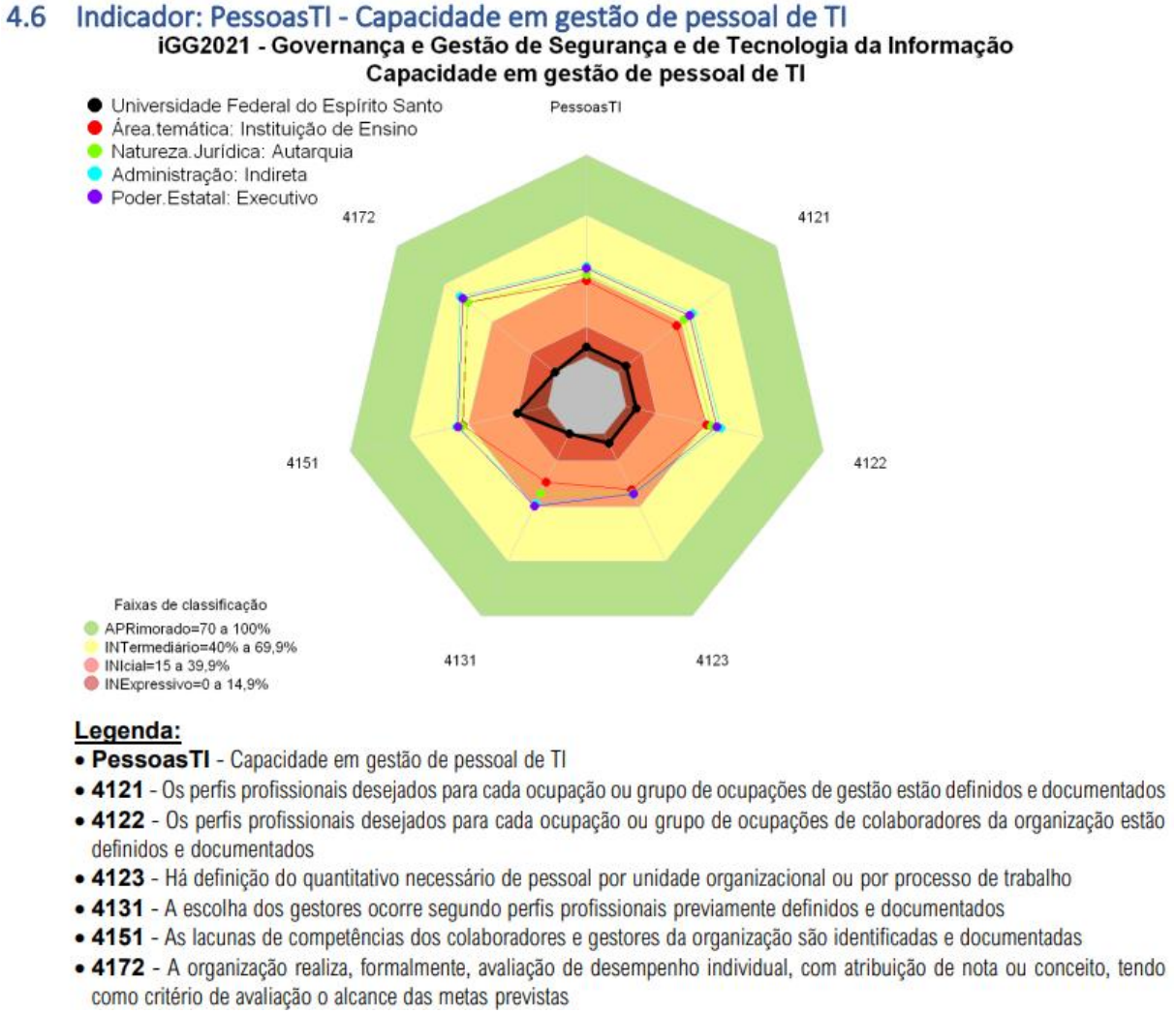
As questões utilizam a seguinte escala gradativa de adoção: “não adota”, “há decisão formal ou plano aprovado para adotá-la”, “não se aplica”, “adota em menor parte”, “adota parcialmente” e “adota em maior parte ou totalmente”. São considerados inexpressivos os graus de adoção “não adota” e “há decisão formal ou plano aprovado para adotá-la”. A faixa de implementação Iniciando é considerado o grau de adoção “adota em menor parte”, em Intermediário o grau “Adota parcialmente” e em aprimorado o grau “adota em maior parte ou totalmente”.

Consta no PDI 2021-2030 da Ufes, no mapa estratégico – Gestão (pg. 114), a meta 3 que é de “Atingir a faixa intermediária no Índice de Gestão de TI (iGovTI)”, tendo como indicado o próprio IGovTI levantado pelo TCU. Assim, com base no último levantamento do índice realizado pelo TCU, que ocorreu em 2021, foram verificadas as questões dos índices que estavam classificados abaixo de Intermediário e as subquestões referentes a elas foram aplicados ao STI para avaliar a situação em que se encontram para o atendimento da meta do PDI.

[7] Levantamento de Governança IGG. Disponível em https://portal.tcu.gov.br/governanca/governancapublica/organizacional/levantamento-de-governanca/levantamento-de-governanca.htm. Acesso em 30.04.2024

Por exemplo, na figura 06, que se refere ao indicador PessoasTI – Capacidade em gestão de pessoal de TI e que é parte do relatório[8] do IGG 2021, apresenta todas as questões (4121, 4122, 4123, 4131, 4151, 4172) abaixo da faixa de classificação Intermediária (amarela). Dessa forma, todas as subquestões referentes à essas questões foram aplicadas ao STI.

Figura 06 – Indicador PessoasTI do IGG 2021



Legenda:

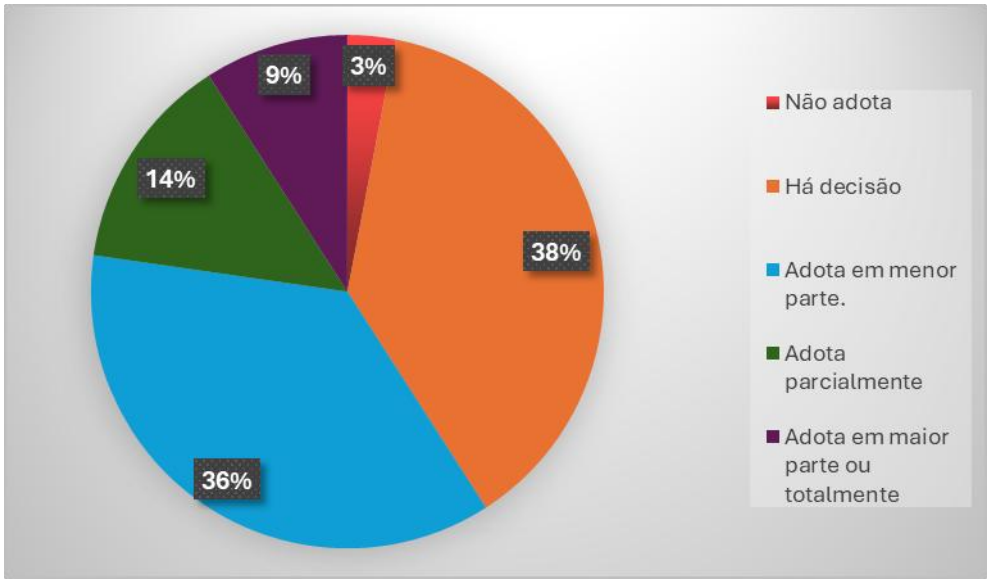
- **PessoasTI** - Capacidade em gestão de pessoal de TI
- **4121** - Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de gestão estão definidos e documentados
- **4122** - Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de colaboradores da organização estão definidos e documentados
- **4123** - Há definição do quantitativo necessário de pessoal por unidade organizacional ou por processo de trabalho
- **4131** - A escolha dos gestores ocorre segundo perfis profissionais previamente definidos e documentados
- **4151** - As lacunas de competências dos colaboradores e gestores da organização são identificadas e documentadas
- **4172** - A organização realiza, formalmente, avaliação de desempenho individual, com atribuição de nota ou conceito, tendo como critério de avaliação o alcance das metas previstas

Fonte: TCU - Levantamento de Governança e Gestão Públicas 2021

Assim, foram aplicadas ao STI 132 subquestões que se encontravam na faixa de classificação abaixo de Intermediário. Conforme o gráfico 01, para 3% das subquestões foram atribuídas o grau de adoção "não adota" e para 38% foram classificados como "há decisão formal ou plano aprovado para adotá-la", representando que 41% das subquestões ainda se enquadram na classificação "Inexpressivo". Para 36% das subquestões foi atribuído o grau "adota em menor parte", que representa a faixa "Inicial". Foi atribuído "Adota parcialmente" para 14%, que se refere à faixa "Intermediária" e para outros 9% "adota em maior parte ou totalmente", se enquadrando na faixa de "Aprimorado".

Gráfico 01 – Grau de adoção das subquestões

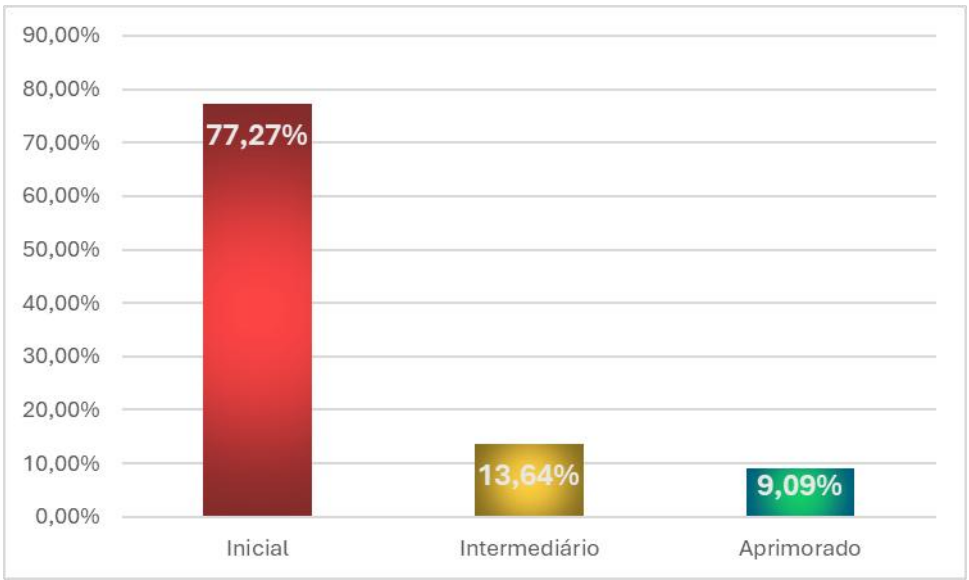
[8] Relatório de Levantamento de Governança e Gestão Públicas 2021 da UFES. Disponível em https://www.tcu.gov.br/igg2021/iGG2021%20-%20161%20-%20UFES.pdf. Acesso em 30.04.2024.



Fonte: Elaboração Própria

No gráfico 02, podemos verificar que o percentual de subquestões em níveis iniciais é bastante elevado: 77,27%. São considerados no nível inicial a classificação “inexpressivo” e “iniciando”. As subquestões classificadas como “não adota”, “há decisão formal ou plano aprovado para adotá-la” e “adota em menor parte”, que representam o nível inicial, estão apresentadas no Apêndice A e merecem maior atenção e planejamento de ações para que se possa atingir a meta do PDI.

Gráfico 02 – Percentual de subquestões por nível de classificação



Fonte: Elaboração Própria

Portanto, constatou-se que 77,27% das subquestões avaliadas referentes à boas práticas de governança em TI estão em nível inicial de adoção. Pressupõe que se as práticas de governança forem integralmente adotadas, não só o índice de governança de TI (IGovTI) se elevará, mas também o índice de governança pública institucional (IGG da UFES) terá sua classificação direcionada para um estágio mais elevado.

7. Fragilidade na segurança da informação quanto ao controle no descarte de equipamentos de TI.

Referente à segurança da Informação que pode ser respondida em análise conjunta pelas subquestões SQ 2.3 A unidade realiza gestão de risco de vazamento de dados/informações? e SQ 4.1 O descarte de equipamentos é realizado conforme recomenda o POSATI? pode-se verificar fragilidade nos controles e processos de descarte dos equipamentos de TI.

Conforme resposta apresentada por meio da SA nº 68/2023, o STI informou que não tem responsabilidade sobre o descarte de equipamentos e produtos eletrônicos, sendo esta da Diretoria de Materiais e Patrimônio DMP/Proad. O STI apenas regula a questão por meio do POSATI e POSIN, devendo a DMP seguir as recomendações dessas políticas.

Por seu turno, a DMP informou, por meio da SA nº 11/2024, que realiza o recolhimento dos bens a partir do lançamento da solicitação em sistema de informação e gestão patrimonial (módulo do SIE), por meio de uma programação semanal de coleta. No entanto, não realizam nenhuma triagem de condição do equipamento (reuso, inservível, defasado, sucata etc.) por não dispor de servidor qualificado em TI e local e equipamentos adequados (bancada de testes) no Depósito de inservíveis do Patrimônio, mas que a "avaliação é feita por meio de declaração do usuário, observando o estado físico do bem e se o mesmo está funcional, completo ou faltando peça".

A unidade informou ainda que os bens recolhidos ficam à disposição do público interno e que geralmente a cada 3 anos é realizado a desmobilização dos bens através de doação e/ou leilão. Também, que responsabilidade dos dados é um compromisso de gestão e do usuário dos equipamentos, acreditando que quando é solicitado o recolhimento de um equipamento os requisitos constantes na Posin tenham sido atendidos.

Nesse sentido, a ABNT NBR ISO/IEC 17799:2005[9] aponta no seu item 9.2.6, que trata da reutilização e alienação segura de equipamentos, sobre o controle que "convém que todos os equipamentos que contenham mídias de armazenamento de dados sejam examinados antes do descarte, para assegurar que todos os dados sensíveis e softwares licenciados tenham sido removidos ou sobregravados com segurança".

Junto a isso, é notório que muitos dos usuários não detém conhecimento suficientes sobre segurança da informação e/ou utilização de ferramentas ou procedimentos de informática mais sofisticados, como desinstalar programas, transferir e deletar informações com segurança, etc. Além do fato que os computadores da universidade, em regra, não permitem ao usuário o status de administrador do equipamento.

A norma supracitada ainda prevê como diretriz de implementação que "os dispositivos que contenham informações sensíveis sejam destruídos fisicamente ou as informações sejam destruídas, apagadas ou sobregravadas por meio de técnicas que tornem as informações originais irrecuperáveis, em vez de se usarem as funções-padrão de apagar ou formatar".

[9] ABNT NBR ISO/IEC 17799:2005: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Disponível em https://www.facom.ufu.br/~william/Disciplinas%202012-2/BSI%20-%20Auditoria%20e%20Seguranca/Material%20Adicional/NBR%20ISO-IEC%2017799-2005-PORTUGUES.pdf, acesso em 26.08.2024

Portanto, pode ser frágil apenas confiar nas ações dos usuários para garantir a segurança das informações contidas nos equipamentos descartados.

Outra frente de atuação é aumentar a participação dos servidores na segurança da informação ajudando a minimizar os riscos, é necessário investir em treinamentos e conscientização sobre o assunto.

A esse respeito o Posin 2022-2024 da Ufes diz que compete ao Gestor de Segurança da Informação:

> - Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;
> - Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão ou na entidade;

Corroborando, a cartilha denominada Cinco Controles de Segurança Cibernética para Ontem[10], produzida pelo TCU em 2022, diz no controle 14 (Conscientização Sobre Segurança e Treinamento de Competências) que precisa:

> Estabelecer e manter programa contínuo e permanente de conscientização e treinamento, para que os colaboradores tenham conhecimentos adequados em segurança (da informação e cibernética) e, consequentemente, adotem comportamentos e procedimentos que reduzam os riscos para a organização

Como exemplo de boa prática, o TCU instituiu um programa para conscientização de servidores com foco na difusão de conceitos básicos, práticas gerais e hábitos de trabalho fundados na preocupação com a segurança da informação. O programa é composto de ações periódicas de divulgação de políticas e normas internas, dicas, orientações e notícias de iniciativas no TCU ligadas à segurança da informação, além de contato direto com servidores por meio de visitas às unidades para discutir problemas, sanar dúvidas e captar diferentes percepções sobre segurança da informação. Também conta com o "Dia da Segurança da Informação no TCU", com palestras de convidados internos e externos, e atividades lúdicas e educacionais.

8. Fragilidade no processo de manutenção de equipamentos de TI

Na questão 2 buscou verificar se as manutenções nos equipamentos de TI da universidade são realizadas de forma satisfatória, em especial os desktop e notebooks.

Analisando o processo de manutenção dos equipamentos, verificamos que o STI adotou como estratégia de manutenção a garantia estendida dos equipamentos. Conforme reposta apresentada na SA nº 63/2023 "a superintendência adota a estratégia de garantia dos seus equipamentos para um período de 36 a 60 meses", mediante contrato de garantia estabelecido com o fabricante.

[10] Brasil. Tribunal de Contas da União. Cinco controles de segurança cibernética para ontem / Tribunal de Contas da União. – Brasília: TCU, 2022. 36 p.: il. Color. Disponível em https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A81881E7FF0EF4B0182B8F5CE4A3D8D

Informou ainda (SA nº 08/2024) que a Ufes tem realizado a compra centralizada do governo federal, portanto não temos autonomia para especificação de todos os termos de garantia, mas todos contemplam, no mínimo, o período de 36 meses.

No entanto, a unidade não especificou como as garantias são controladas, acionadas e os serviços fiscalizados. Por exemplo, quando questionados de como é realizada a abertura dos chamados não esclareceu o procedimento se limitando a informar que o atendimento é realizado no local do equipamento. Também, quando questionados sobre procedimentos adotados em caso de rejeição do chamado pela assistência técnica da garantia, alegando não cobertura ou mal uso do equipamento a unidade alegou que "há mecanismos para contestação da recusa", mas que "não temos gerência sobre os termos, que podem variar por tipo de equipamento".

Sobre o controle dos prazos de garantia de cada equipamento a unidade se manifestou (SA nº 08/2024) apenas acerca da importância dele, mas não se possui e de como é realizado, mencionando que "o controle de prazo de garantia assegura que os equipamentos estejam sempre sob proteção, minimizando riscos e custos com manutenções não planejadas." Assim, percebemos que não há um com controle eficiente da garantia e manutenções dos equipamentos.

Outro fator relevante verificado nas atividades de manutenção de equipamentos de TI, são a realização de serviços em equipamentos sem o controle e supervisão técnica da superintendência devido a distribuição de técnicos que não fazem parte do quadro de servidores do STI pelas unidades acadêmicas e administrativas, em especial nos campi localizados nas regiões sul e norte do estado, visto que há uma "variedade de operações descentralizadas executadas por técnicos que não fazem parte da equipe da Superintendência" (SA nº 09/2024).

Portanto, constatamos fragilidades no processo de manutenção dos equipamentos no que tange o controle das garantias dos equipamentos, a avaliação dos equipamentos para verificação dos serviços necessários, o acionamento dos serviços de garantia estendida e a verificação do atendimento dos serviços necessários e executados.

9. Aquisições de peças de computadores de forma descentralizada

No decorrer dos trabalhos constatamos que há aquisições de peças de TI de forma descentralizadas, com centros realizando contratações individualmente para atender suas demandas.

Verificamos, por exemplo, o Pregão Eletrônico nº 92011/2024 realizado pela UASG 153050 que realizou registro de preços peças para computadores como: bateria, cabo sata, disco rígido SSD, fonte ATX, memória DDR4, placa de memória e placa de rede, visando a manutenção dos computadores da UFES unidade de Alegre descobertos pelo prazo de garantia dos fabricantes.

Em resposta à SA nº 09/2024 o STI informou que há um esforço na Universidade Federal do Espírito Santo (Ufes), particularmente nos setores responsáveis pela aquisição de materiais, visando centralizar o processo de compra desses e de outros itens. Contudo, essa centralização ainda não foi concretizada.

Nesse sentido, o acórdão nº 4039/2020-Plenário determina para:

> 9.5.7.8. avaliar se a solução é divisível ou não, levando em conta o mercado que a fornece e atentando que a solução deve ser parcelada quando as respostas a todas as quatro perguntas a seguir forem positivas: " (I) é tecnicamente viável dividir a solução? (II) é economicamente viável dividir a solução? (III) não há perda de escala ao dividir a solução? (IV) há o melhor aproveitamento do mercado e ampliação da competitividade ao dividir a solução?

A centralização de compras de mesmos itens para as diversas UASG pode gerar o ganho de escala e melhoria dos controles das peças demandadas e utilizadas, consequentemente melhorando o processo de planejamento das aquisições, gerando economicidade para o órgão.

10. Informação

Em relação aos planos sob responsabilidade do Comitê de Governança Digital, conforme art.2º da portaria nº 342/2020, sendo eles o Plano de Transformação Digital, Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) e o Plano e Dados Abertos, verificamos que há o PDTIC 2022-2025 da Ufes vigente até 2025. Entretanto, o Plano e Dados Abertos 2017-2021 e o Plano de Transformação Digital 2020-2022, já se encerraram no sendo constatado a existência de novos planos.

Contudo, a Diretoria de Governança, Controles Internos e Integridade – DGCI, que atua como instância de segunda linha (ou camada) de defesa, para supervisão, monitoramento e tratamento de riscos, controles internos, integridade e compliance, informou, por meio da SA nº 10/2024, que o Plano de Dados Abertos da Ufes 2024-2026 está em fase final de revisão, sendo posteriormente disponibilizado para consulta pública e após enviado para aprovação do Comitê de Governança Digital da Ufes, conforme pode ser verificado no site https://governanca.ufes.br/dados-abertos.

Quanto ao Plano de Transformação Digital, o normativo era específico para o período de 2020 a 2023. Assim, estavam aguardando novos normativos para a confecção do novo plano. No mês de junho/2024 foram publicados o do Decreto nº 12.069/2024, que institui a Estratégia Nacional de Governo Digital para o período de 2024 a 2027, e a Portaria SGD/MGI Nº 4.248/2024, que estabelece recomendações para o alcance dos objetivos da Estratégia Nacional de Governo Digital para o período de 2024 a 2027. Para o mês de setembro está previsto a publicação da Estratégia Federal de Governo Digital 2024-2027, documento que define os objetivos e as iniciativas com as respectivas metas para o Governo Federal. Esse conjunto de normativo permitirá a elaboração do Plano de Transformação Digital 2024-2026 da Ufes alinhado com o governo federal.

No tocante ao Comitê de Governança Digital da Ufes, instituído pela Portaria nº 1634/2016-GR e alterada pela portaria nº342/2020-GR, consta que haverá reuniões ordinárias, no mínimo, trimestrais. No entanto, constatamos a ocorrência de 2 reuniões em 2022 e 1 reunião em 2023. Ainda não há registro de reuniões em 2024. Também constatamos servidores nas portarias que já participam do comitê.

Assim, é importante que os normativos e o que de fato ocorre sejam congruentes, sendo necessário avaliar as quantidades e reuniões realmente necessárias para o comitê, bem como os servidores que efetivamente atuam e ajustar as portarias.

RECOMENDAÇÕES

À Superintendência de Tecnologia da Informação (STI)

Achado n° 1

1 – Reestruturar a sistemática de classificação dos atendimentos realizados pelo suporte ao usuário de forma que todos os chamados sejam devidamente classificados.

2- Instituir indicadores de desempenho dos atendimentos realizados pelo suporte ao usuário.

Achado nº 2

3 - Finalizar e revisar o mapeamento dos riscos e elaborar o mapeamento dos principais processos, criando uma sistemática de revisão periódica.

Achado nº 3

4 - Realizar o dimensionamento da força de trabalho necessária a fim de conhecer a real necessidade de mão de obra e a qualificação requerida para as funções, solicitando à Progep o suprimento da demanda.

Achado nº 4

5 – Revisar a Política de Sustentabilidade Ambiental em Tecnologia de Informação e Comunicação – Posati, sanando as inconsistências e atualizando com base na legislação vigente, adotando uma periodicidade de revisão.

Achado n° 5

6 – Corrigir as inconsistências no Painel de Monitoramento das ações planejadas - PDTIC 2022 a 2025 e atualizá-lo para que apresente informações tempestivas e fidedignas, mantendo uma periodicidade de atualização (diária, semanal, mensal, etc.).

Achado n° 6

7 - Implementar ações que melhorem as práticas de governança que estão em nível inicial do IGovTI da Ufes, para possibilitar atingir o nível intermediário do IGovTI, meta do PDI 2021-2030.

Achado nº 7

8 – Instituir campanhas periódicas de conscientização dos servidores sobre a segurança da informação, em especial acerca das normas e procedimentos a serem realizados antes da solicitação de recolhimento dos equipamentos.

À Superintendência de Tecnologia da Informação (STI) em conjunto com a Diretoria de Materiais e Patrimônio (DMP)

9 – Proceder a um estudo técnico de viabilidade quanto ao custo-benefício em implementar uma instância de controle com a verificação dos equipamentos a serem descartados a fim de garantir a segurança das informações neles contidas.

Achado nº 8

10- Proceder à gestão técnica dos contratos de garantia estendida, visando acompanhar e proceder a avaliação prévia do equipamento antes do mesmo ser enviado para a empresa garantidora do conserto.

11- Proceder a um estudo técnico de viabilidade quanto ao custo-benefício para a terceirização da manutenção de software e hardware dos equipamentos de informática no âmbito da Ufes, após período de garantia estendida.

12- Verificar a viabilidade administrativa de o STI absorver os técnicos de TI que não fazem parte do seu quadro de servidores para que fiquem sob a supervisão técnica e administrativa da Superintendência, implementando controles sobre todos os serviços de TI executados.

Achado nº 9

13- Proceder análise junto aos setores de responsáveis pela aquisição de materiais o custo-benefício de centralizar as aquisições de peças de TI e o melhor método que atenda essa necessidade e de requisição única pelo STI.

CONCLUSÃO

Por meio da auditoria realizada nos macroprocessos de regularidade da gestão da tecnologia da informação, visando garantir o planejamento estratégico alinhado ao Plano de Desenvolvimento Institucional (PDI) e a LDO/LOA 2023.9.2, foi possível constatar que há oportunidade de melhorias nos controles e na governança da unidade.

Em relação ao suporte ao usuário constatamos oportunidade de melhoria no gerenciamento da atividade com a criação de indicadores para acompanhamento das atividades. Também pode-se melhorar os controles para categorização correta dos atendimentos realizados fornecendo informações mais fidedignas para a tomada de decisões.

Quanto ao mapeamento de processo, ainda não há o mapeamento, precisando iniciar para formalizar os fluxos de trabalho e oportunamente melhorar os processos. Já o mapeamento de riscos precisa de aprimoramentos, devido ainda estar incompleto.

Durante as análises verificou-se a deficiência de Recursos Humanos na unidade, devendo realizar um dimensionamento da força de trabalho necessária para buscar suprir as necessidades, pois com o aumento do uso de tecnologias para a prestação de serviços a Superintendência necessita de um olhar mais atento para evitar problemas, em especial invasões hackers e roubo de informações.

Não obstante foram constatadas fragilidades no processo de manutenção dos equipamentos de TI no que se refere à controle da garantia dos equipamentos e do acompanhamento dos serviços executados.

Ainda se constatou a deficiências e desatualização da Política de Sustentabilidade Ambiental em Tecnologia de Informação, necessitando ser revisada, e inconsistências no painel de monitoramento das ações do PDTIC, devendo buscar melhorar os controles do painel. Também há a possibilidade de melhoria na governança de TI com a adoção e aprimoramento de práticas levantadas no IGovTI pelo TCU e cumprir a meta do PDI 2021-2030 de atingir nível intermediário do referido índice.

Por fim, a Audin, por meio da emissão do Relatório de Auditoria, com as devidas recomendações, espera atingir como benefícios para a gestão da Universidade a melhoria nos controles no gerenciamento do STI, aprimorar a governança, fornecer mais transparência com informações mais fidedignas e melhorar a capacidade do setor de atender às demandas de TI cada vez mais crescentes.

ANEXOS

I – MANIFESTAÇÕES DAS UNIDADES AUDITADAS

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 55/2023 – Tarefa e-Aud #1536729

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 63/2023 – Tarefa e-Aud #1558788

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 67/2023 - Tarefa e-Aud #1536727

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 68/2023 - Tarefa e-Aud #1576304

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 69/2023 - Tarefa e-Aud #1593051

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 08/2024 - Tarefa e-Aud #1639236

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 09/2024 - Tarefa e-Aud #1685226

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 10/2024 - Tarefa e-Aud #1685612

Manifestação da Superintendência de Tecnologia da Informação em resposta à Solicitação de Auditoria nº 11/2024 - Tarefa e-Aud #1685683

APENDICE

A – RESPOSTAS ÀS QUESTÕES DO IGOVTI

Indicadores IGG TCU - Gestão da tecnologia e da segurança da informação				
Indcador: iGestSegInfo - Índice de Gestão da Segurança da Informação				**Grau de adoção (avaliação do TCU)**
item	**Questão**	**Subquestões**		
4242	A organização executa processo de gestão de continuidade de serviços de tecnologia da informação	a)	a organização elabora um plano de continuidade de serviços de TI;	Adota em Menor Parte
		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;	Adota em menor parte
		c)	o plano de continuidade de serviços de TI é testado e revisado periodicamente;	Adota em Menor Parte
		d)	o processo de gestão de continuidade de serviços de TI integra o processo institucional de gestão de continuidade do negócio;	Adota em Menor Parte
		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);	Adota em Menor Parte
		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.	Adota em Menor Parte
4271 F	A organização executa um 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;	Adota em Menor Parte
Indicador: PessoasTI - Capacidade em gestão de pessoal de TI				
item	**Questão**	**Subquestões**		
4121	Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de gestão estão definidos e documentados	a)	as responsabilidades e atribuições dos gestores da área finalística estão definidas, documentadas e publicadas;	Há Decisão
		b)	as responsabilidades e atribuições dos gestores da área finalística são revisadas periodicamente e publicadas;	Há Decisão
		c)	as responsabilidades e atribuições dos gestores da área administrativa estão definidas, documentadas e publicadas;	Há Decisão
		d)	as responsabilidades e atribuições dos gestores da área administrativa são revisadas periodicamente e publicadas;	Há Decisão
		e)	relacionou-se no perfil profissional, além de requerimentos de ordem legal, um conjunto de competências que os ocupantes dos cargos de gestão devem possuir;	Há Decisão
		f)	f) a aderência entre os perfis profissionais definidos e as necessidades organizacionais é revisada periodicamente;	Há Decisão
		g)	g) a organização utiliza mecanismos de transparência ativa para disponibilizar às partes interessadas internas e externas os perfis profissionais definidos para as ocupações de gestão.	Há Decisão

4122	Os perfis profissionais desejados para cada ocupação ou grupo de ocupações de colaboradores da organização estão definidos e documentados	a)	as responsabilidades e atribuições das ocupações, ou grupo de ocupações, da área finalística estão definidas, documentadas e publicadas;	Há Decisão
		b)	as responsabilidades e atribuições das ocupações, ou grupo de ocupações, da área finalística são revisadas periodicamente e publicadas;	Há Decisão
		c)	as responsabilidades e atribuições das ocupações ou grupo de ocupações da área administrativa estão definidas, documentadas e publicadas;	Há Decisão
		d)	as responsabilidades e atribuições das ocupações ou grupo de ocupações da área administrativa são revisadas periodicamente e publicadas;	Há Decisão
		e)	relacionou-se nos perfis profissionais, além de requerimentos de ordem legal, um conjunto de competências que o ocupante do cargo deve possuir;	Há Decisão
		f)	a organização utiliza mecanismos de transparência ativa para disponibilizar às partes interessadas internas e externas os perfis profissionais definidos.	Há Decisão
4123	Há definição do quantitativo necessário de pessoal por unidade organizacional ou por processo de trabalho	a)	há política de orientação para o dimensionamento da força de trabalho;	Há Decisão
		b)	definiu-se o quantitativo necessário por unidade organizacional, ou processo de trabalho, com base em critério(s) ou procedimento(s) técnico(s);	Há Decisão
		c)	definiu-se, de maneira documentada, um quantitativo necessário de pessoal por unidade organizacional, ou processo de trabalho, da área finalística;	Há Decisão
		d)	definiu-se, de maneira documentada, um quantitativo necessário de pessoal por unidade organizacional, ou processo de trabalho, da área administrativa;	Há Decisão
		e)	há revisão periódica do quantitativo de pessoal necessário por unidade organizacional ou processo de trabalho.	Há Decisão
4131	A escolha dos gestores ocorre segundo perfis profissionais previamente definidos e documentados	a)	avalia-se, previamente à nomeação/designação, se o gestor possui impedimentos legais decorrentes de sanções administrativas, cíveis, eleitorais ou penais, incluindo envolvimento em atos de corrupção;	Adota em Menor Parte
		b)	os gestores da área de finalística são selecionados com base em perfil profissional, previamente, definido e documentado, e compatível com o cargo ou função para o qual tenha sido indicado;	Adota em Menor Parte
		c)	os gestores da área administrativa são selecionados consoante perfil profissional, previamente, definido e documentado, e compatível com o cargo ou função para o qual tenha sido indicado;	Adota em Menor Parte
		d)	são utilizadas ferramentas estruturadas para auxiliar a seleção dos ocupantes dos cargos/funções comissionados de gestão;	Adota em Menor Parte
		e)	são utilizados mecanismos de transparência ativa para disponibilizar às partes interessadas externas e internas o currículo dos ocupantes dos cargos/funções de gestão.	Adota em Menor Parte

4172	A organização realiza, formalmente, avaliação de desempenho individual, com atribuição de nota ou conceito, tendo como critério de avaliação o alcance das metas previstas	a)	há normativo que trata da avaliação de desempenho dos colaboradores e gestores;	Adota Parcialmente
		b)	a avaliação abrange o desempenho de todos os gestores da área finalística;	Adota Parcialmente
		c)	a avaliação abrange o desempenho de todos os gestores da área administrativa;	Adota Parcialmente
		d)	a avaliação abrange o desempenho de todos os colaboradores da área finalística;	Adota Parcialmente
		e)	a avaliação abrange o desempenho de todos os colaboradores da área administrativa.	Adota Parcialmente
Indicador: iGestServicosTI - Capacidade em Gerir Serviços de TI				
item	**Questão**	**Subquestões**		
4221	A organização elabora um catálogo de serviços de tecnologia da informação	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);	Adota em Menor Parte
		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 tecnologia da informação e as áreas de negócio da organização;	Adota em Menor Parte
		c)	o catálogo é de fácil acesso e está amplamente disponível a seus usuários e às equipes de suporte.	Adota Parcialmente
4222	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);	Adota em Menor Parte
		b)	mudanças são previamente comunicadas a todas as partes que possam ser afetadas;	Adota em Menor Parte
		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;	Adota em Menor Parte
		d)	a realização de cada mudança é precedida de planejamento e testes;	Adota em Menor Parte
		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;	Adota em Menor Parte
		f)	lições aprendidas com as mudanças são compartilhadas, com vistas ao aprimoramento do processo (ex: Wiki);	Adota em Menor Parte
		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);	Adota em Menor Parte

		h)	a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de mudanças e promove eventuais ajustes necessários.	Adota em Menor Parte
4223	A organização executa processo de gestão de configuração e ativos (de serviços de tecnologia da informação)	a)	a organização mantém uma base de dados consolidada com as configurações dos serviços e ativos de TI e o relacionamento entre eles;	Adota Parcialmente
		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;	Adota Parcialmente
		c)	a base de dados de configurações é mantida atualizada;	Adota Parcialmente
		d)	a base de dados de configurações é utilizada como insumo para o planejamento e o acompanhamento das mudanças;	Adota Parcialmente
		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);	Adota Parcialmente
		f)	a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de configuração e ativos e promove eventuais ajustes necessários.	Adota Parcialmente
4224	A organização executa processo de gestão de incidentes de serviços de tecnologia da informação	a)	a organização definiu regras para a priorização e o escalamento de incidentes;	Há Decisão
		b)	a resolução de incidentes considera os níveis de serviços especificados em acordos com as áreas clientes;	Há Decisão
		c)	bases de conhecimento sobre erros conhecidos e problemas são utilizadas como insumos na resolução de incidentes;	Há Decisão
		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);	Há Decisão
		e)	a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de incidentes de serviços de tecnologia da informação e promove eventuais ajustes necessários.	Há Decisão

Indicador: iGestRiscosTI - Capacidade em gerir riscos de TI

item	Questão	Subquestões		
4241	A organização executa processo de gestão dos riscos de tecnologia da informação relativos a	a)	a organização identifica e avalia os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio;	Adota em Menor Parte
		b)	a organização trata os riscos de tecnologia da informação dos processos organizacionais críticos para o negócio, com base em um plano de tratamento de risco;	Adota em Menor Parte

	processos de negócio	c)	a organização atribuiu a responsabilidade por coordenar a gestão de riscos de tecnologia da informação;	Adota Parcialmente
		d)	o processo de gestão dos riscos de tecnologia 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 Adota
		e)	a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de riscos de tecnologia da informação e promove eventuais ajustes necessários.	Não Adota
4242	A organização executa processo de gestão de continuidade de serviços de tecnologia da informação	a)	a organização elabora um plano de continuidade de serviços de TI;	Adota em Menor Parte
		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;	Adota em Menor Parte
		c)	o plano de continuidade de serviços de TI é testado e revisado periodicamente;	Adota em Menor Parte
		d)	o processo de gestão de continuidade de serviços de TI integra o processo institucional de gestão de continuidade do negócio;	Adota em Menor Parte
		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);	Adota em Menor Parte
		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.	Adota em Menor Parte
2113	O processo de gestão de riscos da organização está implantado	a)	objetivos e elementos (processos, produtos, atividades, ativos) críticos da organização estão identificados;	Há Decisão
		b)	há lista integrada de riscos, incluindo causas, fontes, efeitos;	Há Decisão
		c)	os riscos constantes da lista integrada foram analisados e avaliados;	Há Decisão
		d)	o tratamento dos riscos está documentado;	Há Decisão
		e)	os responsáveis pelo tratamento dos riscos participam do processo de escolha das respostas aos riscos;	Há Decisão
		f)	os riscos críticos identificados são informados aos membros das instâncias superiores de governança.	Há Decisão
2114	Os riscos considerados críticos para a organização são geridos	a)	os riscos críticos estão identificados;	Adota em Menor Parte
		b)	os riscos críticos estão analisados e avaliados;	Adota em Menor Parte
		c)	o tratamento dos riscos críticos está documentado;	Adota em Menor Parte
		d)	há monitoramento periódico dos riscos críticos identificados.	Adota em Menor Parte
Indicador: EstruturaSegInfo - Capacidade em definir políticas de responsabilidades para a gestão da TI				

4252	A organização dispõe de comitê de segurança da informação	a)	o comitê de segurança da informação realiza as atividades previstas em seu ato constitutivo;	Adota em Menor Parte
		b)	o comitê formula diretrizes para a segurança da informação;	Adota Parcialmente
		c)	o comitê propõe a elaboração e a revisão de normas e de procedimentos inerentes à segurança da informação;	Adota em Maior parte ou Totalmente
		d)	o comitê é composto por representantes de áreas relevantes da organização.	Adota em Maior parte ou Totalmente
4253	A organização possui um gestor institucional de segurança da informação	a)	o gestor institucional de segurança da informação foi designado formalmente pela alta administração;	Adota em Maior parte ou Totalmente
		b)	o gestor institucional de segurança da informação reporta-se diretamente à alta administração;	Adota em Maior parte ou Totalmente
		c)	o gestor institucional de segurança da informação coordena o processo de gestão de riscos de segurança da informação em âmbito institucional;	Adota em Maior parte ou Totalmente
		d)	o gestor institucional de segurança da informação coordena ações de segurança da informação em âmbito institucional;	Adota Parcialmente
		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;	Adota Parcialmente
		f)	o gestor institucional de segurança da informação detém as prerrogativas e os recursos necessários para o desempenho de todas as suas competências.	Adota Parcialmente
Indicador: ProcessoSegInfo - Capacidade em estabelecer processos e atividades para a gestão da TI				
4261	A organização executa processo de gestão de riscos de segurança da informação	a)	a organização identifica e avalia riscos de segurança da informação;	Há Decisão
		b)	a organização trata riscos de segurança da informação com base em um plano de tratamento de riscos;	Há Decisão
		c)	a organização possui um gestor formalmente responsável por coordenar a gestão de riscos de segurança da informação;	Há Decisão
		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);	Há Decisão
		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.	Há Decisão
4263	A organização executa processo de gestão de ativos	a)	a organização mantém um inventário dos ativos associados à informação;	Adota em Menor Parte
		b)	a organização definiu responsabilidades pelos ativos associados à informação;	Há Decisão

	associados à informação	c)	o inventário identifica as informações críticas que os ativos armazenam, processam ou transmitem;	Há Decisão
		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;	Há Decisão
		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;	Há Decisão
		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);	Há Decisão
		g)	a organização avalia periodicamente o desempenho e a conformidade do processo de gestão de ativos associados à informação e promove eventuais ajustes necessários.	Há Decisão
4264	A organização executa processo para classificação e tratamento de informações	a)	informações pessoais são identificadas e rotuladas, com vistas a viabilizar adequado tratamento e proteção;	Há Decisão
		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;	Há Decisão
		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 Decisão
		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 Decisão
		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;	Há Decisão
		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;	Há Decisão
		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 tratamento e proteção;	Há Decisão

		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 Decisão
		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);	Há Decisão
		j)	a organização avalia periodicamente o desempenho e a conformidade do processo de classificação e tratamento de informações e promove eventuais ajustes necessários.	Há Decisão
4265	A organização executa processo de gestão de incidentes de segurança da informação	a)	a organização definiu e comunica amplamente o ponto de contato a ser notificado no caso de ocorrência de incidente de segurança da informação, bem como os canais de comunicação apropriados;	Adota em Menor Parte
		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;	Adota em Menor Parte
		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;	Adota em Menor Parte
		d)	a organização instituiu equipe de tratamento e resposta a incidentes em redes computacionais (ETIR) ou estrutura equivalente;	Adota em Maior parte ou Totalmente
		e)	o processo de gestão de incidentes 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);	Adota em Menor Parte
		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.	Adota em Menor Parte
4266	A organização executa atividades de gestão da segurança dos recursos de processamento da informação, inclusive dos recursos de computação em nuvem	a)	a organização gerencia (inventaria e controla) os dispositivos conectados em sua rede;	Não Adota
		b)	a organização gerencia (inventaria e controla) os softwares instalados nos dispositivos conectados em sua rede;	Não Adota
		c)	a organização gerencia vulnerabilidades técnicas em seus ativos de software, de hardware e de rede críticos para o negócio;	Adota em Maior parte ou Totalmente
		d)	a organização implementa configurações seguras em seus ativos de software, de hardware e de rede críticos para o negócio;	Adota em Maior parte ou Totalmente
		e)	a organização mantém, monitora e analisa logs de auditoria dos ativos de software, de hardware e de rede críticos para o negócio;	Adota em Menor Parte

		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;	Adota em Maior parte ou Totalmente
		g)	a organização implementa defesas contra malware (ex: vírus) e outras ameaças cibernéticas (ex: phishing);	Adota Parcialmente
		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;	Adota em Maior parte ou Totalmente
		i)	a organização implementa defesa de perímetro das conexões de sua rede interna com a internet e outras redes externas;	Adota em Maior parte ou Totalmente
		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;	Adota em Maior parte ou Totalmente
		k)	a organização executa regularmente testes de segurança em seu ambiente de TI (detecção de vulnerabilidades e testes de penetração).	Adota em Menor Parte
Indicador: ResultadoTI - Capacidade em prestar serviços públicos com qualidade				
3132	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)	a organização observa as recomendações do Documento de Referência da arquitetura e-PING - Padrões de Interoperabilidade de Governo Eletrônico ou, no caso de organização que não integra o Poder Executivo Federal, observa as melhores práticas equivalentes;	Adota em Menor Parte
		b)	a organização observa as recomendações do guia Padrões Web em Governo Eletrônico: Cartilha de Usabilidade ou, no caso de organização que não integra o Poder Executivo Federal, observa as melhores práticas equivalentes;	Adota em Menor Parte
		c)	a organização garante o acesso da pessoa com deficiência aos serviços e informações que oferece na internet, por meio da adoção de melhores práticas de acessibilidade adotadas internacionalmente (p. ex.: eMAG - Modelo de Acessibilidade em Governo Eletrônico);	Adota em Menor Parte
		d)	as operações de tratamento de dados pessoais utilizados na prestação de serviços públicos pela organização são realizadas de modo a preservar a intimidade, vida privada, honra e imagem das pessoas às quais se referem;	Adota em Menor Parte
		e)	a organização informa em seu sítio eletrônico as hipóteses em que, no exercício de suas competências, realiza o tratamento de dados pessoais, bem como fornece informações claras e atualizadas sobre a previsão legal, a finalidade, os procedimentos e as práticas de tratamento que utiliza;	Adota em Menor Parte