MINISTÉRIO DA EDUCAÇÃO

INSTITUTO FEDERAL SUL-RIO-GRANDENSE

UNIDADE DE AUDITORIA INTERNA GOVERNAMENTAL

RELATÓRIO DE AUDITORIA 005/2021

Unidade auditada: Diretoria de Tecnologia da Informação

Área: Tecnologia da Informação – Segurança da Informação

Objeto da auditoria: Infraestrutura de Tecnologia da Informação (disponibilidade de sistemas, *backup* de dados, integridade da informação, suporte à estrutura física, projetos de infraestrutura lógica) na Reitoria

Período: 22/02/2021 a 30/08/2021

Nº da ação no PAINT: 13

Ordem de Serviço: 005/2021

Memorandos emitidos: Mem. IF-UAIG/n. 6/2021, 11/2021, 14/2021, 47/2021, 54/2021, 64/2021, 72/2021 e 73/2021

Memorandos recebidos: Mem. IF-DTI/n. 3/2021, 4/2021, 10/2021, 14/2021 e 15/2021

Solicitações de Auditoria: 005/2021 e 005-A/2021

1 INTRODUÇÃO

A presente auditoria teve como objeto a infraestrutura de tecnologia da informação (disponibilidade de sistemas, *backup* de dados, integridade da informação, suporte à estrutura física, projetos de infraestrutura lógica) na Reitoria.

A unidade auditada foi a Diretoria de Tecnologia da Informação (DTI), uma vez que possui competências regimentais nesse sentido, conforme segue:

> Art. 132. À Diretoria de Tecnologia da Informação compete:
> I. propor políticas e diretrizes da área de tecnologia da informação do IFSul;
> IX. garantir a segurança e integridade das informações;
> XIV. zelar pela Política de Segurança da Informação e seus regulamentos;
> XVIII. coordenar ações para promover a Política de Segurança da Informação no IFSul.

1.1 Objetivos

O objetivo geral definido no Programa de Auditoria arquivado junto aos papéis de trabalho foi o de avaliar a conformidade dos procedimentos e a adequação e a suficiência dos controles internos administrativos quanto à infraestrutura de tecnologia da informação (PDI – Eixo Infraestrutura – Metas 6.1 a 6.4).

Como objetivos específicos, foram elencados os seguintes.

Disponibilidade de sistemas

Em relação à disponibilidade dos sistemas de Tecnologia da Informação (TI), o objetivo específico é a manutenção do funcionamento dos sistemas de TI de modo a evitar a interrupção das atividades e proteger os processos críticos contra efeitos de falhas ou desastres significativos, ou ainda assegurar o reestabelecimento dos sistemas, caso ocorram às interrupções, em tempo hábil[1].

a) Verificar a existência, no âmbito do Instituto Federal Sul-rio-grandense, de Planos de Continuidade do Negócio (PCN), relacionados à área de TI.

b) Verificar se os PCN foram desenvolvidos e implementados para manutenção ou recuperação das operações de modo que assegure a disponibilidade da informação no nível e tempos requeridos, após a ocorrência de falhas ou interrupções dos processos críticos.

c) Verificar a existência de estrutura básica nos PCN, de modo que se possa identificar sua consistência para contemplar os requisitos de segurança da informação.

d) Verificar se os PCN são testados e atualizados regularmente, de forma a assegurar sua permanente atualização e efetividade.

***Backup* de dados**

[1] ABNT NBR ISO/IEC 27002:2007, pg. 153 e ABNT NBR ISO/IEC 27002:2005, p. 103

Também conhecido como cópias de segurança das informações, são sistemas que buscam garantir a proteção contra a perda de dados. No caso, requer-se que cópias de segurança das informações, *softwares* e das imagens do sistema sejam efetuadas e testadas regularmente conforme a política de geração de cópias de segurança definida[2].

e) Verificar a existência de política de *backup* e se esta estabelece e define os requisitos da organização relativos às cópias de segurança das informações, dos *softwares* e dos sistemas.

f) Verificar se a política de *backup* define os requisitos para proteção e retenção de modo a manter a integridade e disponibilidade da informação.

g) Verificar se os recursos adequados para a geração de cópias de segurança são disponibilizados para garantir que toda informação e *softwares* essenciais possam ser recuperados após um desastre ou a falha de uma mídia.

h) Verificar se os serviços e sistemas críticos possuem mecanismos de geração de cópias de segurança que abranjam todos os sistemas de informação, aplicações e dados necessários para a completa recuperação do sistema em um evento de desastre.

i) Verificar a existência de sistema de redundância de modo a evitar que os *backups* sejam armazenados na mesma estrutura física e de equipamentos.

Integridade da informação

A integridade, juntamente com a confidencialidade e a autenticidade das informações, constitui os pilares da Política de Segurança de Informações, estando intimamente relacionada aos controles de acesso às informações. Consiste na fidedignidade de informações. Sinaliza a conformidade de dados armazenados com relação às inserções, alterações e processamentos autorizados efetuados. Sinaliza, ainda, a conformidade dos dados transmitidos pelo emissor com os recebidos pelo destinatário. A manutenção da integridade pressupõe a garantia de não violação dos dados com intuito de alteração, gravação ou exclusão, seja ela acidental ou proposital[3].

j) Verificar se as responsabilidades pela segurança da informação estão definidas e atribuídas em documentos institucionais.

[2] ABNT NBR ISO/IEC 27002:2013, eletrônica, pg. 63, ABNT NBR ISO/IEC 27002:2005, p. 38-10.5, 117 e Manual de Boas Práticas em Segurança da Informação TCU: 2004, p. 73

[3] Manual de Boas Práticas em Segurança da Informação TCU: 2004, p. 11 e Política de Segurança da Informação – IFSul Versão: 1.07 – dez/2012 http://www.ifsul.edu.br/diretorias/diretoria-de-tecnologia-da-informacao/documentos-dti

k) Verificar a existência de procedimento de inventário de ativos de informação, de maneira que todos estes (dados, *hardware*, *software* e instalações) estejam inventariados e tenham um proprietário responsável.

l) Verificar a existência de serviço de gestão de incidentes, o qual consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa, bem como a identificação de tendências.

m) Verificar a existência de processo de gestão de riscos que podem causar interrupções aos processos de negócio, junto à probabilidade e impacto de tais interrupções e as consequências para a segurança da informação.

n) Verificar a existência de controles físicos que monitorem e que impeçam ou limitem o acesso (por exemplo, estabelecimento de perímetro de segurança, acesso de pessoas e veículos, cadeados, cofres, sala-cofre, etc.).

o) Verificar a existência de controles lógicos, sendo estes um conjunto de medidas e procedimentos, administrativos ou intrínsecos aos *softwares*, responsável pela proteção dos recursos computacionais (dados, programas) contra tentativas de acesso não autorizadas.

p) Verificar a existência de controles ambientais que visem proteger os recursos computacionais contra danos provocados por desastres naturais e por falhas estruturais (por exemplo, sistema de energia, de refrigeração, detectores e supressores de água e fogo, redundância, *backup*, etc.).

Suporte à estrutura física

Para garantir a segurança da informação em determinada organização, deve-se atentar para a necessidade do estabelecimento de infraestrutura que propicie o seu gerenciamento. A infraestrutura é sustentada/mantida por meio do suporte realizado pelos recursos humanos disponíveis na área de TI[4].

q) Verificar a adequação/suficiência de servidores, terceirizados e estagiários responsáveis pelo suporte à infraestrutura disponível.

r) Verificar a existência de procedimentos-padrão devidamente documentados com políticas claras de seleção, de treinamento, de avaliação de desempenho, de segregação de funções, de controles de acesso, das responsabilidades e dos papéis dos profissionais de TI.

[4] ABNT NBR ISO/IEC 27001:2006, pg.10, ABNT NBR ISO/IEC 27002:2005, p.25 e Manual de Boas Práticas em Segurança da Informação TCU: 2004, p. 64

Projetos de infraestrutura lógica

Empresas, organizações públicas e privadas, entre outras, necessitam dos serviços de TI para realizarem suas atividades básicas e para garantirem a expansão e desenvolvimento de suas atividades. As tecnologias são distribuídas e acessadas por meio de estruturas físicas de redes lógicas (redes de dados) e, para que o funcionamento ocorra de modo eficiente, faz-se necessário organizar, planejar e gerenciar os serviços que dão esse suporte à tecnologia da informação. Diante disso, os projetos de infraestrutura lógica devem considerar os objetivos e estratégias de negócio da organização, resultando na previsão e identificação de vulnerabilidades e ameaças aos ativos[5].

s) Verificar a existência de equipe de desenvolvimento de projetos de infraestrutura de redes lógicas, formalmente constituída.

t) Verificar a existência de terceirização de projetos de infraestrutura de redes lógicas e como ocorrem as etapas de contratação.

u) Verificar se consta nas contratações de projetos de infraestrutura lógica processo formal de planejamento das contratações e se são estabelecidos requisitos técnicos de segurança e Sistema de Gestão de Segurança da Informação (SGSI).

1.2 Escopo

Os exames de auditoria recaíram sobre a infraestrutura de tecnologia da informação (disponibilidade de sistemas, *backup* de dados, integridade da informação, suporte à estrutura física, projetos de infraestrutura lógica) na Reitoria.

2 HISTÓRICO E ANÁLISE

Os trabalhos de auditoria foram iniciados em 22/02/2021, com a emissão da Ordem de Serviço (OS) n. 005/2021. Inicialmente, em 24 de fevereiro de 2021, realizou-se a reunião de abertura dos trabalhos, na sala *https://meet.google.com/gkp-sigi-vvx*, com a presença da Diretora de Tecnologia da Informação, do Coordenador de Infraestrutura e Suporte, do Coordenador de Sistemas de Informação, do Auditor Geral e deste relator. Nessa ocasião, foram apresentados a

[5] ABNT NBR ISO/IEC 27001:2006, p.10 e Manual de Boas Práticas em Segurança da Informação TCU: 2004, p. 11

Ordem de Serviço, o Programa de Auditoria, contendo o escopo do trabalho, os objetivos gerais e específicos, e a Matriz de Planejamento e encaminhados o Mem. IF- UAIG/N.º 6/2021, o qual informa sobre a abertura dos trabalhos, e a SA n. 005/2021, na qual foi solicitada a colaboração da Diretoria de Tecnologia da Informação no fornecimento de informações e documentos relativos às nossas solicitações de auditoria.

Conforme o Programa de Auditoria, as questões que nortearam os exames foram as seguintes:

a) O IFSul possui instituído um Plano de Continuidade do Negócio (PCN)?

b) O PCN apresenta estrutura básica requerida pela norma ABNT NBR ISO/IEC 27002:2007?

c) O PCN foi desenvolvido e implementado para manutenção ou recuperação das operações de modo que assegure a disponibilidade da informação no nível e tempos requeridos, após a ocorrência de falhas ou interrupções dos processos críticos?

d) O PCN é testado e atualizado regularmente, de modo que assegure sua permanente atualização e efetividade?

e) O IFSul possui instituída uma política de *backup* ou de cópias de segurança? No caso de não existir política implementada, existe normativo interno que oriente para os procedimentos de cópias de segurança?

f) São disponibilizados recursos adequados para geração de cópias de segurança?

g) Os serviços e sistemas críticos possuem mecanismos de geração de cópias de segurança que abranjam todos os sistemas de informações, aplicações e dados necessários à completa recuperação do sistema?

h) O IFSul utiliza cópias de segurança de modo que as cópias sejam armazenadas em localidade remota (sistema de redundância), a uma distância segura para escapar de danos de um desastre que possa ocorrer no local principal?

i) O IFSul possui uma Política de Segurança da Informação (PSI) claramente definida, publicada, atualizada e apoiada pelos dirigentes da organização?

j) A DTI realiza o procedimento de inventário de ativos de informação, de maneira que todos esses ativos (dados, *hardware, software* e instalações) estejam inventariados e tenham um proprietário responsável?

k) A DTI disponibiliza do serviço de gestão de incidentes em operação?

l) A DTI realiza gestão de riscos sobre o processo de gestão da segurança da informação?

m) Quais os controles físicos utilizados pela DTI para restrição de acesso as áreas sensíveis à segurança da informação?

n) Quais os controles lógicos utilizados pela DTI para proteção de recursos computacionais?

o) Quais os controles ambientais utilizados pela DTI que visem a proteger e manter os recursos computacionais contra danos provocados por desastres naturais ou falhas estruturais?

p) A DTI possui adequação e suficiência de servidores, terceirizados e estagiários responsáveis ao adequado suporte a infraestrutura de TI?

q) A DTI possui procedimentos padrão documentados em relação às responsabilidades e aos papéis dos profissionais de TI?

r) A DTI possui equipe de desenvolvimento de projetos de infraestrutura de redes lógicas, formalmente constituída? No caso de não haver equipe constituída, esses projetos são contratados? Como ocorrem as etapas de contratação?

s) As contratações de projetos de infraestrutura apresentam processos formais que demonstram as etapas de planejamento das contratações? O planejamento da contratação tem estabelecidos os requisitos técnicos de segurança e Sistema de Gestão de Segurança da Informação?

Na sequência, a Unidade de Auditoria Interna Governamental (UAIG), encaminhou o Mem. IF-UAIG/n. 11/2021, reiterando o prazo exaurido de resposta à solicitação de auditoria inicial. A unidade auditada encaminhou o Mem. IF-DTI/n. 3/2021, justificando o atraso na resposta e solicitando dilação no prazo, sendo atendida por meio do Mem. IF-UAIG/n. 14/2021, ocasião em que foi concedido novo prazo. A DTI encaminhou, para subsidiar a resposta aos questionamentos, o Mem. IF-DTI/n. 4/2021 e seus anexos. Destaca-se que foi necessário o envio de nova solicitação de auditoria para obter esclarecimentos e informações complementares. Diante disso a UAIG encaminhou o Mem. IF-UAIG/n. 47/2021 e que foi reiterado pelo Mem. IF-UAIG/n. 54/2021, uma vez que o prazo de resposta, novamente, não foi atendido. Por fim, a unidade auditada encaminhou por meio do Mem. IF-DTI/n. 10/2021 os esclarecimentos, bem como as informações complementares que possibilitaram o andamento do trabalho de auditoria.

A metodologia utilizada encontra-se detalhada no Programa de Auditoria e consistiu, basicamente, em indagação escrita e oral, análise documental, exame dos registros e diligência.

Salienta-se que, em decorrência da pandemia de Covid-19, não foi possível a realização de diligências. Porém, foram solicitados os registros fotográficos das áreas físicas e equipamentos da DTI, de forma complementar aos questionamentos, como será visto na sequência.

Inicialmente, solicitou-se que fosse informado sobre a **Disponibilidade dos Sistemas** de Tecnologia da Informação. Buscou-se evidenciar a existência de normativos internos que tratam do Plano de Continuidade do Negócio (PCN) e se este se encontra publicado no sítio eletrônico

institucional, se o PCN apresenta a estrutura básica requerida pela norma ABNT NBR ISO/IEC 27002:2007, se o PCN foi desenvolvido e implementado para manutenção ou recuperação das operações de modo que assegure a disponibilidade da informação no nível e tempos requeridos, após a ocorrência de falhas ou interrupções dos processos críticos e se o PCN é testado e atualizado regularmente, de modo que assegure sua permanente atualização e efetividade. Em resposta, a unidade auditada se manifestou conforme segue:

> O IFSUL não possui um plano de continuidade de negócio formalmente instituído. (*sic*)
> Não possuímos um documento, mesmo que informal, de continuidade de negócio. (*sic*)

No que concerne ao ***Backup* de dados**, foi solicitado informar e apresentar, caso possuísse instituída uma política de *backup* ou de cópias de segurança, ou então, normativo interno que oriente para os procedimentos de cópias de segurança. Em resposta, a unidade auditada informou que:

> A instituição não possui uma política de *backups* formalmente instituída, porém, segue rotinas de *backup* diário para os arquivos compartilhados em rede e para as bases de dados com *SGBD MySQL, Postgresql* e *SQL*. *(sic)*
> A instituição não possui normativas internas que orientem a implementação de *backups*. (*sic*)

Nesse sentido, solicitou-se à gestora que informasse sobre como ocorrem essas rotinas de *backup* diário, esclarecendo se ocorrem de modo automatizado, se são supervisionadas por servidores designados e se já houve incidentes por falhas nesses *backups*, ao que foi informado:

> A rotina automatizada de *backup* ocorre diariamente, sem a supervisão de servidor designado. de forma incremental, sem nos servidores de arquivos e nas bases de dados do SUAP, Q-acadêmico e Intranet.
> Já houve incidentes a alguns anos, por falha de software, e assim que o problema foi identificado houve a correção da falha e não houveram mais incidentes. (*sic*)

Adiante, solicitou-se à gestora que informasse se são disponibilizados recursos adequados – Estruturas físicas, de *hardware* e de *software* – para geração de cópias de segurança, ao que foi informado:

> A infraestrutura física atual, em tese poderia permitir a implementação de uma política de *backup* porém é necessário adquirir os *softwares* que permitam acesso aos recursos disponíveis para geração e recuperação das cópias de segurança. (*sic*)

Diante da resposta, solicitou-se à gestora que informasse se já foi providenciada, em algum

momento, a solicitação, justificativa de aquisição e termo de referência para aquisição desses *softwares*, ao que foi respondido:

> Não foi feita solicitação ainda, pois a Coordenadoria de infraestrutura tem outras prioridades e equipe reduzida para a alocação neste projeto, que envolve além do processo de aquisição a apropriação do conhecimento e desenvolvimento e implantação do projeto. (*sic*)

Na sequência, solicitou-se à gestora que informasse se os serviços e sistemas críticos possuem mecanismos de geração de cópias de segurança automatizados que abranjam todos os sistemas de informações, aplicações e dados necessários à completa recuperação do sistema, sendo informado o que segue:

> Temos implantadas rotinas de backup diário para o sistema de arquivos compartilhados em rede; para as bases de dados dos sistemas críticos, tais como SUAP, Intranet e Q-adadêmico. (*sic*)

Também, solicitou-se à gestora que informasse se o IFSul utiliza cópias de segurança de modo que sejam armazenadas em localidade remota (sistema de redundância), a uma distância segura para escapar de danos de um desastre ocorrido no local principal, ao que foi respondido:

> A instituição não possui redundância das cópias de segurança. (*sic*)

De modo complementar a questão, solicitou-se à gestora que informasse se está entre as prioridades da DTI a implantação de um sistema de redundância e quais providências já foram ou estão sendo tomadas nesse sentido, ao que foi respondido:

> A DTI entende que esta é uma demanda urgente, porém, ainda estamos em processo de avaliação das possibilidades, pois podemos escolher entre 2 possibilidades relacionadas a esta demanda. Uma dela seria a implantação de cópias de segurança em nuvem e a segunda seria investir em infraestrutura própria alocada em algum campus do IFSul. Em ambas as alternativas possui um alto custo envolvido. (*sic*)

Finalmente, no que concerne ao *Backup* de dados, foi questionado à gestora se a Diretoria de Tecnologia da Informação tem, entre suas prioridades, a implementação de uma Política de *Backups* e qual o prazo previsto para implementação, ao que foi informado:

> A Diretoria de TI entende a necessidade e importância de implantação da política de *backup*, e pretende incluir nas demandas prioritárias, porém a necessidade de pessoal envolvido nesta atividade acaba inviabilizando o projeto. Principalmente neste momento em que temos um servidor da coordenação em afastamento para doutorado e outro que

está saindo para assumir outro concurso. (*sic*)

Em relação à **Integridade da informação**, questionou-se se IFSul possui uma Política de Segurança da Informação (PSI) claramente definida, publicada, atualizada e apoiada pelos dirigentes da organização. Em resposta, a unidade auditada manifestou-se conforme segue:

> A instituição possui política de segurança aprovada e publicada.
> Sim, a PSI aprovada está aprovada e publicada, porém, necessita ser revisada.
> http://www.ifsul.edu.br/diretorias/diretoria-de-tecnologia-da-informacao/documentos-dti/item/download/21_feecf47ff59d5731451af258b15757e5 (*sic*)

O *link* disponibilizado foi acessado e, também, verificado por consulta na ferramenta de busca na página do sítio eletrônico institucional. Dessa verificação, restou evidenciado que o documento se encontra não atualizado, uma vez que existem alterações regimentais, havendo, inclusive, a exclusão de instâncias administrativas, atualização da legislação vigente, não cumprimento do item 10, restando evidenciado que a Política de Segurança da Informação não passa por revisão, há, pelo menos, 8 anos e sete meses. Segue a transcrição das evidências:

> 3. INSTÂNCIAS ADMINISTRATIVAS
> Para os efeitos desta política e das normas nela originadas, entende-se por
> c) Coordenadoria de Estratégia de Tecnologia (CESTEC): coordenadoria a qual compete incentivar a pesquisa de soluções tecnológicas em todas as áreas de atuação da Diretoria de Tecnologia da Informação e Comunicação, além de acompanhar a implantação de soluções tecnológicas, em todas as áreas de atuação desta Diretoria, atuando junto aos campi para que novas soluções sejam desenvolvidas e propor a padronização para aquisição de equipamentos e contratação de serviços (Art. 76 – Regimento Geral). (*sic*)
>
> 10. REVISÕES E ATUALIZAÇÃO Esta Política será revista anualmente e alterada sempre que as atribuições e normas do IFSul justificarem tais alterações. (*sic*)
>
> Política de Segurança da Informação do IFSul - Versão: 1.07 – dez/2012 (*sic*)

Em relação à prescrição da Política de Segurança da Informação do IFSul, a gestora foi instada a informar se está entre as prioridades da DTI e qual a data prevista para a revisão da Política de Segurança da Informação do IFSul, ao que foi respondido:

> Já estamos com a minuta da política finalizada, para apreciação do CGD. Estamos aguardando a portaria da formalização da nova composição do CGD, conforme aprovação pelo último CONSUP, para submetermos a Política para aprovação.
> Assim que a portaria for publicada, uma reunião do CGD será convocada para a avaliação deste documento. (*sic*)

Solicitou-se à unidade auditada que informasse se a DTI realiza o procedimento de inventário de ativos de informação, de maneira que todos esses ativos (dados, *hardware*, *software*

e instalações) estejam inventariados e tenham um proprietário responsável. Em resposta, a unidade auditada manifestou-se conforme segue:

> A DTI possui inventário de dados e softwares, e estes estão vinculados a um responsável. Porém, o inventário de dados não é realizado. (*sic*)

A resposta apresentada deixou dúvida e não esclarece o ponto. Diante disso, solicitou-se à gestora que informasse com maior clareza se é ou não realizado o inventário de dados de modo que não se tenha dúvidas na resposta. Nesse sentido, a unidade auditada manifestou-se conforme segue:

> A resposta foi dada de forma equivocada. O IFSul não possui inventário de dados. Acabamos fazendo uma interpretação equivocada da questão e respondemos considerando o inventário de bens e softwares. (*sic*)

Outra questão de auditoria buscou verificar se a DTI disponibiliza o serviço de gestão de incidentes em operação, evidenciando as etapas de recebimento, filtragem, classificação e resposta aos alertas, bem como a verificação da existência do procedimento de análise dos incidentes de segurança e se estes são efetivamente tratados. Em resposta, a unidade auditada manifestou-se conforme segue:

> A DTI não possui um plano de gestão de incidentes formalmente publicado. No entanto, busca atender incidentes na medida que eles são detectados. Quando isso ocorre a situação é investigada por alguém da equipe designado para essa tarefa e que busca compreender melhor o incidente a fim de mitigar o problema e buscar evitar que o mesmo se repita. (*sic*)

Sendo a área de tecnologia da informação estratégica para gestão do IFSul, uma vez que toda a informação institucional (acadêmica, administrativa, pessoal, entre outras), encontra-se armazenada em bancos de dados, solicitou-se à unidade auditada que informasse se realiza gestão de riscos sobre o processo de gestão da segurança da informação, demonstrando como é realizada, em caso afirmativo, ao que foi respondido:

> A DTI não possui uma política de gestão de riscos formalmente publicada, porém, realiza a gestão dos riscos..... (*sic*)

Diante da resposta encaminhada, aprofundou-se a questão, solicitando-se informar se a gestora considera estratégico o papel da gestão de riscos sobre o processo de gestão da segurança da informação, ao que foi respondido:

> Sim, considero estratégica e importante a gestão de riscos, principalmente em um ambiente de missão crítica como o DC da instituição. Neste sentido, a elaboração da política de gestão de riscos está nas nossas demandas. Porém, devido ao quando reduzido de pessoal, estamos com uma certa dificuldade. (*sic*)

Nesse sentido, solicitou-se que informasse se está entre as prioridades da DTI e qual data prevista para implementação do processo de gestão de riscos, uma vez que consta das Diretrizes Gerais da Política de Segurança da Informação que será estabelecido um processo de gestão de riscos. Decorridos 8 anos e 5 meses da instituição do PSI do IFSul (na data do envio da SA 005-A/2021), ainda não há processo de gestão de riscos instituída. Em resposta, a unidade auditada manifestou-se conforme segue:

> Embora considere de extrema importância, não estamos conseguindo absorver esta demanda, frente ao montante de demandas urgentes que ocorrem, principalmente levando em consideração o número reduzido da equipe. (*sic*)

Por fim, solicitou-se que a gestora esclarecesse a informação, descrevendo-a: "a DTI não possui uma política de gestão de riscos formalmente publicada, porém, realiza a gestão dos riscos....", ao que foi respondido:

> O SISP, órgão setorial sob o qual a área de TI está vinculada, define alguns norteadores que devem ser implementados no âmbito do governo federal e a DTI segue dentro de suas possibilidades as orientações enviadas. (*sic*)

A resposta final apresentada pela unidade auditada não esclareceu o ponto, restando evidenciada a não realização da gestão de riscos dos processos internos da Diretoria de Tecnologia da Informação.

Na sequência, solicitou-se que informasse quais os controles físicos utilizados pela DTI para restrição de acesso de servidores as áreas sensíveis à segurança da informação, ao que foi respondido:

> O datacenter da instituição possui um sistema de controle de acesso por biometria. (*sic*)

De modo complementar e devido à dificuldade de realização de diligência, solicitou-se que fosse apresentado registro fotográfico do sistema de controle de acesso por biometria ao *datacenter*. A unidade auditada encaminhou o registro fotográfico com cinco imagens. Anexamos a este Relatório quatro imagens que evidenciam o controle de acesso ao *datacenter*, por meio de biometria, conforme segue:

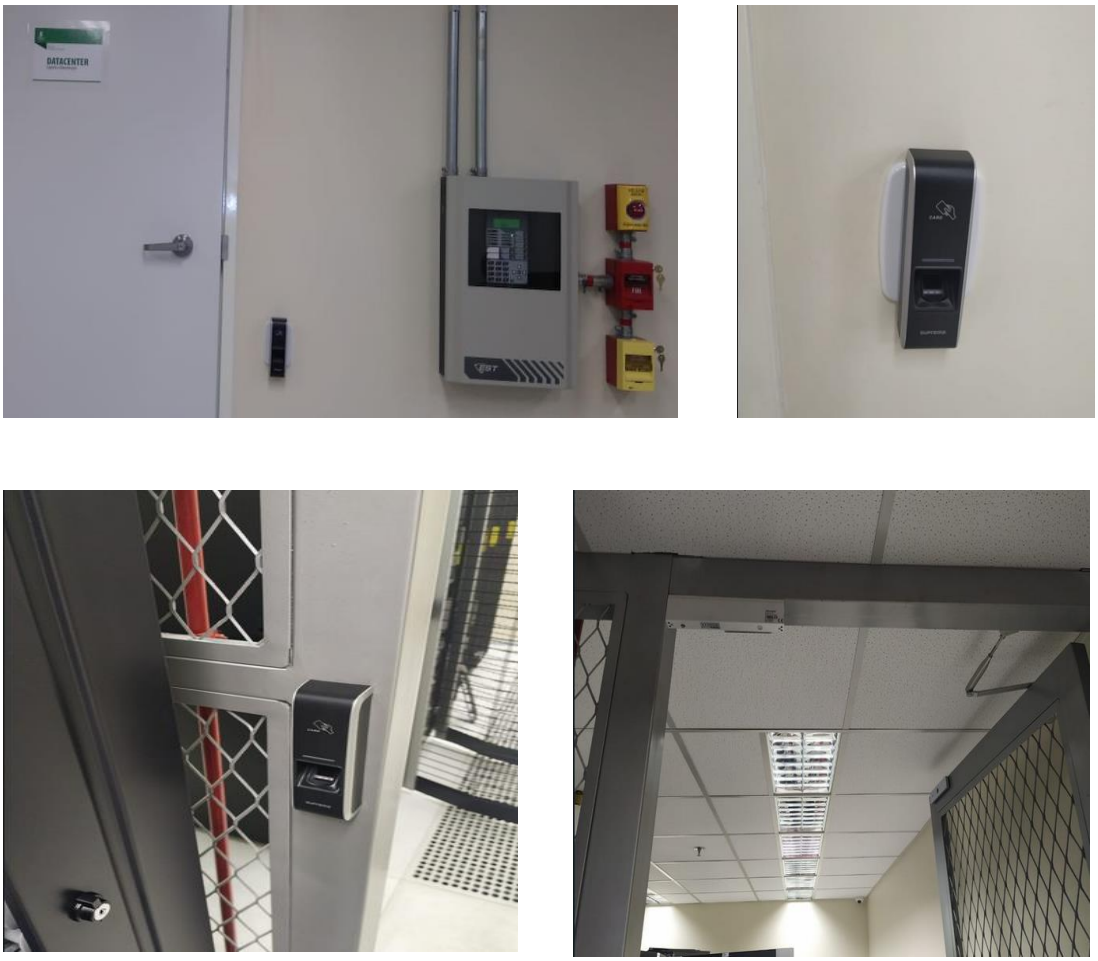


Figura 1 – Sistema de biometria instalado junto às portas externa e interna do *Datacenter*. Fonte: Diretoria de Tecnologia da Informação.

No que concerne aos controles lógicos utilizados pela DTI para a proteção de recursos computacionais, solicitou-se que informasse quais os existentes, ao que foi respondido:

> Utilização de usuário e senha (pessoal e intransferível), associados a diferentes tipos de permissões de acesso aos recursos.
> Utilização de firewall geral da rede e específico em algumas máquinas que contém aplicações.
> Utilização de sistema para atualizações de segurança de servidores e computadores (*sic*)

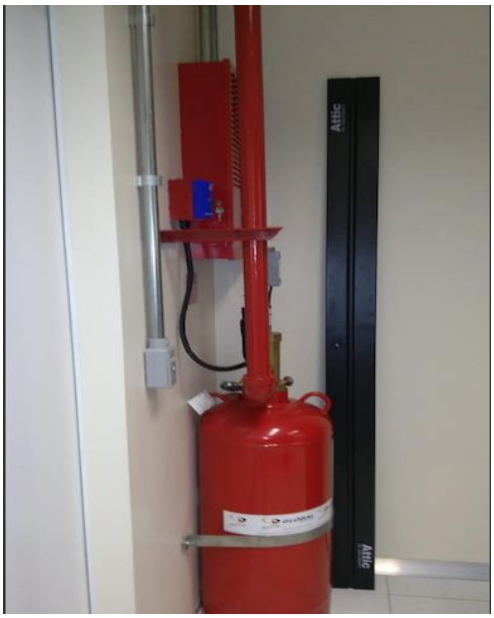
Por fim, em relação aos controles aplicados à **Integridade da Informação**, solicitou-se informar quais os controles ambientais (sistemas de energia, refrigeração, detecção e supressão de água e fogo, redundância e cópias de segurança), utilizados pela DTI, que visem a proteger e manter os recursos computacionais contra danos provocados por desastres naturais ou falhas estruturais. Em resposta, a unidade auditada manifestou-se conforme segue:

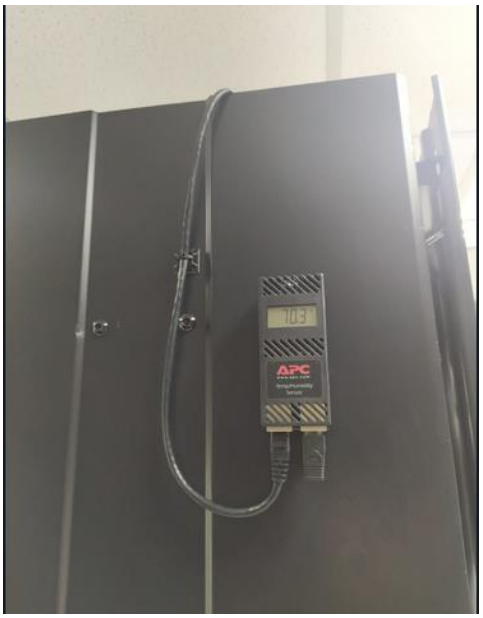
> Sistema de climatização com controle preciso de temperatura;
> Controle de partículas em dispersão;

Sistema de detecção de incêndio – Combate e detecção;
Sistema de energia - Sistema de Nobreaks – UPS
Sistema de piso elevado (*sic*)

Solicitou-se que fosse apresentado registro fotográfico dos sistemas de controles ambientais, com a respectiva descrição, utilizados pela DTI, obtendo-se, como resposta, o que segue:

> Sistema de Detecção e Alarme de Incêndio conjugado com um sistema fixo automático de Combate de Incêndio por gás FM200 e Sistema de Detecção Precoce de Incêndio (HSSD) para a proteção patrimonial e a seguridade das áreas integrantes do Datacenter, fornecendo proteção para o ambiente, entrepiso e entreforro.
> O sistema é dotado de detectores de fumaça que trabalham em conjunto com um sistema de detecção por aspiração de alta sensibilidade – HSSD (High Sensitivity Smoke Detector) na identificação rápida e segura do princípio de incêndio. Com base nas informações dos sensores citados, a central de incêndio deverá tomar a decisão sobre o início do processo de combate.
> O processo de combate é semi-automático, inclui uma seqüência de eventos pré-programados que inclui:
> - O aviso aos ocupantes e áreas adjacentes através de sirenes multitonais e sinalizadores visuais do tipo strobe;
> - Desligamento de máquinas de ar-condicionado (opcional);
> - Atuação sobre o controle de acesso das salas;
> - Ativação do solenóide de liberação do gás do cilindro de FM-200.
> - Comunicação via sistema de monitoramento ambiental do evento ocorrido.
>
> O sistema será dotado ainda de acionamento manual direto no cilindro de FM-200, permitindo a atuação manual/mecânica do sistema, mesmo que ocorra pane total do sistema elétrico/eletrônico. O Painel Central do Sistema de Detecção e Combate de Incêndio está interligado ao Sistema de Monitoramento Ambiental do Datacenter. Sendo que o sinal deverá ser disponibilizado por contato seco do tipo NA/NF. O Sistema de Monitoramento Ambiental é programado para informar aos usuários cadastrados quando ocorrer uma detecção de incêndio ou falha do sistema. (*sic*)





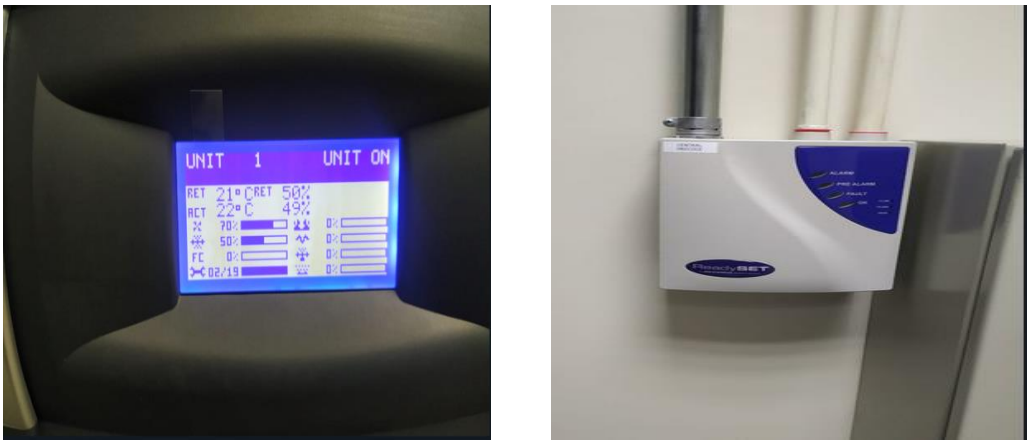


Figura 2 – Sistema de combate a incêndio, instalado para proteção do *Datacenter*. Fonte: Diretoria de Tecnologia da Informação.

Embora a unidade auditada tenha informado a existência dos sistemas de controles ambientais, conforme citado (sistema de climatização com controle preciso de temperatura; controle de partículas em dispersão; sistema de detecção de incêndio – combate e detecção; sistema de energia – sistema de *nobreaks* – UPS e sistema de piso elevado), foi apresentada à UAIG apenas a descrição e o registro fotográfico do sistema de detecção e combate de incêndio. Desse modo, registra-se a incompletude da informação oferecida à SA n. 005-A/2021.

No que tange ao **Suporte à estrutura física**, solicitou-se informar se a DTI possui adequação e suficiência de servidores, terceirizados e estagiários responsáveis ao adequado suporte a infraestrutura de TI. Em resposta, a unidade auditada manifestou-se conforme segue:

> A equipe da DTI é muito reduzida, não temos nenhum servidor da área de governança, não temos uma equipe de especialistas em segurança da informação e não temos uma equipe responsável pelas aquisições e contratações. A estrutura é muito enxuta, não possibilitando o atendimento de todas as demandas de forma adequada. A estrutura é composta pela diretoria, onde tem somente a diretora lotada e 2 coordenações, uma de sistemas e outra de infraestrutura.
> - A coordenação de sistemas é responsável pela manutenção/adequação/ajustes em todos os sistemas do IFSul, além da gestão das ferramentas que disponibilizamos e da gestão de contratos que ainda são mantidos. É responsável também pela implementação de novas soluções para atender demandas dos câmpus e da reitoria.
> A equipe é composta pelo coordenador, 4 analistas de tecnologia da informação e 2 técnicos de tecnologia da informação.
> - A coordenação de infraestrutura é responsável pela manutenção do datacenter; troca/manutenção/aquisição de equipamentos; responsável também pela contratação e gestão de contratos de diversos serviços; responsável pela gestão dos dados; responsável por atender incidentes de segurança; responsável por disponibilizar e manter atualizados sistemas de software para uso do público interno e externo.
> A equipe é composta pelo coordenador 4 analistas de tecnologia da informação, sendo que um está em afastamento para doutorado por 4 anos e 1 técnico de tecnologia da informação.
> Neste sentido, podemos afirmar que a equipe não é suficiente para o atendimento às demandas e manutenção da conformidade da área de Tecnologia da Informação. (*sic*)

Não obstante a inadequação e a insuficiência de servidores, terceirizados e estagiários responsáveis ao adequado suporte a infraestrutura de TI, solicitou-se à unidade auditada que informasse se os papéis dos profissionais de TI possuem procedimentos padrão documentados em relação às responsabilidades de cada um dos recursos humanos alocados nessa área, ao que foi respondido:

> As responsabilidades são definidas regimentalmente e pela própria estrutura dos cargos do plano de carreira. (*sic*)

Diante da resposta apresentada, evidencia-se, ao observar o Regimento Interno do IFSul, que as competências relacionadas a garantir a segurança e integridade das informações, zelar pela Política de Segurança da Informação e seus regulamentos e coordenar ações para promover a Política de Segurança da Informação no IFSul estão concentradas na Diretoria da Tecnologia da Informação.

No que se refere à descrição dos cargos do PCCTAE, foram analisados os cargos de Técnico de Tecnologia da Informação (Nível médio – D / Código CBO 3171-10) e Analista de Tecnologia da Informação (Nível superior – E / Código CBO 2124-05). A análise recaiu sobre competências relacionadas à segurança da informação, os cargos possuem uma descrição sumária e outra descrição de atividades típicas do cargo. Em relação ao cargo de Técnico em TI, não foram encontradas tais competências. Já em relação ao cargo de Analista de TI, há, nas descrições de atividades típicas do cargo, competências que mantêm relação com a segurança da informação, conforme segue:

> Cargo: Analista de Tecnologia da informação
> Nivel: E – Superior
> Descrição de atividades típicas do cargo:
> • Administrar ambiente informatizado:
> Monitorar performance do sistema; administrar recursos de rede ambiente operacional, e banco de dados; executar procedimentos para melhoria de performance de sistema; identificar falhas no sistema; corrigir falhas no sistema; controlar acesso aos dados e recursos; administrar perfil de acesso às informações; realizar auditoria de sistema. (*sic*)

Porém, a norma ABNT NBR ISO/IEC 27002:2005 orienta para que os papéis e responsabilidades pela segurança da informação de funcionários, fornecedores e terceiros sejam definidos e documentados de acordo com a Política de Segurança da Informação da organização. Nesse caso, não há documento que expresse os papéis e responsabilidades dos profissionais de TI envolvidos com a segurança da informação. Além disso, a PSI do IFSul encontra-se desatualizada.

Por fim, questionou-se sobre **Projetos de infraestrutura lógica**, solicitando informar se a DTI possui equipe de desenvolvimento de projetos de infraestrutura de redes lógicas, formalmente constituída, ao que foi respondido:

> Não possuímos equipe de desenvolvimento de projetos de infraestrutura de redes lógicas e não existem servidores com qualificação técnica para exercer esta atribuição. (*sic*)

Diante disso, solicitou-se informar se as contratações de projetos de infraestrutura apresentam processos formais que demonstram as etapas de planejamento das contratações e se são considerados e ou estabelecidos os requisitos técnicos de segurança e Sistema de Gestão de Segurança da Informação, obtendo-se a seguinte resposta:

> O processo de contratação e planejamento da contratação de TI é regulado pela Instrução Normativa 01/2019, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação. (*sic*)

Neste contexto da análise das informações prestadas pela unidade auditada, em observância ao Regimento Geral, aos normativos que tratam da Infraestrutura de Tecnologia da Informação (disponibilidade de sistemas, *backup* de dados, integridade da informação, suporte à estrutura física, projetos de infraestrutura lógica), conclui-se pela existência de competências regimentais que abarcam etapas de gestão da segurança da informação na instituição. Todavia, verifica-se a presença de fragilidades no estabelecimento de normativos acerca de um plano de continuidade de negócio, ausência de uma política de *backups*, ausência de normativos internos que orientem a implementação de *backups*, falta de *softwares* que permitam implementar uma política de *backup*, falta de redundância, em local remoto, das cópias de segurança, sendo o armazenamento realizado somente no *datacenter* da Reitoria. Além disso, a Política de Segurança da Informação encontra-se desatualizada, inexiste procedimento de inventário de ativos de informação, não há um plano de gestão de incidentes formalmente publicado, somado a um quadro de servidores insuficientes para atender as demandas e manutenção da conformidade da área de tecnologia da informação.

3 ACHADOS DE AUDITORIA

3.1 CONSTATAÇÃO

A Diretoria de Tecnologia da Informação não possui um plano de continuidade de negócio formalmente instituído.

3.1.1 Critério

Norma ABNT NBR ISO/IEC 27002:2005 (p. 105)

Manual de Boas Práticas em Segurança da Informação / Tribunal de Contas da União (p. 99)

3.1.2 Evidências

Mem. IF-DTI/n. 4/2021 e 5/2021 e seus anexos, item 1.

3.1.3 Causa

Não implementação do Plano de Continuidade de Negócios previsto na Norma Técnica Brasileira.

Fragilidades na distribuição da força de trabalho na área de TI entre a Reitoria e os câmpus do IFSul.

3.1.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> A Diretoria de TI tem consciência da necessidade da elaboração deste documento, neste sentido, estamos com uma minuta em fase de finalização para enviar ao CGD para discussão e ajustes.
> O Principal fator que contribui para a situação evidenciada é o tamanho da equipe de TI, que é muito reduzida, levando em consideração todas as demandas que são absorvidas por esta diretoria. A DTI necessita de uma equipe de Governança, a fim consolidar a governança de TI institucional e colocar a instituição em conformidade, levando em consideração as melhores práticas e as normativas existentes. Além disso, existe a necessidade ainda de uma equipe de segurança da informação, constituída e capacitada.
> O próprio guia de boas práticas de segurança da informação do TCU, na página 35 enfatiza a necessidade de criação de uma equipe de segurança da informação conforme segue:
> "A alta administração deve designar uma equipe de segurança especifica para elaboração, implementação, divulgação, treinamento, testes, manutenção e coordenação do Plano de Continuidade do Negócio." (*sic*)

3.1.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado

de auditoria. De fato, observou-se que a DTI possui um quadro de servidores enxuto, apesar das diversas demandas a serem atendidas, entre estas, as de segurança da informação. Apesar disso, a gestora informa que o plano está em fase de finalização. Convém destacar o caráter estratégico da segurança da informação para a gestão do IFSul. Diante disso, mantém-se a constatação.

3.1.6 Recomendações

Recomenda-se à Diretora de Tecnologia da Informação que providencie a aprovação do Plano de Continuidade de Negócios do IFSul e que dê ampla publicidade no âmbito institucional.

3.2 CONSTATAÇÃO

A instituição não possui uma política de *backup* ou de cópias de segurança formalmente instituída.

3.2.1 Critério

Norma ABNT NBR ISO/IEC 27002:2013 (p. 62)

Manual de Boas Práticas em Segurança da Informação / Tribunal de Contas da União (p. 73)

3.2.2 Evidências

Mem. IF-DTI/n. 4/2021 e 5/2021 e seus anexos, itens 5 a 8 e itens 2 e 3, respectivamente.

3.2.3 Causa

Fragilidades na distribuição da força de trabalho na área de TI entre a Reitoria e os câmpus do IFSul.

Insuficiência de conhecimentos técnicos específicos na área de *backups.*

3.2.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> Da mesma forma que a resposta anterior, é impossível não enfatizar, que o tamanho da equipe seja o fator mais relevante para justificar as constatações evidenciadas na auditoria. Outro fator importante é a necessidade de termos uma equipe responsável pela segurança da informação constituída e capacitada. Atualmente a Coordenação de infraestrutura possui em seu quadro 1 coordenador e 5 servidores, e destes 2 estão afastados para o doutorado.
> Conhecemos a necessidade da termos uma política de Backups, neste sentido, estamos com uma minuta sendo elaborada para enviar ao CGD para discussão e ajustes. (*sic*)

3.2.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado de auditoria. De fato, observou-se que a DTI possui um quadro de servidores enxuto, apesar das diversas demandas a serem atendidas, entre estas, as de segurança da informação. Apesar disso, a gestora informa que a política de *backups* está em vias de aprovação. Convém destacar o caráter estratégico da segurança da informação para a gestão do IFSul e, em especial, as questões referentes aos *backups* e cópias de segurança, uma vez que toda a informação institucional está armazenada e concentrada nos servidores de dados da Reitoria. Diante disso, mantém-se a constatação.

3.2.6 Recomendações

3.2.6.1 Recomenda-se à Diretora de Tecnologia da Informação que providencie a aprovação da Política de *backups* e cópias de segurança no âmbito do IFSul e que dê ampla publicidade no âmbito institucional.

3.2.6.2 Recomenda-se à Diretora de Tecnologia da Informação que providencie e promova a criação de um núcleo de segurança da informação e que busque a composição desse núcleo por meio dos diversos servidores existentes nas áreas de TI de todo o IFSul.

3.6.2.3 Recomenda-se à Diretora de Tecnologia da Informação que providencie e promova a capacitação dos integrantes do núcleo de segurança da informação com conhecimentos técnicos específicos na área de *backups* e cópias de segurança.

3.3 CONSTATAÇÃO

A Diretoria de Tecnologia da Informação não possui redundância das cópias de segurança em local remoto.

3.3.1 Critério

Norma ABNT NBR ISO/IEC 27002:2013 (p. 63)

Manual de Boas Práticas em Segurança da Informação / Tribunal de Contas da União (p. 74)

3.3.2 Evidência

Mem. IF-DTI/n. 4/2021 e 5/2021 e seus anexos, item 8 e item 4, respectivamente.

3.3.3 Causa

Insuficiência de recursos necessários à implementação de um sistema de *backup* redundante em relação às necessidades de maior urgência em matéria de TI.

3.3.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> Para viabilizarmos a manutenção de redundância de segurança, seria necessário que investíssemos um infraestrutura em outro campus, Pois atualmente nenhum dos nossos campus possui infraestrutura compatível com a demanda que seria necessária.
> A Diretoria de TI não possui recursos de investimento. O ideal seria criarmos um centro de custo direcionado a investimento de TI. Isso conduziria a uma possibilidade de organização interna, levando a um planejamento dos investimentos. Facilitando a alocação de recursos para projetos com esta finalidade. (*sic*)

3.3.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado de auditoria. Informa que carece de recursos para possibilitar a criação de infraestrutura. Quando questionada por meio de solicitação de auditoria, informou que, apesar da escassez de recursos, está seria uma demanda urgente. Convém destacar o caráter estratégico da segurança da informação para a gestão do IFSul e, em especial, as questões referentes aos *backups* e cópias de segurança, uma vez que toda a informação institucional está armazenada e concentrada nos

servidores de dados da Reitoria. Diante disso, mantém-se a constatação.

3.3.6 Recomendação

Recomenda-se à Diretora de Tecnologia da Informação que proponha e promova, junto ao Senhor Reitor e Diretores-gerais de câmpus, a criação de centro de custos da área de TI com o objetivo de redistribuir recursos orçamentários da Reitoria e dos câmpus do IFSul em prol da segurança da informação institucional.

3.4 CONSTATAÇÃO

A Política de Segurança da Informação do IFSul (versão 1.07 – dez/2012) encontra-se desatualizada.

3.4.1 Critério

Norma ABNT NBR ISO/IEC 27002:2013 (p. 8 e 9)

Manual de Boas Práticas em Segurança da Informação / Tribunal de Contas da União (p. 9)

3.4.2 Evidências

Mem. IF-DTI/n. 4/2021 e 5/2021 e seus anexos, itens 9 e 10 e item 5, respectivamente.

3.4.3 Causa

Não priorização da atualização da Política de Segurança da Informação do IFSul.

3.4.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> A política de segurança da informação do IFSul foi elaborada e publicada em 2012, e considerando as melhores práticas de segurança da informação deve ser atualizada, para atender as Normas e as melhores práticas na segurança da informação. No entanto, desde sua publicação não houve atualização. Evidenciamos isso assim que assumimos a atual

> gestão em 2017, porém, os mesmo fatores levantados nas respostas anteriores, não nos permitiram ainda elaborar uma nova política. Também conforme as anteriores, estamos construindo uma minuta de política de segurança da informação para encaminhar ao CGD. (*sic*)

3.4.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado de auditoria. De fato, observou-se que a atual gestão da DTI recebeu o documento desatualizado. Entretanto, apesar de decorridos quatro anos, não houve providências em reestabelecer a vigência e validação da Política de Segurança da Informação. A UAIG entende que não carece construir uma nova política e sim promover a atualização da existente, de acordo com a evolução das normas que se encontram vigentes, bem como a atualização das estruturas de TI existentes e suas competências regimentais. Diante disso, mantém-se a constatação.

3.4.6 Recomendação

Recomenda-se à Diretora de Tecnologia da Informação que promova a atualização da Política de Segurança da Informação do IFSul e que dê ampla publicidade no âmbito institucional.

3.5 CONSTATAÇÃO

A Diretoria de Tecnologia da Informação não realiza o procedimento de inventário de ativos de informação (dados, *hardware*, *software* e instalações).

3.5.1 Critério

Norma ABNT NBR ISO/IEC 27002:2013 (p. 23).

Manual de Boas Práticas em Segurança da Informação / Tribunal de Contas da União (p. 58)

3.5.2 Evidência

Mem. IF-DTI/n. 4/2021 e 5/2021 e seus anexos, item 11 e item 6, respectivamente.

3.5.3 Causa

Fragilidades na distribuição da força de trabalho na área de TI entre a Reitoria e os câmpus do IFSul.

3.5.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> A Diretoria de TI realiza apenas inventário de hardwares e softwares, pois estes constituem o patrimônio institucional, sendo assim, possuem registro e são atribuídos a um responsável.
> No caso de dados, ainda não houve tempo e pessoal disponível para realizar o mapeamento dos dados institucionais. (*sic*)

3.5.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado de auditoria. Observou-se que a DTI possui um quadro de servidores enxuto e que possui diversas demandas a serem atendidas, entre estas, as de segurança da informação e, por conseguinte, o levantamento e registro dos dados produzidos e armazenados diariamente pela instituição. Convém destacar o caráter estratégico da segurança da informação para a gestão do IFSul. Diante disso, mantém-se a constatação.

3.5.6 Recomendação

Recomenda-se à Diretora de Tecnologia da Informação que promova a realização dos inventários de ativos de informação (dados, *hardware*, *software* e instalações) no âmbito do IFSul.

3.6 CONSTATAÇÃO

A Diretoria de Tecnologia da Informação não possui um planejamento para a gestão de incidentes de segurança da informação.

3.6.1 Critério

Norma ABNT NBR ISO/IEC 27002:2013 (p. 23)

Manual de Boas Práticas em Segurança da Informação / Tribunal de Contas da União (p. 95)

3.6.2 Evidências

Mem. IF-DTI/n. 4/2021 e seus anexos, item 12.

3.6.3 Causa

Fragilidades na distribuição da força de trabalho na área de TI entre a Reitoria e os câmpus do IFSul.

3.6.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> Da mesma forma que as respostas dadas anteriormente, o principal fator que afeta a DTI é o tamanho da equipe, justificando as constatações evidenciadas na auditoria. Outro fator importante é a necessidade de termos uma equipe responsável pela segurança da informação constituída e capacitada. Atualmente a Coordenação de infraestrutura possui em seu quadro 1 coordenador e 5 servidores, e destes 2 estão afastados para o doutorado. (*sic*)

3.6.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado de auditoria. De fato, observou-se que a DTI possui um quadro de servidores enxuto e que possui diversas demandas a serem atendidas, entre estas, as de segurança da informação. Convém destacar o caráter estratégico da segurança da informação para a gestão do IFSul e, em especial, as questões referentes ao estabelecimento de um planejamento para a gestão de incidentes de segurança da informação. Diante disso, mantém-se a constatação.

3.6.6 Recomendação

Recomenda-se à Diretora de Tecnologia da Informação que promova a realização de planejamento para a gestão dos riscos de incidentes de segurança da informação.

3.7 CONSTATAÇÃO

A Diretoria de Tecnologia da Informação não realiza gestão de riscos sobre o processo de gestão da segurança da informação.

3.7.1 Critério

Norma ABNT NBR ISO/IEC 27005:2011

3.7.2 Evidências

Mem. IF-DTI/n. 4/2021 e 5/2021 e seus anexos, item 13 e item 7, respectivamente.

3.7.3 Causa

Não priorização da realização de gestão de riscos sobre os processos de Gestão da Segurança da Informação.

3.7.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> A gestão de riscos de segurança da informação está sendo abordada na elaboração da minute de política de segurança da informação que está em fase de elaboração. (*sic*)

3.7.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado de auditoria. A gestora informa que a gestão de riscos de segurança da informação está contemplada na Política de Segurança da Informação e que esta se encontra em elaboração. Orienta-se a gestora que realize o inventário dos processos internos e externos a sua diretoria e que observe, na elaboração da gestão de riscos, as seguintes etapas: mapeamento dos processos,

identificação dos pontos críticos de controle, estabelecimento de controles internos necessários para garantir a segurança das informações e teste de efetividade dos controles internos.

Novamente, destaca-se o caráter estratégico da segurança da informação para a gestão do IFSul e, em especial, as questões referentes à gestão dos riscos envolvidos na área de TI, uma vez que toda a informação institucional está armazenada e concentrada nos servidores de dados da reitoria. Diante disso, mantém-se a constatação.

3.7.6 Recomendação

Recomenda-se à Diretora de Tecnologia da Informação que implemente a gestão de riscos do processo de gestão da segurança da informação.

3.8 CONSTATAÇÃO

A Diretoria de Tecnologia da Informação possui equipe insuficiente para o adequado suporte à infraestrutura de TI.

3.8.1 Critério

Norma ABNT NBR ISO/IEC 27002:2013 (p. 17).

Manual de Boas Práticas em Segurança da Informação / Tribunal de Contas da União (p. 64)

3.8.2 Evidências

Mem. IF-DTI/n. 4/2021 e seus anexos, item 17.

3.8.3 Causa

Fragilidades na distribuição da força de trabalho na área de TI entre a Reitoria e os câmpus do IFSul.

3.8.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> Atualmente a Coordenação de infraestrutura, que trabalha diretamente com as questões relacionadas a segurança possui em seu quadro Além do coordenador, mais 5 servidores, sendo que destes 2 estão afastados para o doutorado. Com estes 4 servidores está toda a manutenção dos serviços institucionais, tais como portal, Intranet, SUAP, entre outros, além de atividades como:
>
> - Rotinas de Backup;
> - Segurança (Sistemas, BD, Rede...);
> - Contratações de bens e serviços de TI;
> - Gestão e manutenção do serviço de e-mail institucional;
> - Serviço de autenticação CAFÉ - Disponibiliza acesso a vários serviços;
> - Modele nas nuvens – RNP;
> - Plataforma Mundo - EaD
> - Conectividade;
> - Suporte – Reitoria.
>
> Considerando o Manual de boas práticas de segurança da informação elaborado pelo TCU orienta, que a instituição constitua uma equipe de segurança da informação, conforme segue:
> "A alta administração deve designar uma equipe de segurança especifica para elaboração, implementação, divulgação, treinamento, testes, manutenção e coordenação do Plano de Continuidade do Negócio."
> Com o quadro e as demandas que são absorvidas pela Coordenação de infraestrutura, não existe viabilidade para que todas as atribuições necessárias para a conformidade com a segurança da informação seja mantida, a menos que toda a equipe, ou seja 4 pessoas ficassem exclusivamente trabalhando com foco em segurança da informação. (*sic*)

3.8.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado de auditoria. De fato, observou-se que a DTI possui um quadro de servidores enxuto e que possui diversas demandas a serem atendidas, entre estas, as de segurança da informação. Convém destacar o caráter estratégico da segurança da informação para a gestão do IFSul e, em especial, as questões referentes ao Plano de Continuidade de Negócios, *backups* e cópias de segurança, uma vez que toda a informação institucional está armazenada e concentrada nos servidores de dados da Reitoria. Diante disso, mantém-se a constatação.

3.8.6 Recomendação

Recomenda-se à Diretora de Tecnologia da Informação que diligencie junto ao Senhor Reitor, dando ciência de situação critica enfrentada e da urgente necessidade de atendimento aos normativos e orientações emanadas pelo próprio TCU em relação à estrutura de equipe para tratar das questões de segurança da informação.

3.9 CONSTATAÇÃO

A Diretoria de Tecnologia da Informação não possui documentos que estabeleçam os papéis e responsabilidades pela segurança da informação de servidores, fornecedores e terceiros, de acordo com a Política de Segurança da Informação.

3.9.1 Critério

Norma ABNT NBR ISO/IEC 27002:2005 (p. 11)

Manual de Boas Práticas em Segurança da Informação / Tribunal de Contas da União (p. 65)

3.9.2 Evidências

Mem. IF-DTI/n. 4/2021 e seus anexos, item 18.

3.9.3 Causa

Não priorização da atualização da Política de Segurança da Informação do IFSul e da gestão de riscos sobre os processos de gestão da segurança da informação.

3.9.4 Manifestação da gestora

A Diretora de Tecnologia da Informação manifestou-se nos seguintes termos:

> Levando em consideração todas as questões abordadas em todas as respostas, referente a pessoal, fica inviável definir responsabilidades e papeis considerando o tamanho da nossa equipe. Ainda assim, a definição de alguns papéis e responsabilidades está dentro do escopo da política de segurança da informação e da política de backup, que estão em fase de elaboração. Neste sentido, entende-se que na prática, em níveis institucionais, papéis e responsabilidades de segurança serão designadas como tarefas como por exemplo, na política de backup será definido o início do backup em uma determinada hora do dia. Estas tarefas deveriam ser dadas a pessoas que já estão provavelmente fazendo-as, só que agora estes papéis e responsabilidades serão mais formais.
> No meu entendimento então, não há necessidade de ter um documento que definiria de forma central todos os papéis e responsabilidades em detalhes. Tal documento não seria prático por conta da redundância. No momento em que alguma mudança ocorra em algum papel ou responsabilidade em um procedimento em particular, seria necessário mudar isso também neste documento central. Mais cedo ou mais tarde, uma discrepância poderia ocorrer, causando inconsistência. (*sic*)

3.9.5 Análise da manifestação

A Diretora de Tecnologia da Informação manifesta-se no sentido de corroborar o achado de auditoria. De fato, observou-se que a DTI possui um quadro de servidores enxuto e que possui diversas demandas a serem atendidas, entre estas, as de segurança da informação. Entretanto, esta Unidade de Auditoria Interna Governamental observa, na execução de seu trabalho, o contido nas normas técnicas e manuais de orientações, a partir da implementação de um conjunto de controles adequados, incluindo políticas, processos, procedimentos, estruturas de pessoal, de *hardware* e de *software* que garantam e suportem a sua Política de Segurança da Informação.

Entende-se que os documentos que estabeleçam os papéis e responsabilidades pela segurança da informação de servidores, fornecedores e terceiros, de acordo com a Política de Segurança da Informação seja uma boa prática de gestão e fundamental para apurar responsabilidades nos casos de colapsos, falhas ou extravio de informações.

Convém destacar o caráter estratégico da segurança da informação para a gestão do IFSul e, em especial, as questões referentes ao Plano de Continuidade de Negócios, *backups* e cópias de segurança, uma vez que toda a informação institucional está armazenada e concentrada nos servidores de dados da Reitoria. Diante disso, mantém-se a constatação.

3.9.6 Recomendação

Recomenda-se à Diretora de Tecnologia da Informação que promova a elaboração de documentos que estabeleçam os papéis e responsabilidades pela segurança da informação de servidores, fornecedores e terceiros, de acordo com a Política de Segurança da Informação.

4 CONCLUSÃO

O presente trabalho de auditoria voltou-se a avaliar a conformidade dos procedimentos e a adequação e suficiência dos controles internos administrativos quanto à Infraestrutura de Tecnologia da Informação e a gestão da Diretoria de Tecnologia da Informação nos aspectos referentes à segurança da informação.

Por meio da avaliação de conformidade, buscou-se verificar a adequada aderência da Diretoria de Tecnologia da Informação aos normativos e manuais de orientação referentes às boas práticas em segurança da informação vigentes.

Evidencia-se fragilidades por meio das constatações exaradas no Relatório, as quais carecem de observação e atenção por parte dessa Diretoria, uma vez que o negócio da área de TI possui caráter estratégico para a gestão do IFSul.

Dessa forma, verifica-se a necessidade da atuação efetiva da Diretoria de Tecnologia da Informação sobre as questões referentes à Política de Segurança da Informação, ao Plano de Continuidade de Negócios, Políticas de *backups* e cópias de segurança, recomposição e adequação do quadro permanente de servidores dessa unidade sistêmica e que atenda ao IFSul em sua totalidade, uma vez que toda a informação institucional está armazenada e concentrada nos servidores de dados da Reitoria.

Diante do exposto, encaminha-se o presente Relatório de Auditoria para que a gestora tome ciência das recomendações, salientando que o não cumprimento destas implica na aceitação dos riscos pela gestora e a sua implementação será, no futuro, objeto de avaliação por esta Unidade de Auditoria Interna Governamental.

Pelotas, 30 de agosto de 2021

HENRIQUE ZIGLIA MAIA,
Administrador

De acordo.

LAERTE RADTKE KARNOPP,
Auditor Geral