MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO OESTE DA BAHIA

AUDITORIA INTERNA

RELATÓRIO FINAL DE AUDITORIA Nº 02/2021

Universidade Federal do Oeste da Bahia - UFOB

Exercício 2021

Agosto de 2021

Auditoria Interna - AUDIN UFOB

Universidade Federal do Oeste da Bahia – UFOB

RELATÓRIO DE AVALIAÇÃO

Órgão: Universidade Federal do Oeste da Bahia

Período auditado: 2020

Unidades Examinadas: Pró-Reitoria de Tecnologia da Informação e Comunicação - Protic

Município/UF: Barreiras/BA

Ordem de Serviço Nº: 02/2021

Relatório FINAL de Auditoria: 02/2021

Ação de auditoria - nº 01 - Administração de Infraestrutura de TIC

Missão da Audin

Adicionar valor à gestão, melhorando as operações, analisando e aprimorando a eficácia dos processos, analisando o gerenciamento de riscos, os controles internos, a integridade e a governança da UFOB.

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?

O Presente trabalho é uma auditoria realizada para analisar a Infraestrutura de Tecnologia da Informação na Universidade Federal do Oeste da Bahia com o intuito de Avaliar os controles internos e o estágio de implementação da gestão de riscos relacionados à Segurança da Informação, ressaltando-se eventuais impropriedades que impactaram o atingimento de resultados, além de destacar as boas práticas administrativas e seus impactos no desempenho das unidades, informando também as providências corretivas necessárias.

POR QUE A AUDIN REALIZOU ESSE TRABALHO?

Trata-se de auditoria que faz parte do processo anual de contas, conforme previsto no Plano Anual de atividades de auditoria – PAINT 2021.

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

O presente relatório refere-se a infraestrutura de Tecnologia de Informação e Comunicação - TIC. Esta ação foi contemplada no PAINT 2021 - Planejamento Anual das atividades de Auditorias Internas.

Deste relatório originaram-se os achados e recomendações abaixo relacionados:

- **Achado nº 01:** Data center insuficiente e exposto a riscos diversos.

Recomendação nº 01: Adequação da estrutura arquitetônica e civil do Data center/ou sua realocação em um espaço adequado e melhorias estruturais nos sistemas críticos como Sistema de refrigeração e Rede de energia elétrica.

Recomendação nº 02: Separação dos equipamentos de telecomunicações e dados, em ambientes diferentes.

- **Achado 02:** Força de trabalho insuficiente

Recomendação nº 03: Envidar esforços para aumento e adequação da força de trabalho na Protic.

- **Achado 03:** Ausência de política de segurança da informação e comunicação – Posic, e de controle de acesso à informação, aos recursos e serviços de TIC.

Recomendação nº 04: Aprovar a política de segurança da informação e comunicação – Posic, englobando o controle de acesso aos sistemas Institucionais, recursos e Serviços de TIC.
Recomendação nº 05: Implantar Comitê de Segurança da Informação e Comunicação (ou estrutura equivalente).
Recomendação nº 06: Estabelecer mecanismos de controle de bens de TIC em posse de servidores em afastamento ou desligamentos.

- **Achado 04:** Ausência de política de gestão de riscos

Recomendação nº 07: Aprovar a política de Gestão de riscos Institucional, englobando a política de gestão de riscos de TIC, ou outro normativo equivalente.
Recomendação nº 08: Elaborar e implementar a Matriz de riscos Institucionais e o Plano de Gestão de riscos.

Recomendação nº 09: Implantar Comitê de Gestão de riscos (ou estrutura equivalente).

- **Achado 05:** Política e sistema de cópias de segurança (backup) e restauração de dados.

  Recomendação nº 10: Normatizar e Implantar Sistema de cópia de Segurança (Backup) ou estrutura equivalente, que atenda a necessidade de cópia de segurança na Universidade.

LISTA DE SIGLAS E ABREVIATURAS

ABNT	Associação Brasileira de Normas Técnicas
AUDIN	Auditoria Interna
CNR	Câmara de Normas e Recursos
CONSUNI	Conselho Universitário
CGU	Controladoria Geral da União
DSIC	Departamento de Segurança da Informação e Comunicações
GSIPR	Gabinete de Segurança Institucional
MEC	Ministério da Educação e Cultura
PAINT	Plano Anual de Auditoria Interna
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicação
PNSI	Política de Segurança da Informação
POSIC	Política de Segurança da Informação e Comunicação
Protic	Pró-Reitoria de Tecnologia da Informação e Comunicação
SISP	Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP
SACRES	Superintendência Administrativa do *Campus* Reitor Edgar Santos
TIC	Tecnologia da Informação e Comunicação
TCU	Tribunal de Contas da União
UFOB	Universidade Federal do Oeste da Bahia

Índice de Tabelas

Índice de Figuras

SUMÁRIO

1. INTRODUÇÃO

Em cumprimento ao Plano Anual de Atividades da Auditoria Interna da Universidade Federal do Oeste da Bahia - UFOB exercício 2021, aprovado pela Câmara de Gestão Administrativa e Governança – CGAG, assessora do Conselho Superior, por meio do ato decisório nº 07/2020, de 17 de dezembro de 2020, e considerando as atribuições da unidade de Auditoria Interna estabelecidas no art. 1º e inciso XVII do art. 11, da Resolução Câmara de Normas e Recursos - CNR nº 001, de 22 de outubro de 2020, que aprova o Regulamento da Auditoria Interna, e no art. 18 do Decreto nº 9.203/2017, apresentamos o presente trabalho de avaliação de infraestrutura de Tecnologia da Informação e Comunicação - TIC de acordo com os preceitos contidos na Ordem de Serviço nº 02/2021.

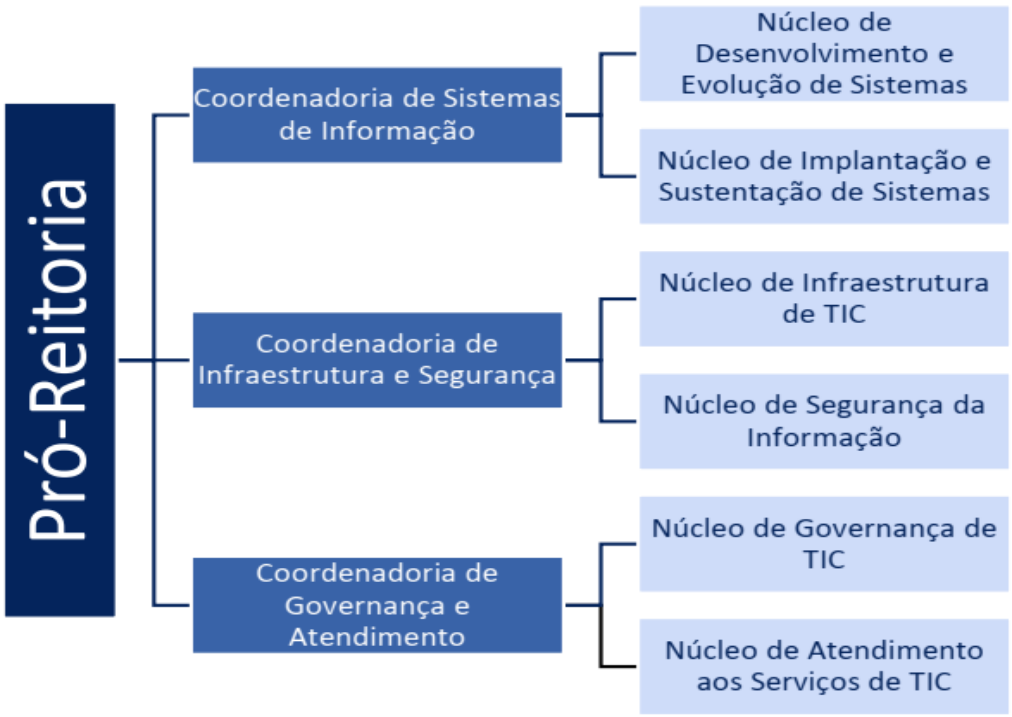
Cabe ressaltar que a realização dos exames respeitou as normas de auditoria aplicáveis à administração pública, não havendo por parte da área avaliada, qualquer restrição aos trabalhos da Auditoria Interna - Audin.

2. VISÃO GERAL DO OBJETO

A Tecnologia da Informação e Comunicação (TIC) desempenha papel essencial e estratégico no processo de desenvolvimento institucional, as atividades de TIC permeiam todas as áreas de atuação da UFOB.

As operações, controle e supervisão de recursos de TIC na UFOB estão sobre a responsabilidade da Pró-Reitoria de Tecnologia de Informação e Comunicação, que foi criada em 2014 e consta com a seguinte estrutura:

Figura 1 - Composição da Protic



Fonte: Site da Protic

A equipe da Protic é gerida por uma Pró-Reitora, que é responsável pela gestão da Pró-Reitoria e também compõe o Comitê Gestor de Tecnologia da Informação e Comunicação (CGTIC). O segundo nível hierárquico da estrutura possui as seguintes unidades:

- **Coordenadoria de Governança e Atendimento:** CGA – promover a gestão por processos, manter o portfólio de serviços atualizado, fomentar as metodologias de gerenciamento de projetos, promover treinamentos e melhoria contínua dos serviços, planejar e acompanhar os processos de atendimento, promover o atendimento proativo e programas de treinamento.
- **Coordenadoria de Infraestrutura e Segurança -** CIS – implementar a Política de Segurança da Informação, monitorar recursos de rede e de telefonia, gerir o parque

tecnológico, sistemas operacionais, sistemas de banco de dados, ferramentas de segurança e de produtividade.

- **Coordenadoria de Sistemas de Informação:** CSI: desenvolver ou contratar sistemas de informação, portais e sites, implantar e prestar suporte aos sistemas de terceiros e manter sistemas legados.

2.1 Os Objetivos

Os objetivos do trabalho foram definidos no programa de trabalho e tiveram como objetivo geral avaliar a adequação dos mecanismos de controle na área de Infraestrutura de Tecnologia da Informação e como objetivos específicos:

- Verificar se existem políticas e diretrizes definidas para governança e gestão de tecnologia da informação;
- Verificar a estrutura de Segurança das Informações;
- Verificar os controles internos relacionados à Segurança da Informação.

2.2 Escopo e Amostra

Para atingir os objetivos do trabalho, o escopo envolveu questões relativas à estrutura organizacional, aos processos operacionais, à gestão da informação e à transparência obrigatória.

Os trabalhos envolveram a Protic e o Comitê Gestor de Tecnologia da Informação e Comunicação CGTIC. O período analisado foi o exercício 2020. As análises se deram de 19/04/2021 a 28/06/2021.

2.3 Legislação e Documentos de Suporte

- **Lei 14.063/2020** - Dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, em atos de pessoas jurídicas e em questões de saúde e sobre as licenças de softwares desenvolvidos por entes públicos; e altera a Lei nº 9.096, de 19 de setembro de 1995, a Lei nº 5.991, de 17 de dezembro de 1973, e a Medida Provisória nº 2.200-2, de 24 de agosto de 2001.
- **Lei nº 12.527, de 18 de novembro de 2011.** Regula o acesso a informações previsto no inciso XXXIII do art.5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5

de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências.

- **Decreto nº 9.637, de 26 de dezembro de 2018 -** Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
- **Decreto nº 10.641, de 2 de março de 2021 -** Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação;
- **Decreto nº 10.332, de 28 de abril de 2020 -** Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.
- **Portaria nº 778, de 4 de abril de 2019** - Dispõe sobre a implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP.
- **Instrução Normativa nº 1, de 27 de maio de 2020** - Dispõe sobre a estrutura de gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.
- **Norma Complementar nº 04/IN01/DSIC/**GSIPR – Gestão de Riscos de Segurança da Informação e Comunicações – GRSIC;
- **Norma Complementar nº 07/IN01/DSIC/**GSIPR – Diretrizes para Implementação de controles de Acesso Relativos à Segurança da Informação e Comunicações;
- **Norma Complementar 06/IN01/DSIC/GSIPR**, de 11 de novembro de 2009, que estabelece diretrizes para Gestão de Continuidade de Negócios,
- **ABNT NBR 11515** – Guia de práticas para segurança física relativas ao armazenamento de dados
- **Acórdão TCU nº 1.603/2008 – Plenário;**
- **Acórdão TCU nº 2.308/2010 – Plenário**
- **Guia de comitê de TI do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP);**
- **Relatório - Levantamento de Governança de TI 2016 TCU – iGovTI 2016.** Avalia a situação de governança de TI na Administração Pública Federal, através de questionários que abordam práticas de governança e de gestão de TI previstas em leis, regulamentos, normas técnicas e modelos internacionais de boas práticas.
- **Plano de Desenvolvimento Institucional –** PDI 2019 – 2013.
- **Plano Diretor de Tecnologia da Informação e Comunicação da Universidade Federal do Oeste da Bahia** – PDTIC UFOB.
- **Resolução Consuni no 007/2018** - Estabelece as normas de uso de recursos de Tecnologia da Informação e Comunicação (TIC) no âmbito da Universidade Federal do Oeste da Bahia.

3. EXECUÇÃO DOS TRABALHOS

A análise de conformidade examinou a aderência dos normativos internos aos externos. As análises ocorreram com base nas informações e documentos disponibilizados pela Protic, pelas informações prestadas pelos servidores envolvidos e em respostas às solicitações de auditoria, assim como em dados extraídos do site da Pró-Reitoria e Universidade.

Para fins deste trabalho, nossas ponderações estão divididas em "Informação", quando se referir a avaliações de caráter informativo e opinativo, não havendo prejuízo ou restando prejudicada as providências a serem tomadas, e "Constatação", quando houver a necessidade de alertar sobre falhas ou fragilidades passíveis de infringência às normas legais e riscos de conformidade e que ensejam medidas corretivas.

INFORMAÇÃO 01: - EQUIPE PROATIVA, COM ALTO NÍVEL DE QUALIFICAÇÃO TÉCNICA E EFETIVIDADE NOS CHAMADOS PROTIC.

A Protic possui uma força de trabalho jovem e proativa, ainda que em número menor que o desejável. Conforme demonstrado no quadro abaixo, a equipe possui alto nível de qualificação técnica, o que é determinante para o nível de efetividade dos serviços prestados pela Pró-Reitoria.

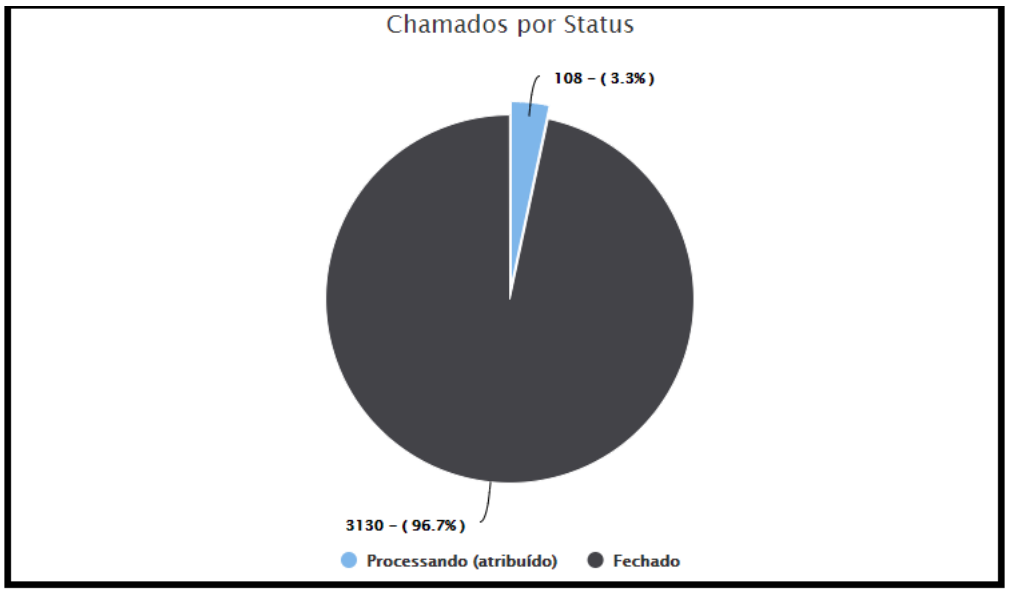
Tabela 1 - Qualificação Técnica equipe Protic

NOME	CARGO	graduação	Especialização	Mestrado
P. F.F.	Assistente em Administração	x		
B. do S.S.	Técnico de TI	x		X
F.F. de N. N.	Técnico de TI	x	X	
G. B. S.	Técnico de TI	x		
L. S.P.N dos R.	Técnico de TI	x	X	
I.A.S.s de J.	Técnico em Telecomunicações	x	X	
J.T.C	Administrador	x		x
C.M.S	Analista de TI	x	X	
D.D	Analista de TI	x	X	X
D.C.S.	Analista de TI	x	X	X
F. O. H.	Analista de TI	x		
Y. K. A. da S.	Analista de TI	x		

L. H.F.D.	Analista de TI	x	X	X
U. R.A. S.	Analista de TI	x	X	x
V.G.K.	Analista de TI	x	X	x

Fonte: Elaboração própria

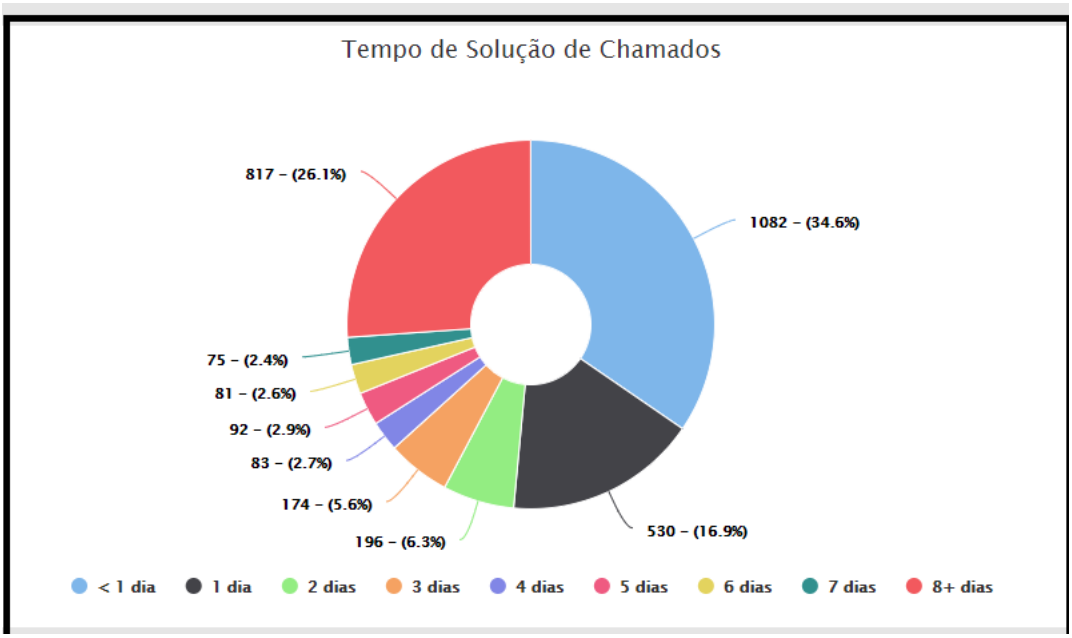
Figura 2 - Percentual de Conclusão dos Chamados



Fonte: Protic

O relatório de chamados demonstra um alto nível de conclusão dos atendimentos, conforme demonstrado no gráfico acima. O quadro abaixo demonstra o tempo de atendimento dos chamados.

Figura 3 - Tempo médio de Atendimento dos Chamados



Fonte: Protic

INFORMAÇÃO 02: IT DIGITAL – ASSINATURA DIGITAL ICPEdu

A lei 14063/2020 que dispõe sobre o uso de assinaturas eletrônicas em interações com entes públicos, determina em seu artigo 18: "Os sistemas em uso na data de entrada em vigor desta Lei que utilizem assinaturas eletrônicas e que não atendam ao disposto no art. 5º desta Lei serão adaptados até 1º de julho de 2021". A UFOB através da Portaria nº 283/2021 instituiu a assinatura digital. A Protic de pronto emitiu Manual de uso e instalação dos certificados, disponível em: https://drive.google.com/file/d/18Bmssf6iH6PM7YMGMA9MNNdfSQIGy1zV/view, atendendo no prazo estipulado, a exigência da legislação supra.

3.1 Exames

Após a emissão da ordem de serviços, o ofício Nº 06/2021/AUDITORIA/UFOB com data de 19/04/2021 foi encaminhado a Protic informando a abertura da ação e apresentando a auditora responsável pela ação.

A coleta de dados ocorreu mediante:

a) Análise da legislação interna existente em comparativo com os normativos

federais;

b) Reunião remota com a Pró-Reitora e Coordenadores.
c) Reuniões remotas e Aplicação de questionários às coordenações e aos servidores da Pró-Reitoria.
d) Análise do portal da Protic e dos documentos e serviços lá disponibilizados.
e) Visita in-loco no data center.

3.2 Da Avaliação dos Controles Internos

O conjunto do trabalho possibilitou a identificação de eventos de riscos e de fragilidades nos controles internos que podem comprometer o atingimento do objetivo final, a eficiência e eficácia do processo auditado. Ademais, foram utilizadas, como critério de avaliação dos controles, as principais fragilidades apontadas pela avaliação de riscos realizada pela Audin, da qual participaram todos os gestores da UFOB, a fim de compor o Plano de auditoria 2021. Observamos algumas fragilidades nos controles internos, especialmente no que diz respeito à governança, estabelecimento de políticas e diretrizes, tais fragilidades são apontadas nos achados de auditoria, abaixo relacionados.

3.3 Achados de Auditoria

Ao analisarmos os dados encontrados, concluímos sobre a existência das seguintes inconsistências:

- **Achado nº 01:** Data center insuficiente e exposto a riscos diversos
- **Achado 02:** Força de trabalho insuficiente
- **Achado 03:** Ausência de política de segurança da informação e comunicação – Posic, e de controle de acesso à informação, aos recursos e serviços de TIC.
- **Achado 04:** Ausência de política de gestão de riscos
- **Achado 05:** Carência de Política e sistema de cópias de segurança (backup) e restauração de dados.

ACHADOS

ACHADO 01: DATA CENTER INSUFICIENTE E EXPOSTO A RISCOS DIVERSOS

O data center da UFOB não está em conformidade com as normas e especificações existentes para seu funcionamento, sendo um risco para o funcionamento das atividades na Instituição, tendo em vista a importância da tecnologia da informação nos tempos atuais. O data center funciona em uma sala de 18 m², não possui a infraestrutura mínima exigida e está exposto a

diversos riscos, como: umidade, incêndios, refrigeração inadequada, ausência de gerador; insetos e muitos outros. Uma Equipe de trabalho da Protic elaborou um documento bem completo e relevante, expondo a situação do DATA CENTER da UFOB e apresentando possíveis soluções para o problema, dentro das possibilidades da universidade. O relatório pode ser acessado em: https://Protic.UFOB.edu.br/projetos.

Critério ou situação Esperada – ABNT NBR 11515 - Condições ambientais exigíveis para o armazenamento de dados em condições operacionais ou cópia de segurança; PDTIC UFOB. O Datacenter institucional mantém a infraestrutura de Tecnologia da Informação (TI), que sustenta todos os sistemas informatizados essenciais para o funcionamento da UFOB. Um Data Center completo é composto por uma sala dotada de sistemas de climatização, energia e segurança próprios para ambientes de missão crítica e por diversos equipamentos e softwares de alta complexidade.

Condição ou situação Encontrada – O Data center da UFOB apresenta diversas vulnerabilidades, a saber:

- Tamanho da sala;
- Infraestrutura – rachaduras, umidade, brechas que permitem a entradas de insetos, não possui piso elevado, porta estreita, formato da sala (formato retangular da sala prejudica movimentação dos técnicos) ambiente único (telecomunicação demanda manutenção de pessoal técnico externo)
- Quadro de energia elétrica compartilhado
- Climatização inadequada
- Ausência de sistema de detecção de incêndio;
- Ausência de controle de acesso

Causas prováveis – Cortes orçamentários, grande rotatividade de servidores na Protic, outras demandas de recursos de TIC (computadores de mesa, notebooks para atendimento da comunidade universitária no geral).

Efeito ou consequência – Todos os riscos já apontados são de alto impacto e alta probabilidade, tendo em vista a alta vulnerabilidade existente. As consequências advindas deles podem ser irreversíveis, com perda de dados e paralisação dos serviços, especialmente no trabalho remoto.

Grau da Achado: (x) Grave; ( ) Moderada; ( ) Leve

ACHADO 02: FORÇA DE TRABALHO INSUFICIENTE

A Protic possui 16 servidores nela lotados, sendo 14 da área de TIC (8 analistas de TI, 5 técnicos de TI e 1 técnico em telecomunicação) destes, 2 estão afastados por prazo indeterminado. Existem 5 técnicos de TI lotados nos campi, conforme quadro abaixo:

Tabela 2 - Força de trabalho Protic

CARGO	Protic	SACRES	CMB	CMBJL	CMLEM	CMSMV	Total
Administrador	1						1
Analista de TI	8						8
Assistente em administração	1						1
Técnico de TI	5	1	1	1	1	1	10
Técnico em telecomunicação	1						1
Técnico em audiovisual		2				1	3

Fonte: Protic

Critério ou situação Esperada – Decreto nº 10.332, de 28 de abril de 2020, iniciativa 18.3. PDTIC UFOB NC11.

Condição ou situação Encontrada – A equipe de trabalho da Protic é insuficiente para atender a toda demanda de trabalho da Pró-Reitoria. Só o SIG – Sistema de Informações Gerenciais, utilizado pela universidade, recomenda uma equipe de trabalho dedicada a ele de 22 pessoas, número maior que o total de servidores na Pró-Reitoria.

Causas prováveis – Grande rotatividade de servidores na Universidade (redistribuições), ausência de planejamento institucional (para que as demandas sejam enviadas com tempo hábil a Protic), falta de recursos para capacitações.

Efeito ou consequência – Equipe sobrecarregada, trabalhando a maior parte do tempo com as prioridades e urgências e ficando impossibilitada de realizar atividades de planejamento, projetos e governança, a capacitação também fica prejudicada.

Grau da Achado: (x) Grave; ( ) Moderada; ( ) Leve

ACHADO 03: AUSÊNCIA DE POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO – POSIC, E DE CONTROLE DE ACESSO À INFORMAÇÃO, AOS RECURSOS E SERVIÇOS DE TIC.

A Política de Segurança da Informação deve estabelecer as diretrizes para a Segurança da Informação, visando assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação. A UFOB não possui uma política institucional de segurança da informação, tampouco Política de controle de acesso à informação, aos recursos e serviços de TIC.

Critério ou situação Esperada – O Regimento interno do Comitê Gestor de Tecnologia da Informação e comunicação – CGTIC, em seu art. 4º, VI, estabelece que cabe ao CGTIC elaborar e revisar a política de Segurança da Informação; O art. 15, II do Decreto nº 9.637, de 26 de dezembro de 2018, assim estabelece:

> Art. 15. Aos órgãos e às entidades da administração pública federal, em seu âmbito de atuação, compete:
> II - Elaborar sua política de segurança da informação e as normas internas de segurança da informação, observadas as normas de segurança da informação editadas pelo Gabinete de Segurança Institucional da Presidência da República;
> III - designar um gestor de segurança da informação interno, indicado pela alta administração do órgão ou da entidade;
> IV - instituir comitê de segurança da informação ou estrutura equivalente, para deliberar sobre os assuntos relativos à PNSI;

A Resolução Consuni nº 007/2018 estabelece as normas de uso de recursos de Tecnologia da Informação e Comunicação (TIC), contudo é necessário que se estabeleça a política de controle de acesso à informação, aos recursos e serviços de TIC, em que se estabeleça diretrizes e regras mais abrangentes, a qual poderá ser inserida ou contemplada pela Política de Segurança da Informação e Comunicação – POSIC.

Condição ou situação Encontrada – A UFOB não possui política de segurança da Informação, Comitê ou gestor responsável, também não há diretrizes estabelecidas para controle de acesso à informação e aos recursos de TIC. Observamos que não há procedimento estabelecido para averiguar a posse de bens de TIC, quando há afastamentos de servidores. Só é exigida certidão de inexistência de pendências, quando há vacância.

Causas prováveis – Universidade tem apenas 8 anos e possui uma grande demanda de normativos estruturantes, possui um número pequeno de servidores técnicos e há uma sobrecarga de participação dos servidores em comitês e comissões.

Efeito ou consequência – Falhas nos controles internos, ausência de padrões.

Grau da Achado: ( ) Grave; (x) Moderada; ( ) Leve

ACHADO 04: AUSÊNCIA DE POLÍTICA DE GESTÃO DE RISCOS

A Política de gestão de riscos é a declaração das intenções e diretrizes gerais de uma organização relacionadas à gestão de riscos. A UFOB ainda não aprovou a proposta institucional. O regimento interno do comitê gestor de tecnologia da informação e comunicação – CGTIC, em seu art. 4º, V, estabelece que cabe ao CGTIC elaborar e revisar a política de Gestão de Riscos de TIC;

Critério ou situação Esperada – Instrução Normativa conjunta nº 1, de 10 de maio de 2016.

> Art. 3º Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar os controles internos da gestão, tendo por base a identificação, a avaliação e o gerenciamento de riscos que possam impactar a consecução dos objetivos estabelecidos pelo Poder Público (...).
>
> Art. 17. A política de gestão de riscos, a ser instituída pelos órgãos e entidades do Poder Executivo federal em até doze meses a contar da publicação desta Instrução Normativa, deve especificar ao menos:
> I - princípios e objetivos organizacionais;
> II - diretrizes sobre:
> a) como a gestão de riscos será integrada ao planejamento estratégico, aos processos e às políticas da organização;
> b) como e com qual periodicidade serão identificados, avaliados, tratados e monitorados os riscos;
> c) como será medido o desempenho da gestão de riscos;
> d) como serão integradas as instâncias do órgão ou entidade responsáveis pela gestão de riscos;
> e) a utilização de metodologia e ferramentas para o apoio à gestão de riscos; e
> f) o desenvolvimento contínuo dos agentes públicos em gestão de riscos; e
> III - competências e responsabilidades para a efetivação da gestão de riscos no âmbito do órgão ou entidade.

Condição ou situação Encontrada – A UFOB não possui política de gestão de riscos, nem matriz de riscos Institucionais, ficando exposta às intempéries advindas da não prevenção e tratamento de riscos.

Causas prováveis – Grande demanda de normativos estruturantes, número pequeno de servidores técnicos.

Efeito ou consequência – Falhas nos controles internos, ausência de padrões, não tratamento e exposição a riscos.

Grau da Achado: ( ) Grave; (x) Moderada; ( ) Leve

ACHADO 05: CARÊNCIA DE POLÍTICA E SISTEMA DE CÓPIAS DE SEGURANÇA (BACKUP) E RESTAURAÇÃO DE DADOS

A Política de Cópia de Segurança e Restauração dos Dados deve estabelecer diretrizes para o processo de cópia e armazenamento dos dados a serem executadas pelo órgão responsável pela TIC, visando garantir a segurança, integridade e recuperação das informações. A UFOB não possui política ou normas internas estabelecidas. Também há deficiência de sistema de Backup.

Critério ou situação Esperada – Decreto nº 10.332, de 28 de abril de 2020, que institui a estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional;

Condição ou situação Encontrada – Atualmente a UFOB não possui política ou norma que estabeleça as diretrizes para Cópia de Segurança e Restauração dos Dados. O sistema de Backup existente não comporta todos os sistemas da universidade, abrangendo somente os mais críticos.

Causas prováveis – Grande demanda de normativos estruturantes, restrições orçamentárias.

Efeito ou consequência – Perdas de informações e dados, paralisação dos serviços e sistemas.

Grau da Achado: (x) Grave; ( ) Moderada; ( ) Leve

4. RECOMENDAÇÕES E BENEFÍCIOS ESPERADOS

Por todo o exposto recomenda-se, como práticas de melhoria da gestão da Infraestrutura de TIC na Universidade:

- **Achado nº 01:** Data center insuficiente e exposto a riscos diversos.
  Recomendação nº 01: Adequação da estrutura arquitetônica e civil do Data center/ou sua realocação em um espaço adequado e melhorias estruturais nos sistemas críticos como Sistema de refrigeração e Rede de energia elétrica.

  Recomendação nº 02: Separação dos equipamentos de telecomunicações e dados, em ambientes diferentes.

- **Achado 02:** Força de trabalho insuficiente
  Recomendação nº 03: Envidar esforços para aumento e adequação da força de trabalho na Protic.

- **Achado 03:** Ausência de política de segurança da informação e comunicação – Posic, e de controle de acesso à informação, aos recursos e serviços de TIC.
  Recomendação nº 04: Aprovar a política de segurança da informação e comunicação – Posic, englobando o controle de acesso aos sistemas Institucionais, recursos e Serviços de TIC.
  Recomendação nº 05: Implantar Comitê de Segurança da Informação e Comunicação (ou estrutura equivalente).
  Recomendação nº 06: Estabelecer mecanismos de controle de bens de TIC em posse de servidores em afastamento ou desligamentos.

- **Achado 04:** Ausência de política de gestão de riscos
  Recomendação nº 07: Aprovar a política de Gestão de riscos Institucional, englobando a política de gestão de riscos de TIC, ou outro normativo equivalente;
  Recomendação nº 08: Elaborar e implementar a Matriz de riscos Institucionais e o Plano de Gestão de riscos.
  Recomendação nº 09: Implantar Comitê de Gestão de riscos (ou estrutura equivalente).

- **Achado 05:** Política e sistema de cópias de segurança (backup) e restauração de dados
  Recomendação nº 10: Normatizar e Implantar Sistema de cópia de Segurança (Backup) ou estrutura equivalente, que atenda a necessidade de cópia de segurança na Universidade.

5. CONCLUSÃO

Este relatório objetivou avaliar a adequação dos mecanismos de controle da Infraestrutura de Tecnologia da Informação e Comunicação e responder às seguintes questões:

1- Existem políticas e diretrizes definidas para governança e gestão de tecnologia da informação?

2 - Os planos estratégicos institucional e de TI fornecem suporte apropriado à governança e à gestão de TI?

3 - As necessidades relacionadas ao desenvolvimento de pessoas e à força de trabalho da área de TI são gerenciadas e suficientes?

4 - Há políticas relacionadas à Segurança da informação e Governança de TIC?

Das respostas de tais questões foram relacionados cinco achados que originaram dez recomendações para gestão da Universidade, com destaque para a elaboração de planos e importantes políticas institucionais.

Assim sendo, os apontamentos deste relatório indicam serem necessários esforços da área auditada, bem como o patrocínio da alta administração para a aprovação das políticas de segurança da informação e comunicação, de gestão de riscos, de cópias de segurança e para atendimento das demais recomendações atinentes ao tema. As prescrições de providências aqui apontadas visam assegurar a integridade das informações eletrônicas no âmbito da universidade, tendo em vista a crescente demanda de ativos de informação, o que atrela por conseguinte, riscos que podem impactar negativamente os objetivos da Universidade.

Os trabalhos foram realizados em consonância com as normas de auditoria interna e não houve nenhum impedimento por parte da unidade auditada. Ao final dos trabalhos, realizou-se a reunião de busca conjunta de soluções, momento em que oportunizou-se discutir soluções adequadas para atendimento das constatações do relatório preliminar de auditoria.

Por fim, lembramos que este relatório não tem a intenção de esgotar as possibilidades de riscos passíveis de serem observados, mas sim de servir como orientação para as boas práticas da Administração Pública.

Em atendimento ao inciso XX do art. 11 da Resolução CNR nº 01/2020, que aprovou o regimento interno da auditoria, encaminhe-se à Reitoria e à PROTIC, para conhecimento e providências, e publique-se na página da Auditoria Interna para conhecimento da comunidade universitária.

ANEXOS

MANIFESTAÇÃO DA UNIDADE AUDITADA

A Audin enviou relatório preliminar para manifestação da unidade, que se pronunciou nos seguintes termos:

Achado nº 1. Data center insuficiente e exposto a riscos diversos

Manifestação: A Pró-Reitora de Tecnologia da Informação e Comunicação manifestou concordância com os achados e recomendações.

Achado nº 2. Força de trabalho insuficiente

Manifestação: A Pró-Reitora de Tecnologia da Informação e Comunicação manifestou concordância com os achados e recomendações e encaminhou apenas um apontamento em relação ao achado 02, conforme segue: "com a redistribuição do servidor Dilerval Carvalho Silva, no momento a PROTIC conta com 13 servidores (7 analistas de TI, 5 técnicos de TI e 1 técnico em telecomunicação)".

Além disso, a universidade está iniciando o mapeamento de seus processos, que possibilitará dimensionar a força de trabalho de cada setor.

Achado nº 3. Ausência de política de segurança da informação e comunicação – Posic, e de controle de acesso à informação, aos recursos e serviços de TIC
Manifestação: A Pró-Reitora de Tecnologia da Informação e Comunicação manifestou concordância com os achados e recomendações.

Achado nº 4. Ausência de política de gestão de riscos

Manifestação: A Pró-Reitora de Tecnologia da Informação e Comunicação manifestou concordância com os achados e recomendações

Achado nº 5. Política e sistema de cópias de segurança (backup) e restauração de dados
Manifestação: A Pró-Reitora de Tecnologia da Informação e Comunicação manifestou concordância com os achados e recomendações.

ANÁLISE DA AUDITORIA INTERNA

Em consonância com a reunião de busca conjunta de soluções e com a manifestação da unidade auditada, mantemos todas as recomendações para acompanhamento.