Relatório de Auditoria – Macroprocesso Gerir Tecnologia da Informação

2024

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

REITORIA

AUDITORIA GERAL - Relatório de Auditoria – Macroprocesso Gerir Tecnologia da Informação

João Pessoa

2024

Missão

Desempenhar uma atividade independente e objetiva de avaliação e consultoria desenhada para adicionar valor e melhorar as operações do Instituto Federal da Paraíba, buscando auxiliá-lo a realizar seus objetivos, através da aplicação de uma abordagem sistemática e disciplinada, para avaliar e melhorar a eficácia dos processos de governança, de gerenciamento de riscos e de controles internos.

Visão

Ser reconhecido, em longo prazo, no Brasil, como órgão de excelência competente pela avaliação e consultoria dos controles internos, da governança e da gestão de risco contribuindo para o fortalecimento da gestão e para o desenvolvimento institucional.

Valores

I) Comportamento ético;

II) Cautela e zelo profissional;

III) Independência;

IV) Imparcialidade;

V) Objetividade;

VI) Conhecimento técnico e capacidade profissional;

VII) Atualização dos conhecimentos técnicos;

VIII) Cortesia;

IX) Intransferibilidade de Funções;

X) Sigilo e Discrição;

XI) Responsabilidade;

XII) Interesse Público;

XIII) Comunicação eficaz;

XIV) Alinhamento com as estratégias, objetivos e riscos da organização;

XV) Atuação respaldada na eficiência, eficácia, efetividade e economicidade;

XVI) Controle de qualidade; e

XVII) Transparência dos resultados.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA

Relatório de Auditoria

Gerir Tecnologia da Informação

Natureza da Auditoria

Conformidade e desempenho

Período de Abrangência

2023

Unidade

Diretoria de Tecnologia da Informação

Responsáveis

Fábio de Albuquerque Silva

Relatório nº

07/2023

Equipe de trabalho

Alisson Câmara de Abreu - Auditor Interno

Pedro Victor Santana Nicéas de Albuquerque – Coordenador da Divisão de Planejamento e Execução de Auditoria

Erick Miranda da Silva – Auditor Geral

Victor Hugo Paiva de Assunção – Auditor Especialista

Joedson do Nascimento Marques – Auditor Especialista

João Pessoa

2024

LISTA DE SIGLAS E ABREVIATURAS

CGU – Controladoria Geral da União

COSO – Committee of Sponsoring Organizations of the Treadway Commission (Comitê das Organizações Patrocinadoras da Comissão Treadway)

DTI – Diretoria de Tecnologia da Informação

IFPB – Instituto Federal da Paraíba

IN – Instrução Normativa INTOSAI – International Organization of Supreme Audit Institutions (Organização Internacional de Entidades Fiscalizadoras Superiores)

ISO – International Organization for Standardization Organização Internacional para Padronização)

MP – Ministério de Planejamento

PAINT - Plano Anual de Atividades da Unidade de Auditoria Interna

PDP - Plano de Desenvolvimento de Pessoas

PLANEDE - Planejamento Estratégico Decenal

PRAE – Pró-Reitoria de Assistência Estudantil

SA – Solicitação de Auditoria

SUAP – Sistema Unificado de Administração Pública

TCU – Tribunal de Conta da União

UAIG – Unidade de Auditoria Interna Governamental

AGRADECIMENTOS

Nós, que fazemos para da Unidade de Auditoria Interna do IFPB - UAIG -, agradecemos a todos que colaboraram com o planejamento e execução desse trabalho.

Em especial, agradecemos aos servidores Victor Hugo Paiva de Assunção e Joedson do Nascimento Marques, que fizeram o trabalho como auditores especialistas. Sem eles esse trabalho não seria possível, em face da especialidade do tema. Registramos nosso muito obrigado e consideração.

Agradecemos também a toda equipe de servidores da Diretoria Geral de Tecnologia da Informação, na pessoa do Diretor Geral, Fábio de Albuquerque Silva, que sempre foi solícito, atencioso e respondeu tempestivamente aos questionamentos da auditoria.

Por fim, registre-se agradecimentos aos auditores Coordenador, Pedro Victor Santana Nicéas de Albuquerque e Auditor-Geral, Erick Miranda da Silva, que auxiliaram na condução desse trabalho, sempre nos ajudando nas correções e orientações gerais na forma como deveríamos proceder com os trabalhos.

1. INTRODUÇÃO

A informática está presente em quase todas as áreas de nossas vidas. Torna-se difícil conceber a vida em sociedade sem a presença dos ativos de Tecnologia da Informação (T.I), seja quando o utilizamos para o trabalho, para atividades domésticas seja até mesmo para o uso recreativo.

A T.I automatizou a coleta, armazenamento e provimento de pronto acesso a incontáveis quantidades de informação que são usadas nas tomadas de decisão e operacionalização dos processos básicos de uma organização.

Todavia, com a sua presença na vida das pessoas e das organizações, a T.I também traz consigo diversas vulnerabilidades inerentes. Nesse sentido, cada uma delas precisa ser identificada, mitigada e controlada.

Nesse norte, destaca-se a importância da Auditoria em T.I, compreendida como o processo de garantir que o desenvolvimento, a implantação e a manutenção de Sistemas de T.I atinjam os objetivos da organização, zelem pelo uso de ativos e mantenham a integridade dos dados. Em outras palavras, a Auditoria de T.I é a fiscalização de Sistemas e Controles de T.I para assegurar que supram as necessidades da organização sem comprometer a segurança, privacidade, custo e outros elementos.

2. ESCOPO

Conforme define a Norma de Auditoria do Tribunal (NAT) 92: "o escopo envolve a definição das questões de auditoria, a profundidade e o detalhamento dos procedimentos, a delimitação do universo auditável (abrangência), a configuração da amostra (extensão) e a oportunidade dos exames."

Os trabalhos acontecerão no 2º semestre de 2023, envolverão a execução, na Diretoria de Tecnologia da Informação (DTI) em João Pessoa.

As questões de Auditoria foram selecionadas a partir de planilha de análise de riscos e controles, elaborada conjuntamente com a Diretoria de Tecnologia da Informação, consoante se encontra no Anexo 01.

Ressalte-se que, posteriormente, deliberou-se pela necessidade de apoio de auditores técnicos para auxiliar na execução desta auditoria.

Dessa forma, selecionaram-se 2 analistas de T.I do Campus João Pessoa para esse mister, os quais também contribuíram para identificação de riscos e controles (Anexo 02). Frise-se, todavia, que, em diálogo com eles, decidiu-se pela não inclusão desses riscos e controles,

em razão de alguns já coincidirem com os já elaborados pelo Diretor de T.I e também para não haver a ampliação do escopo e extrapolar os prazos de execução.

Os riscos e controles selecionados foram os seguintes:

1) Riscos: Falhas de *hardware*, faltas de *backup* e de legalização do *software* afetando a execução do processo.

Controles:

a) Preventivo: migração de serviços para nuvem.

b) Atenuação e recuperação: realização de backup periódico e ativação do plano de continuidade de operação.

Justificativa para seleção: probabilidade média e impacto alto.

2) Riscos: interrupção do serviço de internet.

Controles:

a) Preventivo: contratação de *link* de internet redundante.

b) Atenuação: roteamento de dados móveis; acionamento do link secundário.

Justificativa para seleção: probabilidade média, impacto alto e controles inexistentes.

3. OBJETIVOS

3.1 Objetivo Geral

Os objetivos desta auditoria são: aprimoramento dos processos de governança, de gerenciamento de riscos e de controle, os quais estão fortemente relacionados entre si.

3.2 Objetivos específicos

Analisar se:

No caso de interrupção do serviço de internet, o Instituto dispõe de meios para mitigar o risco?

No caso de falhas de hardware, de faltas de *backup* e de legalização do *software* que afetem a execução do processo, os controles são capazes de atuar para que o risco residual se torne baixo?

A Diretoria de Tecnologia da Informação possui formalizada sua gestão de riscos?

4. CRITÉRIOS DE AUDITORIA

Os critérios utilizados para nesta auditoria são:

a) Art. 70, caput, da CF;

Art. 70. A fiscalização contábil, financeira, orçamentária, operacional e patrimonial da União e das entidades da administração direta e indireta, quanto à legalidade, legitimidade, economicidade, aplicação das subvenções e renúncia de receitas, será exercida pelo Congresso Nacional, mediante controle externo, e pelo sistema de controle interno de cada Poder.

b) Art. 95, I e II do Regimento Interno do IFPB;

Art. 95. São competências e atribuições da Diretoria Geral de Tecnologia da Informação:

I – planejar, dirigir, avaliar e executar as políticas de tecnologia da informação e comunicação (TIC) em todo o Instituto, em articulação com as Pró-Reitorias e as Direções Gerais dos campi;

II – gerenciar o desenvolvimento e a operação dos sistemas de informação do Instituto, no âmbito de sua competência;

c) Arts. 3º, 9º e 13 da Instrução Normativa Conjunta 01/2016 da CGU.

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. Os controles internos da gestão se constituem na primeira linha (ou camada) de defesa das organizações públicas para propiciar o alcance de seus objetivos. Esses controles são operados por todos os agentes públicos responsáveis pela condução de atividades e tarefas, no âmbito dos macroprocessos finalísticos e de apoio dos órgãos e entidades do Poder Executivo federal. A definição e a operacionalização dos controles internos devem levar em conta os riscos que se pretende mitigar, tendo em vista os objetivos das organizações públicas. Assim, tendo em vista os objetivos estabelecidos pelos órgãos e entidades da administração pública, e os riscos decorrentes de eventos internos ou externos que possam obstaculizar o alcance desses objetivos, devem ser posicionados os controles internos mais adequados para mitigar a probabilidade de ocorrência dos riscos, ou o seu impacto sobre os objetivos organizacionais.

§ 1º Os controles internos da gestão, independentemente do porte da organização, devem ser efetivos e consistentes com a natureza, complexidade e risco das operações realizadas.

§ 2º Os controles internos da gestão baseiam-se no gerenciamento de riscos e integram o processo de gestão.

§ 3º Os componentes dos controles internos da gestão e do gerenciamento de riscos aplicam-se a todos os níveis, unidades e dependências do órgão ou da entidade pública.

§ 4º Os dirigentes máximos dos órgãos e entidades devem assegurar que procedimentos efetivos de implementação de controles internos da gestão façam parte de suas práticas de gerenciamento de riscos.

§ 5º Controles internos da gestão adequados devem considerar todos os componentes definidos na Seção III e devem ser integrados ao processo de gestão, dimensionados e desenvolvidos na proporção requerida pelos riscos, de acordo com a natureza, complexidade, estrutura e missão do órgão ou da entidade pública.

Art. 9º Os controles internos da gestão devem ser estruturados para oferecer segurança razoável de que os objetivos da organização serão alcançados. A existência de objetivos claros é pré-requisito para a eficácia do funcionamento dos controles internos da gestão.

Art. 13. Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar o processo de gestão de riscos, compatível com sua missão e seus objetivos estratégicos, observadas as diretrizes estabelecidas nesta Instrução Normativa.

5. QUESTÕES DE AUDITORIA

a) No caso de interrupção do serviço de internet, o Instituto dispõe de meios para mitigar o risco?

Profundidade e detalhamento dos procedimentos:

- Indagação oral (entrevista) ao Diretor Geral de Tecnologia da Informação (DGTI).

b) No caso de falhas de hardware, de faltas de backup e de legalização [1]do software que afetem a execução do processo, os controles são capazes de atuar para que o risco residual se torne baixo?

Profundidade e detalhamento dos procedimentos:

- Indagação oral (entrevista) ao Diretor Geral de Tecnologia da Informação;
- Inspeção física para aplicação de roteiro de testes.

[1] A equipe de auditoria deliberou pela retirada da avaliação da legalização de *software* do escopo, uma vez que, conforme ressaltado pelos auditores técnicos, há a necessidade de profissional advogado especialista na área para realizar análise do objeto.

- No que concerne ao *backup*, serão aplicados testes, a fim de observar se ele está sendo feito corretamente, qual o tempo que se leva para fazê-lo e se a restauração é eficaz.

Os *hardwares* selecionados para compor a amostra são:

1. *Switch Brocade ICX 6450-24*
2. *Blade PowerEdge M1000e*
3. *Dell EqualLogic Storage*
4. *HPE 3par Service Processor*
5. *Dois 3PAR StoreServ 8000*
6. *3PAR StoreServ 8200*

O Software selecionado para compor a amostra é o sistema de bibliotecas (*koha*).

c) A Diretoria de Tecnologia da Informação possui formalizada sua gestão de riscos?

Profundidade e detalhamento dos procedimentos:

- Indagação oral e escrita ao Diretor Geral de Tecnologia da Informação sobre a existência de uma gestão de riscos.

6. ACHADOS DE AUDITORIA

Como resultado da comparação entre os critérios preestabelecidos e a condição real encontrada durante a realização dos exames, comprovadas por meio de evidências, apresentamos os achados de auditoria.

6.1.1 Questão de auditoria

No caso de interrupção do serviço de internet, o Instituto dispõe de meios para mitigar o risco?

6.1.2 Descrição sumária

Inexistência de *link* de internet redundante.

6.1.3 Critérios

1) Art. 70, caput, da CF;

2) Art. 95, I e II do Regimento Interno do IFPB;

3) Arts. 3º, 9º e 13 da Instrução Normativa Conjunta 01/2016 da CGU.

6.1.4 Condição ou situação encontrada

Atualmente não existe o link de internet redundante1[2]. A Diretoria Geral de Tecnologia da Informação (DGTI) já iniciou um processo para aquisição do link (está em estudo técnico preliminar).

Nesse sentido, constata-se atualmente a inexistência do mencionado controle.

6.1.5 Evidências

a) Matriz de riscos e controles elaborada pela DGTI;

b) Entrevista realizada junto com ao Diretor-Geral (Ata 12/2023).

6.1.6 Causa

Eventos externos causados por contingenciamento de recursos.

6.1.7 Efeito

Caso um dos caminhos, por onde a internet percorre, seja interrompido, os usuários poderão ter os serviços prejudicados, em razão da ausência do link de internet redundante.

6.1.8 Manifestação do setor auditado

A Diretoria-Geral de Tecnologia da Informação se manifestou dessa forma:

> *"Esta situação permanece da mesma forma que foi reportada na "Matriz de Riscos - Gerir Tecnologia da Informação - T.I.", fornecida no início deste processo de auditoria. Nesta planilha, na coluna M e linha 22; é informada a Inexistência dos referidos controles. Os referidos controles foram colocados como parte da gestão de riscos cotidiana realizada pela DGTI, caracterizando ações desejadas para prevenção do risco, mas que ainda não foram implantadas por falta de recursos."*

6.1.9 Análise da auditoria interna

Conforme a própria gestão reconhece, as ações não foram implementadas, em razão de falta de recursos.

---

[2] No contexto de Tecnologia da Informação, redundância é a duplicação de componentes essenciais que aumentam a confiabilidade e segurança de determinado sistema, assim como sua disponibilidade. Em outras palavras, a redundância de link é oferecer ao cliente mais de um "caminho" para que a internet chegue até ele – assim, caso um desses caminhos esteja congestionado ou interrompido, a internet pode percorrer outras vias, evitando que haja a queda do serviço.

A falta de internet representa uma desvantagem que pode gerar transtornos tanto para empresas quanto para pessoas.

A redundância do link evita o congestionamento ou interrupção do serviço, assegurando a qualidade e a segurança nos serviços de internet.

6.1.10 Recomendação

Contratar link comercial de internet com outra operadora diferente da RNP/Rede Metro.

6.1.11 Benefícios esperados

Manter o serviço de internet funcionando sem interrupção com qualidade e segurança.

6.2.1 Questões de auditoria

No caso de falhas de *hardware* e de legalização do *software* que afetem a execução do processo, os controles são capazes de atuar para que o risco residual se torne baixo?

6.2.2 Descrição sumária

Inexistência de garantias para *BLADE* (processamento e memória).

6.2.3 Critérios

1) Art. 70, caput, da CF;

2) Art. 95, I e II do Regimento Interno do IFPB;

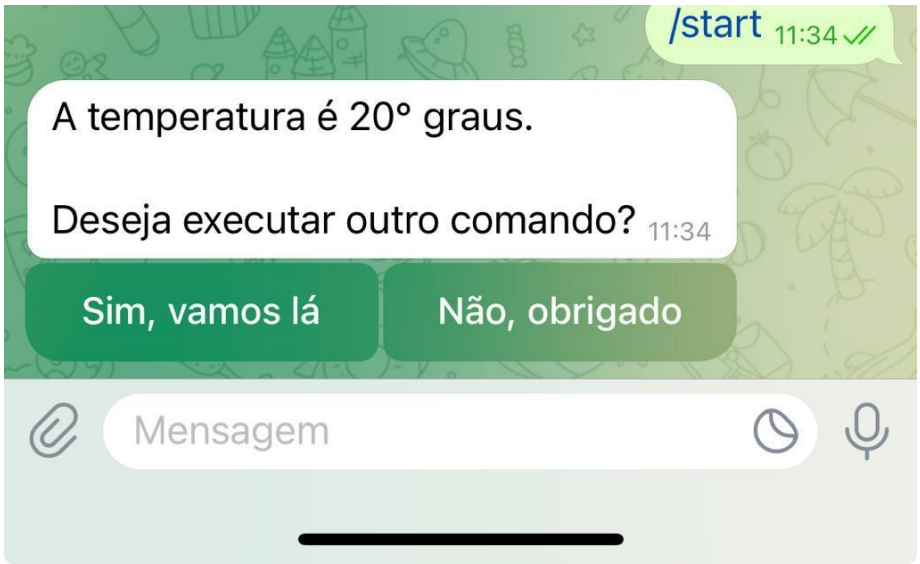
3) Arts. 3º, 9º e 13 da Instrução Normativa Conjunta 01/2016 da CGU.

6.2.4 Condição ou situação encontrada

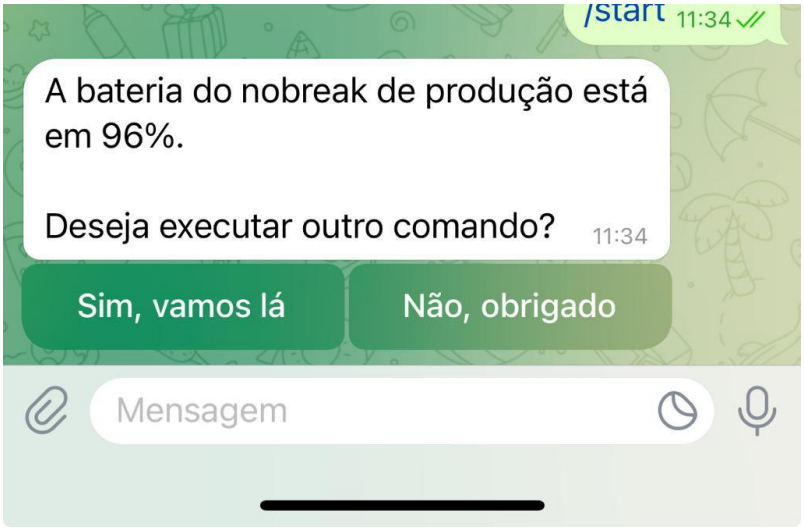
De início, registre-se que a equipe de auditoria entendeu pela retirada da avaliação da legalização de *software* do escopo, uma vez que, conforme ressaltado pelos auditores técnicos, há a necessidade de profissional advogado especialista na área para realizar análise do objeto.

No mesmo sentido, no que concerne aos *hardwares*, a Auditoria Interna, composta pelo Auditor Executor, Coordenador e Auditor-Geral, em concordância com os auditores técnicos, deliberou por não executar testes nos *hardwares*, que estavam alocados na Diretoria-Geral de Tecnologia da Informação, em face dos riscos existentes, que poderiam afetar toda a Instituição, no caso de haver algum erro.

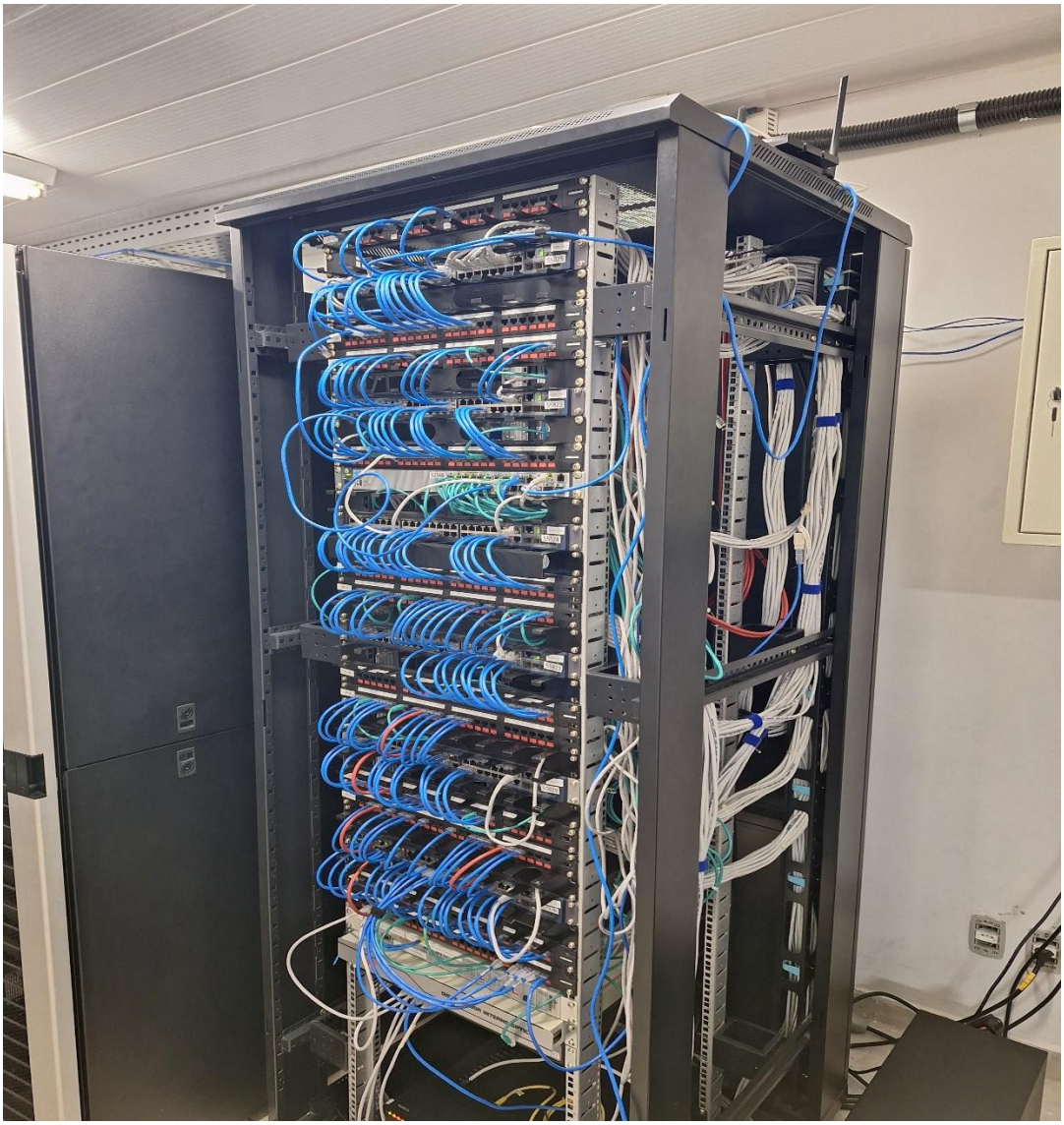
Porém, impende destacar que a sala onde estão localizados os *hardwares* dispõe de diversos controles, de que são exemplos ar-condicionados, que são desligados de modo a poder não os sobrecarregar, sistema de detecção de temperatura, para evitar aumento de temperatura, aplicativo com envio de mensagens sobre a temperatura, câmera filmadora registrando a entrada e saída no ambiente.




11:16
TELEGRAM
39
CIMR bot
bot
C
3 de maio
/start 13:38
Até logo! 13:38
/start 14:04
A bateria do nobreak de produção está em 97%.
Deseja executar outro comando? 14:04
Sim, vamos lá
Não, obrigado
25 de agosto
/start 11:34
Qual operação deseja executar? 11:34
TEMPERATURA
HUMIDADE
BATERIA NB
DESLIGAMENTO DC
Mensagem



No mais, observou-se que foi assinado contrato de extensão de garantia para o *Storage HPE*, (CONTRATO 0027/2023 - INEXIGIBILIDADE DE LICITAÇÃO No 013/2023 - Processo Administrativo n.° 23381.000721.2023-82).



Porém, falta contratar a extensão para a *Blade* (processamento e memória).

Dessa forma, constata-se que há equipamentos fora de garantia no *data cente*r e que carecem de contratação de serviço de extensão.

6.2.5 Evidências

a) Entrevista realizada junto com ao Diretor-Geral (Ata 12/2023);

b) Manifestação sobre os achados de auditoria.

c) Inspeção física no ambiente.

6.2.6 Causa

Tecnologia sem a proteção que se dá por meio de garantias.

6.2.7 Efeito

Dispêndio de recursos, visto que ausentes as garantias, que poderiam cobrir esses gastos.

6.2.8 Manifestação do setor auditado

Na Reunião de Busca Conjunta de Soluções, o Diretor-Geral de T.I afirmou que já foi assinado contrato de extensão de garantia para o *Storage HPE*, portanto, está ativo (CONTRATO 0027/2023 - INEXIGIBILIDADE DE LICITAÇÃO No 013/2023 - Processo Administrativo n.° 23381.000721.2023-82).

Todavia, falta contratar a extensão para a *Blade* (processamento e memória).

Nesse sentido, há equipamentos fora de garantia no *data cente*r e que carecem de contratação de serviço de extensão.

6.2.9 Análise da auditoria interna

Observam-se ações da DGTI no sentido de implementar o controle.

Porém, até que se conclua o processo de extensão da garantia, considerar-se-á como inexistente aquela.

Os controles internos da gestão devem ser estruturados para oferecer segurança razoável de que os objetivos da organização serão alcançados. A existência de objetivos claros é pré-requisito para a eficácia do funcionamento dos controles internos da gestão.

Os objetivos dos controles internos da gestão são: salvaguardar e proteger bens, ativos e recursos públicos contra desperdício, perda, mau uso, dano, utilização não autorizada ou apropriação indevida. Nesse sentido, as garantias protegem os hardwares contra esses eventos negativos.

6.2.10 Recomendação

Contratar a extensão da garantia para a *Blade* (processamento e memória).

6.2.11 Benefícios esperados

Salvaguardar e proteger os *hardwares* contra o mau uso, danos, utilização não autorizada ou apropriação indevida.

6.3.1 Questão de auditoria

No caso de falhas de *backup* que afetem a execução do processo, os controles são capazes de atuar para que o risco residual se torne baixo?

6.3.2 Descrição sumária

O processo de *backup* do software *Koha* aconteceu normalmente.

6.3.3 Critérios

1) Art. 70, caput, da CF;

2) Art. 95, I e II do Regimento Interno do IFPB;

3) Arts. 3º, 9º e 13 da Instrução Normativa Conjunta 01/2016 da CGU.

6.3.4 Condição ou situação encontrada

No dia 25 de outubro do presente ano, na sede da DGTI, participaram do teste no *software Koha* o Auditor Interno Alisson Câmara, o Auditor Técnico Especialista Joedson do Nascimento Marques e, o Diretor-Geral de Tecnologia da Informação Fábio de Albuquerque Silva e os Tecnólogos Pedro Henrique Bezerra Ayres de Albuquerque e Victor Hugo Azevedo dos Santos

Nesse sentido, o processo de restauração da máquina com o banco de dados do *Koha* foi disparado por Pedro, que enfrentou problemas de conexão na máquina local e sugeriu que Victor assumisse o processo usando outro computador.

Esse continuou o processo de restauração, que levou cerca de 60 minutos.

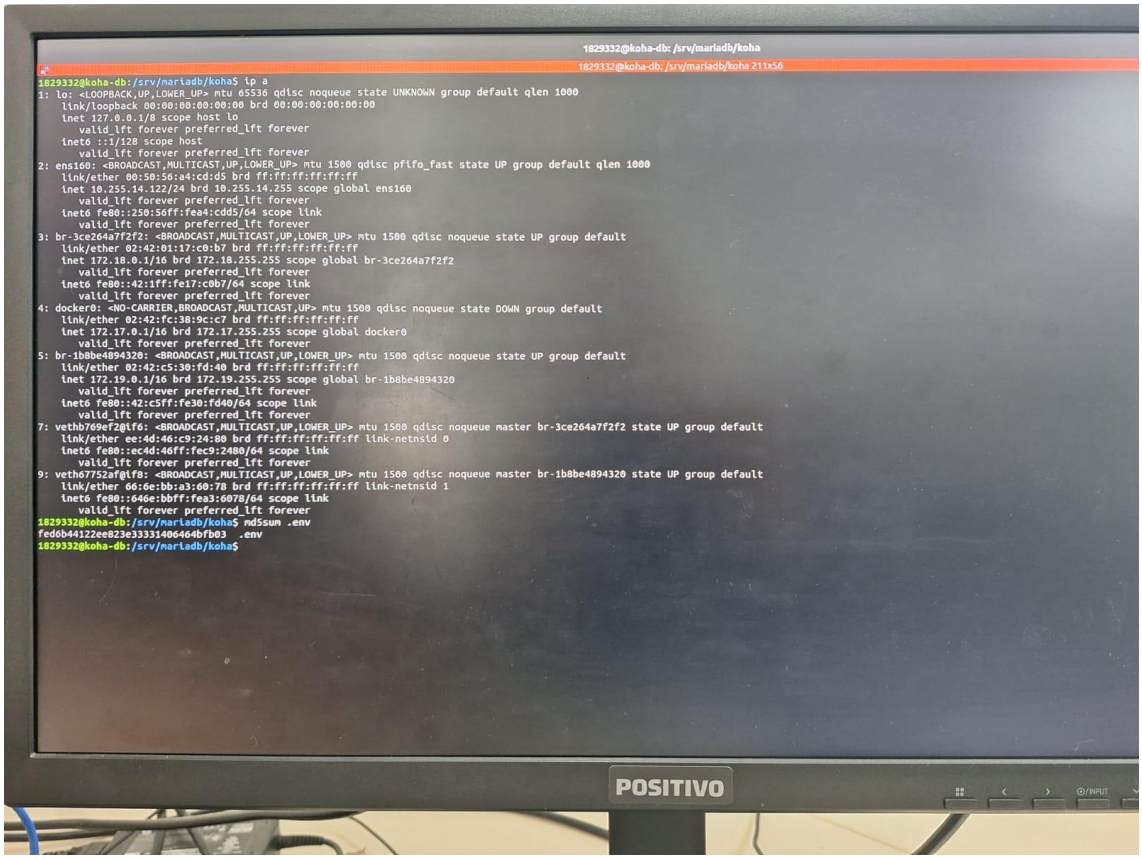
Após o *backup*, Victor recuperou o ambiente, primeiro ajustando a máquina virtual com o banco de dados que veio do *backup* e transferindo o código da aplicação para outro servidor virtual, usando o gitlab.

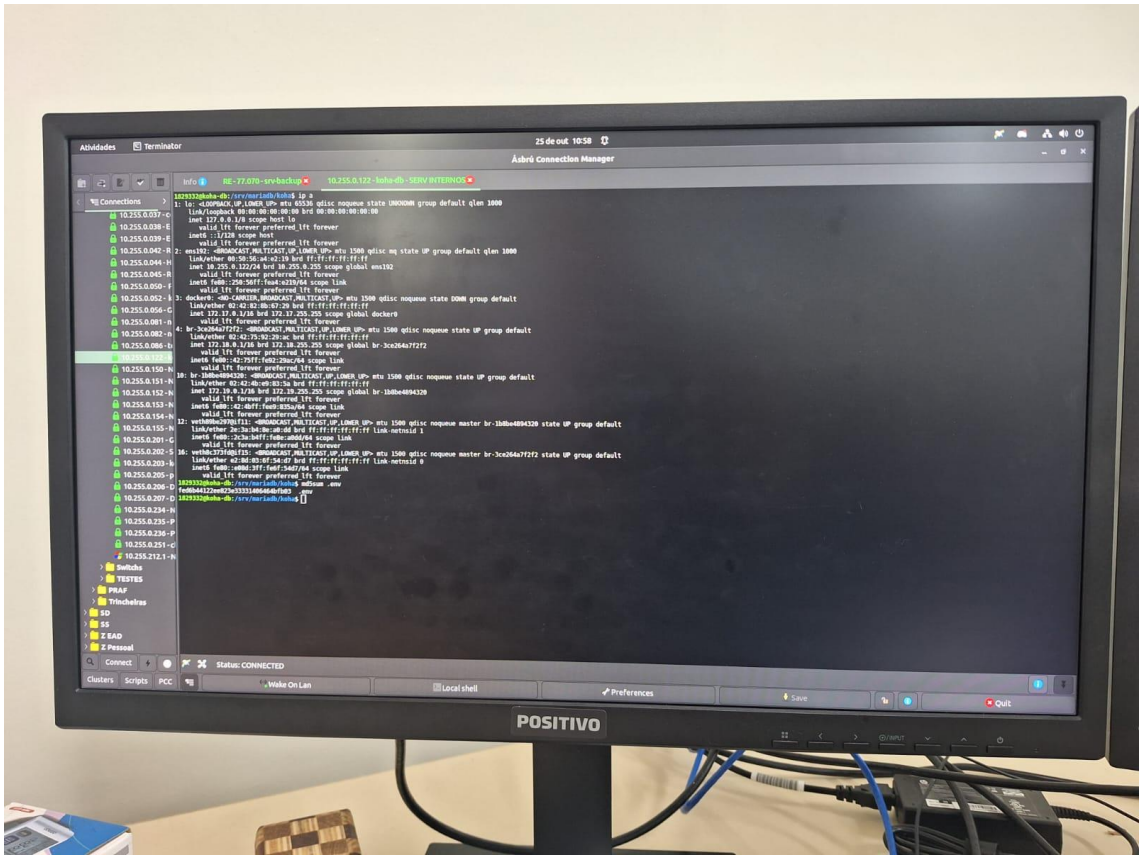
Após a recuperação, verificou-se que a aplicação foi restaurada com êxito.

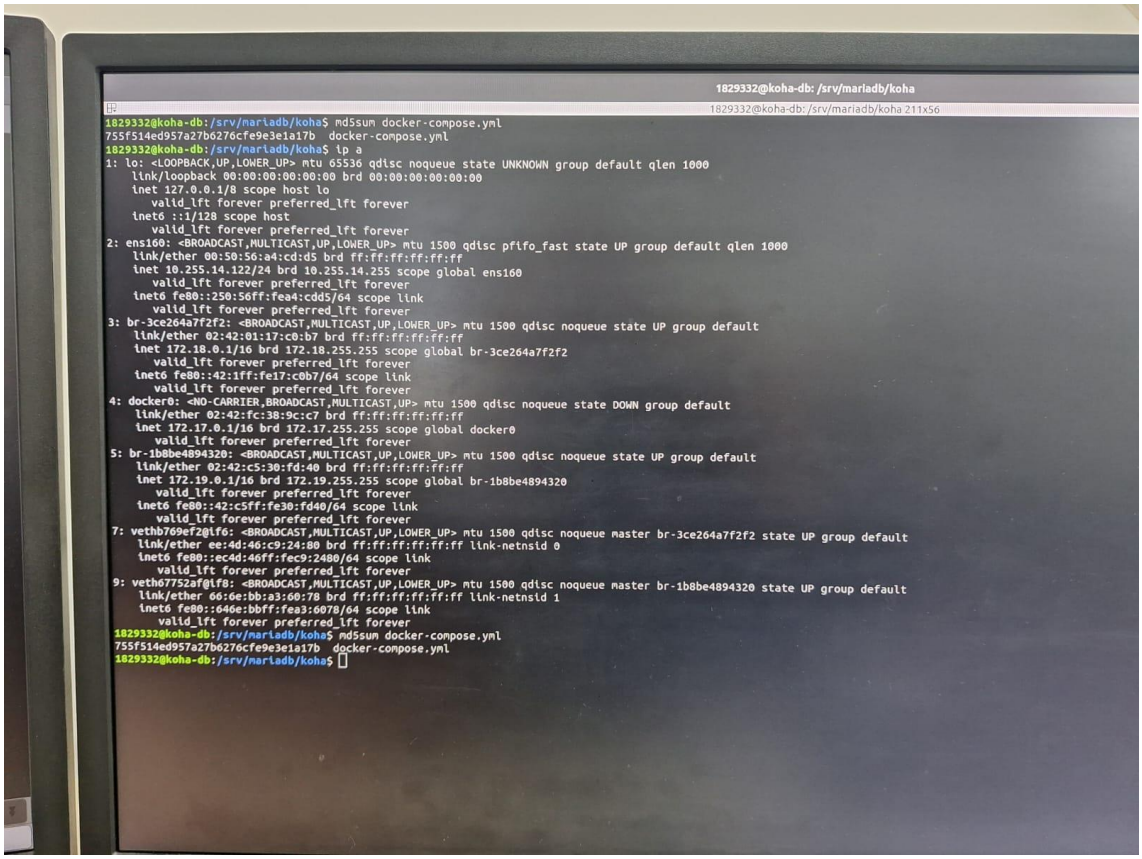
Fez-se a comparação entre o ambiente restaurado e o ambiente de produção.

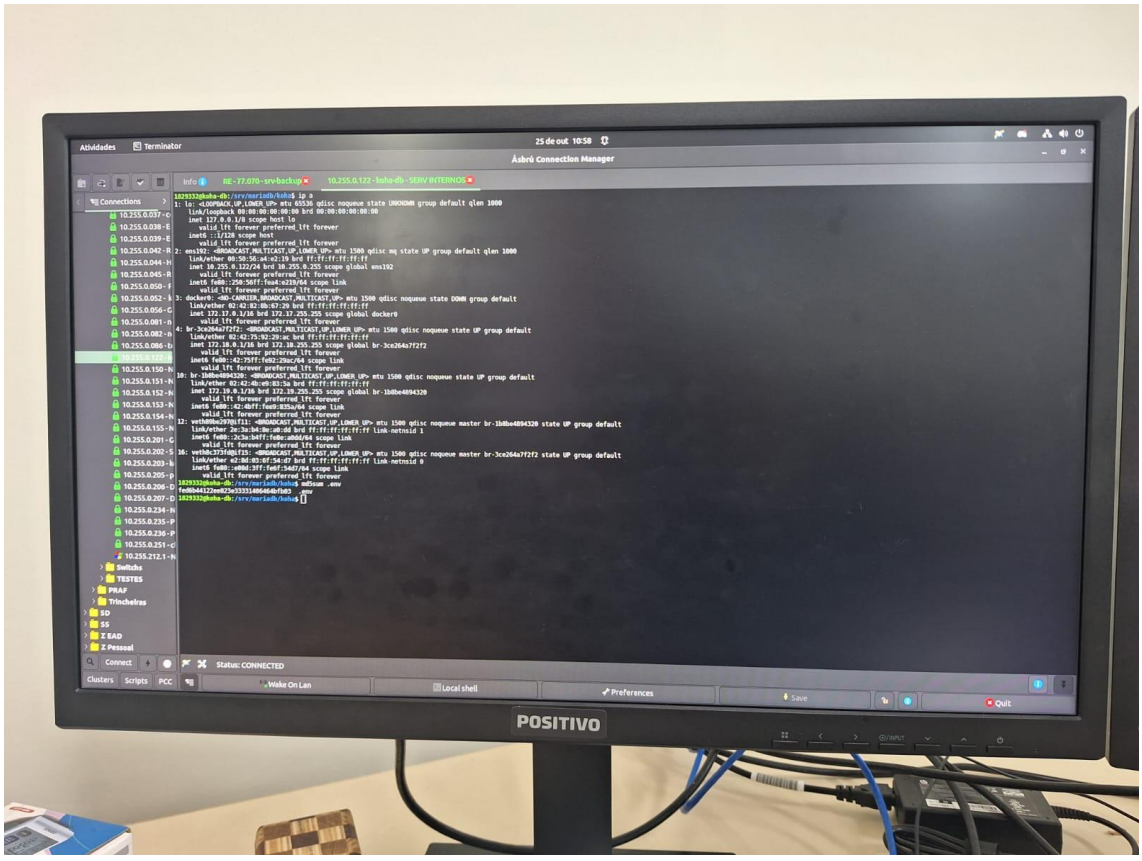
Para garantir a integridade do *backup*, foi solicitada a comparação dos *hashs* de alguns arquivos entre o servidor restaurado e o servidor de produção.

Os arquivos "*docker-compose.yml*" e "*.env*" foram comparados, confirmando que os *hashs* eram idênticos, demonstrando a integridade do *Backup*.




Atividades
Terminator
25 de out 10:58
Ásbrú Connection Manager
POSITIVO


1829332@koha-db: /srv/mariadb/koha
1829332@koha-db:/srv/mariadb/koha$ md5sum docker-compose.yml
755f514ed957a27b6276cfe9e3e1a17b docker-compose.yml
1829332@koha-db:/srv/mariadb/koha$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo
valid_lft forever preferred_lft forever
inet6 ::1/128 scope host
valid_lft forever preferred_lft forever
2: ens160: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
link/ether 00:50:56:a4:cd:d5 brd ff:ff:ff:ff:ff:ff
inet 10.255.14.122/24 brd 10.255.14.255 scope global ens160
valid_lft forever preferred_lft forever
inet6 fe80::250:56ff:fea4:cdd5/64 scope link
valid_lft forever preferred_lft forever
3: br-3ce264a7f2f2: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
link/ether 02:42:01:17:c0:b7 brd ff:ff:ff:ff:ff:ff
inet 172.18.0.1/16 brd 172.18.255.255 scope global br-3ce264a7f2f2
valid_lft forever preferred_lft forever
inet6 fe80::42:1ff:fe17:c0b7/64 scope link
valid_lft forever preferred_lft forever
4: docker0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default
link/ether 02:42:fc:38:9c:c7 brd ff:ff:ff:ff:ff:ff
inet 172.17.0.1/16 brd 172.17.255.255 scope global docker0
valid_lft forever preferred_lft forever
5: br-1b8be4894320: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
link/ether 02:42:c5:30:fd:40 brd ff:ff:ff:ff:ff:ff
inet 172.19.0.1/16 brd 172.19.255.255 scope global br-1b8be4894320
valid_lft forever preferred_lft forever
inet6 fe80::42:c5ff:fe30:fd40/64 scope link
valid_lft forever preferred_lft forever
7: vethb769ef2@if6: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-3ce264a7f2f2 state UP group default
link/ether ee:4d:46:c9:24:80 brd ff:ff:ff:ff:ff:ff link-netnsid 0
inet6 fe80::ec4d:46ff:fec9:2480/64 scope link
valid_lft forever preferred_lft forever
9: veth67752af@if8: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue master br-1b8be4894320 state UP group default
link/ether 66:6e:bb:a3:60:78 brd ff:ff:ff:ff:ff:ff link-netnsid 1
inet6 fe80::646e:bbff:fea3:6078/64 scope link
valid_lft forever preferred_lft forever
1829332@koha-db:/srv/mariadb/koha$ md5sum docker-compose.yml
755f514ed957a27b6276cfe9e3e1a17b docker-compose.yml
1829332@koha-db:/srv/mariadb/koha$



6.3.5 Evidências

1) Ata de teste de *backup*;

2) Fotos do dia dos testes.

6.4.1 Questões de auditoria

A Diretoria de Tecnologia da Informação possui formalizada sua gestão de riscos?

6.4.2 Descrição sumária

A gestão de riscos não está formalizada.

6.4.3 Critérios

1) Art. 70, caput, da CF;

2) Art. 95, I e II do Regimento Interno do IFPB;

3) Arts. 3º, 9º e 13 da Instrução Normativa Conjunta 01/2016 da CGU.

6.4.4 Condição ou situação encontrada

Em entrevista com o Diretor-Geral de Tecnologia da Informação, observou-se que, apesar de no dia a dia haver ações que impliquem na gestão de riscos, essa não está devidamente formalizada.

6.4.5 Evidências

a) Entrevista realizada junto com ao Diretor-Geral (Ata 12/2023);

b) Manifestação do setor auditado.

6.4.6 Causa

Processo de governança mal concebido.

6.4.7 Efeito

Alcance dos objetivos podem ser comprometidos em razão da não observação dos ricos e controles.

6.4.8 Manifestação do setor auditado

A Diretoria-Geral de Tecnologia da Informação se manifestou dessa forma:

> *"Segundo a Norma Complementar 04/IN01/DSIC/GSIPR, o processo de gestão de riscos é responsabilidade do Gestor de Segurança da Informação (GSI). Esta função só foi preenchida em 04/05/2023, através da PORTARIA 749/2023 - REITORIA/IFPB. Após a conclusão de outras ações prioritárias identificadas pelo GSI, como o normativo para a Equipe de Tratamento e Resposta a Incidentes de Segurança da Informação - ETIR, será construído o processo formal de gestão de riscos da TI."*

6.4.9 Análise da auditoria interna

Os controles internos da gestão devem ser estruturados para oferecer segurança razoável de que os objetivos da organização serão alcançados.

Os órgãos e entidades do Poder Executivo federal deverão implementar, manter, monitorar e revisar o processo de gestão de riscos, compatível com sua missão e seus objetivos estratégicos, observadas as diretrizes estabelecidas na Instrução Normativa 01/2016.

Nesse sentido, a Auditoria entende que a DTI pode ser um agente importante na construção da Gestão de Riscos, ainda que formalmente essa competência pertença a outro órgão.

6.4.10 Recomendação

Dialogar com o Gestor de Segurança da Informação, construir e implementar a Gestão formal de Riscos da DGTI.

6.4.11 Benefícios esperados

A gestão de riscos irá oferecer segurança razoável de que os objetivos institucionais serão alcançados.

7. RESUMO DAS CONSTATAÇÕES E RESPECTIVAS RECOMENDAÇÕES

Constatação	Recomendação
Inexistência de link de internet redundante.	Contratar link comercial de internet com outra operadora diferente da RNP/Rede Metro.
Inexistência de garantias para *BLADE* (processamento e memória).	Contratar a extensão da garantia para a *Blade* (processamento e memória).
A gestão de riscos não está formalizada.	Dialogar com o Gestor de Segurança da Informação, construir e implementar a Gestão formal de Riscos da DGTI.

8. PLANO DE AÇÃO ENVIADO PELO GESTOR

Achado: Inexistência de link de internet redundante.

Situação encontrada: atualmente não existe o link de internet redundante. A Diretoria Geral de Tecnologia da Informação (DGTI) já iniciou um processo para aquisição do link (está em estudo técnico preliminar). Nesse sentido, constata-se atualmente a inexistência do mencionado controle.

Recomendação: contratar link comercial de internet com outra operadora diferente da RNP/Rede Metro.

O que fazer	Por que	Onde	Quem	Início	Fim	Como	Quanto
Contratar link comercial de internet com outra operadora diferente da RNP/Rede Metro	Aumentar disponibilidade dos Sistema hospedados no data center da reitoria (casa rosada)	Data center da reitoria (casa rosada)	CIMR-RE e PRAF-RE	02/01/24	28/06/24	Realização de Processo licitatório para instalação de link Comercial de Internet no data center da casa Rosada.	Aproximadamente R$1.100,00/mês

Achado: Inexistência de garantias para *BLADE* (processamento e memória).

Situação encontrada: Foi assinado contrato de extensão de garantia para o *Storage HPE*, (CONTRATO 0027/2023 - INEXIGIBILIDADE DE LICITAÇÃO No 013/2023 - Processo Administrativo n.° 23381.000721.2023-82).

Porém, falta contratar a extensão para a *Blade* (processamento e memória).

Dessa forma, há equipamentos fora de garantia no *data cente*r e que carecem de contratação de serviço de extensão.

Recomendação: Contratar a extensão da garantia para a *Blade* (processamento e memória).

O que fazer	Por que	Onde	Quem	Início	Fim	Como	Quanto
Contratar a extensão da garantia para a *Blade*	Aumentar Disponibilidade dos Sistema hospedados no data center da reitoria (casa rosada)	Data center da reitoria (casa rosada)	CIMR-RE e PRAF-RE	02/01/24	28/06/24	Realização de processo Licitatório para contratação de extensão de garantia da *Blade*	Aproximadamente R$100.000,00/ano

Achado: A gestão de riscos não está formalizada.

Situação encontrada: em entrevista com o Diretor-Geral de Tecnologia da Informação, observou-se que, apesar de no dia a dia haver ações que impliquem na gestão de riscos, essa não está devidamente formalizada.

Recomendação: dialogar com o Gestor de Segurança da Informação, construir e implementar a Gestão formal de Riscos da DGTI.

O que fazer	Por que	Onde	Quem	Início	Fim	Como	Quanto
Escrita e aprovação da política de gestão de riscos da DGTI.	Ter um processo documento para a Gestão de Riscos.	Portal institucional – página da DGTI	CGSI	01/03/24	28/06/24	Elaboração de política de gestão de riscos e aprovação pelo CGS	R$ 0,00

9. CONCLUSÃO

Concluiu-se, após testes aplicados, que a DGTI carece de um *link* de internet redundante, diversas ações mitigadoras já foram implantadas, porém, devido à falta de recursos o controle principal ainda não foi implantado, nesse sentido, a recomendação é para que haja a contratação de um *link* de internet com outra operadora diferente da *RNP/Rede Metro*.

Ademais, no que concerne aos *hardwares*, observa-se que há equipamentos fora de garantia no *data center* e que precisam de contratação do serviço de extensão (*BLADE* - processamento e memória).

Em relação aos *softwares*, foi realizado um teste de *backup* no Koha e observou-se que que aquele foi bem-sucedido.

Por fim, observou-se que, malgrado ocorrerem diversas ações cotidianas, visando a controlar os riscos, a Diretoria de Tecnologia da Informação não possui gestão de riscos formalizada.

João Pessoa, 05 de fevereiro de 2024

Alisson Câmara de Abreu

Auditor

Matrícula: 1841813

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DA PARAÍBA
Reitoria
Av. João da Mata, 256, Jaguaribe, CEP 58015-020, Joao Pessoa (PB)
CNPJ: 10.783.898/0001-75 - Telefone: (83) 3612.9701

Documento Digitalizado Restrito

Relatório Definitivo

Assunto:	Relatório Definitivo
Assinado por:	Alisson Abreu
Tipo do Documento:	Anexo
Situação:	Finalizado
Nível de Acesso:	Restrito
Hipótese Legal:	Auditoria Interna - Controle Interno (Art. 26, $ 3o, da Lei no 10.180/2001)
Tipo do Conferência:	Cópia Simples

Documento assinado eletronicamente por:

- **Alisson Camara de Abreu**, **AUDITOR**, em 05/02/2024 09:04:00.

Este documento foi armazenado no SUAP em 05/02/2024. Para comprovar sua integridade, faça a leitura do QRCode ao lado ou acesse https://suap.ifpb.edu.br/verificar-documento-externo/ e forneça os dados abaixo:

Código Verificador: 1072052
Código de Autenticação: d83f68ad7b