Universidade Federal de Ouro Preto

Relatório de Auditoria

Núcleo da Tecnologia da Informação

Março de 2024

Unidade de Auditoria Interna

RELATÓRIO DE AVALIAÇÃO

Núcleo de Tecnologia da Informação - NTI

Unidade de Auditoria Interna (Audin)

RELATÓRIO DE AVALIAÇÃO
Órgão: **Universidade Federal de Ouro Preto (UFOP)**
Unidade Auditada: **Núcleo de Tecnologia e Informação (NTI)**
Município/UF: **Ouro Preto / MG**
Relatório de Avaliação: **01/2023**

Missão

Providenciar, de forma autônoma e objetiva, serviços de avaliação e consultoria com o propósito de agregar valor à UFOP, otimizando a sistemática de controle dos processos e cooperando para a consecução dos objetivos institucionais.

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?

Analisar os aspectos básicos da Segurança da Informação: a autenticidade, a preservação da disponibilidade, a integridade e a confidencialidade da informação.

Verificar a conformidade de diretrizes de segurança de informações estabelecidas e controles internos adotados e implementados.

POR QUE A UNIDADE DE AUDITORIA INTERNA REALIZOU ESSE TRABALHO?

Segundo dados obtidos no Levantamento do Índice Integrado de Governança e Gestão Públicas (iGG 2021), emitido pelo Tribunal de Contas da União - TCU e disponibilizado no Relatório individual da autoavaliação da UFOP, mais precisamente no tocante à segurança da informação, foi constatado fragilidade alta quanto à implantação dessa atividade na organização

QUAIS AS CONCLUSÕES ALCANÇADAS PELA UNIDADE DE AUDITORIA INTERNA?

QUAIS AS RECOMENDAÇÕES QUE DEVERÃO SER ADOTADAS?

O Núcleo de Tecnologia da Informação ostenta um corpo técnico comprometido em seus procedimentos laborais e ciente dos desafios a eles inerentes. Além disso, a alta administração da referida unidade, bem como as pessoas chaves dos processos sujeitos à auditoria, evidenciam um interesse manifesto na busca pela melhoria contínua, possuindo, ademais, considerável domínio sobre suas atividades.

É oportuno salientar que a unidade objeto de auditoria se encontra em estágio incipiente no que concerne à governança e gestão de riscos, situação análoga as demais unidades administrativas da universidade.

As recomendações preponderantes orbitam em torno da imperatividade de formalização de diretrizes operacionais por meio do estabelecimento de políticas internas e a delineação de procedimentos normativos. Além disso, observa-se a imperiosidade de alocação de recursos em ativos físicos e a intensificação do contingente de recursos humanos como meio de fortalecer a capacidade operacional da unidade avaliada.

LISTA DE SIGLAS E ABREVIATURAS

UFOP	Universidade Federal de Ouro Preto
CGU	Controladoria Geral da União
TCU	Tribunal de Contas da União
AUDIN	Unidade de Auditoria Interna
MOT	Manual de Orientações Técnicas da Atividade de Auditoria Interna Governamental
NTI	Núcleo de Tecnologia e Informação
PDTiC	Plano Diretor de Tecnologia da Informação e Comunicação
LGPD	Lei Geral de Proteção de Dados
CTIC	Comitê de Tecnologia da Informação e Comunicação
PROPLAD	Pró Reitoria de Planejamento

SUMÁRIO

INTRODUÇÃO **8**

RESULTADOS DOS EXAMES **9**

1. Ausência de acompanhamento, avaliação e renovação do Plano Diretor de Tecnologia da Informação e Comunicação – PDTiC. 9
2. Insuficiência de controles sobre ativos tecnológicos. 10
3. Não utilização da ferramenta de descoberta ativa de rede. 11
4. Ausência de classificação de dados 12
5. Ausência de gerenciamento de contas de usuários 13
6. Ausência de critérios de segurança de senhas 14
7. Ausência de registros de LOG's e trilha de auditoria 15
8. Ausência de diretrizes de Backup e estrutura segura de armazenamento. 16
9. Não realização de testes de vulnerabilidade e análise de incidentes. 17
10. Deficiência na estrutura física do datacenter. 18

RECOMENDAÇÕES **19**

1. Elaborar Políticas Administrativas 19
2. Elaborar e gerenciar o Plano Diretor da unidade - PDTiC 19
3. Submeter ao Comitê de Tecnologia de Informação e Comunicação - CTIC as questões de governança, direcionamento estratégico e tomada de decisões 20
4. Realizar inventário dos ativos tecnológicos de valor significativo 20
5. Estabelecer controle sobre os itens/peças utilizadas para manutenção de equipamentos ... 21
6. Executar testes periódicos de descoberta ativa de rede 21
7. Implementar o perfil de contas nos sistemas institucionais. 22
8. Implementar CheckList para exoneração de servidores 22
9. Implementar parâmetros de gerenciamento de senhas nos sistemas institucionais 22
10. Diagnóstico da infraestrutura necessária de T.I 23
11. Realizar testes de completude e fidedignidade dos Backups 24
12. Análise dos setores com carência de pessoal 24
13. Reforçar estrutura do Data Center 24

INTRODUÇÃO

O presente relatório de auditoria abrange a avaliação do Núcleo de Tecnologia da Informação (NTI) da Universidade Federal de Ouro Preto (UFOP), campus Ouro Preto. O escopo da auditoria centra-se nos aspectos fundamentais da Segurança da Informação, notadamente autenticidade, preservação da disponibilidade, integridade e confidencialidade dos dados e informações. Adicionalmente, objetiva-se verificar a conformidade com as diretrizes de segurança de informações estabelecidas e a implementação de controles internos. A condução dos trabalhos orientou-se pelo Manual de Orientação Técnica da Atividade de Auditoria Governamental (MOT) e pela ISO 27001. Cumpre salientar que o escopo da auditoria não abrange recomendações técnicas relativas à qualidade dos ativos tecnológicos ou quais dos mesmos devem ser utilizados ou adquiridos pelo NTI, em razão da ausência de conhecimento técnico da equipe de auditoria nessas áreas. Importante ressaltar que os procedimentos não foram estendidos aos demais campus da UFOP, Mariana e João Monlevade.

A motivação deste trabalho originou-se através do levantamento do Índice Integrado de Governança e Gestão Públicas (iGG 2021) do Tribunal de Contas da União (TCU), o qual constatou uma elevada fragilidade na implementação de atividades relacionadas à segurança da informação na UFOP.

Os objetivos da auditoria consistem em identificar os principais processos de atividade da unidade avaliada quanto à segurança e a disponibilidade dos recursos tecnológicos e das informações, visando avaliar a gestão de riscos e a efetividade dos controles em suas atividades de mitigação de riscos.

Para definição da metodologia a ser utilizada no processo de auditoria, primeiramente, foi realizado o levantamento dos principais aspectos considerados pela ISO 27001 e, os quais o auditor seria capaz de avaliá-los. Posteriormente, uma reunião de *kickoff* foi realizada entre o diretor da unidade, o atual responsável pela gestão de riscos e o auditor responsável pela condução dos trabalhos de auditoria para alinhamentos. Diversas reuniões com servidores de carreira, considerados pela diretora como pessoas chaves sobre os processos auditados, foram conduzidas para compreensão dos processos, riscos inerentes e controles implementados. Após essa etapa, o auditor procedeu a uma análise minuciosa dos processos, avaliando a eficácia dos desenhos de controle, sua operacionalização e se esses de fato mitigam os riscos a eles vinculados.

Como limitação ao trabalho é relevante destacar a formação e a experiência dos membros da unidade de auditoria, os quais não possuem formação na área de tecnologia da informação. Tais membros basearam-se em conhecimentos teóricos obtidos por meio da leitura de materiais técnicos, incluindo a ISO 27001, e esclarecimentos fornecidos pelos servidores do NTI.

RESULTADOS DOS EXAMES

1. Ausência de acompanhamento, avaliação e renovação do Plano Diretor de Tecnologia da Informação e Comunicação – PDTiC.

1.1 - Contextualização

A imperatividade do cumprimento do Plano Diretor de Tecnologia da Informação e Comunicação (PDTiC) encontra-se consagrada na Instrução Normativa SGD nº 01 de 4 de abril de 2019. Este plano deve ser meticulosamente concebido pela unidade competente dos órgãos e entidades, sendo, em seguida, submetido à aprovação pelo respectivo Comitê de Governança Digital.

É incumbência essencial que o PDTiC seja publicado de forma acessível no portal institucional do órgão ou entidade em questão, com o intuito de conferir maior nitidez e transparência às informações e decisões atinentes. Nesse contexto, a Auditoria Interna (AUDIN) direcionou seus esforços para avaliar a gestão do PDTiC por parte do Núcleo de Tecnologia da Informação da Universidade Federal de Ouro Preto (NTI/UFOP), centrando-se nas seguintes indagações de auditoria: A unidade avaliada procedeu à avaliação dos resultados obtidos em consonância com as metas delineadas no plano diretor? O Plano Diretor, devidamente aprovado pela alta administração ou conselho superior, está em vigor dentro do período de escopo em análise?

Além disso, constatou-se que a Universidade não possui políticas dotadas de diretrizes e procedimentos devidamente mapeados para suas atividades primordiais, especialmente aquelas suscetíveis a riscos significativos. A referida constatação evidencia a lacuna na conformidade com a estrutura mínima de uma política, consoante à descrição subsequente.

- **Título:** O título deve ser claro e indicar o propósito da política.
- **Introdução:** Uma breve introdução que destaca a importância da política e fornece uma visão geral do seu conteúdo.
- **Objetivo:** Declaração clara dos objetivos que a política visa alcançar.
- **Escopo:** Definição dos limites e aplicação da política, indicando quais áreas ou aspectos da empresa ela cobre.
- **Definições:** Se houver termos específicos ou conceitos importantes para a compreensão da política, é útil incluir definições claras.
- **Responsabilidades:** Detalhamento das responsabilidades específicas de cada cargo/função ou departamento em relação à política.
- **Procedimentos:** Descrição passo a passo dos procedimentos que devem ser seguidos para garantir o cumprimento da política.
- **Diretrizes e Regras:** Listagem das diretrizes, regras e padrões que os funcionários devem seguir.
- **Consequências:** Esclarecimento das consequências associadas ao não cumprimento da política.
- **Comunicação:** Informações sobre como a política será comunicada a todos os servidores e sociedade, assim como os meios de comunicação utilizados.
- **Revisão e Atualização:** Instruções sobre como a política será revisada e atualizada, indicando a periodicidade ou os gatilhos para revisões.
- **Referências:** Inclusão de referências a leis, regulamentações ou outras políticas relevantes que possam estar associadas.
- **Aprovação:** Identificação das partes responsáveis pela aprovação da política (coordenação, diretoria do NTI, Comitê e, nos casos que pese, o CUNI) e a data de aprovação.
- **Histórico de Revisões:** Registro das alterações feitas na política ao longo do tempo, incluindo datas e resumos das mudanças.

- **Anexos (se aplicável)**: Adição de documentos, formulários ou outros materiais relacionados à política

1.2 - Situação identificada

Após realização de reuniões, identificamos que a UFOP não realizou uma avaliação relativa ao Plano Diretor de Tecnologia e Comunicação (PDTiC) – Biênio 2020-2021. Adicionalmente, ressaiu que a unidade em questão não ostenta um plano diretor atualizado devidamente referendado pela alta administração e pelo Comitê de Tecnologia de Informação e Comunicação - CTIC.

1.3 - Possíveis consequências

1. Desalinhamento estratégico da unidade com os objetivos da UFOP: A supervisão e avaliação periódica do PDTiC constituem elementos cruciais para assegurar que as operações de Tecnologia da Informação estejam em consonância com os objetivos estratégicos da universidade. A ausência dessa diligência pode acarretar desalinhamento, resultando em projetos e iniciativas de TI que não atendem às metas e necessidades gerais da universidade.
2. Retardo ou incapacidade de identificar riscos e corrigir desvios: o monitoramento das atividades delineadas no planejamento revela-se fundamental para identificar desvios, ajustar estratégias e mitigar riscos
3. Impacto na Governança de TI: A governança efetiva envolve monitoramento constante, avaliação de desempenho e adaptação às mudanças nas circunstâncias internas e externas.
4. Subutilização de recursos: O planejamento tem por objetivo a eficiente e eficaz utilização dos recursos disponíveis. A ausência de avaliação e monitoramento do plano diretor pode resultar em uso inadequado dos recursos à disposição.
5. Falta de transparência e prestação de contas - Accountability: A avaliação e monitoramento do PDTiC são imprescindíveis para assegurar transparência e prestação de contas dos responsáveis. A ausência dessas atividades pode comprometer a capacidade de demonstrar a eficácia e eficiência das operações da unidade perante a alta administração da universidade e à sociedade

1.4 - Conclusão

Diante o exposto, infere-se que a UFOP não realizou a avaliação do PDTiC, carecendo de uma versão vigente do referido plano. Ademais, constata-se que o Comitê de Tecnologia da Informação e Comunicação (CTIC) não participa das deliberações referentes à avaliação e desenvolvimento do plano diretor.

2. Insuficiência de controles sobre ativos tecnológicos.

2.1 - Contextualização

A *International Organization for Standardization* - ISO, por meio da revisão e adaptação em âmbito nacional pela Associação Brasileira de Normas Técnicas - ABNT, estabelece as diretrizes normativas da ISO 27001, a qual se refere ao sistema de gestão de segurança da informação, focando, sobretudo, na salvaguarda dos ativos de informação. No âmbito da ISO 27001, especificamente no seu *Controle 5 - Controles Organizacionais*, delineia-se que a organização deve manter um inventário de ativos, abrangendo dispositivos móveis, e zelar pela segurança adequada desses dispositivos. Assim, a unidade de auditoria buscou analisar se a unidade NTI implementa controles que garantam a segurança dos ativos físicos e se realiza um inventário dos mesmos.

2.2 - Situação identificada

Verificamos que o controle dos ativos tecnológicos, sob a ótica do NTI, reside no inventário conduzido pela Pró-Reitoria de Planejamento - PROPLAD, mediante a constituição de uma comissão de inventário patrimonial, o que implica na ausência de um inventário direto dos ativos tecnológicos pelo NTI. Além

disso, observou-se que o NTI mantém um estoque de peças de reposição, utilizado na manutenção dos ativos tecnológicos, contudo, o controle desse estoque é realizado através de planilha de Excel e não contempla a totalidade dos itens presentes no estoque. No tocante às atividades de substituição de peças em garantia por terceiros, salienta-se, conforme manifestação dos servidores do NTI, que não ocorre a atualização patrimonial dos dispositivos, exemplificando-se com o equipamento Switch. No que concerne aos ativos não físicos, como softwares, a instalação destes nos computadores dos usuários ocorre de forma livre, sendo a responsabilidade do controle atribuída ao chefe/coordenador da unidade, conforme estabelecido em termo de responsabilidade.

2.3 - Possíveis consequências

1. Falta de conhecimento e catologalização dos ativos críticos/significativos: A ausência de um inventário de ativos pode acarretar na falta de compreensão dos ativos críticos para as atividades e operações da unidade. Por consequência, tal situação pode resultar na inadequada priorização adequada na aplicação de medidas de segurança e investimento, deixando ativos importantes vulneráveis a ameaças.
2. Gestão ineficiente de riscos: A ausência de um inventário de ativos pode impedir a unidade de avaliar de maneira adequada os riscos associados a seus ativos, dificultando a implementação de controles eficazes para mitigar esses riscos.
3. Desperdício de recursos: A universidade pode alocar tempo e esforços em áreas menos críticas, enquanto aspectos mais relevantes da segurança da informação podem ser negligenciados.

2.4 - Conclusão

Portanto, verifica-se que a gestão do inventário de ativos é de primordial importância para a universidade. Esta atividade contribui não apenas para a conformidade com a norma ISO 27001, mas também para o fortalecimento geral da postura de segurança dos ativos da universidade.

3. Não utilização da ferramenta de descoberta ativa de rede.

3.1 - Contextualização

A descoberta ativa é uma prática fundamental dentro do contexto da ISO 27001, pois desempenha um papel crucial na identificação de ameaças, vulnerabilidades e na manutenção da segurança da informação. Além disso, a descoberta ativa envolve a busca proativa por potenciais riscos de segurança, em vez de apenas responder a incidentes quando eles ocorrem. Assim, a unidade de auditoria buscou compreender junto a unidade NTI sobre as atividades e utilização da ferramenta de descoberta ativa de rede.

3.2 - Situação identificada

A UFOP utiliza um sistema, versão gratuita, para realizar o procedimento de descoberta ativa de rede. Porém, os servidores destacaram que realizam a inspeção eventualmente, não existindo uma periodicidade definida. Além disso, foi ressaltado pelos servidores que os ativos que utilizam a rede WiFi não podem ser identificados. Por fim, foi salientado que as redes das entidades federais são monitoradas pelo CAIS/RNP, o qual identifica anomalias na rede das entidades governamentais federais e notifica tais ocorrências por meio de e-mails e abertura de tickets de suporte. As unidades notificadas são incumbidas de analisar e, se necessário, tratar os chamados abertos pelo CAIS, fornecendo retorno sobre as providências tomadas. Na UFOP, além de registrar o retorno no sistema de comunicação do CAIS, os servidores realizam o controle e monitoramento das ocorrências no sistema interno da UFOP destinado ao gerenciamento de chamados.

3.3 - Possíveis consequências

1. Descoberta de dispositivos desconhecidos: Novos dispositivos podem ser adicionados à rede sem o conhecimento da unidade NTI, o que implica que dispositivos não autorizados possam representar potenciais pontos de vulnerabilidade ou riscos de segurança.
2. Riscos de segurança: A ausência de visibilidade sobre os dispositivos conectados à rede pode resultar em vulnerabilidades não detectadas, acarretando em riscos à segurança da informação.
3. Dificuldades na resolução de problemas: A falta de uma ferramenta de descoberta ativa atualizada pode dificultar a identificação e resolução eficaz de problemas na rede em tempo hábil.

3.4 - Conclusão

Conclui-se que a utilização regular de ferramentas de descoberta ativa de rede é essencial para manter a segurança, eficiência operacional e conformidade da rede. A ausência de monitoramento sistemático por parte da unidade pode resultar em vulnerabilidades não detectadas, ineficiências operacionais e dificuldades na resolução oportuna de problemas.

4. Ausência de classificação de dados

4.1 - Contextualização

A classificação dos dados de acordo com a ISO 27001 é uma prática essencial para garantir a segurança da informação em uma organização. Outrossim, a Lei Geral de Proteção de Dados (LGPD) regulamenta o tratamento dos dados pessoais por organizações públicas e privadas, sendo um de seus princípios basilares a Segurança e Medidas Técnicas Administrativas de proteção dos dados. Esse princípio corrobora com a necessidade de classificação dos dados, ajudando a identificar a sensibilidade dos dados e a aplicar os controles apropriados.

A classificação de dados desempenha um papel importante e proporciona uma abordagem estruturada para a proteção de informações sensíveis. Nesse contexto, os trabalhos de auditoria propuseram-se a analisar de que maneira a unidade NTI realiza a gestão dos dados institucionais.

4.2 - Situação identificada

A UFOP não possui uma política de gerenciamento de dados que estabeleça os critérios de classificação das informações e dos dados, bem como estabeleça as formas de armazenamento dos mesmos em detrimento a uma classificação e que define quem possui acesso aos dados em relação a sua classificação. Em virtude da inexistência de uma política, não há segregação de dados quanto ao armazenamento e processamento destes, excetuando-se os dados gerenciados pelo sistema SEI. Adicionalmente, a instituição não dispõe de termo de responsabilidade relativo à confidencialidade para os colaboradores terceirizados. Cabe ressaltar, contudo, que os servidores enfatizaram que apenas os servidores de carreira detêm acesso aos dados dos servidores.

4.3 - Possíveis consequências

1. Risco de segurança e deficiência na gestão de riscos: A ausência de uma classificação dos dados pode resultar na falta de compreensão dos distintos níveis de sensibilidade e importância dos dados, expondo a instituição a riscos desconhecidos ou a controles ineficientes.
2. Proteção ineficaz dos dados sensíveis: A falta de classificação dificulta a aplicação de controles de segurança específicos para diferentes categorias de dados. Dados sensíveis podem não receber a proteção adequada, aumentando o risco de acesso não autorizado, vazamento ou comprometimento.
3. Violações de privacidade e conformidade: Considerando que a UFOP administra dados pessoais e informações sensíveis sujeitas a regulamentações de privacidade, a exemplo a LGPD, a ausência

de classificação pode resultar em violações de conformidade legal. Isso pode resultar em penalidades legais e danos à reputação da universidade.

4. Deficiência na implementação de controles de acesso: Com a ausência de uma classificação a universidade pode enfrentar dificuldades na definição de quais usuários devem ter acesso a quais tipos de dados e informações, resultando em práticas de controle de acesso ineficazes.
5. Resposta ineficaz a incidentes: Em caso de violações de dados a falta de classificação dos dados pode dificultar a priorização e a resposta adequada. A unidade pode possuir dificuldades em identificar quais dados foram comprometidos e qual deve ser a resposta apropriada.

4.4 - Conclusão

Conclui-se que a inexistência de uma política e da classificação dos dados e informações pode sujeitar a universidade a uma série de riscos de segurança, violações legais e desafios operacionais, os quais, por sua vez, podem ter impactos significativos na segurança da informação e na reputação da UFOP.

5. Ausência de gerenciamento de contas de usuários

5.1 - Contextualização

A gestão de contas de usuários é um importante procedimento no quesito segurança e é um dos aspectos abordados pela ISO 27001. O devido gerenciamento permite um maior controle de acesso, controle de privilégios, monitoramento de atividades, segregação de funções e gestão de identidades. Isto posto, os trabalhos de auditoria objetivaram avaliar como a unidade NTI realiza o gerenciamento das contas de usuários nos sistemas institucionais da universidade.

5.2 - Situação identificada

Constata-se que a responsabilidade pelo gerenciamento das contas ativas e inativas, bem como pelos privilégios atribuídos a cada usuário em determinado sistema, repousa sobre a unidade administrativa que utiliza referido sistema. Nesse sentido, é incumbência da unidade administrativa informar ao NTI acerca da necessidade de inativação de usuários, bem como inclusão e exclusão de privilégios nos sistemas. Todavia, não se evidencia a existência de uma política formal que defina esse processo, existindo apenas um entendimento informal entre as unidades.

Adicionalmente, não há formalização quanto à periodicidade e responsabilidade do NTI em realizar o inventário de contas de usuários que permanecem ativas, mas não realizam o acesso, "log-in", aos sistemas por determinado período. Destaca-se que a unidade dispõe de um sistema para efetuar tal levantamento e fornecer um relatório.

Outro aspecto que merece consideração é referente aos sistemas utilizados pela UFOP não utilizarem o perfil de usuário padrão - interface de usuários - assim, um servidor que compartilha o mesmo cargo de outro na mesma unidade e desempenha funções análogas pode deter privilégios no sistema que seu equivalente não possui. Consoante a equipe do NTI, a padronização é viável, desde que a unidade administrativa responsável pelo sistema realize o levantamento dos privilégios necessários para cada cargo/função.

Outrossim, não há formalização quanto a quem e em quais situações a conta de usuário ADMINISTRADOR deve ser utilizada. Adicionalmente, inexistem disposições formais sobre as circunstâncias em que as contas de usuários com privilégio de administrador devem ser empregadas em relação a conta administrador.

Em relação aos bolsistas que trabalham no NTI e possuem acesso a algum nível no servidor da instituição, quando ocorre o fim de seu vínculo não há um procedimento formalmente definido que

estabeleça quem e como será realizado o encerramento dos acessos do bolsista ao servidor.

5.3 - Possíveis consequências

1. Risco de acesso não autorizado: A ausência de um robusto gerenciamento de contas pode ensejar riscos significativos de acesso não autorizado. Usuários podem ter permissões excessivas ou não revogadas após a mudança de funções ou alteração de unidade administrativa de atuação, o que pode resultar em acesso não autorizado a dados sensíveis.
2. Comprometimento da privacidade: A ausência de gerenciamento adequado sobre as contas de usuários pode comprometer a privacidade e vazamento dos dados.
3. Segregação ineficaz de função: A falta de uma segregação eficaz de função dentro dos privilégios pode resultar em situações em que um único usuário tem acesso e controle sobre todas as funções críticas. Tal situação aumenta o risco de atividades fraudulentas e erros não intencionais.
4. Resposta ineficaz a incidentes: Em caso de incidentes de segurança, a falta de um gerenciamento eficaz de contas pode dificultar a resposta rápida e precisa. A incapacidade de identificar e isolar contas comprometidas pode prolongar o tempo de resposta e aumentar os danos.

5.4 - Conclusão

A ausência de diretrizes formalizadas acerca do gerenciamento de contas de usuários pode resultar em uma série de riscos de segurança, violações de privacidade, acesso a informações não pertinentes à função, não conformidade com regulamentações e impactos negativos na reputação da universidade.

6. Ausência de critérios de segurança de senhas

6.1 - Contextualização

O gerenciamento de senhas é objeto de diversos controles e requisitos na ISO 27001, especialmente no âmbito do controle de acesso. Este gerenciamento aborda aspectos como a complexidade e requisitos mínimos das senhas exigidas nos softwares institucionais, a temporalidade (rotação) das senhas, a notificação de senhas, entre outros. O escopo do trabalho realizado pela unidade de auditoria neste aspecto visa analisar se a UFOP possui, devidamente parametrizados em seus sistemas, os critérios de segurança relativos a senhas.

6.2 - Situação identificada

Durante a realização dos testes e análises de auditoria, identificou-se que a universidade não dispõe de uma política contendo critérios de segurança específicos para a gestão de senhas. Além disso, constatou-se que no portal "MinhaUFOP", utilizado para acesso aos a maioria dos sistemas institucionais, o método de acesso é o número de CPF do usuário e a senha é escolhida sem a observância de critérios básicos de segurança, como quantidade mínima de caracteres, exigência de caracteres alfanuméricos e especiais. Adicionalmente, nossos testes revelaram que o sistema responsável pela gestão do "MinhaUFOP" permitiu a reutilização de senhas anteriormente utilizadas pelos usuários. Por fim, não há parâmetros nos sistemas para estabelecer o prazo de validade das senhas e exigir sua renovação. Embora o NTI disponha de uma ferramenta capaz de identificar automaticamente o período de inatividade dos usuários no portal "MinhaUFOP", tal informação é consultada apenas em situações especiais

6.3 - Possíveis consequências

1. Comprometimento de contas de usuários: Risco de comprometimento das credenciais dos usuários, o que pode resultar na potencial exploração de contas e em ações maliciosas, como acesso não autorizado e manipulação de dados.
2. Favorecimento a ataques de força bruta: Senhas desprovidas de uma estrutura mínima de

exigência e validade são consideradas fracas, facilitando ataques de força bruta, nos quais invasores tentam adivinhar senhas por meio de repetidas tentativas, utilizando padrões previsíveis.

3. Fraude: Senhas com estruturas consideradas fracas favorecem a usurpação de contas de usuários, assim, essas podem ser exploradas para realizar atividades fraudulentas em nome do usuário afetado.
4. Risco de ataques internos: A ausência de monitoramento adequado, estrutura de segurança e controle sobre senhas pode aumentar o risco de atividades maliciosas por parte de servidores da universidade e ex-servidores, usurpando a conta de usuários de colegas e agindo de forma danosa a instituição.

6.4 - Conclusão

Torna-se imperativo que a UFOP implemente práticas robustas de gerenciamento de senhas a fim de mitigar os riscos supracitados, promovendo a segurança da informação em conformidade com os princípios da boa governança de TI.

7. Ausência de registros de LOG's e trilha de auditoria

7.1 - Contextualização

Com base na ISO 27001, LOG's (registros) e trilhas de auditoria são destacados como componentes essenciais da gestão da segurança da informação. Esses elementos possibilitam o monitoramento, identificação de responsabilidades e responsabilização, investigação de incidentes e avaliação de conformidade. Desta forma, a unidade de auditoria interna objetivou analisar a utilização de LOG's e trilhas de auditoria na gestão da tecnologia da UFOP.

7.2 - Situação identificada

Após análises e informações fornecidas pelos servidores do NTI, destaca-se que apenas alguns sistemas possuem LOGs, não abrangendo a totalidade deles. Somente os sistemas considerados como operações sensíveis dispõem de LOGs. A UFOP não possui uma política de gestão de dados e armazenamento, em decorrência desse fato quem define se o sistema é considerado uma operação sensível para instituição é o cliente solicitante do sistema, no caso a unidade administrativa da UFOP. Nestas operações sensíveis, o mecanismo de LOG registra todas as ações realizadas pelo usuário no banco de dados, permitindo identificar o estado anterior de uma operação antes de qualquer alteração. Em relação aos demais sistemas, que não são considerados operações sensíveis, são registrados os LOGs dos usuários que realizaram alterações, mas não é registrado o conteúdo específico dessas alterações.

Ademais, em virtude da ausência de uma política de armazenamento, os LOG's de autenticação da rede Wifi são armazenados pelo período mínimo de 5 anos. Os LOG's de operações consideráveis sensíveis nunca foram excluídos. No caso dos LOGs dos servidores, estes são excluídos à medida que o espaço de armazenamento atinge sua capacidade total, tendo uma média de duração de armazenamento de um ano. Já os registros de trâmites de atividades em sistemas são armazenados permanente, dado que constituem características do sistema utilizado. Entretanto, caso um cliente, no momento da solicitação da elaboração de um determinado sistema, determine como regra de negócio que o usuário possa excluir determinado trâmite, isso é factível e não é bloqueado pelos desenvolvedores.

7.3 - Possíveis consequências

1. Dificuldades em identificar incidentes de segurança e realizar investigações: A ausência de LOG's de todas as operações podem dificultar a identificação de eventos de segurança, incluindo

incidentes e atividades suspeitas, resultando em atrasos na detecção e resposta a ameaças Ademais, a falta de LOG's e trilhas de auditoria torna a investigação mais complexas, dificultando a reconstrução da cronologia dos eventos, identificação da causa raiz do incidente e implementação de medidas corretivas eficazes.

2. Responsabilidade e responsabilização comprometidas: Com a ausência de LOG's em todos os sistemas torna-se inviável atribuir a responsabilidade por ações específicas aos usuários por suas ações, assim, compromete a capacidade de responsabilização por práticas inadequadas ou maliciosas.

7.4 - Conclusão

Diante do exposto, a manutenção de LOGs revela-se fundamental para a segurança cibernética e eficiência operacional da universidade. Estabelecer uma política com diretrizes bem elaboradas, práticas sólidas de registro e armazenamento de LOGs é uma parte essencial de uma estratégia abrangente de segurança da informação e governança.

8. Ausência de diretrizes de Backup e estrutura segura de armazenamento.

8.1 - Contextualização

O procedimento de backup é fundamental para garantir a continuidade das operações na instituição. Além da proteção contra perda ou danos dos dados, o processo de backup auxilia no reparo de ações que geram danos aos sistemas e as informações, seja por decorrência de fraude ou erro humano. Assim, a unidade auditoria interna objetivou analisar o processo de backup das informações e dados da universidade.

8.2 - Situação identificada

A unidade avaliada apresentou uma política de backup, entretanto, esta exibe diretrizes amplas e genéricas, não refletindo adequadamente os processos e procedimentos executados nas atividades de backup da instituição. Além disso, a política destaca que deve ser revisada a cada dois anos; todavia, não apresenta data de vigência e aprovação pelo CTIC. A formalização de um plano de contingência também não está devidamente delineada.

Conforme discutido em reunião, os servidores salientaram que a infraestrutura para realização dos backups é crítica, considerando os seguintes aspectos:

I. Localização dos servidores - Embora estejam instalados em prédios distintos, encontram-se próximos um do outro.
II. Capacidade de armazenamento de dados operando em seu limite, comprometendo o cumprimento do prazo de armazenamento estipulado pela política.
III. Os softwares utilizados para realização de backup são versões gratuitas, desta forma, não há segurança por parte do software que a execução de suas atividades será realizada de forma completa e eficaz, inexistindo qualquer garantia pela qualidade do serviço pelo fornecedor.
IV. Ausência de criptografia nos backups, devido à falta da tecnologia necessária, prejudicando a segurança da informação.
V. Limitação de espaço nos servidores resultando em backups apenas dos dados, não incluindo configurações de sistemas, servidores e LOGs

Foi destacado que o NTI possui somente um servidor (colaborador) responsável por realizar a gestão de backup de todos os sistemas da universidade, não havendo um substituto caso o servidor se afaste de suas atividades. Outrossim, não há um procedimento e rotinas formalizadas para a realização de

backups; o servidor responsável realiza as atividades com base em sua experiência e disponibilidade de tempo. Na elaboração de novos sistemas institucionais, a capacidade de backups da universidade para atendimento do novo sistema não é avaliada. Por fim, a unidade não realiza testes substantivos para avaliar a completude dos dados armazenados.

8.3 - Possíveis consequências

1. Perda de dados críticos: A falta de políticas e procedimentos adequados de backup coloca a UFOP em risco de perder dados críticos em caso de falha de hardware, não execução do procedimento de backup, ataques cibernéticos, erros humanos ou outros incidentes, acarretando perdas financeiras, danos à reputação e interrupção significativa das atividades.
2. Impacto na continuidade dos negócios da universidade: Um procedimento de backup ineficiente pode resultar em tempo prolongado de inatividade em caso de incidente, prejudicando a recuperação rápida da unidade afetada ou até mesmo da UFOP como um todo.
3. Risco de segurança a informação: A ausência de backups ou a aplicação de uma estratégia inadequada aumenta os riscos de segurança, pois sem cópias de dados seguras e completas, a universidade vulnerável a perdas de dados e a outras ameaças.
4. Prejuízos operacionais: A ausência de recuperação de determinada informação e dados pode resultar em perdas de informações essenciais para execução das atividades pelas unidades e pode gerar a necessidade de retrabalho para transformação de dados em informações que foram perdidas e comprometidas por determinado incidente.
5. Dificuldade na gestão de riscos de TI: A ausência de políticas e procedimentos de backup eficientes dificulta a gestão adequada dos riscos associados à perda de dados e à interrupção das operações.
6. Interrupção das atividades de backup: A dependência de um único servidor para realizar as atividades de backup, sem uma formalização adequada sobre as diretrizes e procedimentos necessários, expõe a universidade ao risco de não realização de backups em caso de ausência desse servidor.

8.4 - Conclusão

A ausência de uma política que reflita de forma mais substancial as diretrizes das atividades de backup da UFOP e a ausência da formalização dos procedimentos, aliadas à ausência de mais um servidor que domine tal atividade, podem resultar em sérias consequências para a segurança da informação, continuidade das atividades e conformidade regulatória da universidade. É crucial implementar práticas de backup adequadas para proteger ativos de informação e garantir a resiliência dos sistemas de informação.

9. Não realização de testes de vulnerabilidade e análise de incidentes.

9.1 - Contextualização

A ISO 27001 enfatiza a importância da realização de testes de vulnerabilidade e análise de incidentes como componentes fundamentais do processo de gestão de segurança. Desta forma, a unidade de auditoria direcionou seus esforços para examinar quais procedimentos são realizados pelo NTI para identificar, registrar e tratar os incidentes de TI, bem como quais testes de vulnerabilidade são realizados.

9.2 - Situação identificada

No ano de 2023, a unidade NTI designou um servidor responsável pelo gerenciamento de riscos, que responde pelos testes de vulnerabilidade e incidentes de rede. Entretanto, durante a reunião com o

servidor responsável, constatou-se que o NTI não mantém um controle e levantamento detalhado dos incidentes ocorridos na instituição durante o período em questão, incluindo as medidas tomadas e os controles estabelecidos para prevenir a recorrência desses incidentes. Adicionalmente, não foram conduzidos testes de vulnerabilidade durante o mesmo período, e o Comitê gestor, responsável pela unidade de tecnologia e informação, não realiza análises ou manifestações sobre a segurança da informação e dos dados da universidade.

9.3 - Possíveis consequências

1. Não identificação de ativos críticos: a unidade não consegue determinar quais ativos estão mais suscetíveis a ameaças e vulnerabilidade.
2. Reincidência de incidentes: Sem uma análise apropriada, a universidade pode não compreender completamente as causas de um determinado incidente, aumentando a probabilidade de reincidência.
3. Exposição a ameaças: Sem a realização de testes de vulnerabilidade torna os sistemas e redes da universidade vulneráveis a ameaças como ataques de hackers e outras formas de exploração.
4. Tempo de resposta prolongado: A ausência de análises adequadas pode resultar em um tempo de resposta mais longo, permitindo que incidentes se tornem mais graves.
5. Não entendimento de um incidente ou ataque: A ausência de análises de incidentes impede a compreensão das técnicas de ataque utilizadas pelos invasores.
6. Exploração e vazamento de dados: Vulnerabilidades não identificadas podem ser exploradas para obter acesso não autorizado, roubo de dados e informações sensíveis da universidade.
7. Interrupção das atividades operacionais da universidade: Ataques à rede e aos servidores podem resultar em tempo de inatividade operacional, afetando a continuidade das operações.
8. Custo de recuperação: A recuperação de um ataque cibernético inclui não apenas a correção das vulnerabilidades, mas também a investigação forense, a restauração de dados e a implementação de medidas de segurança adicionais, além da exposição e impacto na reputação da universidade em mídias sociais e canais de comunicação.

9.4 - Conclusão

A ausência de testes de vulnerabilidade e análise de incidentes em TI pode acarretar implicações graves para a segurança, reputação e continuidade das operações da universidade. É imperativo realizar testes de forma regular, identificar, e corrigir vulnerabilidades para garantir uma postura de segurança robusta. Ademais, é crucial envolver o Conselho Gestor sobre as situações mais críticas.

10. Deficiência na estrutura física do datacenter.

10.1 - Contextualização

A estrutura física de um Data Center desempenha um papel crítico na salvaguarda dos ativos de informação, além de possibilitar a operacionalização dos sistemas institucionais. Em conformidade com determinados requisitos da ISO 27001, a auditoria interna objetiva inspecionar a estrutura física dos data centers da universidade.

10.2 - Situação identificada

A UFOP possui dois Data Center em edifícios distintos. O Data Center localizado no prédio do ICEB – Instituto de Ciências Exatas e Biológicas não apresenta um controle de acesso adequado. Além disso, a sala do Data Center está localizada nos fundos da sala de manutenção de computadores, e a porta de acesso ao Data Center não dispõe de uma tranca de segurança. Em contraste com o Data Center principal, o Data Center nas dependências do ICEB não possui piso elevado, e o acesso não é seguro, constituindo um local facilmente acessível para servidores não autorizados, estudantes e agentes externos à instituição.

10.3 - Possíveis consequências

1. Exposição a ameaças de segurança e falha na proteção física dos equipamentos: A ausência de controle de acesso à dependência do Data Center pode proporcionar ameaças à segurança e manipulação indevida dos dados. Os equipamentos podem estar expostos a riscos físicos caso a infraestrutura não atenda aos padrões de segurança, incluindo falhas na proteção contra acesso não autorizado, roubo de equipamentos e danos acidentais.
2. Interrupção dos serviços: Um Data Center inadequadamente estruturado pode ser mais suscetível a falhas operacionais, resultando em períodos de inatividade e impactando a continuidade das operações da universidade.

10.4 - Conclusão

O Data Center de uma instituição constitui a base de todas as informações e funcionalidade dos sistemas utilizados nas operações administrativas da universidade. Assegurar uma estrutura de proteção observando os requisitos mínimos da ISO 27001 mitiga os riscos expostos acima e garante a operacionalização das atividades institucionais.

RECOMENDAÇÕES

1. Elaborar Políticas Administrativas

Desenvolver políticas administrativas, mapeamento dos processos e procedimentos operacionais padrão (POP) das atividades de risco significativo, principalmente aquelas que apenas um servidor executa toda a atividade. Tais políticas devem delinear as diretrizes e princípios para orientar as atividades nos processos de trabalho. Salientamos observar a estrutura recomendada na Constatação 01.

Achados n°: 1, 2, 3, 4, 5, 6, 7, 8 e 9

Manifestação da unidade auditada

Contextualização: A NTI já iniciou um processo de mapeamento das atividades através da criação de uma wiki (https://wiki.ufop.br/) para concentrar e publicitar as informações. Sendo necessário o mapeamento completo das atividades de risco significativo, principalmente aquelas que apenas um servidor executa toda a atividade para o posterior desenvolvimento e registro das políticas administrativas, mapeamento dos processos e criação do manual de procedimentos operacionais padrão (POP).

Ações a serem realizadas nos próximos 2 anos: Realizar mapeamento; priorizar as atividades; formalizar e registrar as políticas, processos e procedimentos.

2. Elaborar e gerenciar o Plano Diretor da unidade - PDTiC

Elaborar o novo Plano Diretor da unidade de Tecnologia da Informação da UFOP - NTI, PDTiC, considerando exclusivamente as metas pertinentes à unidade e que sejam passíveis de mensuração durante o período de vigência do referido plano diretor.

Achado n°: 1

Manifestação da unidade auditada

O PDTIC atual está em análise de desempenho e resultados em caráter interno para o devido

encerramento, sendo que foi solicitado sua prorrogação até junho de 2024. Serão realizados os trâmites de solicitação de criação da comissão para a elaboração do novo plano a ser publicado até 07/2024.

3. Submeter ao Comitê de Tecnologia de Informação e Comunicação - CTIC as questões de governança, direcionamento estratégico e tomada de decisões

Submeter ao CTIC as avaliações realizadas conduzidas acerca do PDTiC, com o propósito de promover discussões e obter análises, por parte do CTIC, sobre as metas alcançadas, em andamento e as não alcançadas. Nesse contexto, busca-se uma análise aprofundada e colaborativa visando aprimorar a estratégia do NTI e corroboração para a efetividade e eficácia do plano diretor.

Ademais, envolver o CTIC nas questões relacionadas às deficiências identificadas na infraestrutura tecnológica e nas demandas de recursos humanos.

Apresentar ao CTIC os resultados dos testes de vulnerabilidade, promovendo discussões acerca das ações necessárias para mitigar os riscos identificados durante os referidos testes.

Achados n°: 1, 2 e 9.

Manifestação da unidade auditada

O Inventário de Necessidades foi repriorizado e apresentado ao CTIC na reunião realizada em 07 de junho de 2023, às 09h. Na ocasião também foram apresentados aos membros presentes as necessidades identificadas na infraestrutura tecnológica e as demandas de recursos humanos para continuidade de execução do PDTIC

4. Realizar inventário dos ativos tecnológicos de valor significativo

Constituir uma comissão interna para realização periódica de inventário dos itens tecnológicos de valor significativo, com o objetivo de mapear sua localização e avaliar a qualidade dos referidos itens.
Achados n°: 2

Manifestação da unidade auditada

Em relação ao inventário de ativos permanentes da UFOP, incluindo os ativos de TIC, o setor responsável pela gestão desse inventário é a Coordenadoria de Materiais e Patrimônio, vinculada à Pró-Reitoria de Finanças. Esta Coordenadoria realizará o inventário ainda este ano conforme informações no processo SEI 23109.009084/2023-39 e cada setor será responsável por realizar o levantamento dos ativos sob sua responsabilidade. Os ativos de TIC com valores significativos estão sob a responsabilidade da NTI e quando o processo de inventário for iniciado, uma comissão interna será criada para conduzir o inventário em questão.

Considerando a Segurança da Informação, o principal foco do inventário é o de software nos ativos de TIC (desktops, computadores, notebooks e servidores). Este inventário é realizado de forma automática em todos os equipamentos pertencentes à UFOP. Para esta finalidade, utilizaremos o software livre 'OCS Inventory'. Além disso, estamos estudando melhorias para este inventário, considerando a utilização da ferramenta Provedor de Credenciais do Google para Windows (GCPW), disponível no contrato que a UFOP possui com a Google (convênio Google Workspace For Education). Para mais informações sobre o contrato consulte o processo SEI 23109.011836/2021-60.

5. Estabelecer controle sobre os itens/peças utilizadas para manutenção de equipamentos

Definir um servidor de carreira responsável pelo gerenciamento do estoque de itens utilizados para manutenção dos equipamentos.
Achados n°: 2

Manifestação da unidade auditada
A gestão do estoque de itens/peças destinados à manutenção é, atualmente, incumbida ao servidor de carreira Luciano Dias Assunção Coutinho. Além da documentação e monitoramento através de planilhas, empregamos o sistema GLPI para uma administração mais eficaz e estruturada do estoque.

6. Executar testes periódicos de descoberta ativa de rede

Empregar a utilização de um software de acordo com a periodicidade definida em política, conforme Recomendação 01. Os servidores do NTI devem conduzir testes utilizando a ferramenta de descoberta ativa de rede e analisar e tratar as anomalias identificadas conforme a classificação estabelecida em política.
Achado nº: 3

Manifestação da unidade auditada
No achado nº 3, não foi claramente delineado o procedimento para a liberação de equipamentos visando o acesso à rede de dados cabeada e sem fio da UFOP. Atualmente, possuímos um processo bem estabelecido para o acesso dos equipamentos à rede de dados da UFOP, conforme descrito abaixo:

1- Rede de dados cabeada:

Os acessos são liberados por equipamento (desktops, computadores, notebooks e servidores).

Para obter acesso à rede cabeada da UFOP, os responsáveis pelos equipamentos devem seguir as orientações disponíveis no link: https://nti.ufop.br/book/rede-com-fio. É importante ressaltar que não é possível acessar a rede cabeada sem completar este processo de cadastro.

2- Rede de dados sem fio:

O acesso é liberado por usuário, não por equipamento.

Atualmente, a rede sem fio oficial da UFOP, pela qual a NTI é responsável, é a rede com o SSID "eduroam". Para ter acesso, os usuários da UFOP devem seguir as orientações disponíveis no link: https://nti.ufop.br/book/rede-sem-fio. Como o acesso é vinculado ao usuário e não ao equipamento, esta rede possui restrições de acesso e é monitorada com detalhes sobre os acessos dos usuários, independentemente do equipamento utilizado para acessá-la.

Em relação às recomendações, planejamos realizar as seguintes ações:

Ações de curto prazo (1 ano):

1- Realizar varreduras a cada 06 meses para identificar os equipamentos conectados à rede cabeada. Os equipamentos não detectados serão removidos do cadastro e, consequentemente, perderão o acesso à rede cabeada de dados da UFOP;

2- Implementar o uso da ferramenta Provedor de Credenciais do Google para Windows (GCPW), disponível no contrato que a UFOP possui com a Google (convênio Google Workspace For Education), para auxiliar na gestão de inventário e descoberta de rede.

Ação de longo prazo (3 anos):

1- Implementar uma solução automatizada que, por meio de descoberta ativa de rede, impeça que equipamentos que não estejam em conformidade com as políticas de segurança ingressem na rede cabeada e sem fio da UFOP.

7. Implementar o perfil de contas nos sistemas institucionais.

Elaborar, em conjunto a alta administração da universidade, uma determinação que oriente as unidades administrativas a efetuarem o levantamento dos cargos internos e os respectivos acessos ao sistema que são necessários para execução das atividades vinculadas à função. O NTI pode elaborar uma planilha padrão que auxilie as unidades administrativas a realizar tal levantamento e que seja um documento padrão que facilite a parametrização nos sistemas.
Achado n°: 5

Manifestação da unidade auditada
Será elaborado um projeto a ser submetido ao CTIC, pois se trata de uma atividade que necessita de um suporte de sistema de informação integrado à base de dados para uma administração eficiente, além de envolver todas as unidades da UFOP.

Ações a serem realizadas até julho 2024: Elaboração de projeto e submissão ao CTIC.

8. Implementar CheckList para exoneração de servidores

Elaborar um Checklist que deve ser observado em todas as instâncias de exoneração e/ou encerramento de contratos de usuários detentores de acesso a sistemas e servidores da UFOP.
Alinhar junto à PROGEP que o referido Checklist seja subscrito por alçada competente do NTI em cada procedimento de encerramento de atividades no âmbito da UFOP, assegurando, desse modo, que o NTI tenha pleno conhecimento do término do vínculo e que todas as permissões de acesso tenham sido devidamente cessadas.

Achado n°: 5

Manifestação da unidade auditada
Será elaborado um projeto a ser submetido ao CTIC, pois se trata de uma atividade que necessita de um suporte de sistema de informação integrado à base de dados para uma administração eficiente, além de envolver todas as unidades da UFOP.

Ações a serem realizadas até julho 2024: Elaboração de projeto e submissão ao CTIC.

9. Implementar parâmetros de gerenciamento de senhas nos sistemas institucionais

Parametrizar os sistemas institucionais para aderir aos critérios mínimos de senhas definidos em política, conforme Recomendação 01. Isso envolve a consideração do prazo de validade de senhas e que o sistema solicite a renovação da mesma, não permitindo reutilizar as três últimas senhas cadastradas,
Achado n°: 6

Manifestação da unidade auditada
Durante o ano de 2023 foi implementada a ação de critérios de criação de senhas para o portal MinhaUFOP. Além do acesso ao portal os usuários utilizam esta mesma senha para o acesso a diversos outros serviços disponibilizados pela NTI. Sobre a solicitação periódica de troca de senha esta Diretoria

não entende como uma ação segura e pretende implementar uma solução de controle ativo de senhas utilizando as ferramentas de segurança disponibilizadas pelo convênio Google Workspace For Education.

Ações a serem realizadas até dezembro de 2025: Elaboração de projeto e submissão ao CTIC.

10. Diagnóstico da infraestrutura necessária de T.I

Realizar o inventário e diagnóstico da infraestrutura indispensável para as atividades delineadas a seguir, visando assegurar a qualidade, segurança, integridade e autenticidade das informações, bem como a eficácia das operações administrativas. Submeter o diagnóstico ao CTIC e à alta administração da universidade com o propósito de alinhar estratégias que satisfaçam as demandas identificadas.

1. Estrutura de backup: Realizar o inventário de infraestrutura mínima necessária para garantir a realização de backups de dados, informações e LOGs, garantindo a completude, segurança, fidedignidade e qualidade dos mesmos.
2. Segurança: Identificar os equipamentos e softwares essenciais para garantir a segurança das informações, acessos e dados da instituição.
3. Testes de vulnerabilidade: Verificar os softwares necessários para a realização de testes de vulnerabilidade e para o tratamento das ameaças identificadas, evitando agir de modo reativo e sim, preventivo.

Achado n°: 8 e 9.

Manifestação da unidade auditada

Essa diretoria enfatiza a importância de conduzir o diagnóstico por meio do instrumento Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC), que é um mecanismo de análise, planejamento e gestão dos recursos e processos de TIC. Seu objetivo é atender às necessidades finalísticas e de informação de um órgão ou entidade durante um período determinado.

É relevante destacar que a administração da UFOP elabora anualmente um plano que esta diretoria submete, incluindo demandas para aprimorar a infraestrutura. Isso visa garantir a qualidade, segurança e autenticidade das informações, bem como a excelência dos serviços de TIC oferecidos à comunidade. Para ilustrar esses investimentos, apresentamos a seguir os valores alocados em TIC pela UFOP nos últimos 03 anos.

ANO	VALOR
2021	R$ 3.827.138,38
2022	R$ 2.236.839,46
2023	R$ 3.214.505,61

Em relação às recomendações, apresentamos as informações sobre as ações a serem implementadas:

1- Estrutura de backup:

Informação: Foram adquiridas licenças de uma solução de backup de mercado que atende aos requisitos para garantir a completude, segurança, fidedignidade e qualidade dos dados.

Ações de curto prazo (1 ano):

- Implementar a replicação dos backups fora da UFOP, em um projeto conjunto com UFSJ e UFLA, onde cada instituição manterá uma cópia do backup armazenada na infraestrutura da outra;

- Capacitar mais servidores do quadro para operar os sistemas de backup que a NTI mantém.

Ações de longo prazo (3 anos):

- Adquirir mais licenças da solução de backup e incluir mais serviços nos mesmos;

- Implementar um projeto de backup na nuvem.

2- Segurança: Identificar os equipamentos e softwares essenciais para garantir a segurança das informações, acessos e dados da instituição.

Ação de longo prazo (3 anos):

- Reestruturação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Esta ação está no escopo do trabalho da equipe.

Ação de curto prazo (1 ano):

- Testes de vulnerabilidade: Reestruturação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Esta ação está no escopo do trabalho da equipe.

11. Realizar testes de completude e fidedignidade dos Backups

Em conformidade com a periodicidade estipulada em política, conforme Recomendação 01, executar testes aleatório dos dados e informações contidas nos backups, com intuito de validar a acurácia dos dados e informações. As anomalias identificadas devem ser analisadas e reportadas ao CTIC visando a discussão e a identificação de soluções.
Achado nº: 8.

Manifestação da unidade auditada
Ação de curto prazo (1 ano): Reestruturação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Esta ação está no escopo do trabalho da equipe

12. Análise dos setores com carência de pessoal

O conhecimento sobre os procedimentos relativos à realização dos backups dos dados, informações e LOGs encontra-se centralizado em um servidor exclusivo. A fim de mitigar o risco de não realização do procedimento, assim como para outros processos de trabalho do NTI, recomenda-se a condução de um diagnóstico dos setores do NTI avaliando o volume de demandas de trabalho e o corpo técnico disponível e o necessário. Classificar os setores em situação crítica e apresentar o diagnóstico ao CTIC e a alta administração institucional.
Achado nº 2, 5, 8

Manifestação da unidade auditada
Será executado em paralelo com a recomendação 1.

Ação de curto prazo (1 ano): Reestruturação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Esta ação está no escopo do trabalho da equipe.

13. Reforçar estrutura do Data Center

Efetuar um diagnóstico da infraestrutura indispensável do Data Center situado no edifício do ICEB, com o intuito de atender os requisitos mínimos de segurança exigidos pela ISO 27001. Posteriormente, apresentar ao CTIC e alta administração institucional.
Achado nº: 10

Manifestação da unidade auditada

Ações de curto e médio prazo (2 anos): Reestruturação da Equipe de Tratamento e Resposta a Incidentes Cibernéticos (ETIR). Esta ação está no escopo do trabalho da equipe