UNIVERSIDADE FEDERAL DE MINAS GERAIS

AUDITORIA-GERAL

RELATÓRIO DE AUDITORIA Nº 09/2024 AG/UFMG

1. A AUDITORIA-GERAL

A Auditoria-Geral da Universidade Federal de Minas Gerais (UFMG), órgão de assessoramento do Conselho Universitário, conforme seu Regimento Interno, sujeita-se à orientação normativa e à supervisão técnica do Órgão Central do Sistema de Controle Interno do Poder Executivo Federal e atua como órgão de apoio técnico do Comitê de Governança, Riscos e Controle (CGRC) da Universidade. A sua missão é apoiar a UFMG em seu funcionamento e evolução, adicionar valor, melhorar a eficiência, fortalecer a gestão e proteger as suas operações, fornecendo avaliação, assessoria e conhecimento de forma objetiva e baseada em riscos.

O trabalho realizado compreende a avaliação da regularidade na aplicação de recursos públicos, economicidade, eficiência e eficácia da gestão orçamentária, financeira e patrimonial, assim como adequação e suficiência dos mecanismos de governança, controles e transparência estabelecidos e eficácia da gestão na conformidade das atividades executadas.

As avaliações descritas neste Relatório, baseadas nas regulamentações do Órgão Central do Sistema de Controle Interno do Poder Executivo Federal, referem-se aos critérios técnicos, objetivando o auxílio à Unidade Auditada, não devendo ser interpretadas como avaliação dos gestores e servidores envolvidos nos trabalhos analisados por meio da nossa amostra.

2. RESUMO

I. Qual foi o trabalho realizado pela Auditoria-Geral da UFMG?

Trata-se de auditoria para avaliar as ações de Segurança da Informação realizadas pela Universidade Federal de Minas Gerais (UFMG).

Foram analisados procedimentos, instalações físicas e ativos – definidos em amostra não probabilística – visando obter evidência adequada e suficiente sobre a conformidade das atividades da Faculdade de Educação[1] da UFMG em relação às normas sobre Segurança da Informação. Nesse sentido, o objeto foi avaliado sob 5 (cinco) dimensões: i) Gestão de ativos de *hardware*; ii) Gestão de ativos de *software*; iii) Gestão de acesso (conduta dos usuários); iv) Gestão de acesso (utilização de dispositivos); e v) Gestão de ativos de recursos humanos.

O desfecho da avaliação comporá o resultado quanto à legalidade e à legitimidade dos procedimentos; planejamento e controle interno; transparência; e governança e controle interno.

II. Por que a Auditoria-Geral da UFMG realizou este trabalho?

O trabalho realizado teve como objetivo atender ao item nº 24 do Plano Anual de Atividades de Auditoria Interna (PAINT) de 2024, qual seja: avaliar as ações relacionadas à segurança da informação implementadas pela Universidade em consonância à legislação sobre a matéria.

A Segurança da Informação é abordada também no Plano de Desenvolvimento Institucional (PDI) 2018-2023 da UFMG, onde consta como ação, no âmbito do item Tecnologia de Informação:

· Fortalecer a política de Segurança da Informação para Universidade e dar suporte ao monitoramento e implantação de soluções de segurança no ambiente digital.

III. Quais as conclusões alcançadas pela Auditoria-Geral da UFMG? Quais as recomendações?

A partir da execução deste trabalho foi possível identificar pontos positivos e relevantes à organização da referida Unidade, destacando-se a prontidão, a presteza e a qualidade no atendimento às diversas demandas apresentadas.

Em contrapartida, as inconsistências dizem respeito aos seguintes tópicos, em suma:

- Precariedade de controle de inventário de *hardware*, impactando em:
  - divergência entre a real localização dos ativos e sua situação de registro no Sistema de Controle Patrimonial (SICPAT); e
  - não localização de ativos, os quais constam registrados, pelo SICPAT, na referida Unidade;
- Fragilidade no controle referente à manutenção das placas patrimoniais devidamente afixadas;
- Fragilidade nos instrumentos de controle formal para garantir a atualização do SICPAT em hipótese de saída ou movimentação de agente cadastrado como responsável pelos ativos;
- Ausência de medidas de segurança para o uso dos dispositivos de propriedade da organização fora das dependências da unidade, como Termo de Responsabilidade ou instrumento semelhante para este fim;
- Vulnerabilidade no processo de catalogação e mapeamento dos *softwares* utilizados para armazenamento, manipulação ou exclusão das informações e sistemas relacionados a este fim;
- Fragilidade nos procedimentos institucionais para garantir a realização periódica de *backup* dos dados locais dos respectivos setores;
- Vulnerabilidade no controle para garantir que os usuários desligados da unidade tenham cancelados seus direitos de acesso a equipamentos, sistemas e redes;
- Ausência de instrumento de controle para evitar a utilização sem permissão de:
  - dispositivos móveis e mídias removíveis para fins de armazenamento de informação; e
  - aplicativos ou recursos de armazenamento em nuvem não disponibilizados pelo setor responsável;
- Ausência de medidas formais e periódicas e atualizadas de capacitação e/ou conscientização dos recursos humanos sob sua gestão em temas relacionados à segurança da informação.

As recomendações abrangem a promoção da atualização do SICPAT de forma que o sistema reflita a real localização dos bens da unidade e que ocorra a exclusão do usuário nas hipóteses de desligamento ou movimentação do servidor cadastrado como responsável por ativos; adoção de procedimentos sistemáticos para afixação e manutenção de registro patrimonial por meio da plaqueta ou etiqueta destinada a este fim; institucionalização de procedimentos para controle de retirada ou movimentação de bens como assinatura de Termo de Responsabilidade ou instrumento semelhante; instituição de um sistema de inventário/mapeamento dos *softwares* e sistemas de acesso à informação; realização periódica de *backup* da integralidade dos dados gerenciados pela Unidade; estabelecer procedimentos para garantir o cancelamento de direitos de acesso aos usuários desligados da unidade; e promoção de medidas de capacitação e

conscientização sobre temas de Segurança da Informação junto aos servidores (como por exemplo utilização de dispositivos móveis e mídias removíveis, armazenamento de dados em nuvem, orientação sobre a importância de não utilizar correios eletrônicos de domínio privado para fins profissionais, necessidade de se evitar a criação de senhas fraca, utilização de senhas distintas para os diversos sistemas, etc).

3. LISTA DE SIGLAS E ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

APF – Administração Pública Federal

CGU – Controladoria Geral da União

EA – Escola de Arquitetura

ECI – Escola de Ciência da Informação

FAE – Faculdade de Educação

GSI/PR – Gabinete de Segurança Institucional da Presidência da República

IEC – International Electrotechnical Commission

ISO – International Organization for Standardisation

LGPD – Lei Geral de Proteção de Dados

MGI – Ministério da Gestão e Inovação

MP – Ministério do Planejamento, Orçamento e Gestão

NBR – Normas Brasileiras

PAINT – Plano Anual de Atividades de Auditoria Interna

PDTIC – Plano Diretor de Tecnologia da Informação e Comunicação

POSIN – Política de Segurança da Informação

PTA – Plano de Trabalho da Auditoria

PPSI – Programa de Privacidade e Segurança da Informação

SEI – Sistema Eletrônico de Informação

SFC – Secretaria Federal de Controle da Informação

SICPAT – Sistema de Controle Patrimonial

TCU – Tribunal de Contas da União

UFMG – Universidade Federal de Minas Gerais

UAIG – Unidades de Auditoria Interna Governamental

4. INTRODUÇÃO

Por meio deste relatório, apresentam-se os resultados do trabalho de avaliação de conformidade dos procedimentos adotados pela Faculdade de Educação em relação às normas sobre Segurança da Informação aplicáveis. O trabalho foi derivado da apuração da Matriz de Riscos elaborada no Plano Anual de Atividade de Auditoria Interna (PAINT) 2024.

Os procedimentos de Segurança da Informação encontram previsão em leis e decretos. Há, ainda, *frameworks*, normas técnicas e outras normas infralegais que orientam o processo de adequação e também guiaram este trabalho, conforme demonstrado a seguir:

- **Leis e Decretos:**

- Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados (LGPD);
- Decreto nº 9.637, de 26 de dezembro de 2018 – Institui a Política Nacional de Segurança da Informação;
- Decreto nº 10.332, de 28 abril de 2020 – Institui a Estratégia de Governo Digital para o período de 2020 a 2022; e
- Decreto nº 10.748, de 16 de julho de 2021 – Institui a Rede Federal de Gestão de Incidentes Cibernéticos;

- **Normas infralegais do Gabinete de Segurança Institucional (GSI):**
  - Instrução Normativa nº 1 GSI/PR, de 27 de maio de 2020 – Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;
  - Instrução Normativa nº 2 GSI/PR, de 24 de julho de 2020 – Altera a Instrução Normativa nº 1, de 27 de maio de 2020;
  - Instrução Normativa nº 3 GSI/PR, de 28 de maio de 2021 – Dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;
  - Portaria GSI/PR nº 93, de 18 de outubro de 2021 – Aprova o glossário de segurança da informação; e
  - Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) – Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

- **Políticas da UFMG:**
  - Portaria nº 4.668, de 29 de junho de 2021 – Aprova o Plano Diretor de Tecnologia da Informação e Comunicação da Universidade Federal de Minas Gerais (PDTIC/UFMG), com vigência para 2021 e 2024;
  - Política de Segurança da Informação (POSIN-UFMG);

- **Normas técnicas, Guias, Manuais, etc.:**
  - Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos;
  - Guia do *Framework* de Privacidade e Segurança da Informação, Versão 1.1.2 (MGI, 2023).

A seleção deste tema se justifica por critérios de criticidade e relevância. Além disso, trata-se de um assunto atual que tem demandando providências dos órgãos da Administração Pública Federal no âmbito do Programa de Privacidade e Segurança da Informação (PPSI), um conjunto de projetos e processos de adequação voltados a levar a maturidade, a resiliência, a efetividade, a colaboração e a inteligência dos órgãos e entidades, em termos de privacidade e segurança da informação.

Para alcançar o objetivo do trabalho, buscou-se responder às seguintes questões de auditoria:

Questão 1: Gestão de Ativo – Hardware: A unidade gerencia ativamente (inventariar, rastrear e corrigir) os equipamentos utilizados para armazenamento, transmissão e processamento de informação?

Questão 2: Gestão de Ativo – Software: A unidade gerencia ativamente (inventariar, rastrear e corrigir) os *softwares* e sistemas utilizados para armazenamento, transmissão

e processamento da informação?

Questão 3: Gestão de Acesso – Conduta dos usuários: A unidade gerencia ativamente o rol de usuários com acesso aos ativos de informação?

Questão 4: Gestão de Acesso – Utilização de dispositivos: A unidade gerencia ativamente a utilização de dispositivos móveis?

Questão 5: Gestão de Ativos – Recursos Humanos: A unidade adota procedimentos para a disseminação da cultura e boas práticas de Segurança da Informação?

A avaliação do objeto ocorreu por meio de:

· **Testes substantivos:** visando à obtenção de evidência quanto a suficiência, exatidão e validade dos dados produzidos pelos sistemas de informações da entidade; e

· **Testes de observância:** visando a obtenção de uma razoável segurança de que os controles internos estabelecidos pela administração estão em efetivo funcionamento, inclusive quanto ao seu cumprimento pelos funcionários da entidade.

Para tanto, os trabalhos foram realizados em conformidade com os preceitos de auditoria interna aplicáveis ao Poder Executivo Federal, utilizando-se a aplicação de *checklist*, de questionário e de entrevista, além de análise documental e visitas *in loco*. Destaca-se que o uso dessas técnicas consta do Plano de Trabalho de Auditoria (PTA) e que elas visam à adição de valor à Universidade e também à efetividade das respectivas políticas públicas.

Neste trabalho de auditoria, conforme demonstrado no Quadro 1, a análise se deu a partir de 4 (quatro) ferramentas metodológicas, quais sejam: (i) análise documental; (ii) indagação; (iii) observação e (iv) inspeção.

Quadro 1 – Subquestões e técnicas aplicadas

Subquestão	Técnicas
1.1 A unidade possui inventário dos dispositivos que permitem o acesso à informação (exemplo: computadores, notebooks, tablets, celulares, etc.), sob sua responsabilidade?	Análise documental (fonte: SICPAT; sites institucionais) Indagação[2] Inspeção (vide quadro Amostras: "Inventário de *hardware*" e "Inventário de periféricos"[3], disponível no Apêndice)
1.2 A unidade possui instrumento para garantir que servidores cadastrados como responsáveis por ativos em inventário sejam removidos dessa função em hipótese de movimentação ou desligamento da unidade (exoneração, demissão, aposentadoria, remoção redistribuição, etc.)?	Análise documental (fonte: SICPAT; Portal da Transparência) Indagação
1.3 A unidade possui instrumento de controle e identificação do agente público responsável pelo equipamento corporativo? Se sim, o documento é objeto regular de atualização de forma a considerar as movimentações e saídas de agentes?	
1.4 A unidade possui instrumentos de controle para prevenir o acesso físico não autorizado, danos e interferências aos recursos de processamento das informações?	Indagação Inspeção (vide quadro Amostra: "Segurança Física"[4], disponível no Apêndice) Observação (visita *in loco*[5])
1.5 A unidade possui instrumentos de controle para garantir que os ativos de informação estejam protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizados?	Indagação Inspeção (vide quadro Amostra: "Segurança
1.6 A unidade possui instrumentos de controle para garantir que os dispositivos estejam protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das	

utilidades? Quais medidas são tomadas neste sentido?	Física”[6], disponível no Apêndice)
1.7 Os equipamentos são objeto de manutenções e atualizações periódicas para assegurar a sua contínua integridade e disponibilidade? A Unidade possui instrumento de controle para garantir essas realizações periódicas?	
1.8 A unidade possui instrumento de controle para que os equipamentos não sejam retirados do local sem autorização prévia?	Análise documental (fonte: SICPAT; sites institucionais) Indagação Inspeção (vide quadro Amostras: “Inventário de *hardware*” e “Inventário de periféricos”, disponível no Apêndice)
1.9 A unidade possui equipamentos sendo utilizados fora das dependências da organização? Em caso positivo, são tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes ricos decorrentes do fato de se trabalhar fora das dependências da organização? Os usuários autorizados a retirar equipamentos assinam Termo de Responsabilidade ou instrumento congênere?	
1.10 Em hipóteses de reutilização ou descarte de dispositivo, a unidade possui medidas de controle para garantir que todos os dados sensíveis e *softwares* licenciados tenham sido removidos ou sobre gravados com segurança?	Indagação
1.11 A unidade possui instrumento de controle para garantir que as compras de ativos de *hardware* sejam precedidas de análise por setor com o devido conhecimento técnico de forma a evitar a aquisição de equipamentos em desconformidade com as necessidades, requisitos de segurança e infraestrutura da Unidade?	Análise documental (fonte: sites institucionais) Indagação
2.1 A Unidade possui inventário de *softwares* e sistemas de acesso à informação?	Indagação
2.2 A Unidade possui mecanismos de monitoramento quanto ao acesso e uso relativo aos serviços de rede?	
2.3 A Unidade possui procedimentos para evitar a instalação de *softwares* e recursos não autorizados, providos ou homologados pelo setor competente?	Análise documental (fonte: sites institucionais) Indagação
2.4 A Unidade mantém procedimentos para garantir a realização periódica de *backup*?	Indagação Inspeção Observação (visita *in loco*)
2.5 A unidade mantém procedimentos para garantir a atualização periódica de *softwares*?	Indagação
3.1 A Unidade possui instrumentos para evitar o acesso indevido, de visitantes, aos dispositivos móveis com acesso à informação?	Indagação Inspeção (vide “Amostra: Segurança Física”, disponível no Apêndice)
3.2 A Unidade possui processo formal de registro de direitos de acesso ao usuário, de forma a mapear os usuários com acesso aos ativos?	Indagação
3.3 A Unidade possui processo formal de cancelamento de direitos de acesso ao usuário, de forma a garantir o cancelamento de direitos de acesso ao usuário desligado da instituição?	
3.4 A Unidade possui procedimentos para evitar que o usuário tenha acesso a informações que extrapolem sua competência de execução?	
4.1 A Unidade possui instrumentos de controle para evitar a utilização de aplicativos ou recursos de armazenamento em nuvem não disponibilizados pelo setor responsável sem permissão?	
4.2 A Unidade possui instrumento de controle para evitar o acesso sem autorização aos recursos corporativos através de dispositivos móveis particulares?	
4.3 A Unidade possui procedimentos de controle referentes à utilização de dispositivos móveis e mídias removíveis para fins de armazenamento da informação classificada?	Analise documental (fonte: sites institucionais) Indagação
5.1 A Unidade promove medidas de capacitação e/ou conscientização dos recursos humanos sob sua gestão em temas relacionados à segurança da informação?	
5.2 Sob o aspecto da conscientização, a Unidade orienta seus usuários sobre a necessidade de se evitar a criação de “senhas fracas”, a utilização da mesma senha em diferentes sistemas, a exposição indevida a senha com o intuito de recordá-la e o compartilhamento de contas com demais usuários ou agentes externos?	
5.3 Em complemento à temática da conscientização, a Unidade orienta seus usuários sobre a importância de não utilizar correios eletrônicos de domínio privado para fins profissionais? Incluindo tanto o envio e recebimento de mensagens quanto o armazenamento de informações?	

5.4 a Unidade toma medidas para estimular a adoção de políticas de mesa limpa para papéis e mídias de armazenamento removíveis e uma política de tela limpa para os recursos de processamento da informação?	Indagação Observação (visita[7] às salas 1514 e 2109)
5.5 A Unidade mantém procedimentos para garantir a segregação de funções na operacionalização dos sistemas informatizados?	Indagação
5.6 A Unidade busca orientar os usuários sobre as práticas a serem adotadas em hipóteses de acesso à informação classificada?	

Fonte: Elaborado pela Auditoria-Geral

Sob a subquestão específica, identificada por 4.3 (procedimentos de controle referente à utilização de dispositivos móveis e mídias removíveis para fins de armazenamento da informação classificada), verificou-se a não aplicabilidade tendo em vista a inexistência de informação classificada pela UFMG no período[8].

5. RESULTADO DOS EXAMES

Tendo como base a amostra selecionada, constatou-se, em alguns casos, discrepância entre a localização física dos bens e o local de registro no SICPAT.

De acordo com o Controle 1 do *framework* de Segurança da Informação do MGI, as instituições devem:

"Gerenciar ativamente (inventariar, rastrear e corrigir) todos os ativos institucionais conectados à rede, com o objetivo de identificar precisamente quais necessitam ser monitorados e/ou protegidos dentro da empresa, mapeando todos os ativos não autorizados para uma possível remoção ou remediação futura."

Achado 1. Divergência entre a real localização de ativos e a situação registrada no SICPAT.

Para verificar a correspondência entre a localização física dos bens e seus respectivos locais de registro no SICPAT, foram elaboradas duas amostras para fins de inventário. A primeira, denominada "Inventário de *Hardware*", é composta pelos 35 (trinta e cinco) equipamentos de maiores valores. A segunda, intitulada por "Inventário de Periféricos", é composta por 12 (doze) itens de fácil movimentação. Os resultados evidenciaram que alguns dos itens não se encontravam na localização registrada no SICPAT.

Sendo assim, diante dos resultados da inspeção, observou-se a fragilidade no controle referente ao mapeamento de ativos de informação, o que pode resultar em perda de ativos e/ou das características fundamentais da informação.

Achado 2. Fragilidade no controle referente à manutenção das placas patrimoniais devidamente afixadas.

Através de segunda visita *in loco*, para apresentação de ativos que não haviam sido localizados em visita anterior, verificou-se 2 (dois) microcomputadores na sala 1110 – Lab. Audiovisual Imagem e Som (LAIS), os quais não possuíam placa de identificação patrimonial.

Dessa forma, a falta desta identificação impossibilita a correta individualização e mapeamento dos bens em questão.

Achado 3. Ausência de medidas de controle para garantir que o SICPAT seja atualizado em hipótese de desligamento ou movimentação de servidor.

Não se identificou a existência de controle interno formal para garantir a atualização de responsável por ativos cadastrados no SICPAT em hipótese de desligamento ou movimentação

de servidor.

Por meio de relatório extraído do SICPAT, foram elencados todos os agentes cadastrados como responsáveis pelos bens patrimoniados nos setores da unidade auditada. Em seguida, no Portal da Transparência, fez-se a consulta da situação funcional de cada agente. Nessa oportunidade, constatou-se que os servidores B.J. de O., aposentado desde 03/04/2023; C.C.X.T., aposentada desde 11/10/2023; G.M.P.L, aposentado desde 04/08/2023; G.A.S.R., aposentado desse 05/07/2019; J.M.V, aposentado desde 02/04/2022; L.J.G.S, aposentado desde 17/05/2023; L.H.A.L, aposentada desde 15/03/2022; L.L. de C.P.S, aposentada desde 01/01/2015; M.A. de L.G.N, aposentada desde 29/05/2020; M.Z.V.M, aposentada desde 24/05/2017; O.G. de A.J., aposentado desde 08/10/2019; S.D.G.M, aposentada desde 23/01/2020; S.S. do N., aposentada desde 13/02/2023; T.N. de L. e F., aposentada desde 03/10/2022; permaneciam cadastrados como responsáveis pelo conjunto de bens localizados em suas respectivas salas.

Consoante ao Controle 8.1.2 da Norma ABNT NBR ISO/IEC 27002:2013, temos:

> *"Convém que os ativos mantidos no inventário tenham um proprietário."*

Sendo assim, diante da documentação e dos esclarecimentos apresentados pela unidade auditada, observou-se a existência de 14 (quatorze) servidores já desligados do quadro de pessoal da unidade ainda cadastrados como responsáveis por bens patrimoniados, o que pode resultar em ausência de agente competente pela guarda e pela realização do inventário, bem como na impossibilidade de se aplicar uma possível responsabilização na hipótese de danos e/ou extravios de bens.

Achado 4. Fragilidade nas medidas de segurança para o uso de dispositivos fora de suas dependências, incluindo assinatura de Termo de Responsabilidade ou instrumento semelhante para fins de retirada de ativo.

Identificou-se vulnerabilidade nos controles internos formais estabelecidos para a gestão de retirada de ativos de informação para uso externo às dependências da unidade, como a utilização de Termo de Responsabilidade ou instrumento similar para este fim.

Conforme item 11.2.6 - Segurança de equipamentos e ativos fora das dependências da organização 0 da Norma ABNT NBR ISO/IEC 27002:2013, para o controle:

> *"Convém que sejam tomadas medidas de segurança para ativos que operem fora do local, levando em conta os diferentes riscos decorrentes do fato de se trabalhar fora das dependências da organização."*

Dessa forma, as diretrizes para implementação destacam:

> *"Convém que o uso de qualquer equipamento de processamento e armazenamento de informações fora das dependências da organização seja autorizado pela gerência. Isto se aplica aos próprios equipamentos da organização e aos equipamentos pessoais, usados em nome da organização.*
>
> *a) Convém que os equipamentos e mídias removidos das dependências da organização não fiquem sem supervisão em lugares públicos;*
>
> *c) Convém que os controles para as localidades fora das dependências da organização, como, o trabalho em casa e localidades remotas e temporárias, sejam determinados por uma avaliação de riscos, devendo ser aplicados controles adequados para cada caso, por exemplo, arquivos trancáveis, política de "mesa limpa", controles de acesso a computadores, e comunicação segura com o escritório;*
>
> *d) Quando o equipamento fora das dependências da organização é transferido entre diferentes pessoas ou partes externas, convém que seja mantido um registro para definira cadeia de custódia do equipamento, incluindo pelo menos os nomes e organizações daqueles que são responsáveis pelo equipamento."*

Após realização de duas visitas técnicas (25/07/2024 e 18/09/2024) foram apresentadas Notas de Movimentação de Material Permanente referentes à parte dos ativos que não haviam sido

localizados. Neste documento, consta o empréstimo, dentre outros equipamentos, dos ativos de acesso à informação nºs 1312567 e 1312569. Porém, a data informada para este empréstimo é posterior à data da primeira inspeção.

Dessa forma, diante da documentação e dos esclarecimentos apresentados pela unidade auditada, observou-se fragilidade do referido controle, o que pode resultar na perda de ativos ou dos requisitos essenciais das informações registradas ou em acesso indevido aos equipamentos retirados.

Achado 5. Ausência de inventário de *software* e sistemas de acesso à informação.

Não se identificou a existência de um controle de *software* a fim de possibilitar o mapeamento, gerenciamento, rastreabilidade e integridade de todos os sistemas de armazenamento.

Contudo, conforme Controles de Cibersegurança – Controle 2: Inventário e Controle de Ativos Institucionais do *framework* de S.I. do MGI:

> *"Um inventário de software completo é um recursos crítico para prevenir ataques. Os atacantes realizam varreduras na infraestrutura do órgão continuamente em busca de versões vulneráveis de software que possam ser exploradas. Contudo, sem um inventário completo dos ativos de software, um órgão não pode determinar se possui software vulnerável ou se há violações de licenciamento em potencial."*
>
> *"É fundamental inventariar, compreender, avaliar e gerenciar todos os softwares conectados à infraestrutura. Além de revisar seu inventário de software para identificar quaisquer ativos executando software que não sejam necessários para suas atividades."*

Nesse sentido, o Controle 8.1.1 da Norma ABNT NBR ISO/IEC 27002:2013 dispôs que:

> *"Convém que os ativos associados à informação e aos recursos de processamento da informação sejam identificados, e um inventário destes ativos seja estrutura e mantido."*

Sendo assim, diante da documentação e dos esclarecimentos apresentados pela unidade auditada, observou-se a precariedade do referido controle, podendo resultar em falta de gerenciamento e de monitoramento dos *softwares* e dos sistemas de acesso à informação.

Achado 6. Fragilidade nos procedimentos institucionais para garantir a realização periódica de *backup* dos dados locais dos respectivos setores.

Por meio de indagação junto aos gestores, identificou-se vulnerabilidade no controle interno relativo à realização periódica de *backup*. Constatou-se que a gestão atribui a cada setor a competência pela execução de *backup* periódico de seus respectivos dados locais.

De acordo com o Controle de Cibersegurança – Controle 11: Recuperação de Dados do *framework* de S.I. do MGI, as instituições devem:

> *"Criar e manter práticas de recuperação de dados que sejam capazes de restaurar os ativos da organização para um estado pré-incidente ou o estado mais confiável possível."*

Conforme item 8.5.6 da Política de Segurança da UFMG – POSIN/UFMG é competência e responsabilidade dos dirigentes e das chefias da UFMG:

> *"Garantir a utilização exclusiva dos recursos, serviços e sistemas de tecnologia da informação providos ou homologados pela UFMG, ainda que haja alternativas gratuitas."*

Sendo assim, diante da documentação e dos esclarecimentos apresentados pela unidade auditada, observou-se a ausência de procedimentos para garantir a realização periódica de *backup* dos dados locais de setores, o que pode resultar em perda da integralidade e disponibilidade da informação em hipótese de inutilização de *hardware* ou perda de acesso à locais da rede.

Achado 7. Ausência de procedimento de controle para garantir que agentes desligados

da unidade tenham cancelados seus direitos de acesso a equipamentos, sistemas e redes.

Não se identificou, por meio de indagação junto aos gestores, a existência de controle interno para garantir o cancelamento dos direitos de acesso de usuários de equipamentos, sistemas e redes em hipótese de desligamento da instituição.

De acordo com o Controle 9.2.1 da Norma ABNT NBR ISO/IEC 27002:2013:

> *"Convém que um processo formal de registro e cancelamento de usuário seja implementado para permitir atribuição dos direitos de acesso."*

Sendo assim, diante da documentação e dos esclarecimentos apresentado pela unidade auditada, observou-se a inexistência do referido controle.

Achado 8. Ausência de medidas formais de capacitação e/ou conscientização dos recursos humanos sob sua gestão em temas relacionados à segurança da informação.

Não se identificou, por meio de indagação junto aos gestores, a adoção de medidas formais e institucionais de capacitação e conscientização de recursos humanos em temas relacionados à segurança da informação. A unidade informou que há orientações informais junto aos servidores, sem a implementação de uma política institucional de conscientização.

Conforme controle de Cibersegurança – Controle 23: Conscientização e Treinamento do *framework* de S.I. do MGI, as instituições devem:

> *"As pessoas envolvidas no tratamento de dados são instituídas e conscientizadas sobre privacidade, sendo treinadas para desempenhar suas funções e responsabilidades relacionadas à privacidade de acordo com as políticas, processos, procedimentos, acordos e valores de privacidade da organização."*

Nesse sentido, a política de Segurança a Informação da UFMG, em seus itens 8.5.2, 8.5.7 e 8.5.8, determina que compete aos dirigentes e às chefias, respectivamente:

> *"Promover a capacitação dos recursos humanos sob sua gestão em temas relacionados à segurança da informação"; "estimular a cultura de segurança da informação" e "disseminar normas e boas práticas de segurança da informação".*

Por sua vez, a Norma da ABNT NBR ISO/IEC 27002 elenca diversas práticas relacionadas à conscientização e capacitação, tais como:

> *7.2.1 – "Convém que a Direção solicite a todos os funcionários e partes externas que pratiquem a segurança da informação de acordo com o estabelecido nas políticas e procedimentos da organização.";*
>
> *7.2.2 – "Convém que todos os funcionários da organização e, onde pertinente, partes externas recebam treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.";*
>
> *9.3.1 – "Convém que os usuários sejam orientados a seguir as práticas da organização quanto ao uso da informação de autenticação secreta."*

Nessa orientação e considerando os *frameworks*, procedimentos padronizados e normas técnicas de segurança da informação, apresentamos possíveis temas a serem abordados pelos instrumentos de capacitação e conscientização, como por exemplo: os riscos associados ao uso de correios eletrônicos de domínio privado para fins profissionais; a importância de evitar a criação de senhas fracas e a reutilização de senhas em diferentes sistemas; os perigos da exposição indevida das senhas com o intuito de recordá-las e do compartilhamento de contas; os riscos da utilização, sem permissão, de aplicativos ou recursos de armazenamento em nuvem não disponibilizados ou homologados pelo setor de tecnologia da informação da unidade; os riscos da utilização, sem permissão, de dispositivos móveis e mídias físicas removíveis para fins de armazenamento de informação.

Sendo assim, diante da documentação e dos esclarecimentos apresentados pela unidade

auditada, observou-se a inexistência de medidas formais de capacitação sobre Segurança da Informação, o que pode resultar em incidentes decorrentes da atuação de agentes públicos em desconformidade com as normas aplicáveis.

6. RECOMENDAÇÕES

Achado 1. Divergência entre a real localização de ativos e a situação registrada no SICPAT.

A fim de se evitar o risco de perda de ativos e/ou das características fundamentais da informação ou de acesso indevido aos equipamentos de acesso à informação, o órgão deve atender à recomendação a seguir.

Recomendação 01: Providenciar a atualização do SICPAT, de forma que o sistema reflita a real localização dos bens na unidade.

Achado 2. Fragilidade no controle referente à manutenção das placas patrimoniais devidamente afixadas.

A fim de se evitar o risco de perda de ativos e/ou das características fundamentais da informação, de acesos indevido aos equipamentos de acesso à informação, da rastreabilidade dos equipamentos e da individualização dos bens impedindo a distinção entre os patrimônios da unidade e bens de natureza pessoal, o órgão deve atender à recomendação a seguir.

Recomendação 02: Adotar procedimento sistemático de afixação de número de registro patrimonial nos ativos de segurança da informação de natureza permanente, através de gravação, fixação de plaqueta ou etiqueta apropriada.

Achado 3. Ausência de medidas de controle para garantir que o SICPAT seja atualizado em hipótese de desligamento ou movimentação de servidor.

A fim de se evitar o risco de ausência de agente competente pela guarda e realização do inventário, bem como a impossibilidade de responsabilização em hipótese de danos e/ou extravio de bens, o órgão deve atender à recomendação disposta a seguir.

Recomendação 03: Adotar instrumento de controle que garanta a atualização do SICPAT em hipótese de desligamento ou movimentação de servidor cadastrado como responsável por bens no referido sistema.

Achado 4. Fragilidade nas medidas de segurança para o uso de dispositivos fora de suas dependências, incluindo assinatura de Termo de Responsabilidade ou instrumento semelhante para fins de retirada de ativo.

A fim de se evitar o risco de perda de ativos e/ou das características fundamentais da informação ou de acesso indevido aos equipamentos de acesso à informação, o órgão deve atender às recomendações a seguir.

Recomendação 04: Implementar controle interno assegurando que a retirada de ativos de segurança da informação seja precedida do registro da movimentação no SICPAT e da assinatura de Termo de Responsabilidade ou instrumento semelhante pelo agente.

Sob as quatro recomendações já listadas, informamos que após atualização do SICPAT e encaminhamento do relatório gerado por ele à Auditoria-Interna, elaboraremos novo plano amostral para que, após nova inspeção, seja verificada a: (i) compatibilidade entre a real localização dos ativos e sua situação de registro no SICPAT; (ii) manutenção das placas patrimoniais afixadas nos equipamentos de informação; (iii) ausência de servidores desligados da unidade cadastrados como responsáveis por bens no referido sistema; e (iv), em caso de

utilização de equipamentos fora das dependências da unidade, apresentação de Termo de Responsabilidade ou instrumento congênere para fins de retirada de ativo.

Achado 5. Ausência de inventário de *software* e sistemas de acesso à informação.

A fim de se evitar o risco de gestão inadequada de ativos de *software*, aprimorando a governança dos sistemas de informação, o órgão deve atender à recomendação disposta a seguir.

Recomendação 05: Implementar instrumento de mapeamento de todos os *softwares* e sistemas de acesso à informação utilizados pela Unidade, para inventariamento.

Achado 6. Fragilidade nos procedimentos institucionais para garantir a realização periódica de *backup* dos dados locais dos respectivos setores.

A fim de se evitar o risco de perda da integralidade e disponibilidade da informação em hipótese de inutilização de *hardware* ou perca de acesso a locais da rede, o órgão deve atender a recomendação disposta a seguir.

Recomendação 06: Institucionalizar um procedimento sistemático de *backup* para todos os dados gerados e manipulados pela unidade.

Achado 7. Ausência de instrumento de controle para garantir que agentes desligados da instituição tenham cancelados seus direitos de acesso a equipamentos, sistemas e redes.

A fim de evitar o risco de incidentes de segurança da informação decorrentes do acesso indevido, o órgão deve atender à recomendação disposta a seguir.

Recomendação 07: Implementar instrumento de controle para garantir que agentes desligados da instituição tenham cancelados seus direitos de acesso a equipamentos, sistemas e redes.

Achado 8. Ausência de medidas formais de capacitação e/ou conscientização dos recursos humanos sob sua gestão em temas relacionados à segurança da informação.

A fim de evitar o risco de incidentes de segurança da informação decorrentes da atuação de agentes púbicos em desconformidade com as normas aplicáveis, o órgão deve atender à recomendação disposta a seguir.

Recomendação 08: Promover medidas de capacitação e conscientização sobre a Segurança da Informação junto aos usuários dos *softwares* e sistemas de acesso à informação.

7. QUESTIONÁRIO DE GOVERNANÇA E CONTROLES INTERNOS

Tendo em vista o disposto na Instrução Normativa Conjunta MP/CGU nº 01/2016, no Decreto nº 9.203 de 22 de novembro de 2017 e na Instrução Normativa SFC/CGU nº 03/2017, artigo 78 foi aplicado um Questionário de Avaliação de Governança e Controles Internos (Anexo 2).

Este questionário contou com 26 questões e teve como objetivo avaliar a adequação dos processos de governança, gestão de risco e controles internos instituídos pela Faculdade de Educação, referentes ao ambiente interno, fixação de objetivos e atividades de controle. Esta avaliação comporá a opinião geral da Auditoria-Geral no parecer sobre a prestação de contas anual da UFMG, conforme sugerido pela Instrução Normativa SFC/CGU Nº 05/2021.

Para medir o nível de aplicabilidade nas questões do Questionário, foi definido o índice (A) para avaliação de cara perspectiva e o índice (B) para avaliação total do questionário.

Quadro 2 – Referência sobre os cálculos para os índices do Questionário de Governança e Controles Internos

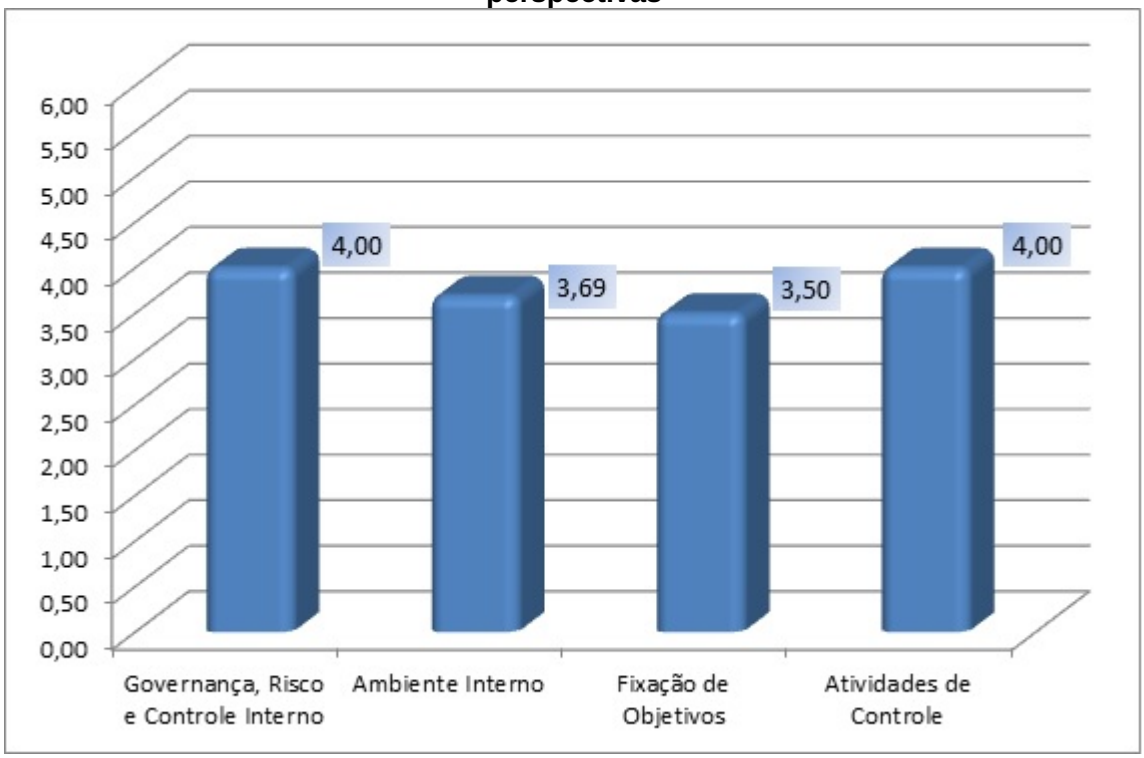
Avaliação de cada perspectiva (A) = X/Y		Avaliação total do questionário (B) = X/Z
X = soma das noras de avaliação - Só das questões de uma perspectiva se avaliação “A”; - De todas as questões do questionário se avaliação “B”	**Y** = nº de questões da perspectiva avaliada (excluindo as “não se aplica” informado pela unidade).	**Z** = nº de questões do questionário (excluindo as “não se aplica” informado pela unidade).

Fonte: Elaborado pela Auditoria-Geral com base nos normativos sobre controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal

De acordo com a metodologia deste questionário, quanto mais próxima a avaliação da perspectiva se encontrar do número 6 – valor máximo a ser obtido – maior a adequação dos procedimentos executados pela unidade auditada ou conhecimentos dos gestores sobre o tema avaliado.

Conforme demonstrado no Gráfico 1, todos os indicadores relativos as perspectivas analisadas no Questionário de Governança e Controles internos da Faculdade de Educação apresentaram nível de maturidade Intermediário – faixa de classificação para as notas presentes no intervalo de 2,70 a 4,49[9].

Gráfico 1 – Índices do Questionário de Avaliação de Governança, Risco e Controles Internos por perspectivas



Fonte: Elaborado pela Auditoria-Geral com base nos dados do Questionário de Avaliação de Governança,

A perspectiva de Governança, Risco e Controle Interno obteve avaliação 4 (quatro) em cada uma das perguntas, ou seja, a Faculdade autoavaliou que o tema tem sido aplicado em parte da unidade.

A avaliação do Ambiente Interno foi realizada por meio de 13 perguntas obtendo índice de 3,69 (três inteiros e sessenta e nove centésimos). Destacam-se as questões relativas à troca nos cargos de função/chefia do setor entre os servidores após um período de tempo; à disseminação das práticas para prevenir, detectar ou coibir fraudes nos processos da unidade; ao processo de *feedback*; e aos procedimentos relativos ao ingresso de servidores novatos, as quais foram autoavaliadas como tema totalmente aplicado na unidade.

A perspectiva de Fixação de Objetivos foi a que obteve o menor indicador de autoavaliação, com pontuação de 3,50 (três inteiros e cinquenta centésimos). Porém, assim como as demais perspectivas avaliadas, seu índice revela um nível intermediário de maturidade.

Por último, o tópico Avaliação de Controle, perspectiva avaliada por 8 questões, obteve índice de 4,00 (quatro inteiros), resultando em um percentual de 66,7%. Sobre este tópico, destacam-se as questões relativas à adequada segregação de funções nos diversos processos da unidade, ao inventário de registros do controle de estoque de almoxarifado; e ao controle na contratação de pessoal terceirizado e estagiário a fim de evitar a contratação de familiar de servidor que exerça cargo em comissão ou função de confiança na UFMG.

Sobre a avaliação total do questionário – índice obtido pelo quociente do somatório das notas de avaliação dividido pelo número de questões do questionário – obteve um indicador de 3,81 conforme quadro 3.

Quadro 3 – Avaliação total do Questionário de Governança, Risco e Controle Interno

Quesitos	Soma das notas de Avaliação	Número de questões da perspectiva avaliada
Governança, Risco e Controle Interno	12	3
Ambiente Interno	48	13
Fixação de Objetivos	7	2
Atividade de Controle	32	8
TOTAL	**99**	**26**
Avaliação total do questionário	**3,81**	

Fonte: Elaborado pela Auditoria-Geral com base nos dados do Questionário de Avaliação de Governança, Risco e Controle Interno

Na avaliação total do questionário, a soma das novas de avaliação da unidade obteve um total de 99 em um universo de 156 pontos, resultando assim em um índice de 3,81. Esse indicador, de quoeficiente amplo, representa um nível intermediário de capacidade sobre a adequação dos processos de governança, risco e controle interno, por evidenciar um percentual de 63,5%.

8. CONCLUSÃO

A Auditoria-Geral da UFMG realizou trabalho de avaliação de conformidade, por meio de amostragem, dos procedimentos adotados pela Faculdade de Educação em relação às normas sobre Segurança da Informação aplicáveis, o que proporciona a obtenção de segurança razoável para a emissão de opinião de auditoria.

Os testes aplicados permitiram concluir que:

A gestão de ativos de *hardware* apresenta algumas práticas adequadas e compatíveis aos *frameworks* de privacidade e de segurança da informação e às normas elaboradas pela Associação Brasileira de Normas Técnicas (ABNT), como o controle para prevenir o acesso físico não autorizado, danos, interferências aos recursos de processamento das informações, evidenciado com a presença de tranca em todas as portas; o controle para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado caracterizado pela disposição dos equipamentos dentro das salas, laboratórios e gabinetes; entre outros. No entanto, é recomendável a implantação dos seguintes controles: i) promoção da atualização do SICPAT, sistema utilizado como inventário de *hardware*, de forma a refletir a real localização dos bens da unidade; ii) adoção de procedimentos sistemáticos de afixação e manutenção de número de registro patrimonial nos ativos de segurança da informação de natureza permanente, por meio de gravação, fixação e manutenção de plaquetas ou etiquetas apropriadas; iii) aprimoramento do instrumento de controle de atualização do SICPAT em hipóteses de desligamento ou movimentação de servidor cadastrado como responsável por bens no sistema de inventário; e iv) implementação do controle interno assegurando que a retirada de ativos de segurança da informação seja precedida do registro da movimentação no SICPAT e da assinatura de Termo de Responsabilidade ou instrumento equivalente pelo agente.

No que diz respeito à gestão de ativos de *software*, ressalta-se que as atividades da unidade se apresentam em conformidade quanto ao monitoramento do acesso e do uso relativo aos serviços de rede, aos procedimentos para evitar a instalação de *softwares* e dos recursos não autorizados, providos ou homologados pelo setor competente, entre outras subquestões relativas ao tema. Entretanto, visando à mitigação de riscos, é recomendável: i) a adoção de inventário de todos os *softwares* e sistemas de acesso à informação, incluindo aqueles adquiridos a partir de recursos destinados aos projetos de pesquisa; e ii) realização de procedimentos periódicos de *backup* de todos os dados gerenciados pela unidade – incluindo os dados locais de cada setor.

Sobre os controles que visam à mitigação dos riscos referentes à gestão de acesso – conduta dos usuários – constatou-se que a unidade possui instrumento para evitar o acesso indevido de visitantes aos dispositivos móveis com acesso à informação. No entanto, recomenda-se um aprimoramento nos procedimentos de controle para garantir que agentes desligados da unidade tenham cancelados seus direitos de acesso a equipamentos, sistemas e redes.

No que se refere à utilização de dispositivos – forma como a unidade gerencia ativamente a utilização de dispositivos móveis – a unidade possui instrumento de controle para evitar o acesso sem autorização aos recursos corporativos por meio de dispositivos móveis particulares. Entretanto, a faculdade deve adotar medidas de conscientização no sentido de que: i) a comunidade utilize apenas soluções confiáveis e institucionalmente homologadas de armazenamento em nuvem; e ii) sejam estabelecidos diretrizes e orientações para o uso de dispositivos móveis e mídias removíveis.

Em relação à gestão de recursos humanos, asseverou-se alinhamento na atuação dos diversos usuários em relação às políticas de mesa limpa e tela limpa. Porém, é recomendável a promoção de medidas formais e institucionais de capacitação e conscientização sobre temas de segurança da informação, utilizando objetos de aprendizagem já disponíveis e/ou elaborando material próprio.

De modo geral, os testes aplicados permitem afirmar que os procedimentos adotados na unidade estão, em grande parte, em conformidade com as normas aplicáveis, podendo ser aperfeiçoados para mitigar os riscos de ocorrência de incidentes de Segurança da Informação. Nesse sentido, ressalta-se a necessidade de melhoria dos procedimentos para registros, manutenção e atualização tempestiva do inventário de *hardware*, controle na movimentação e retirada dos bens – registrando esses fluxos em documentos próprios –, bem como o cadastro dos responsáveis pelos equipamentos a fim de realizar os procedimentos de acompanhamento, e, se necessário, responsabilização nas situações previstas nos respectivos normativos.

Salienta-se, também, sobre a importância da gravação e fixação de plaquetas patrimoniais ou etiquetas apropriadas com o intuito de identificar e localizar os diversos equipamentos que compõem os bens da unidade.

Além disso, a faculdade necessita inventariar os *softwares* e sistemas de acesso à informação em sua completude, de forma a identificar as possíveis vulnerabilidades e garantir a atualização de todos os sistemas. Nessa perspectiva, reforçamos a importância da instituição de um procedimento periódico de *backup* abrangente – incluindo os dados locais dos setores – e destacamos a necessidade de disseminação do conhecimento à comunidade por meio de cursos de capacitação e conscientização, desenvolvendo materiais próprios ou valendo-se de soluções disponíveis em fontes como a Escola Virtual de Governo (EVG), incentivando agentes com acesso a dados pessoais e informações institucionais a adotar medidas de segurança relacionadas ao armazenamento em nuvem e a utilização de dispositivos móveis e mídias removíveis, para reduzir as possibilidades de vazamento de dados e perda das características essenciais da informação.

A segurança da informação é um tema atual cujo arcabouço normativo e procedimentos aplicáveis estão em constante transformação. Em um contexto de digitalização das relações de ensino, consumo, socialização e dados pessoais, as informações institucionais apresentam um valor ainda mais relevante, tornando imprescindível o aperfeiçoamento contínuo de controles para reduzir os riscos de incidentes que comprometam a privacidade dos usuários e as características essenciais da informação. Nesse sentido, a auditoria realizada trouxe como principais benefícios a emissão de recomendações formuladas a partir de um profundo estudo das normas aplicáveis. Caso atendidas, essas recomendações devem contribuir para o aprimoramento da privacidade e do gerenciamento dos dados pessoais na instituição, além de ampliar a confiabilidade e a proteção de sistemas informáticos contra os principais ataques que podem resultar em incidentes de segurança.

Salienta-se que a adequada implementação das recomendações emitidas pela Auditoria-Geral da UFMG é de responsabilidade da unidade auditada, assim como a aceitação formal do risco associado em caso de não adesão a elas, conforme destaca o Referencial Técnico da Atividade de Auditoria Interna Governamental do Poder Executivo Federal (IN SFC/CGU nº 03/2017) em seu item 176, transcrito abaixo:

> *CAPÍTULO V – OPERACIONALIZAÇÃO DAS ATIVIDADES DE AUDITORIA INTERNA*
>
> *Seção IV – Monitoramento*
>
> *Item 176. É de responsabilidade da alta administração da Unidade Auditada zelar pela adequada implementação das recomendações emitidas pela UAIG, cabendo-lhe aceitar formalmente o risco associado caso decida por não realizar nenhuma ação.*

Dessa forma, a Auditoria-Geral, embasando-se em práticas e diretrizes nacionais e internacionais aplicáveis à Administração Pública Federal, evidencia a importância do cumprimento das recomendações por ela emitidas para a agregação de valor organizacional à Universidade.

---

[1] Trabalho de igual metodologia foi realizado também junto à Escola de Ciência da Informação e à Escola de Arquitetura.

[2] Vide respostas às Solicitações de Auditoria, disponíveis no Apêndice.

[3] As amostras “Inventário de *Hardware*“ e “Inventário de Periféricos”, construídas a partir de relatório extraído do SICPAT, são compostas por 47 (quarenta e sete) itens, entre microcomputadores, *notebooks*, *tablets*, e HDs externos.

[4] A amostra “Segurança Física”, constituída a partir de relatório extraído do SICPAT, é composta por 3 (três) salas, em que se encontravam 95 (noventa e cinco) ativos de informação, entre microcomputadores, *notebooks* e *tablets*.

[5] Na visita *in loco*, realizada no dia 25/07/2024, observou-se a existência e utilização de equipamentos de segurança física, como trancas, grades e câmeras.

[6] A amostra “Segurança Física”, constituída a partir de relatório extraído do SICPAT, é composta por 3 (três) salas, em que se encontravam 95 (noventa e cinco) ativos de informação, entre microcomputadores, *notebooks* e *tablets*.

[7] Durante a visita *in loco*, realizada no dia 25/07/2024, verificou-se que as seguintes salas (1415 – Chefia DAE e 2109 – Promestre) possuem impressoras de uso comum.

[8] Informação disponível em: <https://ufmg.br/acesso-a-informacao/informacoes-classificadas-ai>. Acesso em: 18/10/2024.

[9] Classificação apresentada pelo Tribunal de Contas da União em seu Levantamento de Governança, Sustentabilidade e Gestão nas organizações públicas federais de 2024.

Belo Horizonte, 19 de dezembro de 2024.

Maurício de Lima Teixeira Leite
Contador

José Guilherme Magalhães e Silva
Auditor

Terezinha Vitória de Freitas Silva – Coordenadora
Auditora-Geral Adjunto

Octávio Valente Campos
Auditor-Geral

Documento assinado eletronicamente por **Terezinha Vitoria de Freitas Silva**, **Auditor(a)-Geral Adjunto(a)**, em 19/12/2024, às 11:05, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Jose Guilherme Magalhaes e Silva**, **Auditor(a)**, em 19/12/2024, às 11:07, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Maurício de Lima Teixeira Leite**, **Contador**, em 19/12/2024, às 11:11, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

Documento assinado eletronicamente por **Octavio Valente Campos**, **Auditor(a)-Geral**, em 19/12/2024, às 11:38, conforme horário oficial de Brasília, com fundamento no art. 5º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site https://sei.ufmg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3837893** e o código CRC **0EC82278**.