UNIVERSIDADE FEDERAL DE MINAS GERAIS

RELATÓRIO DE AUDITORIA Nº 07/2024 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 Controles (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 nesse 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.

Foram analisados procedimentos, instalações físicas e ativos – definidos em amostra não probabilística – visando obter evidência adequada e suficiente sobre a conformidade das atividades da Escola de Ciência da Informação[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 esse 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 a 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 adotadas?

A partir da realização deste trabalho foi possível identificar como ponto positivo e relevante a utilização do *Business Process Management* (BPM) como ferramenta de gerenciamento para o mapeamento dos diversos procedimentos executados pela Unidade a fim de identificar, avaliar e aperfeiçoar seus processos internos. Essa medida contribui para o instituto da segregação de funções, mitigando, assim, os riscos decorrentes de eventual conflito de interesses por parte do agente público. Nesse sentido, há uma separação das funções de autorização, aprovação, execução e controle. Convém ressaltar a vasta utilização de mecanismos relativos ao subtema “gerenciamento do rol de usuários com acesso aos ativos de informação”, como a presença de catracas na portaria principal, trancas em todas as portas, câmeras nos corredores, travas de segurança nos computadores dos laboratórios de uso comum e observância na disposição dos equipamentos, para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado.

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;

- Utilização de “sala virtual” no SICPAT para a alocação de bens classificados como “Acertos – Não encontrados”;
- Fragilidade no controle referente à manutenção das placas patrimoniais devidamente afixadas;
- Falta de procedimentos de apuração nas hipóteses de não localização dos ativos de *hardware*;
- Ausência de medidas de segurança para o uso dos dispositivos de propriedade da organização fora das dependências da Unidade, como o Termo de Responsabilidade ou instrumento semelhante para este fim;
- Possibilidade de aquisição de ativos de *hardware* sem prévia avaliação junto ao CATI para a verificação das necessidades e compatibilidades do dispositivo às demandas da Unidade;
- Fragilidade nos instrumentos de controle formal para garantir a atualização do SICPAT em hipótese de saída ou movimentação de agente cadastrado como responsável por ativos;
- Vulnerabilidade no processo de catalogação dos *softwares* utilizados no armazenamento, manipulação ou exclusão das informações. Não mapeamento dos sistemas adquiridos diretamente por professores via projetos de pesquisa e situações similares;
- Fragilidade nos controles voltados a garantir a utilização exclusiva de soluções de armazenamento em nuvem disponibilizadas ou homologadas pelo setor de tecnologia da informação da unidade; e
- Não formalização e institucionalização de medidas de capacitação e conscientização dos ativos de Recursos Humanos sobre Segurança da Informação;

As recomendações abrangem:

- Promover a 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;
- Descontinuar a utilização de “sala virtual” realocando os bens cadastrados como “Acertos – Não encontrados” em seus respectivos locais;
- Adotar procedimentos sistemáticos para afixação e manutenção de registro patrimonial através da plaqueta ou etiqueta destinada a este fim;
- Implantar procedimentos de responsabilidade e, se necessário, indenização – nos termo do item 10 da IN nº 205/1988 e demais normativos – em caso de perda de ativos;
- Institucionalizar o procedimento para o controle de retirada de bens ou movimentação de bens como a assinatura de Termo de Responsabilidade ou instrumento semelhante;
- Adotar medidas de avaliação prévia pelo setor de TI para a aquisição de *hardware*;
- Instituir um sistema de inventário dos *softwares* e sistemas de acesso à informação;
- Adotar medidas de conscientização no sentido de que a comunidade utilize apenas soluções confiáveis de armazenamento em nuvem; e
- Promover medidas de capacitação e conscientização sobre a Segurança da Informação junto aos servidores.

3. LISTA DE SIGLAS E ABREVIATURAS

ABNT – Associação Brasileira de Normas Técnicas

APF – Administração Pública Federal

CATI – Centro de Apoio à Tecnologia da Informação

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 Auditoria Interna

PDTIC – Plano Diretor de Tecnologia da Informação e Comunicação

POSIN – Política de Segurança da Informação

PTA – Plano de Trabalho de 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

UFMG – Universidade Federal de Minas Gerais

4. INTRODUÇÃO

Por meio deste relatório apresentam-se os resultados do trabalho de avaliação de conformidade dos procedimentos adotados pela Escola de Ciência da Informação em relação às normas sobre Segurança da Informação aplicáveis. O trabalho foi derivado da apuração da Matriz de Riscos elaborada para o Plano Anual de Auditoria Interna (PAINT) 2024.

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

- **Leis e Decretos:**
  - Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados (LGPD);
  - Decreto n.º 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação;
  - Decreto 10.332, de 28 de abril de 2020 - Institui a Estratégia de Governo Digital para o período de 2020 a 2022;
  - Decreto 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 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 2 GSI/PR, de 24 de julho de 2020 - Altera a Instrução Normativa nº 1, de 27 de maio de 2020;
  - Instrução Normativa 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;
  - 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 a 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 demandado providências dos órgãos da Administração Pública Federal no âmbito do Programa de Privacidade e Segurança da Informação (PPSI), isto é, 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 Ativos – *Hardware*: A unidade gerencia ativamente (inventariar, rastrear e corrigir) os equipamentos utilizados para armazenamento, transmissão e processamento de informação?
- **Questão 2:** Gestão de Ativos – *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 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 à obtenção de uma razoável segurança de que os controles internos estabelecidos pela administração estão em efetivo funcionamento, inclusive quanto ao seu cumprimento pelo quadro de pessoal da entidade.

Para tanto, os trabalhos foram realizados em conformidade aos preceitos de auditoria interna aplicáveis ao Poder Executivo Federal, utilizando-se da aplicação de *checklist*, de questionário e de entrevistas, 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 quatro ferramentas metodológicas, quais sejam: (i) análise documental; (ii) indagação; (iii) observação e (iv) inspeção.

Quadro 1 – Subquestões e técnicas aplicadas

Subquestão	Técnicas Aplicadas
1.1 A unidade possui inventário de dispositivos (exemplo: computadores, celulares, etc) que permitam o acesso à informação?	Análise documental (fonte: SICPAT; sites institucionais) Indagação[2] Inspeção (vide quadro "Amostra: Inventário de *hardware*"[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)?	Análise documental (fonte: SICPAT; Portal da Transparência) Indagação
1.3 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)
1.4 Os equipamentos estão protegidos e colocados em locais para reduzir os riscos de ameaças e perigos do meio ambiente, bem como as oportunidades de acesso não autorizado?	
1.5 Os equipamentos estão protegidos contra falta de energia elétrica e outras interrupções causadas por falhas das utilidades?	
1.6 Os equipamentos são objeto de manutenção correta para assegurar a sua contínua integridade e disponibilidade?	Análise documental (fonte: SICPAT; sites institucionais) Indagação
1.7 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 "Amostra: Inventário de *hardware*", disponível no Apêndice)
1.8 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 riscos decorrentes do fato de se trabalhar fora das dependências da organização?	
1.9 Em hipótese de reutilização ou descarte, 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
1.10 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?	Análise documental (fonte: sites institucionais) Indagação
1.11 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?	Análise documental (fonte: SICPAT; Portal da Transparência) Indagação
2.1 A unidade possui inventário de *softwares* de acesso à informação?	Indagação
2.2 A unidade possui mecanismos de monitoramento do 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
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 quadro "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 procedimento para evitar que o usuário tenha acesso a informações que extrapolem sua competência?	
4.1 A unidade possui instrumentos de controle para evitar a utilização de aplicativos ou recursos de armazenamento em nuvem não disponibilizados pelo setor de tecnologia da informação da unidade sem permissão?	

Subquestão	Técnicas Aplicadas
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?	
5.1 A unidade promove medidas de capacitação e/ou conscientização dos recursos humanos sob sua gestão em temas relacionados à segurança da informação?	Análise documental (sites institucionais) Indagação
5.2 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 Inspeção (vide quadro "Amostra: Mesa Limpa"[5] , disponível no Apêndice)
5.3 A unidade mantém procedimentos para garantir a segregação de funções na operacionalização dos sistemas informatizados?	Indagação (vide Manual – Mapeamento de Processos)

Fonte: elaborado pelos autores.

No que tange às restrições ou limitações aos nossos exames, verificou-se a não aplicabilidade da subquestão 4.3 (procedimentos de controle referente à utilização de dispositivos móveis e mídias removíveis para fins de armazenamento da informação classificada), tendo em vista a inexistência de informação classificada pela UFMG no período[6].

5. RESULTADO DOS EXAMES

Tendo como base a amostra selecionada, não se identificou a compatibilidade entre a localização física dos bens e seu respectivo 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 dos ativos e a situação registrada no SICPAT.

Tendo como base o valor dos equipamentos, foi selecionada uma amostra com 25 (vinte e cinco) itens para verificar a compatibilidade entre a localização física dos bens e seu respectivo local de registro no SICPAT. Os resultados evidenciaram que nenhum dos itens se encontrava na localização registrada no SICPAT.

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

Achado 2. Alocação em "sala virtual" dos itens classificados no SICPAT como "Acertos – Não encontrados".

Diante da existência de 57 (cinquenta e sete) ativos de informação alocados no SICPAT na sala "Ativos – Não encontrados", observou-se a utilização de "sala virtual", representando a não compatibilidade entre a localização dos ativos de informação registrada no SICPAT e sua localização física real.

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

Achado 3. Fragilidade no controle referente à manutenção das placas patrimoniais devidamente afixadas.

Foi realizada uma segunda visita *in loco* para a apresentação de ativos que não haviam sido localizados em visita anterior. Na ocasião, verificou-se que há três *MacBooks*, com especificações idênticas, mas com status distintos: um bem localizado, um bem objeto de crime patrimonial e um bem não localizado. Porém, como o item localizado não possui placa patrimonial, não é possível identificar com exatidão qual dos bens se encontra em cada situação.

Sendo assim, diante dos resultados da inspeção, da documentação analisada e dos esclarecimentos prestados, observou-se a fragilidade no controle referente à manutenção das placas patrimoniais devidamente afixadas, o que pode resultar em perda de ativos.

Achado 4. Ausência de procedimentos para a apuração de responsabilidade referente aos ativos de *hardware* não localizados.

Por meio de duas visitas *in loco* para fins de inspeção, verificou-se que três ativos não foram localizados: Microcomputador ASUS (patrimônio 1221529), Microcomputador ASUS (patrimônio 1221529) e um *Macbook Air* 11 cujo patrimônio não foi possível especificar, conforme exposto no achado anterior.

Inicialmente, a unidade não possuía um procedimento formal para a apuração de responsabilização do servidor responsável pela guarda do bem desaparecido. Posteriormente, foi apresentada pela unidade a Portaria nº 7189, de 19 de agosto de 2024, designando a Comissão de Sindicância Investigatória. Entretanto, por meio da ferramenta Conferência de Autenticidade de Documentos do Sistema Eletrônico de Informações – SEI, não foi possível verificar a autenticidade da referida portaria, pois o documento e seu respectivo processo de origem encontram-se cancelados.

Sendo assim, não ficou demonstrada a abertura de procedimentos previstos na Instrução Normativa nº 205/1988 para fins de apuração da responsabilidade sobre os bens não localizados, o que pode impactar na perda de ativos e no acesso indevido às informações neles armazenadas.

Achado 5. Ausência de medidas de segurança para o uso de dispositivos fora de suas dependências, incluindo a assinatura de Termo de Responsabilidade ou um instrumento semelhante para fins de retirada de ativo.

Não se identificou a existência de controles internos formais estabelecidos para a gestão de retirada de ativos de informação para o uso externo às dependências da unidade, incluindo a assinatura de Termo de Responsabilidade ou um instrumento similar para este fim.

Conforme o item 11.2.6 Segurança de equipamentos e ativos fora das dependências da organização, 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 definir a cadeia de custódia do equipamento, incluindo pelo menos os nomes e organizações daqueles que são responsáveis pelo equipamento.*

Sendo assim, diante da documentação e dos esclarecimentos apresentados pela unidade auditada, observou-se a inexistência 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 6. Fragilidade de controle para garantir que a aquisição de novos ativos de *hardware* seja precedida de avaliação junto ao CATI, a fim de se verificar as necessidades de cada área.

Não se identificou a existência de procedimentos internos de avaliação prévia, junto ao CATI, para aquisição de *hardwares* destinados à unidade.

De acordo com o Controle 1: Inventário e Controle de Ativos Institucionais do *framework* de S.I. da MGI, pois:

> *"As instituições não podem defender aquilo que não está mapeado ou não se tem conhecimento de sua existência [...] As organizações devem saber quais dados são essenciais para elas, e a gestão adequada de ativos ajudará a identificar os ativos institucionais que mantém ou gerenciam esses dados críticos, para que as medidas de segurança apropriadas possam ser aplicadas. Isso também ajudará na identificação de ativos não autorizados e não gerenciados para removê-lo ou remediá-lo."*

Sendo assim, diante da documentação e dos esclarecimentos apresentados pela unidade auditada, observou-se a inexistência do referido controle, o que pode resultar em aquisição de ativos em desconformidade com as necessidades da unidade.

Achado 7. Ausência de medidas de controle para garantir que o SICPAT seja atualizado em hipóteses 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 do servidor.

Por meio do 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 as servidoras L.S. de O.S., aposentada desde 01/02/2019, M. da C.C., aposentada desde 08/08/2017, e M.O.T. de M., aposentada desde 10/07/2019, permaneciam cadastradas como responsáveis pelos ativos das respectivas salas, 4017, 4026 A e 4038.

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

> *"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 servidor já desligado do quadro de pessoal da Unidade ainda cadastrado como responsável 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 8. A unidade não inventaria todos os *softwares* utilizados no armazenamento, manipulação ou exclusão das informações, ficando não mapeados os produtos adquiridos diretamente por professores via projetos de pesquisa e situações similares.

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

Conforme Controle 2: Inventário e Controle de Ativos de *Software* do *framework* de S.I. da 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 softwares que não sejam necessários para suas atividades."*

Nesse sentido, o Controle 8.1.1 a Norma ABNT NBR ISO/IEC 27002 dispõe que:

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

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

Achado 9. Ausência de instrumento de controle para evitar a utilização, sem permissão, de aplicativos ou recursos de armazenamento em nuvem não disponibilizados pelo setor responsável.

Não se identificou, por meio de indagação junto aos gestores, a existência de controle interno para evitar a utilização, sem permissão, de aplicativos ou recursos de armazenamento em nuvem não disponibilizados pelo setor de tecnologia da informação da unidade.

Consoante ao Controle 2 do *framework* de Segurança da Informação do MGI, as instituições devem:

> *"Gerenciar ativamente (inventariar, rastrear e corrigir) todo software na rede para que apenas o software autorizado ser instalado e possa ser executado."*

Nesse sentido, a Política de Segurança da Informação da UFMG, em seu item 8.5.6, determina que compete aos dirigentes e às chefias:

> *"(...) 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 insuficiência no referido controle, o que pode resultar em incidentes de segurança da informação decorrentes da utilização de soluções que não atendam a padrões mínimos de segurança.

Achado 10. Ausência de medidas formais de capacitação e/ou conscientização dos recursos humanos sob sua gestão em termas relacionados à segurança da informação.

Não se identificou, por meio de indagação junto aos gestores, a adoção de medidas formais e institucionais de capacitação de recursos humanos em temas relacionados à segurança da informação. Questionada, a unidade informou transmitir apenas orientações informais junto a servidores.

Posteriormente, conforme Despacho assinado pela Direção da unidade, foi incluído no sítio da Escola uma aba [7] relativa às orientações quanto à movimentação de bens patrimoniados, contemplando assim, uma medida de conscientização sobre o acompanhamento e registro dos respectivos equipamentos. Esta aba possui, além da cartilha referente ao controle patrimonial, Formulário de Movimentação Temporária de Patrimônio, contendo os seguintes campos: 1. Finalidade, 2. Discriminação, 3. Origem e 4. Destino (quando houver).

Conforme Controle 23 do *framework* de Segurança da Informação do MGI:

> *"As pessoas envolvidas no tratamento de dados são instruídas 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 da 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".*

Nessa perspectiva, a Norma 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 apropriadas, 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 das informações de autenticação secreta.*

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 de segurança da informação decorrentes da atuação de agentes públicos em desconformidade com as normas aplicáveis.

6. RESULTADO DOS EXAMES

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 dos bens no SICPAT, de forma que o sistema reflita a real localização

dos bens na unidade.

Achado 2. Alocação em "sala virtual" dos itens classificados no SICPAT como "Acertos – Não encontrados".

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

Recomendação 02: Descontinuar a "sala virtual" e recadastrar os bens classificados como "Acertos – Não encontrados", no SICPAT, realocando-os de forma que reflitam suas reais localizações.

Achado 3. 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 e de acesso indevido aos equipamentos de acesso à informação, o órgão deve atender à recomendação a seguir.

Recomendação 03: Adotar procedimento sistemático de afixação de número de registro patrimonial nos ativos de segurança da informação de natureza permanente, por meio de gravação, fixação de plaqueta ou etiqueta apropriada.

Achado 4. Ausência de procedimentos para apuração de responsabilidade referente aos ativos de *hardware* não localizados.

A fim de se evitar o risco de perda de ativos e/ou das características fundamentais da informação, de acesso indevido aos equipamentos de acesso à informação, da identificação e correção dos problemas ou da implementação de um procedimento de responsabilização adequado, o órgão deve atender à recomendação a seguir.

Recomendação 04: Realizar o procedimento de responsabilidade e, se necessário, indenização, nos termos do item 10 da IN nº 205/1988 e demais normativos aplicáveis, em hipótese de não localização de ativos.

Achado 5. Ausência de 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 à recomendação a seguir.

Recomendação 05: Implementar o 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.

Achado 6. Fragilidade no controle para garantir que as aquisições de ativos de *hardware* sejam precedidas de avaliação junto ao CATI, a fim de verificar as necessidades de cada área.

A fim de se evitar o risco de prejuízos financeiros decorrentes de obtenção de ativos incompatíveis com as necessidades da unidade.

Recomendação 06: Adotar medidas de conscientização sobre a necessidade de que as aquisições de *hardware* sejam precedidas de avaliação pelo setor de T.I.

Achado 7. Ausência de medidas de controle para garantir que o SICPAT seja atualizado em hipóteses 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 07: 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 (ex: criação de processo interno e formulário padronizado no SEI).

Achado 8. A unidade não inventaria todos os *softwares* utilizados no armazenamento, manipulação ou exclusão das informações, ficando não mapeados os produtos adquiridos diretamente por professores via projetos de pesquisa e situações similares.

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 08: Adotar medidas de conscientização no sentido de que todas as aquisições de *software* e sistemas de acesso à informação sejam informadas ao setor de T.I., para fins de inventariamento.

Achado 9. Ausência de instrumento de controle para evitar a utilização, sem permissão, de aplicativos ou

recursos de armazenamento em nuvem não disponibilizados pelo setor responsável.

A fim de se evitar o risco quanto à confiabilidade e à proteção dos sistemas informáticos, mitigando procedimentos que possam resultar em incidentes de segurança, o órgão deve atender à recomendação disposta a seguir.

Recomendação 09: Propor soluções de armazenamento em nuvem homologadas ou disponibilizadas pelo setor de tecnologia da informação da unidade e incentivar sua utilização pela comunidade.

Achado 10. Ausência de medidas formais de capacitação e/ou conscientização dos recursos humanos sob sua gestão em termos relacionados à segurança da informação.

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

Recomendação 10: Promover medidas de capacitação e conscientização sobre Segurança da 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 riscos e controles internos instituídos pela Escola de Ciência da Informação, referente 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.

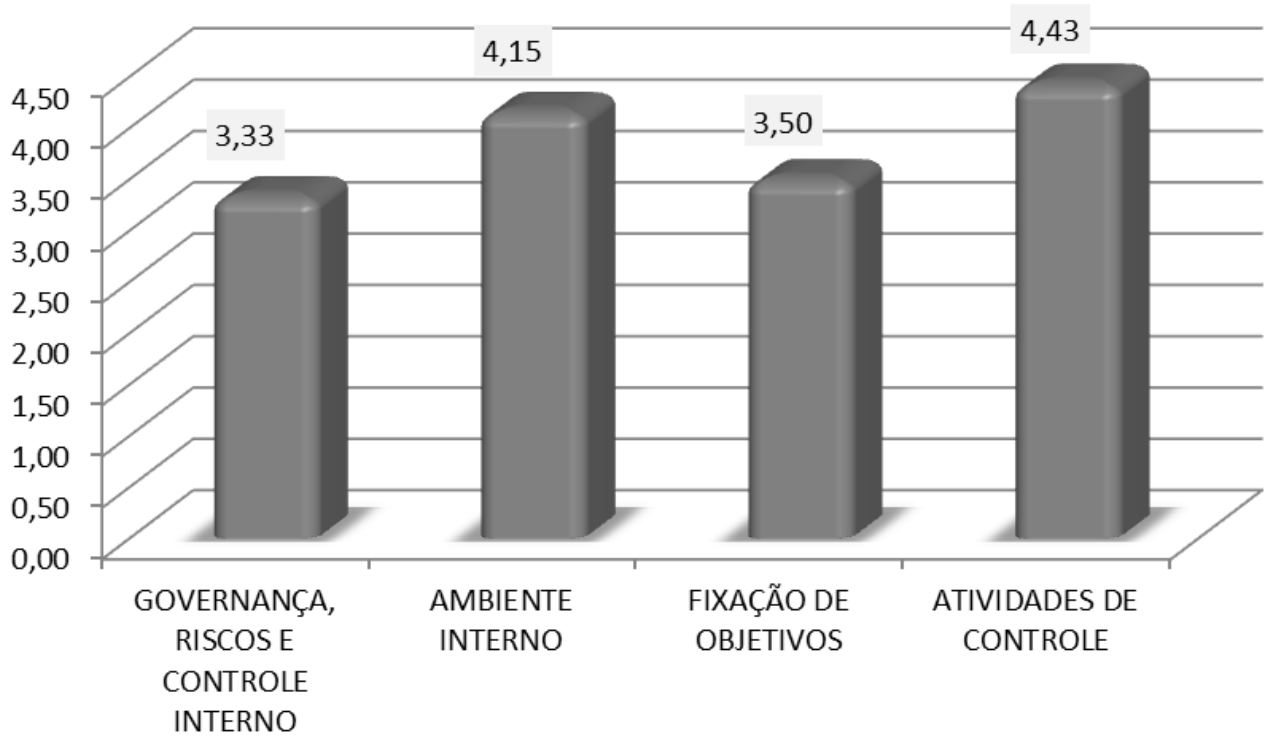
Para medir o nível de aplicabilidade nas questões do Questionário, foi definido o índice (A) para avaliação de cada perspectiva e o índice (B) para avaliação total do questionário.

<table>
<tr><td colspan="2">Avaliação de cada perspectiva (A) = X/Y</td><td>Avaliação total do questionário (B) = X/Z</td></tr>
<tr><td>X = soma das notas de avaliação
- só das questões de uma perspectiva se avaliação “A”.
- de todas as questões do questionário se avaliação “B”</td><td>Y = nº de questões da perspectiva avaliada (excluindo as “não se aplica” informado pela unidade)</td><td>Z = nº de questões do questionário
(excluindo as “não se aplica” informado pela unidade)</td></tr>
</table>

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

A Escola de Ciência da Informação obteve índice superior a 3 (três) e inferior a 4 (quatro) em dois quesitos avaliados, quais sejam, Governança, Riscos e Controle Interno e Fixação de Objetivos; e indicador superior a 4 (quatro) nos seguintes quesitos: Ambiente Interno e Atividades de Controle. 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 conhecimento dos gestores sobre o tema avaliado. O Gráfico 1 apresenta os índices dos quatro quesitos avaliados, demonstrando que a unidade possui estágios de capacidade[8] classificado como intermediário sobre três perspectivas avaliadas e como aprimorado no quesito Atividades de Controle.

Gráfico 1: Índices do Questionário de Governança e Controles internos por quesitos



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

O primeiro quesito avalia qual o grau de domínio dos gestores sobre o tema Governança, Riscos e Controle Interno. O índice de 3,33 reflete um estágio de conhecimento intermediário da gestão sobre o tópico. Ressalta-se que a gestão demonstrou moderado conhecimento sobre o tema e a política interna da UFMG e seu compartilhamento com os demais membros da unidade.

Avaliando o Ambiente Interno, o qual possui um somatório de 78 (setenta e oito) pontos, a unidade alcançou 54 (cinquenta e quatro) pontos, obtendo um percentual de 69,2%. Esse índice demonstra que, para o tópico analisado, a unidade encontra-se no estágio intermediário de capacidade. A gestão avaliou o tema como aplicado totalmente na Unidade/Órgão em cinco das treze perguntas que compõem esse quesito.

Sobre a perspectiva de Fixação de Objetivos, a unidade obteve índice de 3,50, evidenciando uma classificação intermediária sobre este foco. A gestão avaliou como 3 a clareza e formalização dos objetivos da unidade e como 4 o aspecto de indicadores e metas na elaboração, monitoramento e avaliação do Plano de Ação, ou outra forma de Planejamento Estratégico da unidade.

Por último, o tópico relativo às Atividades de Controle obteve índice de 4,43 pontos, resultando em um percentual de 73,8%. O percentual alcançado indica que a gestão da unidade atingiu um patamar de capacidade aprimorada. Esta análise, que é composta por 7 perguntas - pois a questão sobre contratação de pessoal terceirizado e estagiários foi classificada pela gestão como “Não se Aplica” - obteve duas respostas categorizadas como Tema aplicado totalmente na Unidade/Órgão.

A Avaliação relativa ao total do questionário – índice obtido pelo quociente do somatório das notas de avaliação divido pelo número de questões do questionário – obteve indicador de 4,08 conforme Quadro 2.

Quadro 2: Avaliação total do Questionário de Governança e Controles Internos

Quesitos	Soma das notas de Avaliação	Número de questões da perspectiva avaliada
Governança, Riscos e Controle Interno	10	3
Ambiente Interno	54	13
Fixação de Objetivos	7	2
Atividades de Controle	31	7
TOTAL	**102**	**25**
Avaliação total do questionário	**4,08**	

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

Na Avaliação Total do Questionário, a soma das notas de avaliação da unidade obteve um total de 102 em um universo de 150 pontos, obtendo assim um índice de 4,08 pontos. Esse indicador demonstra, baseado neste questionário de autoavaliação, um nível intermediário de capacidade sobre a adequação dos processos de governança, gestão de risco e controles interno por evidenciar um percentual de 68%.

8. CONCLUSÃO

A Auditoria-Geral da UFMG realizou trabalho de avaliação de conformidade, por meio de amostragem, dos procedimentos adotados pela Escola de Ciência da Informação 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 segurança da informação e às Normas Brasileiras 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 catracas na entrada principal, câmeras em funcionamento em todos os andares e trancas 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 da sala de aula; entre outros. No entanto, é recomendável a implantação dos seguintes controles: i) promoção da atualização do sistema de inventário de *hardware* (SICPAT), de forma que este reflita a real localização dos bens da unidade; ii) realocação dos bens cadastrados como “Acertos – Não encontrados” no SICPAT, de forma a descontinuar a utilização de salas virtuais para registro de ativos; iii) adoção de procedimentos sistemáticos de afixação de número de registro patrimonial nos ativos de segurança da informação de natureza permanente, através de gravação, fixação de plaquetas ou etiqueta apropriada; iv) realização de procedimento de responsabilidade e, se necessário, indenização, nos termos do item 10 da IN nº 205/1988 e demais normativos aplicáveis; v) implantação 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 semelhante pelo agente; vi) adoção de medidas de conscientização sobre a necessidade de que as aquisições de *hardware* sejam precedidas de avaliação pelo setor de T.I.; e vii) aprimoramento do instrumento de controle da atualização do SICPAT em hipótese de desligamento ou movimentação de servidor cadastrado como responsável por bens no referido sistema.

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 uso relativo aos serviços de rede e quanto aos serviços de *backup*, entre outras subquestões relativas a esta questão. Entretanto, visando à mitigação de riscos, é recomendável a adoção de inventário de todos os *softwares* e sistemas de acesso à informação, incluindo aqueles adquiridos a partir de recursos destinados a projetos de pesquisa.

Sobre os controles que visam à mitigação dos riscos referentes à gestão de acesso – conduta dos usuários – constatou-se que a unidade possui instrumentos para evitar o acesso indevido de visitantes aos dispositivos móveis com acesso à informação e realiza o mapeamento dos usuários com acesso aos ativos, garantindo que o acesso às funções dos *softwares* e dos sistemas sejam compatíveis com as competências e rotinas de cada cargo.

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, através de *login* e senha específicos e individualizados. Entretanto, a Escola deve adotar medidas de conscientização no sentido de que a comunidade utilize apenas soluções confiáveis e institucionalmente homologadas de armazenamento em nuvem.

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. Evidenciamos que a unidade possui um Manual de Mapeamento de Processos garantindo que funções conflitantes e áreas de responsabilidade sejam segregadas. 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. Nesse sentido, em decorrência das atividades de auditoria em andamento, a unidade, em parceria com a Agência Brasileira de Inteligência (ABIN), disponibilizou para os usuários a primeira turma do curso "Formação para conscientização de boas práticas de tratamento de informações" (n.º no SIEX: 103303).

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 registro, manutenção e atualização tempestiva do inventário de *hardware*, bem como 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 Escola 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.

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 e socialização, dados pessoais e 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 às 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:

CAPITULO V – OPERACIONALIZAÇÃO DAS ATIVIDADES DE AUDITORIA INTERNA

Seção IV – Monitoramento

176. É 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 internacionais e nacionais aplicáveis à Administração Pública Federal, evidencia a importância do cumprimento das recomendações por ela emitidas para a agregação de valor organizacional à Universidade.

José Guilherme Magalhães e Silva

Auditor

Maurício de Lima Teixeira Leite

Contador

Terezinha Vitória de Freitas Silva – Coordenadora

Auditora-Geral Adjunto

Octávio Valente Campos – Supervisor

Auditor-Geral

[1] Trabalho de igual metodologia foi realizado também junto à Escola de Arquitetura e à Faculdade de Educação
[2] Vide respostas às Solicitações de Auditoria, disponíveis no Apêndice.
[3] A amostra “Inventário de Hardware”, construída a partir de relatório extraído do SICPAT, é composta por 25 (vinte e cinco) itens, entre microcomputadores, notebooks e tablets.
[4] A amostra “Segurança Física”, construída a partir de relatório extraído do SICPAT, é composta por 04 (quatro) salas, nas quais se encontravam 154 (cento e cinquenta e quatro) ativos de informação, entre microcomputadores e notebooks.
[5] Amostra “Mesa Limpa”, construída a partir de relatório extraído do SICPAT, é composta por 04 (quatro) setores, nos quais há o uso compartilhado de ativos como impressoras e scanners.
[6] Informação disponível em: . Acesso em 20/08/2024
[7] Informação disponível em: . Acesso em 22/08/2024
[8] Conforme Acórdão nº 2699/2018 – TCU – Plenário: os estágios de capacidade são divididos em três estágios: i) inicial (de 0 a 0,39), ii) intermediário (de 0,40 a 0,70) e iii) aprimorado (de 0,71 a 1). O estágio inicial ainda se subdivide em inexpressivo (de 0 a 0,14) e iniciando (de 0,15 a 0,39).

Documento assinado eletronicamente por **Terezinha Vitoria de Freitas Silva**, **Auditor(a)-Geral Adjunto(a)**, em 27/09/2024, às 10:11, 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 27/09/2024, às 11:51, 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 27/09/2024, às 14:28, 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 27/09/2024, às 14:31, 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 **3589143** e o código CRC **351326A1**.