



**SECRETARIA DE SEGURANÇA PÚBLICA
UNIVERSIDADE ESTADUAL DE GOIÁS – UEG
COORDENADORIA DE ENSINO
COORDENAÇÃO DE ENSINO PRESENCIAL E DE PÓS-GRADUAÇÃO
ESPECIALIZAÇÃO EM GERENCIAMENTO DE SEGURANÇA PÚBLICA**

LUCAS NEPOMUCENO MARTINS LARA

**O Armazenamento de fotografias digitais produzidas no âmbito da Superintendência de
Polícia Técnico Científica do Estado de Goiás**

GOIÂNIA-GO

2024



LUCAS NEPOMUCENO MARTINS LARA

O Armazenamento de fotografias digitais produzidas no âmbito da Superintendência de Polícia Técnico Científica do Estado de Goiás

Projeto de Pesquisa apresentado como exigência parcial para conclusão da disciplina Metodologia Científica do Curso Especialização em Gerenciamento de Segurança Pública (CEGESP) pela Secretaria de Segurança Pública de Goiás e a Universidade do Estado de Goiás, sob a orientação da Prof. Ma. Joara Campos Dias.

GOIÂNIA-GO

2024

**O Armazenamento de fotografias digitais produzidas no âmbito da Superintendência de
Polícia Técnico Científica do Estado de Goiás**

**Digital Photography Storage Produced Within the Scope of the Goiás State Police-
Scientific Superintendence**

Lucas Nepomuceno Martins Lara *

Joara Campos Dias **

Resumo: A Superintendência de Polícia Técnico-Científica de Goiás – SPTC GO desempenha um papel fundamental para o processo penal, produzindo provas materiais que embasam os processos legais, para produção dessas provas utilizamos a fotografia, seja para materializar um vestígio, ou mesmo para retratar uma cena ou um ambiente. Na SPTC tanto a gestão quanto os profissionais da ponta primam pela alta eficiência, pronto atendimento e cientificidade na produção dos laudos, com isso surge a preocupação quanto ao armazenamento das fotografias digitais produzidas na instituição, e os riscos que uma possível falta de padronização pode trazer para instituição. A presente pesquisa visa identificar as formas que os servidores médicos legistas e peritos criminais armazenam as fotografias, analisar os riscos da falta de padronização e propor uma solução que atenda a demanda. Foi realizado uma revisão bibliográfica sobre a evolução da fotografia, cadeia de custódia de vestígios digitais bem como das tecnologias disponíveis atualmente para atender a demanda explicitada ademais foi aplicado um formulário para médicos legistas e peritos com o objetivo de fazer a leitura da percepção desses servidores quanto aos aspectos pesquisados. Tendo como resultado a pluralidade de formas utilizadas pelos servidores para armazenar as fotografias digitais, bem como a falta de padronização e normas. A partir desses resultados sugere-se a necessidade de implementação de políticas de segurança da informação, capacitação dos servidores, padronização de procedimentos de armazenamento bem como a importância de investimentos em tecnologias robustas para tornar todo esse ciclo viável e garantindo a conformidade com as leis e regulamentações em vigor.

Palavras-chave: Fotografia forense; Cadeira de custódia; Armazenamento de dados.

Abstract: The Superintendency of Scientific Police of Goiás (SPTC-GO) plays a crucial role in the criminal process, producing material evidence that supports legal proceedings. Photography is used to materialize traces or portray a scene or environment. At SPTC-GO, both management and frontline professionals strive for high efficiency, prompt service, and scientific rigor in the production of reports, raising concerns about the storage of digital photographs produced by the institution and the risks that a lack of standardization may pose. This research aims to identify how forensic pathologist and crime scene investigator store photographs, analyze the risks of lack of standardization, and propose a solution that meets the demand. A bibliographic review was conducted on the evolution of photography, the chain of custody of digital traces, and the technologies currently available to meet the demand. A survey was applied to forensic pathologist and crime scene investigator to understand their perceptions of the aspects researched. The results showed the plurality of forms used by the servants to store

* Bacharel em Ciências da Computação pela Universidade de Brasília, pós graduado em Perícia Forense Aplicada a Informática, Perito Criminal SPTC-GO atuando em locais de crime, lotado na 3ª Coordenação Regional de Polícia Técnico-Científica de Formosa/GO. Especializando em Gerenciamento de Segurança Pública (SSP-GO/UEG). E-mail: luca19@gmail.com.

** Graduação em Ciências Biomédicas, Mestre em Genética. Perita Criminal 1ª classe SPTC-GO.

digital photographs, as well as the lack of standardization and norms. Based on these results, the implementation of information security policies, server training, standardization of storage procedures, and the importance of investing in robust technologies are suggested to make this cycle feasible and ensure compliance with current laws and regulations.

Keywords: Forensic photography; Chain of custody; Data storage

INTRODUÇÃO

A investigação criminal depende cada vez mais da coleta e análise de vestígios digitais, incluindo fotografias forenses (Edson, 2019). Essas imagens capturam cenas de crime, objetos e indivíduos com precisão e detalhes, fornecendo aos peritos informações fundamentais para a análise, reconstrução de cenas, identificação de suspeitos e elucidação de crimes (Kossoy, 2001).

No entanto, o armazenamento inadequado de fotografias forenses pode comprometer a integridade e a confiabilidade dessas provas, prejudicando o processo investigativo, e, portanto, tendo impacto direto em todo o processo judicial. Essa problemática é especialmente relevante na Superintendência de Polícia Técnico-Científica do Estado de Goiás (SPTC-GO), que possui um grande volume de imagens digitais armazenadas em suas diversas unidades.

O armazenamento correto de evidências digitais é uma fase basilar no ciclo de tratamento de evidências digitais, especialmente no contexto da fotografia forense realizada por Peritos Criminais e Médicos Legistas. Esta pesquisa tem como objetivo fornecer uma breve visão da evolução da fotografia e dos sistemas de armazenamento, bem como o panorama atual do armazenamento de evidências na Superintendência de Polícia Técnico-Científica do Estado de Goiás, distribuída em suas diversas unidades.

A fotografia forense é uma parte essencial do processo de materialização e produção subsequente de laudos científicos elucidativos. Ela serve como um meio para representar a realidade ou estado em que uma determinada cena ou objeto foi encontrada/apresentada à equipe forense. O armazenamento adequado dessas fotografias é necessário para garantir a conformidade legal da cadeia de custódia, bem como a integridade e disponibilidade desses dados. Portanto, a pesquisa proposta sobre o armazenamento de evidências digitais, com foco em fotografias forenses, é de extrema importância para garantir a conformidade legal e a segurança da informação dentro da Superintendência de Polícia Técnico-Científica do Estado de Goiás.

O problema a ser investigado é como adaptar o armazenamento de fotografias forenses às normas atuais de cadeia de custódia do Código de Processo Penal. O atual armazenamento de fotografias digitais na Superintendência de Polícia Técnico-Científica do Estado de Goiás apresenta riscos de segurança tanto para os médicos e peritos quanto para a instituição. Isso levanta a necessidade de identificar as inconformidades, riscos e vulnerabilidades nos métodos de armazenamento atuais e propor soluções viáveis para mitigar esses problemas.

O objetivo geral desta pesquisa é realizar um diagnóstico buscando identificar as diversas formas pelas quais as unidades da Superintendência de Polícia Técnico-Científica do Estado de Goiás armazenam atualmente fotografias forenses, com o objetivo de propor soluções viáveis para mitigar possíveis inconformidades. Os objetivos específicos incluem analisar as inconformidades, riscos e vulnerabilidades que os métodos atuais de armazenamento de fotografias nas unidades da Superintendência de Polícia Técnico-Científica do Estado de Goiás podem gerar para a instituição e os peritos.

Como estratégia de pesquisa esse trabalho foi dividido em três fases distintas: uma revisão da literatura e das normas, a aplicação de um formulário de pesquisa online e a análise dos dados. Os capítulos contemplam tópicos como a importância da fotografia forense, a cadeia de custódia e as normas e melhores práticas para o armazenamento de dados em organizações públicas. Além disso, a pesquisa propôs soluções para mitigar as inconformidades identificadas na Superintendência de Polícia Técnico-Científica do Estado de Goiás, com base em normas e princípios legais atuais.

1 FOTOGRAFIA FORENSE: HISTÓRIA E EVOLUÇÃO

A fotografia, como a conhecemos hoje, surgiu no século XIX, fruto da idealização de pioneiros como Joseph Nicéphore Niépce (Edson, 2019) e Louis Daguerre (Kossov, 2001). Nos primórdios foi utilizada para fins artísticos e documentais (Fotografia, 2024), e em seguida essa nova tecnologia logo despertou o interesse da área jurídica e investigativa.

Na metade do século XIX, a fotografia começou a ser utilizada para registrar cenas de crime e evidências materiais. O primeiro caso documentado de uso da fotografia forense data de 1861, na Inglaterra, quando fotos foram tiradas do corpo da vítima de um assassinato (Edson, 2019).

Com o passar do tempo, a fotografia forense se consolidou como uma ferramenta essencial para a investigação criminal. A constante evolução da tecnologia fotográfica, aliada

ao desenvolvimento de técnicas específicas, permitiu a captura de imagens cada vez mais precisas e detalhadas.

No início do século XX, o uso de câmeras fotográficas com lentes intercambiáveis e filmes de alta sensibilidade expandiu as possibilidades da fotografia forense (Edson, 2019). A evolução da fotografia em cores nas décadas seguintes proporcionou um novo marco para a evolução da tecnologia com o registro ainda mais fiel da cena do crime e das evidências (Kossov, 2001).

Na investigação criminal, a fotografia forense assume um papel fundamental, servindo como fator primordial na materialização do vestígio. As imagens capturadas pelos peritos transcendem a mera documentação, transformando-se em narradoras silenciosas e detalhistas da cena do crime e das evidências materiais (Edson, 2019).

Através das lentes da fotografia forense, a disposição dos objetos, a posição do corpo da vítima e outros elementos relevantes da cena do crime são registrados com precisão (Brasil, 2013). Essa documentação minuciosa se torna uma base sólida para a compreensão dos fatos e a construção da narrativa investigativa.

A fotografia permite perpetuar evidências que podem ser perecíveis ou frágeis, garantindo sua preservação para análise posterior. Esta ferramenta garante que, mesmo que a cena do crime se modifique, as informações essenciais permaneçam intactas para serem analisadas em momento futuro.

As imagens se transformam em peças cruciais, permitindo a reconstrução do crime e a determinação da sequência dos eventos. Através da análise metódica das fotografias, investigadores podem traçar a linha do tempo e constatar informações pertinentes que cercam o crime (Brasil, 2013).

A fotografia forense também contribui para a identificação de vítimas e suspeitos. Através da comparação com bancos de dados, as imagens podem auxiliar na busca por indivíduos envolvidos em crimes, acelerando a resolução do caso e promovendo a justiça.

Em audiências e julgamentos, as fotografias assumem o papel de provas contundentes, corroborando com os laudos periciais e nem sempre com os depoimentos das testemunhas. Essa materialização visual dos fatos contribui para a construção de um argumento sólido e para a busca pela verdade.

Enfim, a fotografia forense se configura como uma ferramenta essencial na investigação criminal, fornecendo um registro fiel e imutável da cena do crime e das evidências materiais. Através da captura precisa dos detalhes, as imagens se transformam em testemunhas

imparciais, guiando os investigadores na busca pela verdade e na construção da justiça (Kossoy, 2001).

É fundamental que a prática da fotografia forense esteja em conformidade com as normas e legislações vigentes, a fim de garantir a confiabilidade e a validade das provas coletadas.

NBR ISO/IEC 27001: Esta norma estabelece requisitos para a implementação de um sistema de gestão da segurança da informação, assegurando a proteção e a integridade dos dados e registros fotográficos (Abnt, 2013).

Código de Processo Penal: O Código de Processo Penal brasileiro regulamenta a produção de provas em processos criminais, incluindo a fotografia forense (Brasil, 1941).

Lei Geral de Proteção de Dados Pessoais (LGPD): A LGPD estabelece princípios e diretrizes para o tratamento de dados pessoais, incluindo a proteção de imagens e informações sensíveis (Brasil, 2018).

Além de normas e leis vigentes temos no contexto do poder público publicações de Procedimentos Operacionais Padrão (POPs): Os POPs da Polícia Federal, e de outros órgãos de investigação definem os procedimentos específicos para a realização da fotografia forense (BRASIL, 2013).

2 A CADEIA DE CUSTÓDIA DIGITAL

A cadeia de custódia é um princípio fundamental na investigação criminal, garantindo a autenticidade, confiabilidade e integridade das provas (Brasil, 1941) desde sua coleta até o uso em juízo. Esse conceito se aplica a todos os tipos de provas, incluindo provas físicas, documentos e, cada vez mais relevante, provas digitais.

As origens da cadeia de custódia originaram-se na investigação de incêndios criminosos no século XIX. A necessidade de documentar a origem e o manuseio de materiais incendiários levou ao desenvolvimento de procedimentos para garantir a confiabilidade das provas. Com o tempo, esses procedimentos foram estendidos a outros tipos de investigações, incluindo crimes contra a pessoa e crimes patrimoniais (Edson, 2019).

Com o advento da era digital, a cadeia de custódia se torna cada vez mais importante. As provas digitais, como arquivos de computador, imagens e mensagens eletrônicas, podem ser facilmente modificadas ou corrompidas, se não forem manuseadas e armazenadas de forma adequada.

A cadeia de custódia digital se baseia em princípios fundamentais, entre eles destacam-se:

A documentação: Todo o manuseio das provas digitais deve ser documentado de forma completa e precisa, incluindo data, hora, local, responsável e ações realizadas (Brasil, 2018).

O controle de acesso: O acesso às provas digitais deve ser restrito a um número mínimo de pessoas autorizadas, com mecanismos de controle de acesso para evitar acessos indevidos (Brasil, 2018).

A preservação: As provas digitais devem ser preservadas em sua forma original, sem alterações ou modificações, utilizando métodos e tecnologias adequadas (Brasil, 2013).

A rastreabilidade: Deve ser possível rastrear o movimento das provas digitais desde sua coleta até o uso em juízo, garantindo a continuidade da cadeia de custódia (Brasil, 2013).

A cadeia de custódia digital é essencial para garantir a autenticidade das provas digitais. A cadeia de custódia documentada comprova que as provas digitais não foram modificadas ou manipuladas desde sua coleta, assegurando sua confiabilidade em juízo (Edson, 2019).

No estudo de 2019, Alves et al. analisam a cadeia de custódia digital em uma delegacia de polícia, identificando falhas e vulnerabilidades no processo de armazenamento e gerenciamento de provas digitais. Os autores propõem soluções para aprimorar a custódia digital, como a utilização de ferramentas tecnológicas adequadas e a implementação de políticas e procedimentos rigorosos.

A cadeia de custódia, um tema crucial no âmbito jurídico, especialmente na área criminal, vem ganhando cada vez mais destaque nos últimos anos. Diversos julgados relevantes dos tribunais superiores, como o Superior Tribunal de Justiça (STJ) e o Supremo Tribunal Federal (STF), consolidam a importância da cadeia de custódia para a admissibilidade e confiabilidade das provas em processos penais.

Os julgados recentes evidenciam a necessidade de um registro preciso e detalhado da cadeia de custódia, desde a apreensão até a análise pericial ou disposição final das provas. Falhas nesse processo podem levar à nulidade das provas, como demonstrado no REsp 1.847.296 do STJ (Quinta Turma, 2023).

A jurisprudência também reconhece a importância de perícias específicas para analisar vícios na cadeia de custódia, como no HC 653.515 do STJ (Segunda Turma, 2023). Essa medida garante um exame técnico e imparcial das provas, assegurando a justiça e o devido processo legal.

Além disso, o STF, no RE 1.040.868 (Segunda Turma, 2024), elevou a cadeia de custódia à condição de garantia fundamental do processo penal, reforçando seu papel crucial na busca pela verdade e na garantia dos direitos do réu.

Com uma cadeia de custódia robusta se torna mais difícil para a defesa contestar a validade das provas digitais, fortalecendo a investigação e a acusação.

O Código de Processo Penal (Brasil, 1941) não define um tempo de custódia específico para fotografias forenses. No entanto, a jurisprudência e as melhores práticas recomendam a retenção das provas por um período suficiente para garantir sua relevância nos processos judiciais e atender às necessidades de investigação.

Diversos fatores influenciam o tempo de custódia ideal, como a natureza do crime, a complexidade da investigação, o potencial de recursos e a legislação vigente. É fundamental que a SPTC-GO estabeleça uma política de tempo de custódia clara e documentada, considerando esses fatores e alinhada às melhores práticas da área (Silva et al., 2019, 2020).

A cadeia de custódia garante que as provas digitais sejam coletadas, armazenadas e utilizadas de forma legal e ética, protegendo os direitos dos investigados, vítimas e testemunhas (Edson, 2019).

A cadeia de custódia digital é um elemento crucial na investigação criminal na era digital. Ao garantir a autenticidade, a confiabilidade e a integridade das provas digitais, a cadeia de custódia contribui para a busca da verdade, a justiça e a proteção dos direitos dos envolvidos no processo judicial.

3 O ARMAZENAMENTO DE FOTOGRAFIA DIGITAIS

3.1 Tecnologias disponíveis

O armazenamento de fotografias digitais em órgãos públicos exige a utilização de tecnologias robustas e confiáveis que garantam a preservação da integridade, autenticidade e acessibilidade das imagens ao longo do tempo. Dentre as principais tecnologias disponíveis, destacam-se:

O armazenamento em nuvem: serviços de armazenamento em nuvem, como *Google Drive*, *Dropbox* e *iCloud*, oferecem flexibilidade, escalabilidade e acesso remoto às fotografias, mas dependem de uma conexão à internet confiável e podem apresentar custos mensais (Borden et al., 2018). Soluções em nuvem oferecem flexibilidade, escalabilidade e segurança para o

armazenamento de grandes volumes de dados, incluindo fotografias digitais. A escolha do provedor de nuvem deve considerar fatores como confiabilidade, segurança e compatibilidade com os sistemas existentes na organização.

Armazenamento local: o armazenamento local em servidores físicos dentro da organização oferece maior controle sobre os dados, mas exige investimento em infraestrutura e equipe qualificada para gerenciamento e manutenção. De acordo com Edson (2019) O armazenamento em discos rígidos, *SSDs* ou *NAS* oferece controle direto sobre as imagens, mas exige investimento em infraestrutura e manutenção.

Armazenamento híbrido: a combinação de armazenamento em nuvem e local pode oferecer o melhor dos dois mundos, proporcionando flexibilidade, escalabilidade e controle sobre os dados (Edson,2019).

3.2 Boas Práticas para Armazenamento de Dados em Órgãos Públicos

Para garantir a segurança e a preservação das fotografias digitais armazenadas em órgãos públicos, é fundamental seguir boas práticas, como:

Definição de políticas de armazenamento: estabelecer políticas claras e objetivas que definem os critérios de armazenamento, retenção e descarte de fotografias digitais, garantindo a conformidade com as leis e regulamentações em vigor (Brasil, 2018).

Implementação de controles de acesso: restringir o acesso às fotografias digitais a usuários autorizados, utilizando mecanismos de autenticação e autorização robustos (Edson, 2019) tal prática é primordial para proteger a confidencialidade das informações e evitar acessos indevidos. Adicionalmente é de extrema importância, para a segurança dos dados, mas também para a segurança institucional primar pelo controle de acesso físico dos locais onde operam os *hardwares* podendo ser utilizados fechaduras ou portas com acesso biométrico dentre outras tecnologias que autenticam os acessos a esses lugares restritos.

Realização de *backups* regulares: criar *backups* regulares das fotografias digitais para garantir a recuperação em caso de perda ou falha de *hardware*. Segundo Borden (2018) a realização de *backups* regulares garante a recuperação das fotografias digitais em caso de perda de dados ou falhas de *hardware*.

Implementação de medidas de segurança: adotar medidas de segurança para proteger as fotografias digitais contra acessos não autorizados, malware e outras ameaças cibernéticas.

Treinamento de funcionários: capacitar os funcionários sobre as boas práticas de armazenamento e gerenciamento de fotografias digitais para garantir o uso adequado das

tecnologias disponíveis. O treinamento de funcionários (Gil, 2019) sobre as boas práticas de armazenamento e gerenciamento de fotografias digitais é essencial para garantir o uso adequado das tecnologias disponíveis e a proteção das imagens.

O armazenamento adequado de fotografias digitais em órgãos públicos é de extrema importância para garantir a preservação desses dados e a investigação de crimes. A escolha da tecnologia de armazenamento e a implementação de boas práticas de segurança são essenciais para proteger a integridade, autenticidade e acessibilidade das fotografias ao longo do tempo.

4 RESULTADOS E DISCUSSÕES

Nesta seção será apresenta-se uma análise dos dados obtidos com a aplicação do questionário enviado aos grupos de médicos legistas e peritos criminais lotados na SPTC GO. Esse levantamento mostrou-se necessário para ter uma avaliação geral das formas utilizadas por esses profissionais para armazenarem as fotografias geradas durante suas atividades laborais, bem como a percepção em relação a segurança da informação.

Para a realização da pesquisa foi elaborado e aplicado um questionário via plataforma *Google forms* composto por questões de múltiplas escolhas, com o objetivo de ter um panorama geral sobre as formas utilizadas para armazenar as fotografias digitais, bem como a garantia de segurança desses dados. O questionário foi disparado por meio de *hiperlink* distribuído por meio de grupos restritos do aplicativo *WhatsApp*.

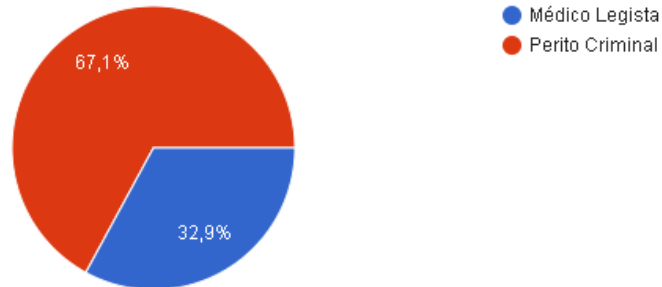
O questionário foi disponibilizado no período de 02 a 04 de abril de 2024 e ficou restrita a médicos legistas e peritos criminais da ativa. De acordo com dados extraídos do Portal da Transparência do Estado de Goiás, atualmente o quadro de médicos legistas ativos é de 183 enquanto o quadro funcional de peritos criminais é de 393 ou seja um total de 576 médicos e peritos ativos na instituição (Estado de Goiás, 2024).

Após disponibilização do formulário houve um retorno de 82 respostas sendo: 27 médicos legistas (32,9%) e 55 peritos criminais (67,1%). Considerando os dados apresentados acima a amostra é de aproximadamente 14, %, conforme apresentado no Gráfico 1.

Gráfico 1 - Sobre o quantitativo de participantes e seu cargo

Qual seu cargo na SPTC

82 respostas

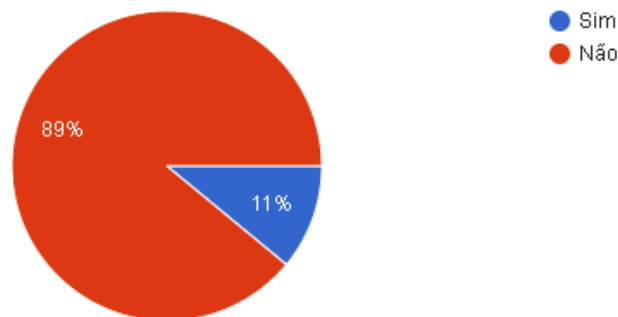


Fonte: O autor (2024)

A segunda questão do questionário foi: “Você recebeu alguma instrução da instituição sobre como proceder quanto ao armazenamento desses dados?”

Gráfico 2 - Sobre a instrução de como proceder para armazenar os dados

82 respostas



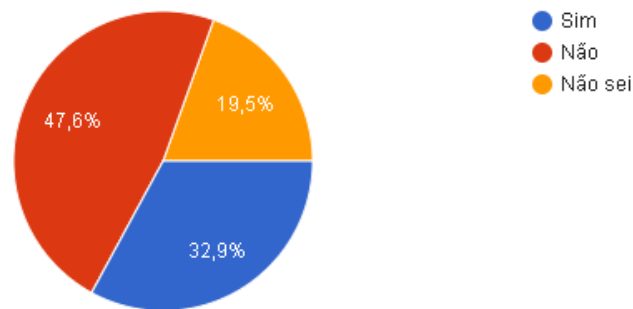
Fonte: O autor (2024)

Das 82 respostas obtidas, 73 pessoas (89%) afirmaram não ter recebido instrução da instituição sobre como proceder para armazenar dados corretamente, ou seja, um fator de risco, pois, trata-se de um tema sensível e importante e que devido a sua criticidade demanda uma maior atenção da instituição. Aproximadamente 90% das pessoas entrevistadas nunca tiveram treinamento ou instrução sobre como proceder. Já 9 pessoas (11%) afirmaram ter recebido a instrução.

A terceira pergunta foi “Segue algum padrão e/ou procedimento para garantir a confidencialidade, integridade e disponibilidade dos dados armazenados?”. Tal questionamento tinha como objetivo avaliar uma das hipóteses que se tratava da falta de padrão ou procedimento institucional.

Gráfico 3 - Sobre a garantia de confidencialidade, integridade e disponibilidade

82 respostas



Fonte: O autor (2024)

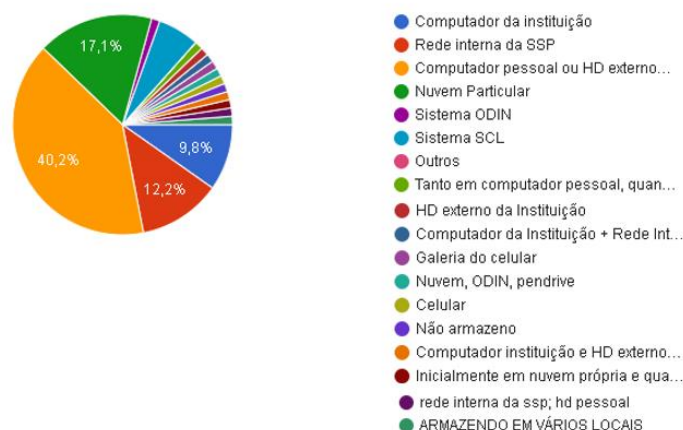
Sobre o seguimento de procedimentos que garantam a confidencialidade, integridade e disponibilidade de dados armazenados, 47,6% responderam não seguir enquanto 19,5% não souberam responder e 32,9% disseram seguir algum procedimento.

Neste questionamento obtivemos que 55 pessoas (67,1%) responderam não ou não sei, o que representa uma população expressiva que não segue nenhum padrão e ou procedimento para garantir os princípios básicos de tratamentos de dados. O total de 27 entrevistados (32,1%) responderam seguir algum procedimento ou padrão.

A quarta pergunta foi “Como você armazena as fotografias realizadas em exames periciais? Seja de local de crime ou exames internos:”

Gráfico 4 - Sobre como é realizado o armazenamento de fotografias

82 respostas



Fonte: O autor (2024)

Nesta pergunta temos que 33 pessoas (40,7%) utilizam computador pessoal, ou *Hd* externo pessoal ou *pendrive* particular para armazenar as fotografias periciais, 14 pessoas (17,1%) utilizam nuvem particular, 10 pessoas (12,2%) utilizam a rede interna da Secretaria de

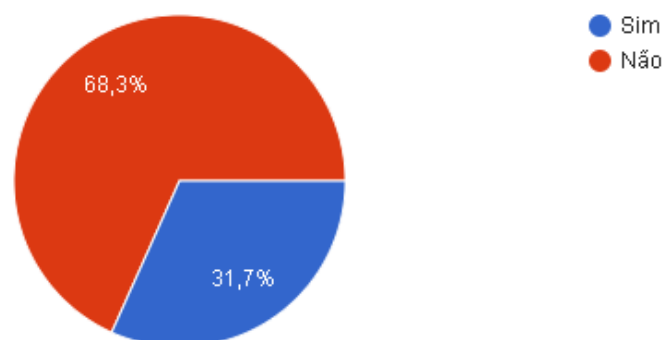
segurança pública(SSP), 8 pessoas (9,8%) armazenam os dados no computador da instituição, 5 pessoas (6,1%) utilizam o sistema SCL - Sistema de cadastro de laudos e os demais participantes que totalizam 12 pessoas (14,6%) que representam a proporção unitária de 1,2% dentre as respostas selecionadas: “computador da instituição”, “rede interna da SSP”, “Sistema Odin”, “Outros” , “tanto em computador pessoal, quanto *Hd* externo pessoal e computador da instituição (três locais distintos com acesso restrito)”, “celular”, “não armazeno”, “inicialmente em nuvem própria e quando o laudo está finalizado, armazeno na rede interna da SSP, e deleteo da nuvem própria”, “rede interna da SSP, *Hd* externo pessoal”, “armazeno em vários locais”.

Aproximadamente 60% das pessoas entrevistadas utilizam nuvem particular ou computador ou *Hd* externo ou *pendrive* pessoal, tal dado demonstra a pluralidade de formas adotados pelos peritos e médicos em realizar o armazenamento, 12,5 % armazenam os dados na rede da SSP. Isso reforça a relevância do tema em que pese a diversidade de tecnologias utilizadas sem nenhuma padronização oficial, gerando um ambiente vulnerável e desforme. Tal resultado demonstra a necessidade do desenvolvimento de procedimentos bem como de instrução e disponibilização de tecnologias para que esses servidores possam armazenar os dados com segurança, e tenham ciência e confiança de que em caso ocorra um sinistro desses dados, exista uma política bem definida de segurança dos dados e de *backup*.

A quinta pergunta “Você se sente seguro em relação ao atual armazenamento utilizado?”

Gráfico 5 – Sobre como as pessoas se sentem em relação a segurança nos armazenamentos utilizados

82 respostas



Fonte: O autor (2024)

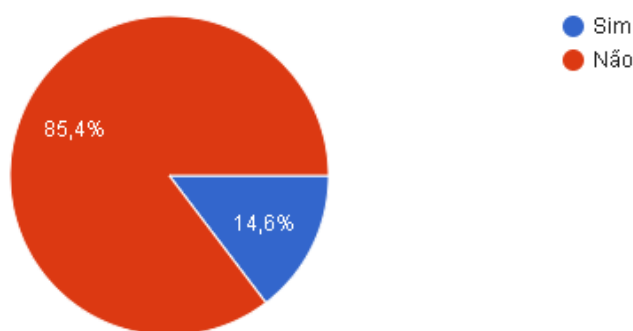
Nesse quesito 56 pessoas, 68,3% afirmaram não se sentir seguro em relação a forma atual utilizada no armazenamento, tal resultado tem confluência com a falta de padronização e de procedimentos a serem seguidos, com isso o profissional que necessita desse material para

realização do trabalho se sente inseguro, e opta por assumir em sua maioria a responsabilidade pelo armazenamento utilizando-se de dispositivos e tecnologias de sua propriedade, conforme respostas da questão três demonstrada no gráfico 4.

A sexta pergunta “Conhece os princípios básicos da segurança da informação e pode afirmar que a forma utilizada atualmente garante esses princípios?”

Gráfico 6 – Sobre o conhecimento da segurança da informação e sua relação com o armazenamento atual

82 respostas



Fonte: O autor (2024)

Nesse questionamento sobre o conhecimento dos princípios básicos da segurança da informação, 85,4% dos entrevistados afirmaram não conhecer esses princípios, um dado alarmante, pois, considerando a transformação digital que está sendo implementada no Estado, faz-se mister uma maior capacitação e implementação de políticas de difusão desses conhecimentos, com o objetivo de proteger os dados gerados e custodiados pela instituição.

5 CONSIDERAÇÕES FINAIS

As considerações finais deste estudo sobre o armazenamento de evidências digitais e fotografia forense na Superintendência de Polícia Técnico-Científica do Estado de Goiás destaca a importância crítica do armazenamento adequado de fotografias forenses para garantir a integridade, autenticidade e acessibilidade das evidências digitais ao longo do tempo. A pesquisa revelou que a falta de padronização e a diversidade de tecnologias utilizadas pelos peritos e médicos legistas na SPTC-GO para armazenar dados representam um ambiente vulnerável e desorganizado. A maioria dos entrevistados utiliza nuvem particular, computador, *HD* externo ou *pendrive* pessoal para armazenamento, demonstrando a necessidade urgente de desenvolvimento de procedimentos, instrução e disponibilização de tecnologias para garantir a segurança dos dados.

Além disso, a pesquisa identificou que 85,4% dos entrevistados afirmaram não conhecer os princípios básicos da segurança da informação, o que ressalta a importância de capacitação e implementação de políticas de difusão desses conhecimentos. A transformação digital em andamento no Estado torna essencial a proteção dos dados gerados e custodiados pela instituição.

Com base nas normas e melhores práticas para o armazenamento de dados em organizações públicas, é fundamental que a prática da fotografia forense esteja em conformidade com as legislações vigentes, a fim de garantir a confiabilidade e a validade das provas coletadas. A cadeia de custódia digital, baseada em princípios fundamentais como documentação completa e precisa, controle de acesso restrito e mecanismos de segurança, é essencial para preservar a integridade das evidências digitais.

Dois soluções principais se apresentam viáveis para o armazenamento seguro de fotografias forenses na SPTC-GO: a criação de um banco de dados local ou a contratação de um serviço de armazenamento em nuvem. A implementação de um banco de dados local oferece controle total sobre a infraestrutura e os dados, proporcionando maior segurança e privacidade. Entretanto, essa opção exige investimento em *hardware*, *software*, equipe qualificada para gerenciamento e manutenção, além de medidas robustas de segurança contra falhas e ataques cibernéticos. Em contrapartida a contratação de um serviço de armazenamento em nuvem oferece praticidade, escalabilidade e custos previsíveis, além de acesso remoto aos dados. Não obstante, é crucial selecionar um provedor confiável que atenda aos requisitos de segurança e privacidade da SPTC-GO.

Recomenda-se a realização de um estudo econômico detalhado, considerando os fatores mencionados acima, para determinar a solução de armazenamento mais econômica e vantajosa para a SPTC-GO. O estudo deve ser realizado por especialistas qualificados e levar em consideração as especificidades da instituição, os requisitos de segurança e privacidade bem como os recursos financeiros disponíveis.

Portanto, as conclusões deste estudo destacam a necessidade de implementação de políticas de segurança da informação, capacitação dos profissionais envolvidos, padronização de procedimentos e tecnologias de armazenamento, a fim de garantir a conformidade legal, a segurança da informação e a preservação das evidências digitais na Superintendência de Polícia Técnico-Científica do Estado de Goiás. A pesquisa também ressalta a importância de investimentos em tecnologias robustas e confiáveis, treinamento contínuo dos funcionários e a criação de políticas claras e objetivas para o armazenamento, retenção e descarte de fotografias digitais, visando garantir a conformidade com as leis e regulamentações em vigor.

REFERÊNCIAS

- ALVES, A. C. et al. **Armazenamento de imagens digitais em nuvem: Uma análise dos riscos e desafios na perspectiva da segurança da informação**. Revista Brasileira de Gestão da Informação e Documentação, v. 13, n. 2, p. 1-15, 2019.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **NBR ISO/IEC 27001:2013**. Tecnologia da informação — Técnicas de segurança — Sistemas de gestão da segurança da informação — Requisitos. Rio de Janeiro, 2013.
- BORDEN, Richard; BYRD, John A.; SCHETTLER, Anthony D. **Sistemas de informação: uma abordagem gerencial**. 13ª ed. Porto Alegre: AMGH, 2018.
- BRASIL. Decreto-Lei nº 3.689 de 03 de outubro de 1941. **Código de Processo Penal**. 1941.
- BRASIL. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Lei nº 13.709, de 14 de agosto de 2018. Diário Oficial da União, Brasília, DF, 15 ago. 2018.
- BRASIL. Ministério da Justiça/SENASP. **Procedimento Operacional Padrão**. Brasília: Perícia Criminal, 2013.
- EDSON, Edson. **Fotografias periciais: definição diplomática de documentos imagéticos forenses**. 2019. Tese (Doutorado em Ciência da Informação) - Universidade de Brasília, Brasília, DF.
- GOIÁS. **Portal da Transparência**. Disponível em <https://transparencia.go.gov.br/> Acesso em 17 abr. 2024.
- FOTOGRAFIA. In: DICIO, **Dicionário Online de Português**. Porto: 7Graus, 2024. Disponível em: <https://www.dicio.com.br/fotografia/>. Acesso em: 12 mar. 2024.
- GIL, A. C. **Metodologia de pesquisa em administração**. 6ª ed. São Paulo: Atlas, 2019.
- KOSSOY, Boris. **Fotografia & história**. 2ª ed. São Paulo: Atelie Editorial, 2001.
- SILVA, R. A. et al. **A importância da cadeia de custódia digital na investigação de crimes cibernéticos**. Revista Brasileira de Direito da Informação, v. 13, n. 1, p. 1-15, 2019.
- SILVA, R. A. et al. **Boas práticas para o armazenamento de imagens digitais em órgãos públicos**. Revista Brasileira de Administração Pública, v. 53, n. 1, p. 1-20, 2020.
- SUPREMO TRIBUNAL FEDERAL. 2ª Turma. **Recurso Extraordinário nº 1.040.868-DF**. Relator: Ministro Edson Fachin. Data de Publicação: 07/03/2024.
- TRIBUNAL SUPERIOR DE JUSTIÇA. 5ª Turma. **Recurso Especial nº 1.847.296-RS**. Relator: Ministro Francisco Falcão. Data de Publicação: 21/03/2023.
- TRIBUNAL SUPERIOR DE JUSTIÇA. 2ª Turma. **Habeas Corpus nº 653.515-RS**. Relator: Ministro Paulo de Tarso João Ribeiro. Data de Publicação: 14/11/2023.

APÊNDICE A – Questionário aplicado

PROJETO DE TCC - CEGESP 2024 - O Armazenamento de fotografias digitais produzidas no âmbito da Superintendência de Polícia Técnico Científica do Estado de Goiás.

Esse formulário visa adquirir dados para subsidiar a pesquisa de tema: O Armazenamento de fotografias digitais produzidas no âmbito da Superintendência de Polícia Técnico Científica do Estado de Goiás.

Sua participação é voluntária e os dados(respostas) serão tratados de forma confidencial. Nenhum dado pessoal será coletado.

O objetivo desta pesquisa busca identificar as diversas formas que as unidades da SPTC armazenam as fotografias forenses, visando propor soluções exequíveis para mitigar possíveis inconformidades.

Agradeço a sua participação!

Indica uma pergunta obrigatória

Qual seu cargo na SPTC *

Marcar apenas uma oval.

- Médico Legista
 Perito Criminal

Você recebeu alguma instrução da instituição sobre como proceder quanto ao armazenamento desses dados? *

Marcar apenas uma oval.

- Sim
 Não

3. Segue algum padrão e/ou procedimento para garantir a confidencialidade, integridade e disponibilidade dos dados armazenados? *

Marcar apenas uma oval.

- Sim
 Não
 Não sei

4. Como você armazena as fotografias realizadas em exames periciais? Seja de local de crime ou exames internos? *

Marcar apenas uma oval.

- Computador da instituição
 Rede interna da SSP
 Computador pessoal ou HD externo ou pendrive particular
 Nuvem Particular
 Sistema ODIN
 Sistema SCL
 Outros
 Outros: _____

5. Você se sente seguro em relação ao atual armazenamento utilizado? *

Marcar apenas uma oval.

- Sim
 Não

6. Conhece os princípios básicos da segurança da informação e pode afirmar que a forma utilizada atualmente garante esses princípios? *

Marcar apenas uma oval.

- Sim
 Não