Faculdade de Tecnologia de Americana "Ministro Ralph Biasi"
Curso Superior de Tecnologia em Segurança da Informação

BOAS PRÁTICAS NO DESCARTE DE UNIDADES HDDS E SSDS

BEST PRACTICES IN THE DISPOSAL OF HDDS AND SSDS

Lucas Gabriel Gama D'angelo, Fatec de Tecnologia de Americana
Lucas.angelo01@fatec.sp.gov.br

Matheus Pancoti Mota, Fatec de tecnologia de Americana
Matheus.mota2@fatec.sp.gov.br

Orientador: Henri Alves de Godoi
henri.godoy@fatec.sp.gov.br

Resumo

Este trabalho investiga as melhores práticas para o descarte seguro e sustentável de unidades de armazenamento de dados, como HDDs e SSDs. Com o aumento do volume de dados digitais, garantir o descarte adequado desses dispositivos é crucial para proteger informações confidenciais e minimizar o impacto ambiental. O estudo analisa métodos de destruição de dados, como desmagnetização, destruição física e sobrescrita, avaliando suas eficácias. Também aborda o impacto causado por um descarte inadequado e examina as dificuldades em relação a tempo e custo aplicados em cada processo. Por meio de estudos de caso e revisão de literatura, o trabalho propõe um guia de boas práticas aplicáveis em ambientes corporativos e institucionais, promovendo a proteção de dados e a sustentabilidade ambiental.

Palavras-chave: Dados digitais, sobrescrever, unidades de armazenamento

Abstract

This paper investigates best practices for the secure and sustainable disposal of data storage units, such as HDDs and SSDs. With the increasing volume of digital data, ensuring the proper disposal of these devices is crucial for protecting confidential information and minimizing environmental impact. The study analyzes data destruction methods, such as degaussing, physical destruction, and overwriting, evaluating their effectiveness. It also addresses the impact caused by improper disposal and examines the challenges related to time and cost in each process. Through case studies and literature review, the paper proposes a guide of best practices applicable in corporate and institutional environments, promoting data protection and environmental sustainability.

***Keywords**: Digital data, data overwriting, storage drives*

1. INTRODUÇÃO

As boas práticas de descarte de unidades de armazenamento, no contexto da segurança da informação, referem-se a processos e técnicas que garantem a eliminação completa de dados sensíveis antes que os dispositivos sejam descartados ou reutilizados. Na área de tecnologia da informação (TI), a confidencialidade e a integridade dos dados são essenciais. Ao remover os dispositivos de armazenamento, como discos rígidos, SSDs, pode-se garantir que as informações confidenciais não sejam acessadas de maneira não autorizada.

> No nosso cenário digital em rápida evolução, a acumulação de dispositivos eletrônicos antigos é uma ocorrência comum. Laptops, smartphones, discos rígidos externos [...] se tornam desatualizados e obsoletos, mas frequentemente contêm uma quantidade significativa de informações sensíveis. Proteger seus dados pessoais e confidenciais durante o processo de descarte é de extrema importância. (Bachchas, 2023).

A ausência de um protocolo rigoroso de descarte de unidades de armazenamento pode resultar em sérias consequências tanto para usuários comuns quanto para grandes empresas. Para o usuário individual, a exposição de dados pessoais, como informações bancárias, fotos e documentos, pode levar a fraudes e roubo de identidade. Para empresas, desde as leis de proteção de dados até as exigências de propriedade intelectual, nunca foi tão importante garantir que os dados sejam tratados de acordo com a conformidade legal e regulatória (Bradshaw 2023). A negligência no descarte seguro pode resultar em violações de segurança, perdas financeiras, danos à reputação e até mesmo penalidades legais, especialmente para corporações que trabalham com grandes volumes de dados.

Exemplos de casos de incidentes são comuns e ressaltam a necessidade de um cuidado maior no descarte de unidades de armazenamento. A *Affinity Health Plan*, uma empresa de planos de saúde com base em Nova York, foi alvo de uma multa de US$ 1,2 milhão em 2010 por não apagar corretamente dados confidenciais de discos rígidos de copiadoras devolvidos a uma empresa de leasing. A falha resultou na exposição de informações de mais de 300.000 pessoas (DataBreachToday, 2013).

Em um outro caso, *Morgan Stanley*, uma empresa multinacional de serviços financeiros e banco de investimentos também com sede em Nova York, foi multada de US$ 60 milhões em 2020 por não apagar adequadamente dados de discos rígidos antigos, expondo informações pessoais e financeiras de clientes (GDPR Register, 2020).

Assim, o argumento principal desse trabalho é sustentado e se baseia na importância de boas práticas no descarte de unidades de armazenamento. A aplicação eficaz dessas estratégias garante que as informações confidenciais não sejam vistas por pessoas não autorizadas e fortalece a visão geral de segurança de uma organização. Para reduzir os riscos e garantir a proteção de dados

valiosos ao longo do ciclo de vida da mídia de armazenamento, é fundamental criar e seguir rígidas políticas de descarte.

2. REFERENCIAL TEÓRICO

O desenvolvimento das unidades de armazenamento de dados passou por várias etapas e fases, refletindo as necessidades tecnológicas e os avanços da engenharia. Os discos rígidos (HDDs), unidades de estado sólido (SSDs) são as tecnologias de armazenamento mais comuns.

Embora tenham o mesmo objetivo, cada tecnologia tem suas próprias características e vantagens. ao longo do tempo, à medida que o design dos computadores melhorou, muitos fabricantes passaram dos HDDs tradicionais para os SSDs (Hepisuthar; Sharma, 2021).

Quando se sabe que cada uma das tecnologias tem características técnicas e aplicações específicas, é possível concluir que essas condições determinaram suas trajetórias de sucesso e durabilidade, tanto no que diz respeito ao uso pessoal em tarefas cotidianas quanto na esfera corporativa, em termos econômicos.

2.1. HDDs (*Hard Disk Drives*)

Os discos rígidos foram introduzidos pela IBM em 1956 com o modelo 305 RAMAC (Alecrim. 2008). Eles funcionam com base em discos magnéticos giratórios (chamados de *platters*) revestidos com material magnético. Para ler e escrever dados nessas superfícies, um braço mecânico chamado de atuador acessa fisicamente diferentes partes do disco. Cada disco é dividido em trilhas e setores. Essas estruturas organizam os dados de forma que podem ser lidos sequencialmente ou aleatoriamente.

Os HDDs têm oferecido a maior capacidade de armazenamento a um custo por *gigabyte* muito baixo (Alecrim, 2008). A capacidade dos HDDs foi crescendo ao longo dos anos, passando de alguns *megabytes* (MB) nos primeiros modelos para vários *terabytes* (TB) nas unidades modernas, ideais para aplicações que exigem armazenamento em massa, como servidores, *data centers* e computadores pessoais.

A velocidade de um HDD é determinada pela rotação dos *platters,* medida em rotações por minuto (RPM), e pela densidade de dados nos discos. Unidades comuns giram a 5400 ou 7200 RPM, enquanto discos de alto desempenho podem atingir 10.000 ou 15.000 RPM (Alecrim. 2008). Mas, como mostra a **Figura 1**, os HDDs têm limitações de velocidade devido ao movimento mecânico necessário para acessar os dados, aumentando sua vulnerabilidade física a danos, principalmente em locais móveis ou vibrantes.

Figura 1 - Nessa figura o HDD está sem a tampa superior, revelando seus componentes internos, como os discos de armazenamento e o braço mecânico, que acessa os dados gravados no disco.

Fonte: Crucial. Disponível em: https://br.crucial.com/articles/about-ssd/ssd-vs-hdd. 2024. Acesso em 3 de agosto de 2024

2.2. SSDs (*Solid State Drives*)

As unidades de estado sólido (*Solid State Drives)* surgiram como uma evolução das tecnologias de armazenamento, utilizando memória *flash* NAND em vez de discos magnéticos. Essa memória é composta por células de memória que podem ser programadas eletricamente para armazenar dados (Carvalho, 2014). A ausência de partes móveis nos SSDs significa que o acesso aos dados é quase instantâneo, sem a latência associada ao movimento físico, como nos HDDs.

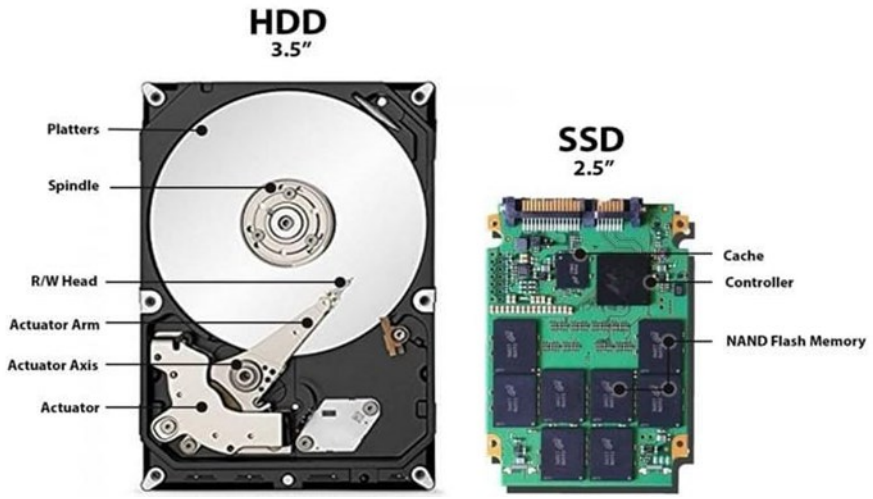
Também pode ser dito que, conforme ilustrado na **Figura 2**, a ausência de componentes mecânicos na estrutura do SSD possibilita uma redução significativa em suas dimensões de escala e tamanho quando comparado a um HDD, o que facilita sua integração em diferentes sistemas computacionais em que for instalado.

Embora os SSDs inicialmente fossem muito mais caros que os HDDs, o custo por *gigabyte* diminuiu consideravelmente nos últimos anos. No entanto, em termos de capacidade máxima, os SSDs ainda são mais caros por *terabyte* em comparação com os HDDs. Eles são mais comumente usados em computadores, *laptops*, e servidores em que a velocidade é primária, mas a capacidade extrema é secundária.

Os SSDs oferecem velocidades de leitura e escrita muito superiores aos HDDs, com tempos de acesso medidos em microssegundos em vez de milissegundos (Carvalho, 2014), melhorando o desempenho em tarefas que exigem acesso frequente ou leitura e gravação de grandes volumes de

dados. Os SSDs também são muito mais resistentes a choques e vibrações, o que os torna ideais para dispositivos móveis e situações em que a confiabilidade é importante.

Figura 2 - Nessa figura traz a comparação entre um HDD (3,5 polegadas) e um SSD (2,5 polegadas) sem as tampas superiores.



Fonte: R4U. Disponível em: https://r4u.com.br/ssd/. 2020
Acesso em 4 de agosto de 2024

2.3. Importância da eliminação dos dados baseado na LGPD

Empresas e organizações têm a responsabilidade de garantir que os dados pessoais que coletam e armazenam sejam confiáveis e seguros. A LGPD exige que essas entidades tomem medidas organizacionais e técnicas adequadas para proteger os dados, incluindo a eliminação segura quando os dados não são mais necessários para o propósito para o qual foram coletados. Levando em consideração o prejuízo monetário caso dados sensíveis sejam identificados por pessoas de má índole e tentem negociar para a não divulgação desses dados, como também o dano que a marca sofrerá após um vazamento (Mateus, 2023), causando a perda de confiança em vários clientes após a experiências de vazamentos de dados. A violação das regras pode resultar em multas graves (Mateus, 2023), incluindo multas que podem chegar a até 2% do lucro da empresa, com o limite de R$ 50 milhões por infração.

Vale pontuar também que a partir de setembro de 2020 as sanções previstas na LGPD começaram a valer após os dois anos de adequação das empresas, levando em consideração que na LGPD (2020), seção IV, artigo 16 é abordado sobre a eliminação dos dados pessoais após o término de seu tratamento, sendo que caso não estejam de acordo, as sanções podem variar desde

advertências com prazo para adoção das medidas corretivas a multas diárias de até 2% do faturamento da empresa, conforme diz o artigo 52, seção I:

> - Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> - I - Advertência, com indicação de prazo para adoção de medidas corretivas; (Brasil, 2020).

2.4. Métodos de eliminação de dados

Essa seção é destinada a descrever os métodos seguros e mais recomendados de eliminação, apagamento e deleção de dados em unidades de armazenamento, sendo descritos por ordem de unidade/tecnologia, os melhores e mais reconhecidos métodos de acordo com a confiabilidade e exatidão no processo de extinguir a informações existentes em HDDs, SSDs

2.4.1. Métodos de eliminação de dados em HDDs

Os métodos para a deleção de arquivos em unidades HDDs são amplamente conhecidos por conta da praticidade dos métodos mais simples e o tempo em que a tecnologia se encontra no mercado, podendo presumir que, quanto maior o tempo que a tecnologia disponível para muitos consumidores com um preço acessível, mais bem explorado será todos os quesitos de funcionamento e melhores práticas para o uso correto e seguro do equipamento.

2.4.1.1. Sobrescrita Simples em HDDs

Em relação à deleção de dados em discos rígidos (HDDs), o processo de sobrescrita simples consiste em substituir os dados existentes por novos dados, geralmente zeros ou padrões aleatórios, com o objetivo de impedir a recuperação dos dados originais. Quando um arquivo é deletado normalmente, o sistema operacional apenas marca o espaço disponível no arquivo como disponível para uso novamente. No entanto, os dados permanecem fisicamente no disco até serem sobrescritos.

Segundo Zhuravel (2023), “Todos os dados no meio de armazenamento são substituídos por caracteres aleatórios. Não há chance de qualquer dado confidencial restante.”

A sobrescrita simples garante que os dados antigos sejam eliminados escrevendo diretamente nos segmentos do disco que os dados antigos estavam armazenados. Esse método diminui significativamente a probabilidade de os dados serem recuperados por meio de métodos de recuperação forense ou uso de *software* especializado.

O Windows inclui uma ferramenta de linha de comando chamada *Cipher* que pode sobrescrever o espaço livre em um disco, ajudando a remover dados deletados anteriormente, se pode utilizar da seguinte forma:

- Abra o Prompt de Comando como administrador.
- Digite cipher /w:C: (substitua "C:" pela letra da unidade desejada).
- Esse comando sobrescreverá o espaço livre na unidade.

No sistema operacional Linux existem várias formas de efetuar essa deleção, a mais simples sendo o comando "*shred*":

- Digite shred -u nome_do_arquivo

Sendo -u: Remove o arquivo após a sobrescrita.

Por padrão, o *shred* sobrescreve o arquivo 3 vezes com dados aleatórios.

Também existem aplicações que são capazes de fazer a eliminação de dados, elas oferecem uma maior abrangência de opções nessa tarefa, mas podem sacrificar a segurança e confiabilidade do processo.

2.4.1.2. Sobrescrita com Padrões Múltiplos

A sobrescrita de padrões múltiplos é uma técnica segura de apagamento de dados de disco rígido (HDD) que usa vários padrões de *bits* para escrever novas informações sobre os dados existentes repetidamente, impedindo que os dados originais não podem ser recuperados por meio desse processo.

> Dados sobrescritos uma ou duas vezes podem ser recuperados subtraindo o que se espera ler de um local de armazenamento do que é realmente lido. Dados que são sobrescritos um número arbitrariamente grande de vezes ainda podem ser recuperados, desde que os novos dados não sejam gravados exatamente no mesmo local que os dados originais (Gutmann, 1996).

Nesse trecho Gutmann ressalta que os dados quando substituídos em padrões múltiplos, no mesmo local dos dados originais dificultam ou impossibilitam que sejam restaurados.

O processo pode ser descrito como:

Um padrão fixo de *bits*, que normalmente consiste em zeros (0) ou uns (1), sobrescreve os dados armazenados no disco rígido interno.

Em seguida, o disco é sobrescrito repetidamente, geralmente com três ou mais passagens, cada uma com um padrão diferente. Esses padrões podem incluir:

- Sequências aleatórias de zeros e uns.
- Padrões complementares (por exemplo, uma passagem com zeros e outra com uns).
- Padrões especificados por algoritmos de apagamento seguro, como o método de Gutmann, que utiliza 35 passagens com diferentes padrões, e o método DoD 5220.22-M, que consiste no processo de 3 a 7 passagens.

2.4.1.3. Método Gutmann

O método Gutmann foi criado em 1996 por Peter Gutmann e visava limpar as informações de discos rígidos (HDDs) de forma que os dados não pudessem ser recuperados, mesmo com métodos de recuperação ou análise forense sofisticados. O método envolve sobrescrever todo o espaço do disco com uma coleção de 35 padrões de dados específicos em várias passagens.

Segundo Gutmann (Guttman, 1996), "Para apagar mídias magnéticas, precisamos sobrescrevê-las várias vezes com padrões alternados"

O processo envolve usar uma sequência específica de padrões binários para sobrescrever cada setor do disco rígido 35 vezes. Esses padrões foram desenvolvidos para atender aos vários tipos de codificação magnética que são usados em diferentes tecnologias de armazenamento de dados. Alguns desses tipos incluem modulação de frequência modificada (MFM) e codificação de longo alcance (RLL).

Embora tenham o mesmo objetivo, essas 35 passagens não são iguais:

- Passagens 1 a 4: Escrevem padrões aleatórios

- Passagens 5 a 31: Escrevem uma coleção de padrões cuidadosamente selecionados com o objetivo de eliminar remanescências específicas relacionadas a várias tecnologias de gravação magnética.

-Passagens 32 a 35: Escrevem novamente padrões aleatórios.

Cada padrão foi desenvolvido para reduzir o risco de recuperação de dados residuais resultantes dos efeitos magnéticos deixados pelas gravações anteriores.

Uma variedade de padrões é implementada para garantir a eficácia do apagamento, independentemente da tecnologia do disco, pois os discos rígidos podem ser codificados de várias maneiras.

Ferramentas como DBAN, *Eraser* e BCWipe são capazes de fazer a deleção e apagamento de dados de acordo com o método Gutmann, cada uma com seu grau de confiabilidade e velocidade de execução

2.4.1.4. Método DoD 5220.22-M

O Departamento de Defesa dos Estados Unidos (DoD) estabeleceu um padrão de sanitização de dados conhecido como DoD 5220.22-M. Ele define como eliminar seguramente dados sensíveis armazenados em mídias magnéticas (Oliveira, 2024).

O método DoD 5220.22-M tem variações, que são geralmente identificadas pelo número de passagens de sobrescrita:

- O método de três passagens é uma variante mais rápida, mas ainda é eficaz em várias situações:

- Primeira Passagem: A mídia é sobrescrita com zeros (0) ou uns (1).
- Segunda Passagem: Se a primeira passagem foi com zeros, esta será com uns, e vice-versa.
- Terceira Passagem: A mídia é sobrescrita por uma sequência aleatória de *bits*, tem como objetivo introduzir entropia, que dificulta a recuperação de dados originais

- O método de 7 Passagens Recomendado para dados altamente sensíveis, oferece um nível adicional de segurança, as primeiras seis passagens alternam entre padrões fixos e aleatórios:

- Primeira passagem: Sobrescrita com zeros (0).
- Segunda passagem: Sobrescrita com uns (1).
- Terceira passagem: Sobrescrita com padrão aleatório.
- Quarta passagem: Repetição dos passos anteriores ou uso de novos padrões específicos até a sétima repetição

De forma prática, esse método pode ser aplicado por ferramentas como DBAN, Eraser ou SDelete suportam o método DoD 5220.22-M.

2.4.1.5. Desmagnetização (*Degaussing*) em HDDs

O método de desmagnetização dos discos rígidos é muito utilizado desde a época do disquete e VHS, é uma boa prática para casos em que realmente não será mais utilizado a unidade de armazenamento e que é necessário realizar a limpeza de todos seus dados.

Nesse método é utilizado um *Degausser* (desmagnetizador), que se trata de um equipamento que afeta o campo magnético do disco rígido o que destrói os arquivos magneticamente nesse processo, porém esse processo acaba destruindo o disco rígido, por afetar os mecanismos de funcionamento da unidade, sendo recomendado utilizar somente em casos em que não será mais utilizado o HD e será encaminhado para destruição física (Araujo, 2023).

É preciso saber se o desmagnetizador é apropriado para o modelo de HDD que será desmagnetizado. Há diversos tipos de desmagnetizadores, alguns desenvolvidos especificamente para determinadas mídias, o processo se inicia colocando HDD na área ou compartimento apropriado do desmagnetizador, o procedimento demora apenas alguns segundos. Certos desmagnetizadores têm indicadores que asseguram a conclusão bem-sucedida do processo. Depois do procedimento, o disco rígido é visto como inútil, já que a desmagnetização também impacta o *firmware* e outros componentes vitais. O disco precisa ser eliminado ou reciclado de maneira apropriada.

> A desmagnetização requer o efeito de desmagnetizar os dispositivos ou retirar as suas propriedades magnéticas. Esse processo pode ser realizado em discos rígidos para eliminar os padrões com o auxílio de um desmagnetizador que destruirá os dados em questão de segundos (Araujo, 2023).

Esse é um método bem seguro, pois evita a reutilização do HD após o processo, em que impossibilita da recuperação dos dados por meio de *softwares* de recuperação, a **Figura 3** ilustra um desmagnetizador modelo Proton T-1, fabricado pela Proton Data Security uma empresa líder em soluções de proteção de dados, o Proton T-1 é frequentemente adotado por organizações que precisam apagar informações sigilosas de maneira permanente.

Figura 3 – Proton T-1 Desmagnetizador

Fonte: CBL Soluções em TI. Disponível em: https://cblsolucoes.com.br/equipamentos/. Acesso em 12 de outubro 2024

Um dos desafios para a implementação em empresas de pequeno e médio porte seria a disponibilidade desses equipamentos no mercado nacional. Pode ser observado que grandes empresas líderes no mercado de desmagnetização, como a ADC (*Advanced Design Corp*.) e a Data Security, Inc., têm suas sedes nos Estados Unidos e Europa, sem escritórios no Brasil e América Latina, deixando apenas a alternativa de importar esses equipamentos, um investimento elevado que muitas vezes as empresas não estão dispostas a fazer.

2.4.1.6. Destruição física dos HDDs

A destruição física é o último processo quando se fala sobre a integridade das informações e segurança contra vazamentos de dados confidenciais, pois após a formatação do disco, após a sobrescrita dos dados e a magnetização do disco rígido ele se encontrará sem utilidade, tendo apenas como destino a destruição e reciclagem do equipamento.

No contexto de Discos rígidos a eliminação física desses aparelhos pode ser feita de diversas formas:

- Trituração: O disco rígido é processado por uma máquina de trituração que corta os discos, o braço de leitura e escrita, entre outros componentes em partes menores.

- Perfuração: Um ou mais cortes são realizados nos pratos, causando instabilidade e impedindo a leitura dos dados com aparelhos convencionais.

- Dobramento: Aparelhos como Destruidor de HDDs (HDD *Destroyer*) têm a capacidade de dobrar o disco rígido, causando danos aos discos internos e à estrutura física.

- Desmontagem manual: Partes do disco, tais como discos magnéticos e cabeças de leitura, podem ser retiradas e eliminadas individualmente (Jacinta, 2024).

A eliminação física de discos rígidos (HDDs) é uma técnica eficiente e muito utilizada, mas, assim como qualquer técnica de eliminação de dados, ela tem seus prós e contras que devem ser levados em conta de acordo com o contexto de aplicação.

Uma das maiores vantagens é o apagamento total dos dados. Ao ser fisicamente danificado, o disco rígido danifica os discos magnéticos que guardam as informações de forma que a recuperação desses dados se torna praticamente inviável (Knolton, 2023), mesmo com a aplicação de técnicas forenses sofisticadas, outra vantagem é a simplicidade e a rapidez do procedimento. Com o auxílio de dispositivos especializados, como trituradores ou prensas hidráulicas, pode-se desmontar um disco rígido em poucos segundos, sendo assim, a destruição física atende a diversas regulamentações de segurança de dados, como as exigências da NSA e do Departamento de Defesa dos Estados Unidos, o que a torna amplamente utilizada em ambientes corporativos que precisam cumprir com padrões rígidos de segurança

A eliminação física de discos rígidos apresenta desvantagens, tais como a inviabilidade de reaproveitamento dos aparelhos, o que pode resultar em custos adicionais para as empresas, aumentando os custos e a complexidade do procedimento. Uma outra questão é o elevado preço dos equipamentos necessários, como trituradores e prensas, que podem ser elevados para empresas de menor porte. Métodos manuais mais econômicos, como o uso de martelos, não são tão eficientes e o procedimento normalmente requer manipulação manual, elevando o tempo e o esforço requeridos.

2.4.2. Métodos de eliminação de dados em SSDs

A remoção segura de dados em SSDs é fundamental para a proteção de informações pessoais e empresariais. Em virtude das particularidades dos SSDs, é crucial selecionar o método apropriado para assegurar que os dados não possam ser recuperados. Adotar as melhores práticas e empregar os instrumentos adequados garante uma eliminação eficiente e segura.

Existem vários fatores que diferenciam o apagamento de dados de um SSD para um HDD, como a diferenças básicas em tecnologia até as mais especificas como detalhes físicos de tamanhos e proporções, mas entre eles existem três fatores que dificultam a deleção de dados em SSDs, esses são Balanceamento de desgaste (*Wear leveling*), Super-provisionamento (*Over-provisioning*) e o

Comando TRIM, que fazem parte crucial do funcionamento do SSD e como a sua tecnologia executa a administração dos dados.

No Balanceamento de desgaste (*Wear leveling*) o SSD evita que ocorra o desgaste de áreas específicas ao espalhar as informações por todo o *drive* (Nikkel, 2019), tornando a sobrescrita simples muito difícil, deixando prováveis resquícios de informação.

O Super-provisionamento (*Over-provisioning*) garante um melhor desempenho e longevidade do equipamento pois deixa uma parte de seu armazenamento vazia, sem dados, o que pode conter dados remanescentes de um uso anterior do *drive*.

> Os discos de estado sólido (SSDs) são fabricados com uma porção reservada do drive (chamada Super-provisionamento) para substituir células de dados à medida que se desgastam. Com o tempo, mais e mais células são substituídas, e uma quantidade significativa de dados pode ser encontrada na área de Super-provisionamento do drive (Nikkel, 2019).

Já o comando TRIM é utilizado para a manutenção e desempenho dos SSDs. Ele permite que o sistema operacional informe ao SSD quais blocos de dados não estão mais sendo usados e podem ser apagados. Quando arquivos são deletados em um SSD, o TRIM ajuda o *drive* a identificar essas áreas como disponíveis para reescrita, melhorando o desempenho a longo prazo e evitando que o SSD fique com o desempenho baixo com o tempo.

2.4.2.1. ATA Secure Erase

O ATA *Secure Erase* é um comando padrão estabelecido pelo protocolo ATA (*Advanced Technology Attachment*) que possibilita a eliminação segura e total de todos os dados contidos em um SSD. Esse comando é realizado internamente pelo *software* do SSD, assegurando a completa limpeza de todas as células de memória *flash* NAND, incluindo áreas normalmente inacessíveis ao usuário ou ao sistema operacional.

O comando é transmitido ao controlador do SSD, que inicia o processo de apagamento sem a necessidade de intervenção externa. Esse processo é gerenciado pelo *firmware* interno do SSD, garantindo uma deleção total dos dados e instruindo o SSD a restaurar todas as células de memória *flash* ao seu estado original, incluindo a limpeza de áreas escondidas, como setores remapeados, áreas de Super-provisionamento e outros espaços reservados que não podem ser acessados através de métodos convencionais.

O ATA *Secure Erase*, por ser um procedimento interno, costuma ser mais ágil do que os métodos de sobrescrita por *software*, sendo assim, o tempo necessário para concluir o processo é determinado pela capacidade do SSD, mas é otimizado para eficiência (Pavlovic, 2024).

Esse procedimento assegura a eliminação irreversível de todos os dados, protegendo informações pessoais e confidenciais, e é visto como crucial na venda, reciclagem ou eliminação de um SSD para prevenir o acesso indevido aos dados (Pavlovic, 2024). Também cumpre os critérios de segurança de dados definidos por leis como a LGPD, GDPR e HIPAA, além de outras regulamentações que demandam a eliminação segura de informações confidenciais.

Um benefício de realizar esse procedimento quando não se tem a intenção de descartar o SSD é que ele pode contribuir para a recuperação do desempenho original do dispositivo, pois as células de memória são reprogramadas, eliminando possíveis fragmentações ou sobras de dados que prejudicam a velocidade.

Para a execução do processo é necessário entender que algumas fabricantes oferecem ferramentas para facilitar o processo, como por exemplo, a Samsung com a aplicação Samsung *Magician Software*, Intel com Intel *Memory and Storage Tool* e a Kingston com Kingston SSD *Manager*. Se o fabricante não oferece uma ferramenta específica, deve-se usar uma ferramenta de terceiros como o *Parted Magic*.

2.4.2.2. Criptografia e Destruição de Chaves

O método de deleção de dados por criptografia e destruição de chaves pode ser descrito inicialmente de forma simples: inicialmente é feita a criptografia dos dados, e em seguida as chaves que quebram essa criptografia são destruídas tornando o conteúdo criptografado inacessível. Apesar da aparente simplicidade, esse procedimento é especialmente eficiente em SSDs devido à maneira como esses dispositivos administram os dados internamente, e faz com que esse método tenha um nível de confiabilidade maior do que a simples sobrescrita de dados.

Antes do armazenamento dos dados, é necessário que o SSD seja configurado para criptografar todas as informações que serão gravadas utilizando uma chave criptográfica única. Essa criptografia pode ser implementada via software, como o *BitLocker* ou o *VeraCryp*t, ou através de funções de criptografia que fazem parte do hardware do SSD, como nos SEDs (*Self-Encrypting Drives*). A chave de criptografia é mantida em um local seguro do SSD, protegida contra acessos não autorizados. É possível utilizar uma senha ou outro sistema de autenticação para impedir o acesso à chave.

A lógica utilizada nesse processo é sólida, pois, uma vez que os dados são criptografados, as chaves da criptografia são o único caminho para a leitura e compreensão dos dados, que, quando destruídas, tornam o entendimento impossível (Nikkel,2019). E mesmo que os dados ainda existam em forma criptografada, não os deletando de forma literal, o novo "formato" desses dados, com a criptografia, faz com que, mesmo que o indivíduo não autorizado tenha posse desses dados, não consiga utilizá-los.

Alguns SSDs oferecem uma opção de reset que apaga todas as chaves de criptografia internas, destruindo todos os dados criptografados. A eliminação dos dados é quase instantânea, já que apenas a chave precisa ser removida, dispensando a necessidade de apagar cada bit de informação individualmente.

2.4.2.3. Destruição física do SSD

Em contraste com os discos rígidos tradicionais, que guardam dados em discos magnéticos, os SSDs utilizam memória flash, o que diferencia algumas técnicas de remoção. No âmbito dos SSDs, esses são os métodos mais comuns de destruição física, vistos como os que apresentam menor taxa de erros e dados irrecuperáveis:

- Trituramento: reduz os componentes do SSD a pedaços minúsculos, geralmente inferiores a 2 mm, utiliza máquinas específicas que quebram os *chips* de memória em fragmentos irreparáveis

- Pulverização: a pulverização a *laser* é uma técnica avançada, em que *lasers* de alta intensidade desintegram os *chips* de memória, destruindo os circuitos e impossibilitando a recuperação dos dados

- Incineração controlada: o SSD é queimado em temperaturas muito altas, destruindo os componentes eletrônicos.

- Uso de substâncias químicas corrosivas: Os componentes do SSD, em particular os *chips* de memória, são mergulhados em substâncias químicas corrosivas, como o ácido nítrico, dissolvendo os materiais que formam o SSD (Yohannes, 2013).

Muitas das vantagens que existem na destruição física de HDDs também existem para SSDs, os benefícios têm como base a inviabilidade de recuperar os dados e a conformidade com regulamentações de segurança de dados (Knolton,2023), também deve-se ressaltar a velocidade do processo, sendo bem rápido para uma eliminação de uma volumetria grande de dados.

As desvantagens também podem ser muito comparadas com HDDs, em que o desperdício de equipamentos é muito grande, causando muito lixo por conta do processo, também vale dizer que o preço dos equipamentos usados nos processos e a complexidade deles podem ser considerados como desvantagem da destruição física de SSDs, com o uso de ácidos, lasers e máquinas de trituramento (Knolton, 2023).

Métodos manuais e mais baratos não garantem a eliminação completa das informações, deixando espaços para futuras tentativas de recuperação.

3. METODOLOGIA

Foram utilizadas como base para a pesquisa uma série de artigos de autores do meio acadêmico, foi possível o acesso a esses artigos por meio de ferramentas de pesquisa como Google, Google acadêmico, IEEE e blogs especializados sendo possível encontrar autores que ainda trabalham no ramo tanto de pesquisa quanto em campo, e o conteúdo teórico pode ser aplicado na pratica, permitindo uma revisão bibliográfica embasada com a certeza de que a literatura disponível corrobora com os pontos abordados neste trabalho.

Na seleção de artigos utilizados foram aplicados uma serie de filtros de qualidade para garantir a confiabilidade e assertividade da informação, foram selecionados artigos publicados nos últimos 11 anos, com exceção do artigo *Secure deletion of data from magnetic and solid-state memory***,** escrito por Peter Guttman em 1996, em que ele descreve o seu método de apagamento de dados por meio de sobrescrita múltipla.

Foram feitos também dois testes práticos para exemplificar a facilidade dos métodos de sobrescrita:

- No primeiro teste realizado, evidenciado no tópico 4.1, foi escolhido o programa *Eraser* versão 6.2.0.2994 no sistema operacional Windows para sobrescrita segura e exclusão dos arquivos em um servidor que utiliza HDD, visto que é um programa gratuito com vários métodos diferentes de sobrescrita, contando até com uma área de tarefas para limpeza recorrente em horários específicos dos diretórios que selecionar. No teste executado o método escolhido foi o Gutmann desenvolvido por Peter Gutmann, especialista em tecnologia de segurança, o método mais seguro para estar utilizando, visto que é realizado o processo de sobrescrita do diretório ou arquivo selecionado trinta e cinco vezes, fazendo com que a possibilidade de recuperação de dados seja quase zero.

- O segundo teste realizado, evidenciado no tópico 4.2, foi o Comando *Shred* no Linux, O comando *shred* é muito interessante para sobrescrita de arquivos e diretórios específicos, como também pode ser utilizado em partições inteiras ou dispositivos externos, como *pendrives* ou um disco rígido externo, sendo necessário a permissão sudo. O *shred* é uma ótima ferramenta para sobrescrita de arquivos no sistema Linux, gratuita sendo acessível a todos administradores de rede e com fácil aprendizado.

Vale ser lembrado que o escopo dos testes realizados está alinhado de acordo com o que é possível na realidade dos autores

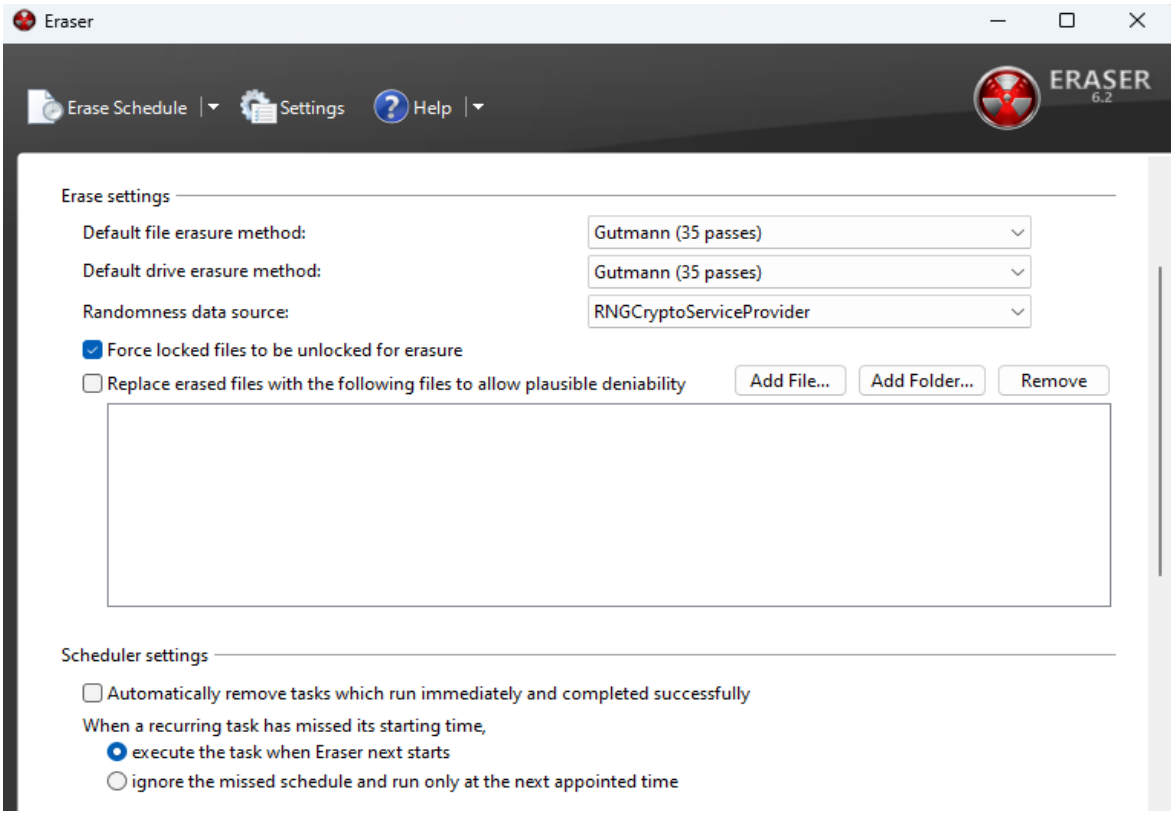
4. DISCUSSÕES, TESTES E RESULTADOS

Essa seção utilizara os métodos acima para compará-los através de um quadro, para avaliar quais são os métodos de descarte, deleção e apagamento de dados mais recomendados quando o intuito é a não recuperação dos dados, também serão demonstrados os resultados dos testes feitos com o objetivo de exemplificar a simplicidade do processo de sobrescrita utilizando métodos no Linux e Windows.

4.1. Sobrescrita pelo Eraser (Windows)

É preciso selecionar o método desejado tanto para arquivos quanto para Unidades, no caso será o método Guttman conforme mostra a **Figura 4**.

Figura 4 - Apresenta as configurações utilizados no programa *Eraser* nos testes realizados no servidor Windows.

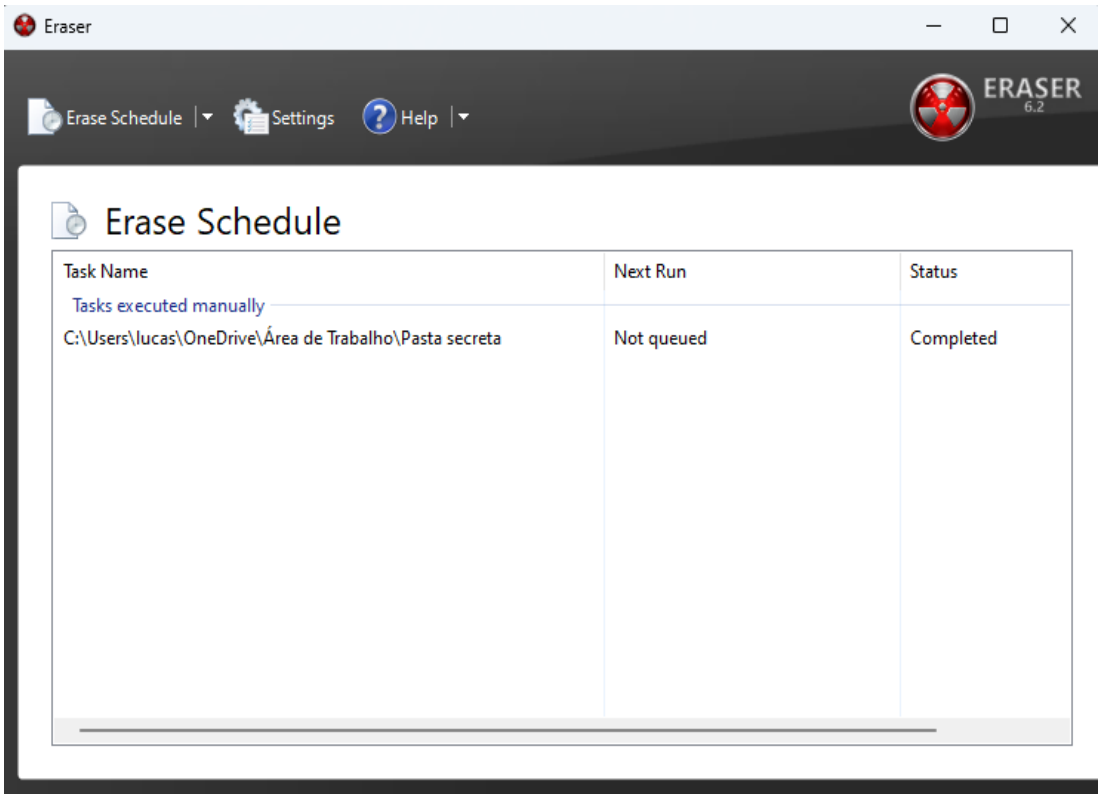


Fonte: Próprio autor usando o *Eraser*

Com as configurações realizadas, é preciso ir ao local da pasta e clicar sobre a pasta com o botão direito, em seguida clique em "Mostrar mais opções", depois em "*Eraser*" e novamente clique em "*Eraser*". Será aberto uma caixa de mensagem perguntando se temos certeza quanto a apagar os arquivos selecionados. Clicando em "*Yes*" ele dará início a sobrescrita e exclusão dos arquivos.

Será apresentada na tela "*Erase Schedule*", em que após ser concluída apresentará uma tela semelhante à figura abaixo, em que é possível visualizar a tela de "*Erase Schedule*" com a tarefa concluída após sobrescrita e exclusão.

Figura 5 - Apresenta a tela "*Erase Schedule*" no programa *Eraser*.



Fonte: Próprio autor usando o *Eraser*

Vale pontuar que devido à quantidade vezes de sobrescrita do arquivo ou unidade, pode demorar um pouco mais para o processo ser concluído, porém, tem-se a garantia de que quantas mais vezes for realizado a sobrescrita, menor são as chances de recuperação dos dados por terceiros.

4.2. Comando *Shred* (Linux)

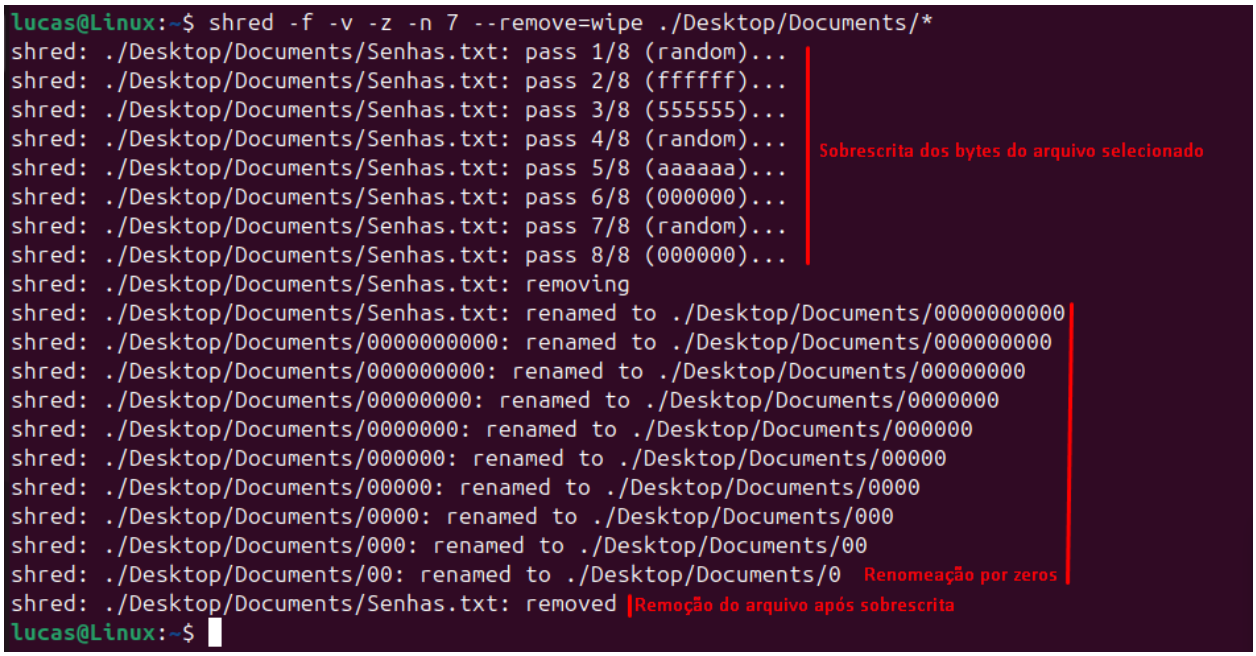
No sistema Linux Ubuntu 24.04.1 LTS, foi utilizado o *Shred* para sobrescrita e exclusão dos arquivos, utiliza-se o seguinte comando:

- "shred -f -v -z -n 7 --remove=wipe ./Desktop/Docs/*"

Sendo "-f" para forçar a permissão de sobrescrita o arquivo, "-v" sendo para mostrar o progresso da ação, "-z" para adicionar uma última sobrescrita com zeros, "-n 7" para realizar a ação de sobrescrita 7 vezes, "--remove=wipe" para iniciar a sobrescrita e remoção pelos bytes nos nomes

dos arquivos, e por fim “./Desktop/Docs/*” que é o caminho dos diretórios, no qual todos os arquivos serão excluídos

Figura 6 – Demonstra a linha de comando com o comando *Shred*



Fonte: Próprio autor utilizando sistema Linux Ubuntu.

4.3. Resultados

A imagem abaixo apresenta um quadro que com base nos dados apresentados no estudo acima, que classifica de forma qualitativa através das variáveis “eficácia”, “custo” e “tempo estimado” o método de apagamento de dados mais recomendado entre os dois equipamentos HDD e SSD.

Segue o quadro classificatório dos métodos de apagamento de dados em HDDs e SSDs**:**

Método	Aplicabilidade (HDDS, SSDS)	Eficácia	Custo	Tempo estimado
Sobrescrita simples	HDD	Moderada	Baixo	Médio
Sobrescrita com padrões múltiplos	HDD	Alta	Médio	Alto
Método de sobrescrita Guttman	HDD	Muito alta	Médio	Muito alto
Método DoD 5220.22-M	HDD	Alta	Médio	Alto
Desmagnetização	HDD	Muito alta	Alto	Baixo
Destruição física	HDD	Muito alta	Variável (médio a alto)	Baixo
ATA *Secure erase*	SSD	Muito alta	Baixo	Baixo
Criptografia e destruição de chaves	SSD	Muito alta	Baixo	Médio
Destruição física	SSD	Muito alta	Variável (médio a alto)	Baixo

Fonte: feito pelo autor usando o Excel

Legenda:

- HDDs
- SSDs
- Muito alto (a)
- Alto (a)
- Variável (médio a alto)
- Médio
- Baixo

Como pode ser visto, apesar de existirem diversos métodos de deleção de dados em HDDs, por conta do tempo que se encontra no mercado e a diminuição do custo de sua tecnologia, muitos desses métodos possuem algum tipo de desvantagem no procedimento, como um alto custo, alto tempo estimado ou baixa eficácia, como o método de sobrescrita Guttman que tem uma alta eficácia mas com tempo estimado muito alto devido as 35 camadas de sobrescrita que são aplicadas no disco, sendo assim, com base nos dados fornecidos pelo quadro, o método mais recomendado para HDDs é a desmagnetização, por conta de sua alta eficácia na deleção de dados e baixo tempo estimado na execução.

Quando olhamos para os métodos designados para SSDs, através de uma breve análise podemos ver que todos os processos citados têm uma alta eficácia, as variáveis que mudam são o preço e o tempo estimado do processo, sendo assim pode-se concluir que o comando ATA *Secure Erase* se destaca dos outros métodos por sua praticidade, baixo custo e tempo empregado no processos, sendo seguido de perto pelo processo de Criptografia e destruição de chaves, que por sua vez possui um tempo estimado médio para a aplicação do processo.

5. CONSIDERAÇÕES FINAIS

Esse trabalho evidenciou a importância das boas práticas no descarte seguro de unidades de armazenamento, destacando os riscos associados ao manejo inadequado desses dispositivos, tanto em termos de segurança da informação quanto a proteção da privacidade e confidencialidade dos dados. A adoção de métodos específicos, como a desmagnetização e a destruição física para HDDs, e o uso do ATA *Secure Erase* e a destruição de chaves de criptografia para SSDs, mostrou-se fundamental para assegurar a proteção contra a recuperação indesejada de dados. Sempre reforçando que a conformidade com regulamentações como a LGPD enfatiza a necessidade de protocolos rigorosos e eficientes para eliminar dados de maneira segura.

Também vale ressaltar os testes práticos presentes nas seções “4.1” e “4.2”, que mostram com objetividade a praticidade de dois métodos citados na seção de métodos de descarte e deleção de dados em HDDs. Pode-se concluir que ambos os processos podem ser concluídos com relativa facilidade, o que corrobora o argumento de que métodos de exclusão de dados não são todos de alto custo e com alto investimento de tempo por parte do executor. Boas práticas e comprometimento com a segurança podem ser alcançados se tanto o usuário comum quanto as instituições tiverem como objetivo principal a preservação da confidencialidade e da integridade das informações. Então, a adoção de procedimentos de descarte seguro pode se tornar uma prática comum e acessível, garantindo que dados sensíveis não sejam indevidamente expostos, ao mesmo tempo em que se contribui para um ambiente digital mais seguro e sustentável. Em um cenário de crescente volume de dados e dispositivos, essas ações se tornam indispensáveis para mitigar riscos e garantir a segurança e a privacidade em ambientes corporativos e institucionais.

Referências

ALECRIM, E. **Como funciona um HD (Hard Disk). InfoWester**, 2008. Disponível em: https://www.infowester.com/hd.php. Acesso em: 10 ago. 2024.

ARAÚJO, Marcelo. **Como funciona a listagem de eliminação de documentos: desmagnetização ou reformatação**. **Ebox Digital**, 2024. Disponível em: https://www.eboxdigital.com.br/blog/como-funciona-a-listagem-de-eliminacao-de-documentos#:~:text=Desmagnetiza%C3%A7%C3%A3o%20ou%20reformata%C3%A7%C3%A3o&text=Esse%20processo%20pode%20ser%20realizado,a%20sua%20substitui%C3%A7%C3%A3o%20por%20outro. Acesso em: 8 out. 2024.

BACHCHAS, K. **Securely disposing of old electronics and data: a forensic guide to protecting your information. AT&T Cybersecurity**, 2023. Disponível em: https://cybersecurity.att.com/blogs/security-essentials/securely-disposing-of-old-electronics-and-data-a-forensic-guide-to-protecting-your-information. Acesso em: 8 ago. 2024.

BRADSHAW, E. **Secure data disposal: methods, considerations, and best practices**. **Data Watchtower**, 2023. Disponível em: https://www.datawatchtower.com/secure-data-disposal-methods-considerations/. Acesso em: 8 ago. 2024.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei geral de proteção de dados Pessoais (LGPD)**. Brasilia, DF: Planalto, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 29 ago. 2024.

CARVALHO, A. V. F. **Viabilidade e impactos do uso de SSDs como dispositivo de armazenamento secundário em detrimento dos HDDs**. Universidade Federal do Piauí, Teresina, 2014 Acesso em: 18 ago. 2024.

DATABREACHTODAY. **$1.2 Million penalty in copier breach**. 2013. Disponível em: <https://www.databreachtoday.com/12-million-penalty-in-copier-breach-a-5991>. Acesso em: 8 ago. 2024.

GDPR REGISTER. **Morgan Stanley fined for failing to secure customer data**.2020. Disponível em: https://www.gdprregister.eu/news/morgan-sanley-fined/. Acesso em: 8 ago. 2024.

GUTMANN, P. **Secure deletion of data from magnetic and solid-state memory**. **USENIX Security Symposium**, 1996. Disponível em: https://www.usenix.org/legacy/publications/library/proceedings/sec96/full_papers/gutmann/index.html. Acesso em: 23 set. 2024.

HEPISUTHAR, Ms.; SHARMA, Dr. Priyanka. **Comparative analysis study on SSD and HDD. Turkish Journal of Computer and Mathematics Education**, p. 3, 2021. Acesso em: 16 ago. 2024

JACINTA. **Como destruir um HD e deixar o HD irrecuperável.** EaseUS, 2024. Disponível em: https://br.easeus.com/hdd-wipe/como-destruir-um-hd.html. Acesso em: 12 set. 2024.

KNOLTON, F. **Why physical data destruction is so important. Infosecurity Magazine**, 2023. Disponível em: https://www.infosecurity-magazine.com/blogs/why-physical-data-destruction-is/. Acesso em: 8 out. 2024.

MATEUS, D. **A importância do correto descarte de mídias CD/DVD, HD´s e documentos físicos que contenham dados pessoais a luz da LGPD**. LinkedIn,2023 [s.d.]. Disponível em: https://www.linkedin.com/pulse/import%C3%A2ncia-correto-descarte-de-m%C3%ADdias-cddvd-hds-e-da-mateus/._Acesso em: 29 ago. 2024.

NIKKEL, Bruce. **Forensic analysis of solid-state drives: the TRIM command. Digital Forensics**, 2019. Disponível em: https://digitalforensics.ch/nikkel19.pdf. Acesso em: 25 out. 2024.

O'BRIEN, K.; SALYERS, D. C.; STRIEGEL, A. D.; POELLABAUER, C. **Power and Performance Characteristics of USB Flash Drives. Research Gate**, [s.d.]. Disponível em: https://www.researchgate.net/publication/4361182_Power_and_performance_characteristics_of_USB_flash_drives. Acesso em: 29 ago. 2024.

OLIVEIRA, V. M. de. **Sanitização de mídias de armazenamento de dados**. **Academia de Forense Digital**, 2023. Disponível em: https://academiadeforensedigital.com.br/sanitizacao-de-midias-de-armazenamento-de-dados/. Acesso em: 24 set. 2024.

PAVLOVIC, Dwight. **How to securely erase an SSD drive: Step-by-Step Guide**. **HP® Tech Takes**, 2024. Disponível em: https://www.hp.com/us-en/shop/tech-takes/how-to-secure-erase-ssd. Acesso em: 13 out. 2024

YOHANNES, Fkrezgy. **SSD Digital Forensics Construction.** Politecnico di Milano, 2013. Acesso em: 5 set. 2024.

ZHURAVEL, Arina. **Data deletion and data erasure: what's the differences?**. **NSYS Group**, 2023. Disponível em: https://nsysgroup.com/pt/blog/data-deletion-and-data-erasure-whats-the-differences/. Acesso em: 16 set. 2024.

Lucas Gabriel Gama D'Angelo
Matheus Pancoti Mota

BOAS PRÁTICAS NO DESCARTE DE UNIDADES HDDS E SSDS

Trabalho de graduação apresentado como exigência parcial para obtenção do título de Tecnólogo em segurança da informação pelo Centro Paula Souza – Faculdade de Tecnologia de Americana – Ministro Ralph Biasi.
Área de concentração: Segurança da Informação.

Americana, 03 de dezembro de 2024

Banca Examinadora:

Henri Alves de Goddy
Doutor
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Ana Lúcia Spigolon
Especialista
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi

Rafael Rodrigo Martinati
Mestre
Faculdade de Tecnologia de Americana – Ministro Ralph Biasi