# DESCARTE SEGURO DE MÍDIAS DE ARMAZENAMENTO: COMO PRESERVAR SUA PRIVACIDADE E ECONOMIZAR RECURSOS

**Raphael Leonardo Bernardo de Souza**
*Pós-graduado, Lato Sensu, de Especialização em Comunicações*

**RESUMO:** Este trabalho está inserido na área de estudo da gestão, na linha de pesquisa da manutenção dos materiais de comunicações e eletrônica. Tem por principal objetivo analisar os procedimentos utilizados no 4° Batalhão de Comunicações (4°BCom), bem como propor melhorias no processo do descarte seguro das mídias informáticas que armazenam informações corporativas. Embora haja orientação para utilização de software que elimine os dados definitivamente, falta indicação de aplicativo padrão para esta finalidade. Assim, este estudo analisa as opções, na busca por um programa confiável para sanitização dessas mídias, considerada a possibilidade de reutilização das mesmas. Para isso, realiza uma pesquisa exploratória, que aborda os tipos de dispositivos de armazenamento, o funcionamento do sistema de arquivos e a sanitização das mídias informáticas. Em seguida, por meio de um questionário, coleta informações sobre os processos executados no 4°BCom. Por fim, realiza experimentos no sistema operacional Linux para exclusão de arquivos de texto em dispositivos magnéticos e eletrônicos. Então, aponta a ferramenta Shred como a mais adequada em comparação a BleachBit e Wipe. Além disso, verifica que os procedimentos executados no 4°BCom garantem o descarte seguro dos materiais que armazenam informações corporativas. Conclui-se que este trabalho contribui para a gestão da informação, ao disponibilizar um método para a efetiva eliminação de documentos, e para a gestão do material, ao possibilitar a reutilização dos dispositivos de armazenamento.

Palavra-Chave: Gestão da informação. Gestão do material. Informações corporativas. Descarte de mídias informáticas. Sobrescrita de dados.

## 1 INTRODUÇÃO

A gestão está no centro do funcionamento das instituições, pois atua em áreas fundamentais para o alcance dos objetivos organizacionais, como a gestão do material e da informação, que influenciam diretamente na disponibilidade e na racionalização de recursos.

Essas áreas estão intrinsecamente associadas ao tratar-se dos materiais de informática, cuja utilização aumentou a partir da década de 1980, o que ocasionou a gradativa migração dos documentos para o formato digital.

Nesse panorama, os meios tecnológicos destacaram-se ao possibilitarem o armazenamento de grandes volumes de informações em suporte digital e a recuperação ágil de conteúdos. (SILVA, 2015).

Contudo, o uso crescente de documentos digitais requer uma atenção especial ao descarte das mídias de armazenamento, para não comprometer a confidencialidade das informações sigilosas.

A cartilha emergencial de segurança de tecnologia da informação e comunicações do Exército Brasileiro instrui que os discos rígidos sejam formatados com software que elimine os dados definitivamente, mas não indica um aplicativo padrão para essa finalidade. Dessa lacuna na padronização dos procedimentos, surge a necessidade de apontar um utilitário confiável, razão que justifica este estudo.

Este trabalho trata sobre o descarte seguro dos materiais que armazenam informações corporativas, com foco nas ferramentas de limpeza definitiva de seus conteúdos.

O ambiente de referência para este trabalho foi o 4° Batalhão de Comunicações (4°BCom) e o estudo limita-se ao sistema

operacional Linux Ubuntu, homologado para uso nas estações de trabalho do Exército Brasileiro. Limita-se ainda à sanitização de mídias magnéticas e eletrônicas, por meio dos aplicativos BleachBit, Shred e Wipe para excluir arquivos de texto .odt.

Assim, formulou-se o problema: as ferramentas de limpeza de conteúdo utilizadas no 4°BCom garantem o descarte seguro dos materiais que armazenam informações corporativas?

Com suas análises, este trabalho contribui para o aprimoramento dos procedimentos empregados pelo 4°BCom no descarte seguro das mídias de armazenamento. Pode servir de estudo para a elaboração de normas de ação para eliminação de dados armazenados em mídias informáticas, no Exército Brasileiro. Pode ainda conscientizar os usuários quanto à segurança das informações particulares.

Este trabalho tem como objetivo geral analisar os procedimentos utilizados no 4°BCom e propor melhorias no descarte seguro das mídias que armazenam informações.

Os objetivos específicos são:

Identificar os tipos de mídias que armazenam informações.

Descrever três ferramentas gratuitas e seus métodos de limpeza de conteúdo de mídias informáticas.

Apontar as vantagens e desvantagens metodológicas dos aplicativos avaliados, demonstrar sua confiabilidade e indicar o mais seguro.

### 1.1 PROCEDIMENTOS METODOLÓGICOS

Trata-se de pesquisa exploratória, com objetivo de descrever os tipos de mídias de armazenamento de informação e as ferramentas apropriadas para a limpeza de seu conteúdo, indicando o procedimento mais seguro, considerando a possibilidade de reutilização do equipamento.

A revisão da literatura possibilitou o embasamento teórico necessário para responder as questões de estudo, abordando os tipos de dispositivos de armazenamento, o funcionamento do sistema de arquivos e a sanitização das mídias informáticas.

Em seguida, foi elaborado um questionário, que foi aplicado à Seção de Informática do 4°BCom, a fim de colher informações concretas a respeito dos processos executados naquela Organização Militar (OM).

A partir dessa base, seguiram-se os experimentos de laboratório, nos quais utilizou-se uma máquina virtual Linux Ubuntu 16.04 LTS, com 10 *Gigabytes* de disco rígido, 1 *Gigabyte* de memória RAM e processador Intel Core i3 64 bits. Os dispositivos de armazenamento utilizados foram um HD externo de 500GB e um pendrive de 4GB de capacidade, ambos com o sistema de arquivos Ext4. O tipo de arquivo utilizado nos testes foi o .odt, por ser o formato padrão para documentos criados no LibreOffice Writer, ferramenta de processamento de texto do Linux.

A pesquisa foi realizada entre os meses de fevereiro e junho de 2017, possibilitando a comparação de diferentes ferramentas de limpeza de conteúdo e a verificação de sua confiabilidade, na busca por resultados práticos para o descarte seguro de mídias informáticas no 4°BCom.

## 2 DESENVOLVIMENTO

### 2.1 DISPOSITIVOS DE ARMAZENAMENTO

A utilização dos materiais informáticos no armazenamento da informação, em substituição ao papel, trouxe vantagens como diminuição do espaço físico e agilidade na recuperação da informação.

Silva (2015) comunica que o registro da informação em suporte digital é realizado em diversos tipos de dispositivos, que são classificados em magnéticos, ópticos e eletrônicos.

### 2.1.1 Armazenamento magnético

Sobre os meios magnéticos, representados pelas fitas magnéticas, disquetes e discos rígidos, Marçula e Benini Filho explicam que:

> Os dados são armazenados magnetizando-se determinados pontos do material magnético, permitindo que os dados sejam mantidos mesmo quando o campo magnético de gravação for retirado. Com isso, a leitura posterior dos dados pode ser realizada detectando-se as correntes induzidas pelos campos magnéticos armazenados. (2008, p. 123).

### 2.1.2 Armazenamento óptico

Quanto ao armazenamento óptico, onde estão incluídos os CDs, DVDs e discos Blu-ray, para a gravação e leitura dos dados, são necessários drives que utilizam o raio laser, conforme destaca Englander:

> Os dados são armazenados no disco na forma de reentrâncias (lands) e saliências (pits) em sequência. Essas são gravadas na superfície do disco máster (mestre) com um laser de alta potência. [...] Um feixe laser é refletido para fora da superfície em relevo do disco à medida que este é girado por um motor. O reflexo é utilizado para diferenciar reentrâncias e saliências, e estas são convertidas em bits. (2011, p. 257 e 258).

### 2.1.3 Armazenamento eletrônico

Acerca dessa tecnologia, que inclui os cartões de memória, *pendrives* e SSDs, Marçula e Benini Filho (2008) destacam suas características de não volatilidade, possibilidade de gravar ou apagar dados por meio de sinais elétricos, baixo consumo de energia e pouco espaço físico ocupado.

## 2.2 SISTEMAS DE ARQUIVOS OU FILESYSTEMS

De acordo com Englander (2011), um arquivo constitui uma unidade lógica de armazenamento e pode ser definido como uma coleção organizada de informações.

Ainda segundo Englander (2011), o gerenciamento de arquivos é realizado pelo sistema de arquivos, que os identifica e manipula pelos nomes, determina seus requisitos físicos, aloca espaço para armazená-los e mantém informações sobre eles, possibilitando sua recuperação.

Para complementar o entendimento, Mota Filho explica:

> Os *filesystems* possuem duas porções básicas: a área de controle e a área de dados. É na área de controle que encontraremos as informações sobre os diversos arquivos espalhados pela partição de disco que contém o *filesystem*. Na área de dados encontraremos o conteúdo dos arquivos. (MOTA FILHO, 2012, p. 153)

É importante destacar que, embora os arquivos sejam armazenados fisicamente nos dispositivos, sua visualização pelo usuário ocorre de forma lógica, conforme o sistema de arquivos, que cria uma estrutura semelhante a uma tabela de conteúdos, localizando os arquivos com facilidade.

Além disso, o *filesystem* mantém uma lista de espaço livre, indicando a disponibilidade para alocação de novos itens, e remaneja o espaço de um arquivo excluído, devolvendo-o à lista de espaço livre.

Mota Filho (2012) informa que os sistemas de arquivos mais conhecidos são FAT16, FAT32 e NTFS para o sistema operacional Windows e Ext2, Ext3, Ext4, ReiserFS, JFS e XFS para o Linux.

## 2.3 SANITIZAÇÃO DE MÍDIAS DE ARMAZENAMENTO

Ao tratar sobre mídias de armazenamento de informações, é importante abordar a correta eliminação dos documentos digitais, para impossibilitar a recuperação dos dados.

A simples exclusão de um arquivo não

atende aos requisitos de segurança, pois segundo Englander (2011, p. 458):

> "[...] os dados em arquivos excluídos não são de fato apagados do disco, a menos que se faça um esforço especial para limpar ou misturar todos os bits nos blocos utilizados pelo arquivo. Trata-se de um risco potencial à segurança".

Na verdade, a deleção tradicional e a formatação simples alteram apenas a área de controle do sistema de arquivos, devolvendo o espaço liberado para a lista de espaço livre, mas mantendo a área de dados inalterada.

Portanto, devem ser consideradas as possibilidades de recuperação de dados, conforme afirmam Farmer e Venema (2007, p. 131): "uma grande quantidade de informações excluídas podem ser recuperadas [...], mesmo quando essas informações foram excluídas há muito tempo".

Isso constitui ameaça à confidencialidade das informações corporativas, o que remete à busca por formas adequadas de eliminação definitiva dos documentos sigilosos, conforme destaca Beal (2008, p. 7):

> No que tange à confidencialidade, o descarte de documentos e mídias que contenham dados de caráter sigiloso precisa ser realizado com observância de critérios rígidos de destruição segura (por exemplo, [...] softwares destinados a apagar com segurança arquivos de um microcomputador que, se simplesmente excluídos do sistema, poderiam ser facilmente recuperados com o uso de ferramentas de restauração de dados).

Entre as ferramentas que se propõem a recuperar arquivos deletados, Mota Filho (2012) indica Foremost, programa que lê a superfície do disco, independentemente de *filesystem*, para regenerar arquivos através de suas propriedades.

A fim de garantir a eliminação segura de documentos digitais, a National Security Agency (NSA) aprova as seguintes técnicas de sanitização: desmagnetização, desintegração, incineração, fragmentação etc, que resultam na destruição total ou inutilização do próprio dispositivo. De acordo com a NSA (2014, p. 10, tradução nossa), sanitização é definida como "a remoção de informação do dispositivo de armazenamento de tal modo a evitar a recuperação de dados usando qualquer técnica conhecida".

Como o final do ciclo de vida de um documento digital não implica na inoperabilidade da mídia que o contém, é necessário estudar ferramentas que eliminem o conteúdo, sem danificar o dispositivo de armazenamento. Isso possibilita o reaproveitamento dos meios informáticos, como ocorre no Exército Brasileiro, para redistribuição interna ou transferência para outros órgãos governamentais, contribuindo para a racionalização dos recursos públicos e o aparelhamento computacional de outras instituições.

Para remover os dados sem comprometer o dispositivo, pode-se utilizar a técnica de wipe, que consiste na sobrescrita das informações. Segundo Diesburg e Wang (2010, tradução nossa), uma forma de remover os dados confidenciais é sobrescrevê-los.

Os métodos mais famosos utilizados pelos programas de sobrescrita de dados são DoD 5220.22 e Gutmann.

O manual DoD 5220.22-M, publicado em 1995 pelo Departamento de Defesa dos Estados Unidos, indica que, para realizar o descarte seguro, é necessário sobrescrever a informação três vezes. Já o método Gutmann, criado em 1996, consiste em sobrescrever a informação 35 vezes com dados aleatórios, objetivando eliminá-la.

Embora esses métodos sejam bastante referenciados, não existe consenso acerca da quantidade de sobrescritas necessárias para garantir a exclusão segura.

Confirmando essa controvérsia, Diesburg e Wang (2010, tradução nossa) afirmam que quanto mais vezes o dado é sobrescrito, mais segura é sua exclusão. Já Ivascu (2011, tradução nossa) declara que, nos dispositivos

atuais, múltiplas sobrescritas não são mais efetivas que uma única, alertando que a execução de três sobrescritas pode demorar mais de um dia para apagar um disco rígido de grande capacidade.

O Exército Brasileiro, por meio da Portaria n° 011-DCT, de 29 de março de 2010, aprovou o Plano de Migração para Software Livre, estabelecendo a migração de 100% dos sistemas operacionais das estações de trabalho para Linux até 2011.

Para o Linux, Silva (2015) indica o aplicativo gráfico BleachBit, que se propõe a eliminar definitivamente documentos e pastas, além de sobrescrever o espaço livre do disco, utilizando o método de sobrescrita única com zeros.

Outro aplicativo apontado por Silva (2015) é o Shred, utilitário de linha de comando nativo do Linux, que, por padrão, realiza três sobrescritas dos dados, mas permite ao usuário escolher quantas sobrescritas deseja executar.

Outra opção é a ferramenta Wipe, aplicativo de linha de comando, que apaga arquivos, diretórios ou o conteúdo dos dispositivos, sobrescrevendo a área de dados, com dados aleatórios. Por padrão, Wipe realiza 34 sobrescritas, entretanto, opcionalmente executa apenas quatro passagens. (MOTA FILHO, 2012).

## 2.4 PROCEDIMENTOS REALIZADOS NO 4° B COM

Após aplicação do questionário, respondido pela Seção de Informática do 4°BCom, foram coletadas as seguintes informações sobre as práticas daquela OM:

a) os tipos de mídias utilizadas são HD externo, DVD e pendrive;

b) antes da doação de dispositivos de armazenamento, realiza-se a limpeza dos conteúdos, por meio da ferramenta Shred com cinco sobrescritas;

c) a ausência de dados é verificada através do aplicativo Foremost;

d) no descarte final, além dos procedimentos anteriores, é feita a desmontagem das peças do HD;

e) na redistribuição interna de computadores, é executada a formatação simples do HD;

f) não há divulgação dos procedimentos ao público geral.

## 2.5 TESTES REALIZADOS

As ferramentas empregadas para a eliminação dos documentos foram BleachBit, Shred e Wipe, que se diferenciam pelos métodos de sobrescrita (única e múltiplas) e formas de funcionamento (gráfico e linha de comando).

Para finalizar os testes e verificar a confiabilidade das técnicas de sanitização executadas, foi utilizado o aplicativo de recuperação de dados Foremost, citado por Mota Filho (2012).

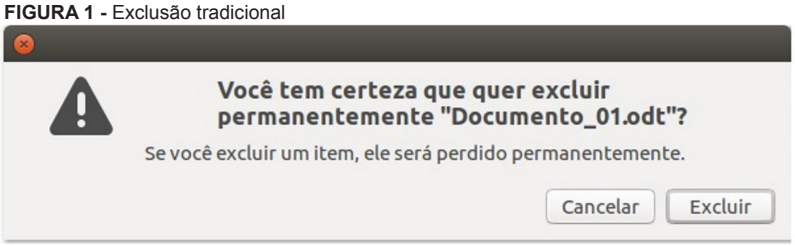
### 2.5.1 Exclusão de dados em meio magnético

Nos testes em meio magnético foi utilizado um HD externo de 500GB, denominado HD_teste.

Inicialmente foram criados os seguintes arquivos e salvos no HD_teste: Documento_01.odt, Documento_02.odt, Documento_03.odt, Documento_04.odt e Documento_05.odt.

O primeiro teste consistiu na exclusão tradicional do Documento_01.odt, por meio das teclas SHIFT + DELETE, que indica a “exclusão permanente” do item.1.1

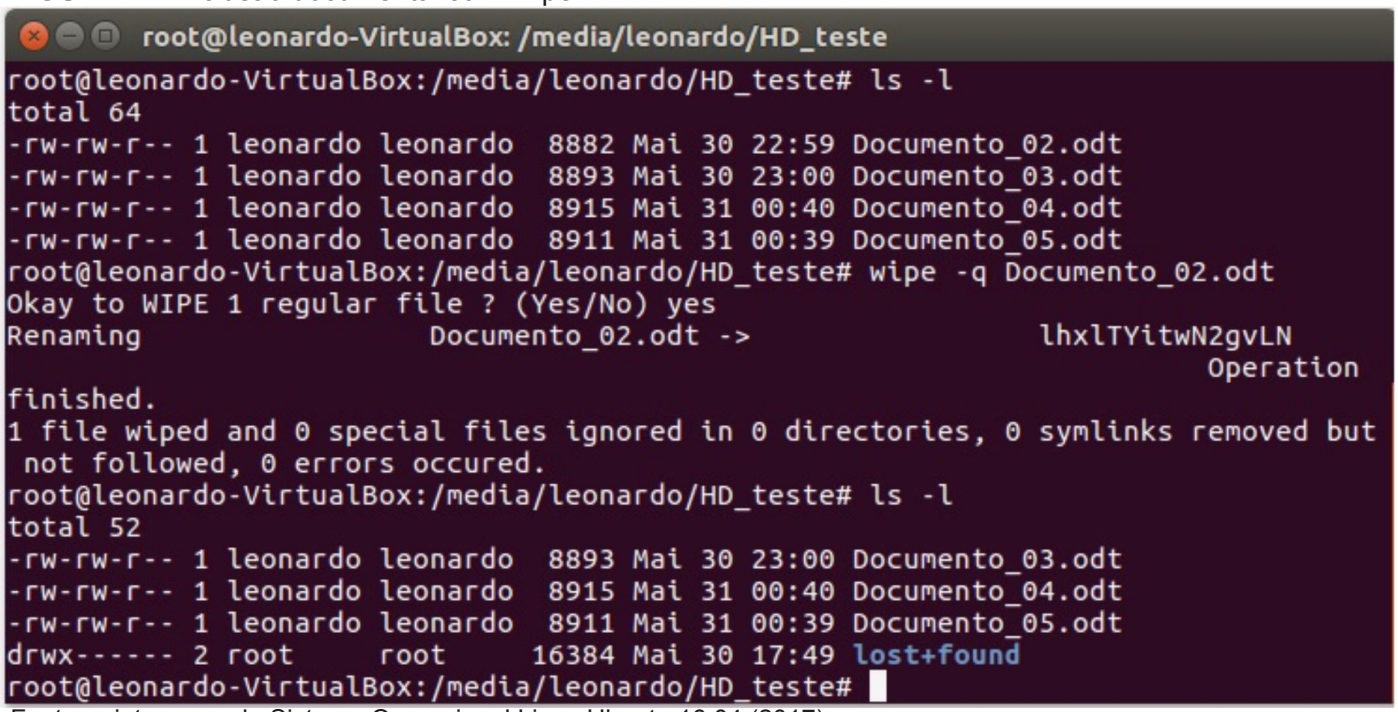
**FIGURA 1 -** Exclusão tradicional




Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Em seguida, procedeu-se a aplicação da ferramenta Wipe, através do comando wipe -q Documento_02.odt, realizando quatro passagens de sobrescrita do arquivo.

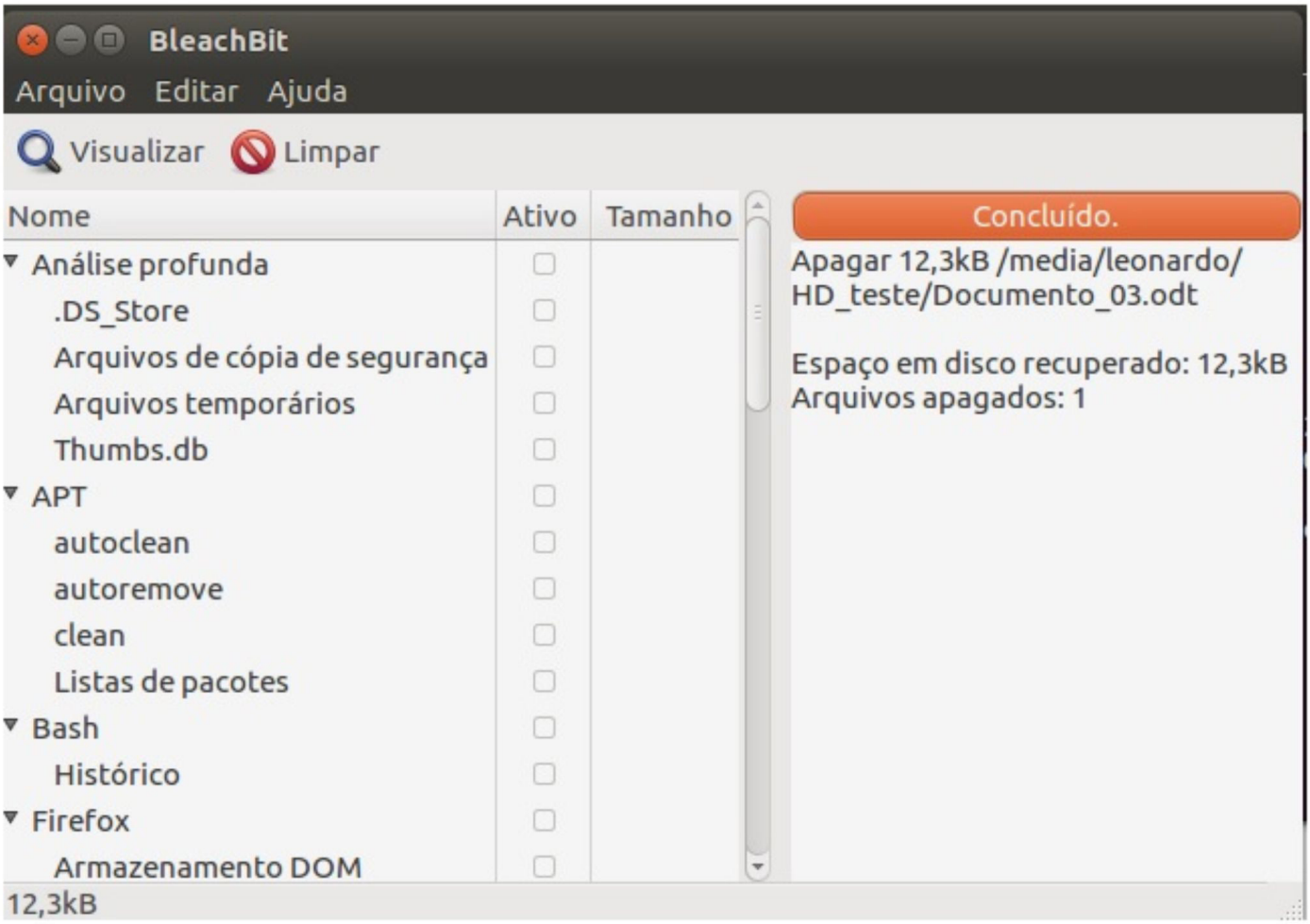
**FIGURA 2 -** Exclusão documental com Wipe.




Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Logo após, foi utilizado o aplicativo BleachBit para realizar a sobrescrita do Documento_03.odt.

**FIGURA 3 -** Exclusão documental com BleachBit




Fonte: print screen do aplicativo BleachBit (2017).

No teste seguinte, foi empregado o utilitário Shred, por meio do comando shred -un 1 Documento_04.odt, realizando uma sobrescrita do arquivo.

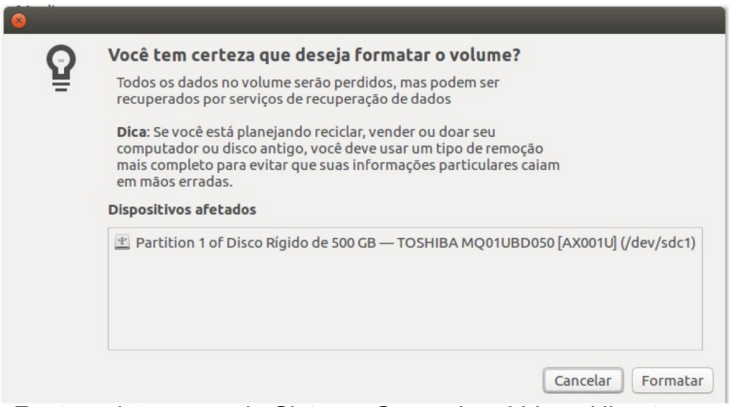
**FIGURA 4 -** Exclusão documental com Shred

```
root@leonardo-VirtualBox:/media/leonardo/HD_teste# ls -l
total 40
-rw-rw-r-- 1 leonardo leonardo  8915 Mai 31 00:40 Documento_04.odt
-rw-rw-r-- 1 leonardo leonardo  8911 Mai 31 00:39 Documento_05.odt
drwx------ 2 root     root     16384 Mai 31 19:14 lost+found
root@leonardo-VirtualBox:/media/leonardo/HD_teste# shred -un 1 Documento_04.odt
root@leonardo-VirtualBox:/media/leonardo/HD_teste# ls -l
total 28
-rw-rw-r-- 1 leonardo leonardo  8911 Mai 31 00:39 Documento_05.odt
drwx------ 2 root     root     16384 Mai 31 19:14 lost+found
root@leonardo-VirtualBox:/media/leonardo/HD_teste#
```

Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Para a eliminação do Documento_05.odt, foi realizada a formatação simples do HD_teste, opção que adverte o usuário para a possibilidade de recuperação dos dados.

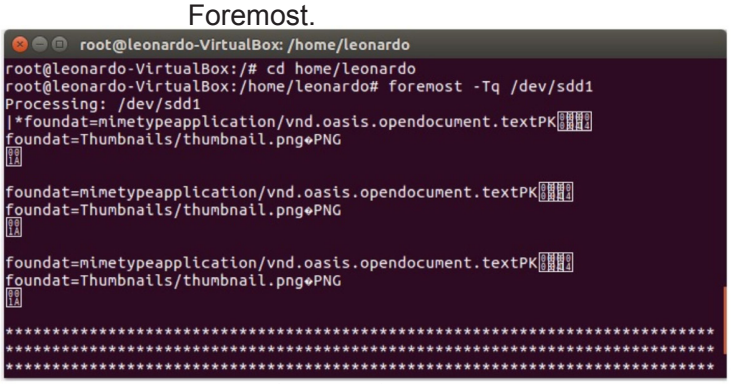
**FIGURA 5 -** Formatação simples




Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Então, foi executado o aplicativo Foremost, na tentativa de recuperar os arquivos supracitados, sendo verificada a existência dos Documento_01.odt, Documento_03.odt e Documento_05.odt.

**FIGURA 06** - Recuperação de arquivos excluídos com Foremost.

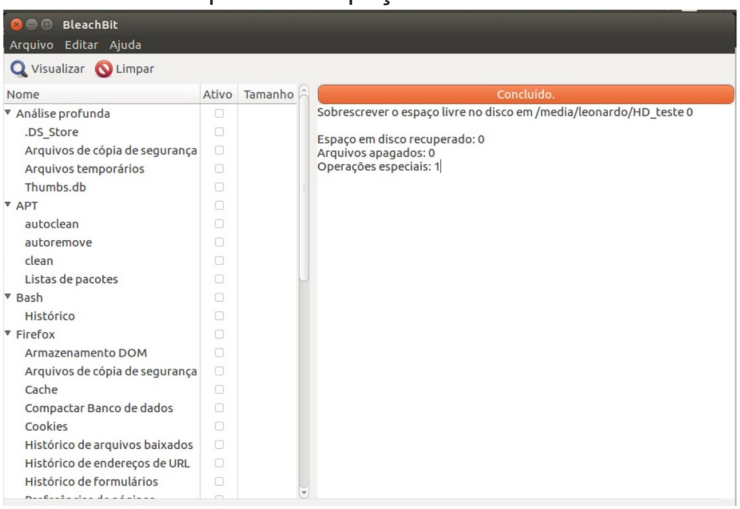



Fonte: print screen do Sistema Operacional Linux Ubuntu 16.04 (2017).

Como foi constatada a permanência de arquivos no dispositivo, procedeu-se a sobrescrita do espaço livre, realizando-se três experimentos isolados e nas mesmas condições de execução.

No primeiro teste, foi empregado o BleachBit, que demorou seis horas para concluir o procedimento. Então, utilizou-se o Foremost e verificou-se a possibilidade de regeneração dos Documento_03.odt e Documento_05.odt.

**FIGURA 7**- Limpeza de espaço livre com BleachBit




Fonte: print screen do aplicativo BleachBit (2017).

Em seguida, realizou-se a sobrescrita do HD_teste, por meio do Wipe, com quatro passagens, o que levou mais de 62 horas para ser concluído, seguido de uma busca com Foremost, que não encontrou nenhum dado.

Finalizando, executou-se o aplicativo Shred para sobrescrever uma única vez o HD_teste, levando cerca de 14 horas para conclusão. Enfim, com o Foremost, verificou-se a inexistência de dados.

### 2.5.2 Exclusão de dados em meio eletrônico

Nos testes em meio eletrônico utilizou-

-se um Pendrive de 4GB, denominado Pendrive_teste.

Inicialmente foram criados os seguintes arquivos e salvos no Pendrive_teste: Documento_06.odt, Documento_07.odt, Documentoe_08.odt, Documentoe_09.odt e Documentoe_10.odt.

No primeiro experimento, realizou-se a exclusão tradicional do Documento_06.odt, por meio das teclas SHIFT + DELETE, que indica a "exclusão permanente" do item.

Em seguida, aplicou-se o Wipe, através do comando wipe -q Documento_07.odt, no Pendrive_teste, realizando quatro passagens de sobrescrita do arquivo.

Logo após, utilizou-se o BleachBit para executar a sobrescrita do Documento_08.odt.

Na sequência, foi empregado o Shred, por meio do comando shred -un 1 Documento_09.odt, realizando uma sobrescrita do referido arquivo.

Para a eliminação do Documento_09.odt, foi realizada a formatação simples do Pendrive_teste. No entanto, essa opção alerta para a possibilidade de recuperação dos dados.

Da mesma forma que o experimento no HD_teste, a execução do aplicativo Foremost, na tentativa de recuperar os arquivos apagados, constatou a existência de três arquivos, sendo os Documento_06.odt, Documento_08.odt e Documento_10.odt.

Em consequência da permanência desses dados no dispositivo, procedeu-se a sobrescrita do espaço livre, realizando-se três experimentos isolados e nas mesmas condições de execução.

No primeiro teste, foi empregado o BleachBit, que levou cerca de 12 minutos para concluir o procedimento. Então, utilizou-se o Foremost e verificou-se a impossibilidade de restauração dos arquivos.

Em seguida, utilizou-se o Wipe para sobrescrever quatro vezes o Pendrive_teste, demorando 1 hora e 15 minutos para conclusão. Logo após, foi procedida uma busca com Foremost, constatando-se a inexistência de dados.

No terceiro teste, executou-se o Shred para sobrescrever uma única vez o Pendrive_teste, levando 22 minutos para ser concluído. Enfim, por meio do Foremost, verificou-se a inexistência de dados.

### 2.6 ANÁLISE DOS RESULTADOS E COMPARAÇÃO DAS FERRAMENTAS

Após todos os testes, observou-se que os resultados foram muito semelhantes, conforme descrito a seguir:

**QUADRO 01 -** Resultados dos testes de exclusão de arquivos

| Dispositivo de armazenamento | Arquivo escluído | Forma de exclusão | Recuperado com Foremost | Integridade do conteúdo recuperado |
|---|---|---|---|---|
| HD_Teste | Documento_01.odt | Deleção tradicional | Sim | 100% |
| HD_Teste | Documento_02.odt | Wipe | Não | - |
| HD_Teste | Documento_03.odt | BleachBit | Sim | 100% |
| HD_Teste | Documento_04.odt | Shred | Não | - |
| HD_Teste | Documento_05.odt | Formatação Simples | Sim | 100% |
| Pendrive_teste | Documento_06.odt | Deleção tradicional | Sim | 100% |
| Pendrive_teste | Documento_07.odt | Wipe | Não | - |
| Pendrive_teste | Documento_08.odt | BleachBit | Sim | 100% |
| Pendrive_teste | Documento_09.odt | Shred | Não | - |
| Pendrive_teste | Documento_10.odt | Formatação Simples | Sim | 100% |

Fonte: Elaborado pelo autor (2017).

a) os arquivos Documento_01.odt e Documento_05.odt, respectivamente apagados pela deleção tradicional e formatação simples do HD_teste, bem como os Documento_06.odt e Documento_10.odt, apagados pela deleção tradicional e formatação simples do Pendrive_teste, foram totalmente recuperados, confirmando a teoria da preservação da área de dados;

b) o aplicativo Foremost não foi capaz de encontrar os Documento_02.odt e Documento_07.odt, concomitantemente eliminados do HD_teste e do Pendrive_teste, pela ferramenta Wipe, o que comprova a eficiência desta na exclusão definitiva de documentos;

c) os arquivos Documento_03.odt e Documento_08.odt, eliminados respectivamente do HD_teste e do Pendrive_teste, através do BleachBit, foram plenamente restaurados, evidenciando que este utilitário não cumpre a proposta de eliminação definitiva de arquivos;

d) o Foremost não encontrou qualquer vestígio dos Documento_04.odt e Documento_09.odt, respectivamente apagados do HD_teste e do Pendrive_teste, com a utilização do Shred, comprovando a confiabilidade dessa ferramenta na exclusão definitiva de documentos;

- A fim de eliminar os três arquivos ainda remanescentes em cada dispositivo, realizou-se a limpeza de espaço livre dessas mídias. Os resultados são expostos abaixo:

**QUADRO 2** - Resultados dos testes de limpeza de espaço livre

| Ferramenta utilizada | Método de sanitização | Tempo de limpeza do HD_teste | Nº de arquivos eliminados no HD_teste | Tempo de limpeza do Pendrive_teste | Nº de arquivos eliminados no Pendrive_teste |
|---|---|---|---|---|---|
| BleachBit | Sobrescrita única com zeros | 6 h | 01 | 12 min | 03 |
| Wipe | quatro sobrescritas com dados aleatórios | 62 h | 03 | 1h 15min | 03 |
| Shred | Sobrescrita única com dados aleatórios | 14 h | 03 | 22 min | 03 |

Fonte: Elaborado pelo autor (2017).

e) a limpeza realizada pelo BleachBit foi eficaz no Pendrive_teste, eliminando definitivamente os arquivos remanescentes. No entanto, foi insatisfatória no HD_teste, uma vez que o Foremost encontrou dois daqueles arquivos ainda intactos na mídia magnética (Documento_03.odt e Documento_05.odt). Embora os tempos de execução desse método (6h no HD e 12min no Pendrive) sejam menores que os tempos das demais ferramentas, seus resultados foram comprometedores no HD;

f) no segundo teste, foi executada a sanitização do HD_teste e do Pendrive_teste, pelo Wipe, na opção de quatro sobrescritas, que eliminou completamente os arquivos remanescentes, impossibilitando a recuperação dos dados em ambos os dispositivos;

g) o último teste consistiu na utilização do Shred, na opção de sobrescrita única, para limpeza do HD_teste e do Pendrive_teste, que se mostrou efetivo, pois nenhum dado foi recuperado pelo Foremost.

A análise dos resultados esclarece que

o aplicativo BleachBit não é confiável para a exclusão definitiva de arquivos e limpeza de espaço livre. Já as ferramentas Wipe e Shred foram aprovadas em todos os testes.

Destacam-se também os tempos gastos para realizar a sobrescrita de dispositivos de maior capacidade, como o HD_teste de 500GB. Enquanto Wipe demorou 62h, Shred gastou 14h nesse processo.

## 3 CONCLUSÃO

O presente trabalho teve por objetivo geral analisar os procedimentos utilizados no 4° B Com e propor melhorias no processo do descarte seguro das mídias informáticas capazes de armazenar informações corporativas.

Assim, verificou-se que os procedimentos executados naquela OM garantem o descarte seguro dos materiais capazes de armazenar informações corporativas, uma vez que utilizam a ferramenta Shred com cinco sobrescritas. No entanto, para aprimorar seus processos e torná-los mais eficientes, passo a listar procedimentos passíveis de melhorias, resultante dos estudos desta pesquisa científica, a saber:

a) alterar a quantidade de sobrescritas de cinco para uma única, pois é suficiente para alcançar o objetivo da sanitização, conforme proposta de Ivascu, comprovada neste trabalho científico;

b) utilizar o aplicativo Shred, o qual os experimentos científicos comprovaram eficiência, para limpeza de HD antes da redistribuição interna de computadores, nos casos em que o destinatário não deva ter acesso a documentos do antigo detentor;

c) divulgar as técnicas de sanitização ao público geral da OM, a fim de contribuir para a conscientização individual relativa à segurança das informações corporativas e particulares do pessoal.

Ficou demonstrado, de forma empírica, como os arquivos apagados de um dispositivo informático por métodos convencionais podem ser facilmente recuperados por programas de recuperação de dados, a exemplo do Foremost. Isso confirmou a necessidade de aplicar um método de exclusão segura.

A análise dos aplicativos selecionados possibilitou a comparação de diferentes métodos, confirmando a declaração de Ivascu (2011) de que múltiplas sobrescritas não são mais efetivas que uma única sobrescrita. Pode-se afirmar também que quanto maiores a capacidade do dispositivo a ser sanitizado e o número de sobrescritas a serem realizadas, maior será o tempo gasto no processo.

Dentre as ferramentas testadas, o Shred apresentou-se como a mais eficiente, por atingir o mesmo grau de segurança na eliminação definitiva dos documentos, com menos sobrescritas de dados e, consequentemente, menor tempo de execução.

Além de contribuir para a melhoria do processo de sanitização das mídias do 4° B Com, este estudo poderá contribuir para a formulação de procedimentos de sanitização citados nas Normas Gerais de Ação (NGA) de cada OM segundo suas peculiaridades.

Pode contribuir também para a conscientização dos usuários, alertando-os para as formas de eliminação segura das informações particulares, evitando exposições desnecessárias.

Como sugestão para trabalhos futuros, apontam-se a análise de outros aplicativos de eliminação segura de dados, como DBAN, secure-delete e os comandos dd e dcfldd, além de testes com outros tipos de arquivos, como imagem, áudio e vídeo.

Enfim, esse trabalho contribui para duas áreas importantes da gestão: a gestão da informação e a gestão do material.

Na primeira, ao disponibilizar um método para a efetiva eliminação de documentos,

evitam-se problemas oriundos da divulgação indevida de informações sigilosas ou informações pessoais.

Na segunda, ao eliminar o conteúdo sem danificar os dispositivos de armazenamento, possibilita-se a reutilização dos mesmos, o que aumenta a disponibilidade e racionalização de recursos.

## SAFE DISPOSAL OF STORAGE MEDIA: HOW TO PRESERVE YOUR PRIVACY AND SAVE RESOURCES

**ABSTRACT**: This work is inserted in the area of study of the management, in the line of research of communication and electronic equipment maintenance. Its main goal is to analyze the procedures used in 4th Signal Battalion (4thBCom), as well as to propose improvements in the safe disposal process of computer media that stores corporate information. Although there is guidance for using software that permanently deletes data, there isn't indication of a standard application for this purpose. Thus, this study analyzes the options, in order to find a reliable program for the sanitization of these media, considering the possibility of reusing them. To do this, it performs an exploratory research, which addresses the types of storage devices, the operation of the file system and the sanitization of computer media. Then, through a questionnaire, it collects information about the processes performed in 4thBCom. Finally, it performs experiments in the Linux operating system to exclude text files on magnetic and electronic devices. So it points to Shred tool as the most appropriate in comparison to BleachBit and Wipe. In addition, it verifies that the procedures performed in the 4thBCom guarantee the safe disposal of materials that store corporate information. It's concluded that this work contributes to the information management - providing a method for the effective elimination of documents, and to the material management - by enabling reuse of storage devices.

Keywords: Information management. Material management. Corporate Information. Disposal of Computer media. Overwriting data.

## REFERÊNCIAS

BEAL, A. **Segurança da Informação:** princípios e melhores práticas para a proteção dos ativos de informação nas organizações. São Paulo: Atlas, 2008.

BRASIL. Portaria nº 011-DCT, de 29 de março de 2010. Aprova o plano de migração para Software Livre no Exército Brasileiro, versão 2010. **Boletim do Exército**, Brasília, DF, Separata ao Boletim do Exército nº17, 30 de abril de 2010.

BRASIL. Portaria nº 720, de 21 de novembro de 2011. Aprova a cartilha emergencial de segurança de tecnologia da informação e comunicações. **Boletim do Exército**, Brasília, DF, Separata ao Boletim do Exército nº47, 25 de novembro de 2011.

DIESBURG, S. M; WANG, A. A. **A survey of confidential data storage and deletion methods**. ACM Computing Surveys, Vol. 43, n. 1, Article 2, 2010.

ENGLANDER, Irv; tradução e revisão técnica TANAKA, Edson. **A Arquitetura de Hardware Computacional, Software de Sistema e Comunicação em Rede**: Uma Abordagem da Tecnologia da Informação. Rio de Janeiro: LTC, 2011.

FARMER, D.; VENEMA, W. **Perícia Forense Computacional**: Teoria aplicada à prática. São Paulo: Pearson Prentice Hall, 2007.

IVASCU, Mihaita. **Data Erasure on Magnetic Storage**. International Conference of Scientific Paper. Brasov: AFASES, 2011.

MARÇULA, Marcelo; BENINI FILHO, Pio Armando. **Informática:** Conceitos e Aplicações. São Paulo: Érica, 2008.

MOTA FILHO, João Eriberto. **Descobrindo o Linux:** entenda o sistema operacional GNU/Linux. São Paulo: Novatec, 2012.

NATIONAL SECURITY AGENCY. **NSA/CSS Storage Device Sanitization Manual**. Disponível em: <https://www.nsa.gov/resources/everyone/media-destruction/assets/files/storage-device-declassification-manual.pdf>. Acesso em 25 abr. 2017, 20:12:32.

SILVA, Silvio Lucas. **O descarte seguro de documentos arquivísticos em suporte digital**. Paraíba: UFPB, 2015. Disponível em: <http://tede.biblioteca.ufpb.br-/bitstream/tede/4968/2/arquivototal.pdf>. Acesso em: 18 fev. 2017, 15:48:24.

O autor é bacharel em Ciências Militares pela Academia Militar das Agulhas Negras (AMAN). 1° Tenente do Serviço de Intendência do Exército Brasileiro. É pós-graduado pela Escola de Comunicações, *Lato Sensu*, de Especialização em Comunicações. Atualmente, exerce a função de Chefe da Seção de Planejamento e Gestão do 4° Batlahão de Comunicações e pode ser contactado pelo email rapha.leo08@gmail.com.