1.Destruição segura de arquivos e dados

1.1 Técnicas físicas de destruição

As técnicas físicas de destruição são métodos que envolvem a manipulação direta dos dispositivos de armazenamento para garantir a eliminação segura dos dados. Essas técnicas visam destruir fisicamente os dispositivos, tornando-os irreparáveis e impossíveis de recuperar informações armazenadas.

1.2 Trituração

A trituração é uma técnica física de destruição que envolve o uso de equipamentos especializados para reduzir os dispositivos de armazenamento em pequenos pedaços. Essa técnica é amplamente utilizada para garantir a eliminação segura dos dados armazenados em discos rígidos, unidades de fita magnética, CDs/DVDs, cartões de memória e outros tipos de mídia.

No processo de trituração, os dispositivos são inseridos em um triturador industrial que utiliza lâminas ou cilindros giratórios de alta potência para triturar os dispositivos em pedaços pequenos e irrecuperáveis. O tamanho dos pedaços pode variar dependendo do equipamento utilizado, mas geralmente são fragmentos de alguns milímetros.

Essa técnica é altamente eficaz na destruição dos dispositivos, pois os torna fisicamente irreconhecíveis e impossíveis de serem montados ou recuperados. Além disso, a trituração também danifica os componentes eletrônicos e magnéticos, inviabilizando qualquer tentativa de recuperação dos dados.

trituração é uma opção popular para empresas e organizações que precisam descartar dispositivos de armazenamento contendo informações confidenciais. É importante observar que, após a trituração, os resíduos resultantes devem ser tratados de acordo com as regulamentações ambientais, garantindo a sua correta destinação e reciclagem.

1.3 Trituração criptográfica

A técnica de trituração criptográfica é um método avançado de destruição segura de dados que combina a criptografia dos dispositivos de armazenamento com a posterior trituração física dos mesmos. Nesse processo, os dados armazenados nos dispositivos são criptografados antes de serem triturados, garantindo que eles se tornem completamente ilegíveis e irrecuperáveis.

Antes de realizar a trituração criptográfica, os dispositivos de armazenamento são submetidos a um processo de criptografia, onde os dados são convertidos em uma forma criptografada utilizando algoritmos complexos. Essa criptografia torna os dados ininteligíveis sem a chave de descriptografia correspondente, garantindo a confidencialidade dos dados.

Após a criptografia dos dispositivos, eles são submetidos à trituração física, onde são destruídos em pequenos pedaços por meio de trituradores especializados. A combinação da criptografia prévia com a trituração física torna praticamente impossível a recuperação dos dados, mesmo que alguém tente reconstituir os dispositivos.

A trituração criptográfica é uma técnica extremamente segura e confiável para a destruição de dados sensíveis. Ela oferece uma camada adicional de proteção, garantindo que mesmo que os dispositivos físicos caiam em mãos erradas, os dados permaneçam inacessíveis e completamente ilegíveis. É importante ressaltar que a trituração criptográfica deve ser realizada por profissionais especializados e seguindo as diretrizes de segurança adequadas.

1.4 Perfuração

A técnica de perfuração é uma forma física de destruição de dispositivos de armazenamento que envolve a criação de furos ou danos significativos nos dispositivos. O objetivo é comprometer a integridade dos mecanismos internos do dispositivo, tornando-o inoperável e impossibilitando a recuperação dos dados.

A perfuração pode ser realizada de diferentes maneiras, dependendo do tipo de dispositivo e do equipamento disponível. São utilizadas máquinas perfuradoras que são capazes de criar orifícios ou danos estruturais nos dispositivos de armazenamento, como discos rígidos, unidades de fita magnética, CDs/DVDs, entre outros.

Ao perfurar um dispositivo, é essencial atingir áreas críticas que contêm os dados armazenados, como os pratos magnéticos em discos rígidos. Os furos criados devem ser suficientemente grandes e profundos para danificar fisicamente os componentes internos, tornando a leitura dos dados impossível.

A perfuração é considerada uma técnica eficaz de destruição segura de dados, uma vez que compromete fisicamente o dispositivo, dificultando qualquer tentativa de recuperação dos dados armazenados. No entanto, é importante observar que, mesmo após a perfuração, alguns resíduos ou fragmentos podem permanecer, e o descarte adequado desses materiais deve ser realizado de acordo com as regulamentações ambientais.

1.5 Incineração

A incineração é uma técnica física de destruição que envolve a queima controlada dos dispositivos de armazenamento. Nesse processo, os dispositivos são submetidos a altas temperaturas em fornos especialmente projetados para essa finalidade. A incineração é realizada de forma a garantir a destruição completa dos dispositivos, reduzindo-os a cinzas.

A incineração é considerada uma técnica eficaz para a destruição segura de dados, pois a exposição a altas temperaturas danifica de forma irreversível os meios de armazenamento, como discos rígidos, CDs/DVDs, unidades de fita magnética, entre outros. O calor intenso

derrete e deforma os componentes físicos dos dispositivos, tornando impossível a recuperação dos dados armazenados.

É importante ressaltar que a incineração deve ser realizada em instalações apropriadas, com equipamentos de controle de poluição e segurança para garantir o descarte adequado dos resíduos resultantes. Além disso, é fundamental seguir as regulamentações ambientais e normas de segurança no manuseio e descarte dos materiais incinerados.

A incineração é frequentemente utilizada em situações em que a segurança dos dados é crítica e a destruição física completa é necessária para atender a requisitos de privacidade e conformidade. No entanto, é importante considerar os impactos ambientais dessa técnica e buscar alternativas sustentáveis sempre que possível.

2.Degaussing

O Degaussing é uma técnica física de destruição que envolve o uso de um dispositivo chamado *degaussing machine*, também conhecido como desmagnetizador. Essa técnica é amplamente utilizada para eliminar de forma segura dados armazenados em mídias magnéticas, como discos rígidos, fitas magnéticas e cartões de crédito com faixa magnética.

O processo de Degaussing envolve a exposição da mídia magnética a um campo magnético intenso e oscilante, que é gerado pelo desmagnetizador. Esse campo magnético intenso faz com que as partículas magnéticas presentes na mídia percam sua orientação magnética original, resultando na eliminação completa e irreversível dos dados armazenados.

O Degaussing é uma técnica muito eficaz para garantir a destruição segura dos dados, pois apaga todas as informações da mídia de maneira rápida e eficiente. É importante ressaltar que, uma vez que a mídia é Degaussada, ela não pode mais ser utilizada para armazenar dados, pois perde completamente sua capacidade de reter informações magnéticas.

Para garantir resultados satisfatórios, é essencial seguir as instruções do fabricante do desmagnetizador e usar o dispositivo corretamente. Além disso, é importante destacar que o Degaussing é uma técnica que deve ser aplicada com cuidado e seguindo as diretrizes de segurança, especialmente no que diz respeito ao descarte adequado dos resíduos gerados durante o processo. A figura mostrada a seguir exemplifica um exemplo de incineração de um equipamento de Degaussing.

3.Desmontagem

A técnica de desmontagem é uma abordagem física de destruição de dados que envolve a separação dos componentes dos dispositivos de armazenamento. Nesse processo, os dispositivos são desmontados manualmente ou com o auxílio de ferramentas especializadas, a fim de expor e separar os componentes internos.

Ao desmontar os dispositivos, os componentes individuais, como discos, chips de memória, placas de circuito impresso e outros, são separados. Essa técnica é especialmente útil quando se trata de dispositivos como discos rígidos, unidades de fita magnética ou cartões de memória, nos quais os dados são armazenados em componentes físicos internos.

Após a desmontagem, os componentes podem ser submetidos a técnicas adicionais de destruição, como trituração, perfuração ou até mesmo desmagnetização individual dos discos. Essa abordagem oferece uma camada adicional de segurança, pois os dados estão dispersos em diferentes partes do dispositivo e exigiriam um esforço significativo para serem recuperados.

A desmontagem adequada dos dispositivos requer conhecimento técnico e habilidades específicas para evitar danos acidentais aos componentes ou exposição a substâncias perigosas, como poeira ou materiais químicos. É importante seguir as práticas recomendadas e aderir a regulamentações ambientais ao realizar a desmontagem dos dispositivos, garantindo um descarte adequado dos componentes resultantes.

4.Técnicas de formatação e sobrescrita de dados

As técnicas de formatação e sobrescrita de dados são métodos utilizados para eliminar ou tornar irrecuperáveis os dados armazenados em dispositivos de armazenamento. Essas técnicas envolvem a manipulação dos bits de dados nos dispositivos, garantindo que sejam apagados de forma segura e permanente.

5.Formatação rápida

A formatação rápida é um procedimento de formatação de dados em um dispositivo de armazenamento que ocorre de forma mais rápida em comparação com uma formatação completa. Nesse processo, o sistema de arquivos é recriado, mas os dados previamente armazenados não são apagados fisicamente.

A formatação rápida geralmente é realizada quando se deseja reutilizar um dispositivo de armazenamento ou resolver problemas de corrupção do sistema de arquivos.

Durante a formatação rápida, o sistema operacional cria uma nova tabela de alocação de arquivos e remove as referências aos arquivos antigos. Os dados existentes no dispositivo permanecem intactos, mas são considerados como espaço livre disponível para uso.

Isso significa que, embora os arquivos não sejam acessíveis através do sistema de arquivos, eles ainda podem ser recuperados usando ferramentas especializadas de recuperação de dados.

É importante ressaltar que a formatação rápida não fornece um nível de segurança adequado para a remoção completa e irreversível dos dados sensíveis. Se a preocupação é garantir que

os dados não possam ser recuperados, técnicas mais robustas de sobrescrita ou destruição física devem ser empregadas.

A formatação rápida é mais adequada para situações em que não há preocupação com a recuperação dos dados existentes e o foco é simplesmente preparar o dispositivo para uso futuro.

5.1 Formatação completa

A formatação completa, também conhecida como formatação de baixo nível, é uma técnica utilizada para apagar todos os dados de um dispositivo de armazenamento, como um disco rígido ou uma unidade flash, reescrevendo todas as áreas do dispositivo com zeros ou padrões específicos.

Essa técnica é mais abrangente do que a formatação rápida, pois além de apagar o sistema de arquivos, também sobrescreve os setores não alocados do dispositivo.

Durante o processo de formatação completa, todos os dados existentes no dispositivo são eliminados, incluindo arquivos, pastas, partições e informações de sistema. A formatação completa é realizada por meio de software específico, como utilitários de formatação fornecidos pelo sistema operacional ou ferramentas de terceiros.

Ao executar uma formatação completa, o software percorre todas as trilhas e setores do dispositivo de armazenamento, substituindo os dados existentes com zeros ou outros padrões. Essa ação de sobrescrever os dados existentes torna-os virtualmente irreversíveis e inacessíveis.

É importante ressaltar que a formatação completa não é um método 100% seguro para a destruição completa dos dados, pois técnicas avançadas de recuperação de dados podem ser capazes de recuperar parte ou todos os dados sobrescritos.

Portanto, em casos em que a segurança é uma preocupação crítica, técnicas adicionais, como a criptografia ou a destruição física do dispositivo, devem ser consideradas.

5.2 Sobrescrita simples

A sobrescrita simples é uma técnica de formatação e eliminação de dados que consiste em substituir os dados existentes por novos dados aleatórios. Nesse método, os dados originais são substituídos por um padrão fixo de bits, geralmente composto por zeros ou uns, tornando os dados anteriores irrecuperáveis.

A sobrescrita simples é realizada por meio de um processo de gravação sequencial nos setores do dispositivo de armazenamento. Cada setor é sobrescrito com os novos dados, substituindo completamente as informações originais.

O número de vezes que os dados são sobrescritos pode variar, mas geralmente uma única passagem é considerada suficiente para impedir a recuperação dos dados originais.

No entanto, é importante mencionar que a sobrescrita simples pode ser menos segura em relação a métodos mais avançados. Com técnicas forenses avançadas e tecnologias de recuperação de dados especializadas, é possível recuperar alguns vestígios dos dados originais mesmo após a sobrescrita simples.

Portanto, em casos de informações altamente sensíveis ou sujeitas a regulamentações específicas, é recomendável o uso de métodos mais robustos de sobrescrita, como a sobrescrita de múltiplas passagens ou o uso de padrões de sobrescrita reconhecidos, como o DoD 5220.22-M.

5.3 Sobrescrita de múltiplas passagens

A sobrescrita de múltiplas passagens é uma técnica utilizada para garantir a eliminação segura de dados armazenados em dispositivos. Nesse método, os dados existentes são substituídos por padrões de bits específicos, repetidas vezes, em várias passagens.

A ideia por trás da sobrescrita de múltiplas passagens é garantir que os dados originais sejam completamente apagados e irreversíveis. Cada passagem consiste em escrever um padrão de bits sobre os dados existentes, seguido de uma nova passagem com um padrão diferente.

Geralmente, são utilizados padrões aleatórios ou sequências predefinidas de bits para maximizar a eficácia da eliminação dos dados.

O número de passagens necessárias pode variar, mas geralmente são recomendadas três ou mais passagens para garantir uma eliminação mais segura. Cada passagem adiciona uma camada adicional de sobreposição de dados, dificultando ainda mais a recuperação dos dados originais.

A sobrescrita de múltiplas passagens é considerada uma técnica eficaz para eliminar dados de forma segura, tornando-os praticamente irrecuperáveis. No entanto, é importante ressaltar que essa técnica pode levar mais tempo, especialmente para dispositivos de armazenamento maiores.

Além disso, é essencial seguir as diretrizes e padrões de sobrescrita reconhecidos pela indústria, como o padrão DoD 5220.22-M, para garantir a eficácia da eliminação dos dados.

5.4 Sobrescrita com o padrão DoD 5220.22-M

A sobrescrita com o padrão DoD 5220.22-M é uma técnica de destruição segura de dados que segue as diretrizes estabelecidas pelo Departamento de Defesa dos Estados Unidos (DoD). Esse padrão especifica um processo de múltiplas passagens para garantir a eliminação completa e irreversível dos dados armazenados em um dispositivo.

De acordo com o padrão DoD 5220.22-M, o processo de sobrescrita envolve três passagens consecutivas de escrita nos dados do dispositivo. Cada passagem é projetada para tornar os dados originalmente armazenados cada vez mais difíceis de serem recuperados.

Na primeira passagem, todos os bits dos dados são sobrescritos com zeros (0). Isso ajuda a apagar os dados existentes, mas ainda pode permitir uma recuperação parcial por meio de técnicas avançadas de recuperação de dados.

Na segunda passagem, todos os bits são sobrescritos com uns (1). Isso ajuda a obscurecer ainda mais os dados remanescentes, dificultando a sua recuperação.

Na terceira e última passagem, os dados são sobrescritos com um padrão aleatório, que pode ser uma combinação de zeros e uns. Essa passagem final visa eliminar qualquer vestígio dos dados originais e garantir que se tornem completamente inacessíveis.

A sobrescrita com o padrão DoD 5220.22-M é considerada uma técnica segura para a destruição de dados. No entanto, é importante ressaltar que a eficácia dessa técnica pode depender do tipo de dispositivo de armazenamento e da tecnologia utilizada.

Em alguns casos, dispositivos de armazenamento específicos podem exigir métodos adicionais de destruição física ou criptografia para garantir a eliminação completa dos dados.

5.5 Sobrescrita com criptografia dos dados antes da formatação/sobrescrita

A técnica de sobrescrita com criptografia dos dados antes da formatação/sobrescrita é um método avançado de eliminação segura de dados. Nessa abordagem, os dados armazenados nos dispositivos são criptografados antes de serem sobrescritos ou formatados, garantindo que eles se tornem completamente ilegíveis e inacessíveis.

Para aplicar essa técnica, os dados são criptografados utilizando algoritmos criptográficos robustos. A criptografia envolve a conversão dos dados em uma forma criptografada, tornando-os ininteligíveis sem a chave de descriptografia correspondente.

Dessa forma, mesmo que os dados sejam sobrescritos ou o dispositivo seja formatado, eles permanecem protegidos por trás da camada de criptografia.

Quando a criptografia dos dados é realizada antes da sobrescrita ou formatação, o processo de eliminação segura se torna ainda mais eficaz. Mesmo que alguém tente recuperar os dados posteriormente, eles permanecerão criptografados e, portanto, inacessíveis. Isso oferece uma camada adicional de proteção, garantindo que os dados permaneçam confidenciais e inutilizáveis.

6.Aplicativos especializados para destruição segura de dados

Aplicativos especializados para destruição segura de dados são programas desenvolvidos com o objetivo de garantir a eliminação irreversível e segura de informações armazenadas em dispositivos de armazenamento, como discos rígidos, SSDs, pendrives e cartões de memória.

Esses aplicativos são projetados para garantir que os dados sejam removidos de maneira definitiva, tornando-os inacessíveis e impossíveis de serem recuperados.

Esses aplicativos oferecem recursos avançados para a destruição segura de dados, como a sobrescrita de arquivos com padrões específicos, a limpeza de áreas não utilizadas nos dispositivos de armazenamento e a verificação da efetividade do processo de eliminação.

Eles podem ser usados tanto por indivíduos como por empresas que desejam descartar dispositivos de armazenamento antigos ou garantir que informações confidenciais não sejam recuperadas por terceiros. Alguns aplicativos são:

6.1 Eraser

Aplicativo especializado para destruição segura de dados que oferece recursos avançados para a eliminação permanente e irreversível de informações confidenciais. Ele permite a sobrescrita de arquivos com padrões específicos, garantindo que os dados sejam apagados de forma segura e tornando-os virtualmente impossíveis de serem recuperados. O Eraser é amplamente utilizado por indivíduos e organizações que buscam proteger a privacidade de suas informações ao descartar ou reutilizar dispositivos de armazenamento, fornecendo uma solução confiável para garantir a eliminação definitiva de dados sensíveis.

6.2 DBAN

Aplicativo especializado para a destruição segura de dados em dispositivos de armazenamento. Ele é amplamente utilizado devido à sua eficácia e recursos avançados. O DBAN é executado em um ambiente inicializável independente do sistema operacional e permite realizar a sobrescrita de dados em discos rígidos, SSDs e outros dispositivos de armazenamento de forma irreversível, tornando os dados inacessíveis e impossíveis de serem recuperados. Ele oferece diferentes opções de sobrescrita, como padrões de preenchimento aleatório ou métodos de criptografia avançada, permitindo que os usuários personalizem o processo de eliminação de acordo com suas necessidades de segurança.

6.3 Secure eraser

É um aplicativo especializado para destruição segura de dados que oferece recursos avançados para garantir a eliminação irreversível de informações em dispositivos de armazenamento. Com opções de sobrescrita de arquivos utilizando diferentes padrões de segurança, o Secure Eraser permite que os dados sejam apagados de maneira permanente, tornando-os inacessíveis e impossíveis de serem recuperados. É uma ferramenta confiável para proteger a privacidade e a segurança dos dados, sendo amplamente utilizada por indivíduos e empresas que buscam uma solução eficaz para o descarte seguro de informações confidenciais.