FACULDADE DE INFORMÁTICA E ADMINISTRAÇÃO PAULISTA
Pós-Graduação MBA Gestão de Segurança da Informação

LEANDRO MERCURIO

MARCELO MARQUES DÁVILA

Descarte Seguro de Informações Armazenadas em Meios Digitais

São Paulo

2010

LEANDRO MERCURIO

MARCELO MARQUES DÁVILA

Descarte Seguro de Informações Armazenadas em Meios Digitais

Trabalho de Conclusão de Curso apresentado à Faculdade de Informática e Administração Paulista, como um dos requisitos para a conclusão do Curso de Pós-Graduação em MBA Gestão de Segurança da Informação

Orientador: Prof. Marcelo Lau

São Paulo

2010

LEANDRO MERCURIO

MARCELO MARQUES DÁVILA

Descarte Seguro de Informações Armazenadas em Meios Digitais

Trabalho de Conclusão de Curso apresentado à Faculdade de Informática e Administração Paulista, como um dos requisitos para a conclusão do Curso de Pós-Graduação em MBA Gestão de Segurança da Informação.

Aprovada em 30 de Setembro de 2010.

BANCA EXAMINADORA

Prof(ª). Marcelo Lau
Orientador

Prof(ª). Dr. ou. Ms Xxx (nome completo)
Componente da Banca

Prof(ª). Dr. ou. Ms Xxx (nome completo)
Componente da Banca

Às nossas esposas, amigos e familiares, que nos apoiaram neste desafio.

AGRADECIMENTOS

Ao nosso orientador, Marcelo Lau

RESUMO

Este documento apresenta ao leitor algumas técnicas de descarte dos meios de armazenamento que contenham informações sigilosas que de forma alguma possam ser recuperadas. Como linha de trabalho, apresentaremos normas vigentes que possuem diretrizes de Gestão de Segurança da Informação, alguns meios de armazenamento de dados, formas de descarte seguro das informações conforme o meio de armazenamento, tais como desmagnetizadores para mídias magnéticas, trituração para mídias ópticas entre outros. Por fim apresentaremos alguns estudos de caso, demonstrando o descarte de informações contidas em disco rígido através de técnicas de sobrescrita.

Palavras-chave: Manufatura Reversa, Gutmann, Descarte Seguro, Desmagnetizador.

ABSTRACT

This document introduces the reader to some discard techniques of storage media containing confidential information that cannot be recovered at all. This work was carried out on presenting the current standards concerned to the Management of Information Security, some data storage media, safe information discard according to storage media, such as demagnetizing devices for magnetic media, and grinding for optical media and so on. Finally some case studies are presented to demonstrate hard disk contained information discard by overwriting techniques.

Keywords: Disassembly, Gutmann, Safe Disposal, Degauss.

LISTA DE ILUSTRAÇÕES

FIGURAS

GRÁFICOS

TABELAS

QUADRO

LISTA DE SIGLAS

BD - Blu-ray Disc

CDROM - Compact Disc Read Only Memory

DVD - Digital Versatile Disc

HD - Hard Disk

DLT - Digital Linear Tape

ISO - International Organization for Standardization

PAN – Personal Account Number

PIN – Personal Identification Number

CID – Card Identification Number

PCI DSS - Payment Card Industry Data Security Standard

BUREAU – Fábrica de Cartões

SUMÁRIO

INTRODUÇÃO

Valor da Informação, esta é uma questão que muitas instituições não se preocupam, o fato de desconhecerem o valor de suas informações acaba gerando uma negligência desnecessária com seu descarte, seja no meio digital ou físico.

Negligência com o descarte pode provocar vazamento de informações importantes que geraria prejuízos incalculáveis para as instituições, podendo até levar à falência da empresa.

Segundo Edson Fontes (Jan / 2010) a empresa Ponemon Institute em seu estudo anual nos EUA sobre o valor de um registro perdido ou roubado, em 2009, este valor estava em U$204,00. Se um pequeno arquivo de mil registros é roubado o prejuízo pode chegar a 204 mil dólares.

Desta forma, torna-se essencial o estudo do Ciclo de vida da informação, isto é, saber todos os momentos que a informação viveu, seja em meio eletrônico ou físico, para determinar quando aquela informação passa a ser desnecessária ou quando ela esta vivenciando o seu ciclo menos seguro, e da classificação das informações, para determinar o nível de classificação da informação, quanto maior o nível maior a necessidade do descarte seguro dos dados.

Este trabalho demonstrará algumas formas utilizadas para garantir a destruição segura de dados, especialmente os classificados como confidenciais, que requerem total atenção. Determinar quando utilizar método de sobrescrita de dados em mídias magnéticas (Métodos de Gutmann, Matriz de Saneamento da NSA, VSITR) ou a total desmagnetização, estes determinados como destruição lógica do dado ou dependendo do tipo de mídia a destruição física como desintegração ou incineração. E em caso de destruição física, qual a melhor forma de descarte sem prejudicar o meio ambiente, conforme as normas da CETESB (Companhia Ambiental do Estado de São Paulo).

Este trabalho também apresenta normas de mercado como o Padrão ISO 27000 que ajuda a avaliar os ricos e a criar uma boa base de gestão da informação, e os padrões da área de cartão de crédito como o PCI-DSS (*Payment Card Industry Data*

Security Standard), que é uma documentação de boas práticas e o *MasterCard Logical Security Requirements for Card Personalization Bureaus* que é uma norma especifica para fábricas que personalizam cartões de pagamento da MasterCard que lida com dados críticos do portador de cartões.

Estas normas, voltadas ao meio de pagamentos por uso de cartões, foram selecionadas para este trabalho devido ao grande foco em segurança de informações. Por se tratar de dados financeiros, empresas como a Master Card, seguem rígidos padrões de segurança de informação, baseados nas melhores práticas e na experiência de anos para manter o sigilo da informação de seus clientes e evitar fraudes.

Ao final do trabalho, será apresentado um estudo de caso onde será demonstrado, um descarte de dados lógico em um Disco Rígido Magnético utilizando softwares *Open Source* que estão disponíveis na internet para os profissionais que desejem descartar suas informações de forma segura.

Objetivo

Descrever e comparar formas de descarte das informações em meios digitais, apresentando o que as principais normas de padrões de tecnologia e segurança de dados financeiros determinam sobre este tema, explicando a gravação dos dados em meios digitais e seu descarte, tanto em forma lógica quanto na forma física.

Problema

- Gerenciamento das informações para evitar a perda ou divulgação não autorizada;
- Necessidade das informações confidenciais não serem acessadas/recuperadas após o seu descarte;
- Métodos de destruição adequados para o descarte de dados armazenados em meios digitais e físicos.

Metodologia

Pesquisa descritiva com estudo de caso que demonstra métodos de descarte de dados digitais através de sobrescrita de dados através de simulações. Análise dos dados de forma dedutiva.

Delimitação do tema

Para analisar o descarte seguro das informações, circunscrito à área de (GSI) Gestão da Segurança da Informação, a presente pesquisa se organizou em torno de quatro capítulos. No primeiro capítulo são apresentadas as normas ISO 27000 que demonstram as melhores práticas de gestão e segurança da informação, a classificação e o ciclo de vida da informação, fazendo uma avaliação em seu nível de criticidade e por quanto tempo a informação se manterá disponível, antes de seu descarte seguro, o PCI e o *MasterCard Logical Security Requirements for Card Personalization Bureau* que apresentam as melhores práticas para a segurança lógica e o descarte seguro das informações para empresas do ramo de fabricação e comunicação de dados de cartões de crédito. No segundo capítulo, é feita uma análise dos tipos de mídia onde é explicado como é feita a gravação do dado em meio digital. No terceiro capítulo apresentamos os métodos para descarte de dados, onde explica quais são as formas de descarte lógico (apagar eletronicamente) e físico (destruição do meio de armazenamento) com a devida preocupação ambiental. Finalizando, temos o quarto capítulo onde apresentamos um estudo de caso demonstrando na prática duas formas seguras de descarte de arquivos. Os dados foram levantados a partir de pesquisas desde o início do curso até o período atual.

1. NORMAS E DOCUMENTAÇÕES

Para auxiliar as empresas na melhor forma de tratar a informação (desde sua criação até o seu descarte) existem normas específicas para cada segmento da indústria, que auxiliam na criação de documentações necessárias para uma boa gestão da informação e determinar controles de criação, acesso e descarte destas. Neste capítulo mencionaremos algumas destas normas utilizadas, que tratam da manipulação da informação em seu ciclo de vida e seu descarte seguro. Citaremos os pontos relevantes com relação à proteção e descarte de informação pertencente à ISO 27000 – norma de segurança da informação. Em complementação à ISO, falaremos sobre classificação e ciclo de vida da informação, fundamental para o controle da informação. Também será apresentado o PCI – guia de boas práticas de segurança desenvolvida para evitar fraudes envolvendo cartões de pagamento, e o *Mastercard Logical Security Requirements for card Personalization Bureaus* – norma com requisitos de segurança para fornecedores e vendedores de cartões que oferecem produtos Mastercard. Os dois últimos são voltados à proteção de dados confidencias do portador do cartão e suas respectivas transações financeiras.

1.1. ISO 27000

Conforme a Associação Brasileira de Normas Técnicas, a série ISO 27000 é uma família de normas destinadas à matéria de segurança da informação, composta por tópicos formados por números crescentes. Esta família é extensa e com muitos tópicos com focos diferentes. Neste trabalho detalharemos tópicos que estabelecem um sistema de gerenciamento de informação, que são as normas ISO 27001 e ISO 27002.

A família 27000 é composta pelas normas abaixo:

- ISO 27001: Cobre todos os tipos de organizações, especifica os requisitos para estabelecer, implantar, operar, monitorar, revisar, manter e melhorar um sistema de gerenciamento de segurança da informação documentado.
- ISO 27002: Substitui a ISO 17799, estabelece diretrizes para iniciar, implementar, manter e melhorar o gerenciamento da segurança da informação para uma empresa.

- ISO 27003: Enfoca os aspectos críticos necessários para a concepção e implantação bem sucedida de um Sistema de Gestão da Segurança da Informação (SGSI), em conformidade com a norma ISO 27001. Ela descreve o processo de especificação e design do SGSI, desde a concepção e a produção de planos de implantação e processos para a aprovação da administração.
- ISO 27004: Fornece orientações sobre o desenvolvimento e a utilização de formas de medição para avaliar a eficácia do Sistema de Gestão de Segurança da Informação (SGSI), através de um dos grupos de controles, está norma é aplicável a todos os tipos e tamanhos de organizações.
- ISO 27005: Estabelece diretrizes para gestão de risco na segurança das informações. Esta norma suporta os conceitos gerais especificados na norma ABNT NBR ISO / IEC 27001 e é concebido para apoiar a execução satisfatória da segurança da informação baseada em uma abordagem de gestão de risco.
- ISO 27006: Especifica os requisitos e fornece orientações para uma auditoria e certificação do Sistema de Gestão de Segurança da Informação (SGSI), além dos requisitos contidos no ABNT NBR ISO / IEC 17021 e a ABNT NBR ISO / IEC 27001.
- ISO 27011: O escopo da presente recomendação é definir as diretrizes de apoio à implantação do Sistema de Gestão de Segurança da Informação (SGSI), nas organizações de telecomunicações. A adaptação desta recomendação Internacional Standard permitirá às organizações de telecomunicações a atender os requisitos de segurança de base como a confidencialidade, integridade, disponibilidade e qualquer propriedade de segurança.

1.1.1. ISO 27001

A norma ISO/IEC 27001:2006 (E) é um padrão para sistema de gestão da segurança da informação (SGSI), publicado em março de 2006 pela ABNT Associação Brasileira de Normas Técnicas, seu nome completo é ABNT NBR *ISO/IEC 27001:2006.*

Seu objetivo é ser usado em conjunto com a ABNT NBR ISO/IEC 17799:2005, o código de práticas para gerência da segurança da informação, o qual lista os objetivos do controle de segurança e recomenda um conjunto de especificações de controles de segurança. Organizações que implementam um SGSI de acordo com as melhores práticas da ISO 17799 estão simultaneamente em acordo com os requisitos da ISO 27001, mas uma certificação é totalmente opcional.

Esta norma adota o modelo PDCA, que é aplicado para estruturar todos os processos do SGSI. A figura abaixo ilustra como um SGSI toma como entrada os requisitos de segurança da informação, e as expectativas das partes interessadas, e como as ações e os processos necessários produzem os resultados de segurança da informação que atenda a essas exigências e expectativas. A adoção do modelo PDCA também reflete os princípios estabelecidos nas orientações da OECD que regem a segurança dos sistemas e redes de informação. Esta norma fornece um modelo para a execução dos princípios que regem as diretrizes de avaliação de riscos, projeto e implementação da segurança, gestão de segurança e de reavaliação.

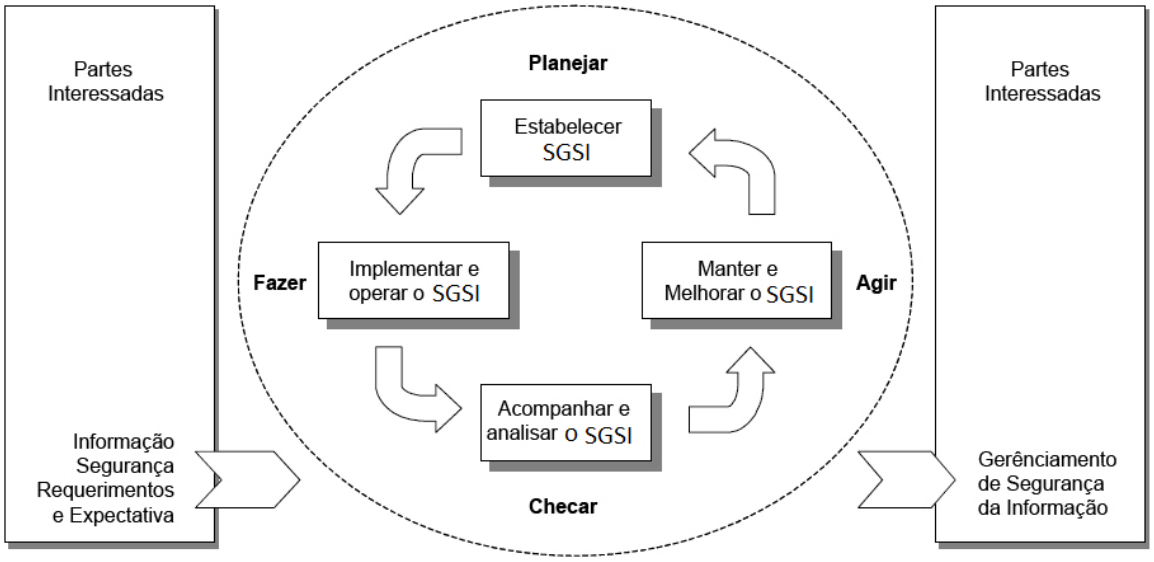

Figura 1 – Modelo PDCA aplicado para processos SGSI – Fonte: ISO 27001 (Out,2005)

- **PLANEJAR** - Estabelecer a política do SGSI, objetivos, processos e procedimentos relativos à gestão de risco, além de melhorar a segurança da informação para fornecer resultados de acordo com as políticas globais de uma organização e objetivos;

- **FAZER** – Implementar e operar a política do SGSI, controles, processos e procedimentos;
- **VERIFICAR** - Avaliar quando necessário, medir o desempenho do processo contra a política do SGSI e gerar relatórios dos resultados da gestão para a revisão;
- **AGIR** - Tomar ações corretivas e preventivas, com base nos resultados da auditoria interna do SGSI e fiscalizar a gestão ou outras informações relevantes, para alcançar melhorias contínuas.

Neste parágrafo mostramos a base de um bom processo de Segurança de informação com o PDCA e que sem um SGSI implantando e funcional, não existirá na organização regras e um bom processo para identificação e proteção de informações, base para a gestão do descarte seguro de informações.

1.1.2. ISO 27002

A norma ABNT NBR ISO/IEC 27002:2006 estabelece as diretrizes e os princípios gerais para iniciar, implementar, manter e melhorar a gestão da segurança da informação em uma organização.

Os objetivos de controle desta norma destinam-se a atender as necessidades identificadas por uma avaliação de risco, podendo servir como um guia prático para o desenvolvimento de novas normas de segurança organizacional e práticas eficazes na gestão da segurança, ajudando a construir a confiança em atividades inter-organizacionais.

A ISO 27002 possui 11 objetivos de controle, onde a ordem dos objetivos não implicam em sua importância, dependendo das circunstâncias, todas as cláusulas podem ser importantes. Para este trabalho iremos apresentar as clausulas que entendemos serem as mais importantes para metodologia de descarte seguro de dados.

- **Política de Segurança** - Um documento de política de segurança deve ser aprovado pela administração, publicado e comunicado a todos os funcionários e partes externas relevantes, o mesmo deve indicar o compromisso de gestão e definir a abordagem da organização para a gestão da segurança da informação, este documento é muito importante para a difusão do entendimento da importância e do valor das informações.

Se a empresa não difundir a Política de Segurança, as pessoas não irão ter conhecimento da importância da informação e com isso não terão atenção ao seu descarte.

- **Organizando a Segurança da Informação** – Um quadro de gestão deve ser estabelecido para iniciar e controlar a execução da segurança da informação dentro da organização.

  A Administração deverá aprovar a política de segurança da informação, atribuir as funções de segurança e coordenar a revisão e implementação de segurança em toda a organização.

  Sem um controle de segurança da informação, não existirá um responsável pelo desenvolvimento dos processos e regras de classificação e descarte de informações.

- **Gestão de Ativos** - Para alcançar e manter a proteção adequada dos ativos da organização, todos os ativos devem ser contabilizados e ter um proprietário designado.

  Os proprietários são responsáveis pela manutenção e atribuição dos controles. A implantação dos controles específicos pode ser delegada pelo proprietário conforme o caso, mas o proprietário continua responsável pela proteção adequada.

  Neste caso, ativo pode ser Informação e o proprietário da mesma irá determinar qual grau de importância dela conforme a classificação da informação. Com isso será possível determinar qual será a melhor forma de descarte.

- **Recursos Humanos e Segurança** – Esta cláusula é extremamente importante para garantir que os funcionários, fornecedores e terceiros compreendam as suas responsabilidades, que entendam a importância da informação para a empresa (através de treinamentos ou integrações), e que sejam adequados para os papéis, reduzindo o risco de roubo, fraude ou desvio de recursos.

  Com as pessoas bem informadas sobre a política de segurança, os riscos de informações serem descartadas de forma indevida diminuem.

- **Segurança Física e Ambiental** – Seu objetivo é impedir o acesso físico não autorizado, dano e interferência às instalações da organização e da informação.

  As instalações de processamento de informações críticas ou sensíveis devem ser mantidas em áreas seguras, protegidas por perímetro de segurança definido, com barreiras de segurança apropriadas e controles de entrada. Elas devem ser fisicamente protegidas contra acesso não autorizado, dano e interferência.

  Isto garante que as informações ainda não descartadas de forma segura, não sejam acessadas fora de um ambiente seguro.

- **Controle de Acesso** – O acesso às informações, processamento de informações e processos de negócios devem ser controladas com base no negócio e requisitos de segurança. As regras para o acesso lógico ou físico aos sistemas ou áreas importantes da organização devem ser criadas através de procedimentos formais visando as necessidades do negócio. Dentre os controles estão a classificação da informação, que apresentaremos a parte.

  Apenas quem tem direito de acesso à informação pode descartá-la. O descarte deve ser feito em ambiente controlado com o acesso restrito.

- **Descarte e Reutilização -** Descarte e a reutilização de equipamento é outro ponto de atenção, é necessário que todos os itens de equipamento que contenha mídia de armazenamento sejam verificados para garantir que os dados sensíveis e softwares licenciados sejam removidos ou substituídos de forma segura antes da eliminação.

  Dispositivos que possuam informações classificadas com um nível de confidencialidade elevado, devem ser fisicamente destruídos ou as informações devem ser totalmente destruídas, utilizando técnicas para tornar a informação original não-recuperável.

  Dispositivos danificados que contenham informações classificadas com um nível de confidencialidade elevado, podem exigir uma avaliação dos riscos para determinar se o itens devem ser fisicamente destruídos ao invés de enviar para reparo ou descartados.

As mídias devem ser eliminadas de maneira segura e cuidadosa quando não forem mais necessárias, através de procedimentos formais, minimizando o risco de vazamento de informações confidenciais à pessoas não autorizadas.

Segue alguns itens de segurança descritos na norma ISO a considerar:

a) Mídias contendo informações sensíveis devem ser armazenadas e eliminadas de forma segura, por exemplo, por incineração, trituração, ou remover os dados através de aplicativos dentro da organização;

b) Os procedimentos devem estar no local para identificar os itens que podem exigir descarte seguro;

c) Muitas organizações oferecem serviços de coleta e eliminação de documentos, equipamentos meios de comunicação social, os cuidados devem ser tomados na escolha de uma contratação adequada com controles adequados e experiência;

d) O descarte de itens que possuem informações classificadas com um alto nível de confidencialidade devem ser registradas, sempre que possível, a fim de manter uma auditoria. Quando acumular mídias para descarte, deve-se considerar o efeito de agregação, que pode causar uma grande quantidade de informações consideradas não confidenciais como confidenciais.

   As informações podem tornarem-se acessíveis através do descarte ou reutilização descuidada do equipamento.

A Norma ISO27000 é muito importante para que se tenha um sistema de gestão de informação. Este sistema será a base para que uma organização administre seus ativos de informação e possa ter controle sobre o descarte e o ciclo de vida da informação. No próximo subitem iremos apresentar mais detalhadamente a classificação e o ciclo de vida da informação, com isto teremos uma melhor noção de como controlar os ativos de informação da empresa.

1.2. Classificação e ciclo de vida da informação

Como apresentado nas normas, ABNT NBR ISO/IEC 2001:2006 e ABNT NBR ISO/IEC 27002:2006, para a segurança dos ativos (informação) deve haver controles sobre estes, um destes controles é a classificação da informação.

Antes de se pensar em descarte de informações de forma segura, é necessário determinar a classificação e em qual estágio do ciclo de vida esta informação está vivendo. Apresentaremos agora os estágios da vida de uma informação até o momento de seu descarte, e a forma de classificação da informação, para determinar o quão crítica esta é, para assim, identificar qual informação deve ser destruída de forma segura, já que para isto é necessário investir tempo e muitas vezes dinheiro conforme veremos no capítulo sobre descarte.

1.2.1. Ciclo de vida da informação

Ciclo de vida da informação mostra todos os momentos vividos pela informação. Estes momentos são aqueles em que a informação é utilizada, seja por meios de armazenamento ou por acessos tecnológicos ou humanos (SÊMOLA, 2003). Assim o ciclo de vida pode ser dividido em quatro fases:

- **Manuseio** – Quando a informação é criada e manipulada, seja ao folhear um maço de papéis, ao digitar informações recém-geradas em uma aplicação Internet, ou ainda, ao utilizar sua senha de acesso para autenticação, por exemplo;
- **Armazenamento** – Quando a informação é armazenada, seja em um banco de dados compartilhado, em uma anotação de papel posteriormente postada em um arquivo de ferro, ou ainda, em uma mídia de disquete depositada na gaveta da mesa de trabalho, por exemplo;
- **Transporte** – Quando a informação é transportada, seja ao encaminhar informações por correio eletrônico, ao postar um documento via aparelho de fax, ou ainda, ao falar ao telefone uma informação confidencial, por exemplo;
- **Descarte** – Quando a informação é descartada, seja ao depositar na lixeira da empresa um material impresso, seja ao eliminar um arquivo eletrônico em seu computador ou servidor, ou ainda, ao descartar uma mídia que foi utilizada e apresentou falha na leitura.

1.2.2. Classificação da informação

A informação necessita de um cuidado especial dependendo de seu conteúdo, pois nem toda informação necessita de cuidados especiais, porém, existem algumas informações que são vitais para a empresa, onde o custo para manter a

informação segura é menor que sua divulgação. Para determinar qual informação necessita de maior cuidado é necessária a classificação da informação em níveis de prioridade, isto varia de empresa para empresa. Conforme (Wadlow, 2000), (Abreu, 2001) e (Boran, 1996) cada classificação tem um nível:

- **Pública** – Informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da empresa, a informação não é vital para a empresa;
- **Interna** – O acesso a esse tipo de informação deve ser evitado por pessoas externas à empresa, embora as consequências do uso não autorizado não sejam vitais à empresa. Sua integridade é importante, mesmo que não seja vital;
- **Confidencial** – Informação restrita aos limites da empresa, sua divulgação ou perda pode levar ao desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;
- **Secreta** – Informação crítica para as atividades da empresa, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas. A manipulação desse tipo de informação é vital para a companhia.

A engenharia da informação, que é um conjunto empresarial de disciplinas automatizadas, dirigido ao fornecimento da informação correta para a pessoa certa no tempo exato (Martin, 1991),(Feliciano Neto,1991), (Furlan, 1988) e (Higo, 1988) já demonstrava a importância da segurança da informação para as empresas.

A qualidade dos processos custa dinheiro, mas a falta dela custa muito mais. Pensando do mesmo modo, a segurança da informação custa dinheiro, mas não tê-la poderá custar muito mais (Crosby, 1992).

Ao final deste, tentamos passar ao leitor a importância dos processos e diretrizes de segurança da informação, para um processo de descarte de informações de forma segura. As normas ISO 27001 e 27002 são diretrizes que podem ser seguidas para implantação de uma equipe de segurança que faça a

administração de políticas e procedimentos, de classificação das informações, de controles de acesso lógicos ou físicos à informação e determinar o ciclo de vida da informação dos processos críticos onde o descarte seguro é necessário.

Apenas implantando uma boa gestão da informação é que se terá uma maior segurança quanto ao descarte seguro desta. Não adianta pensar na forma como a informação será descartada se não houver esta gestão antes.

1.3. PCI

Para demonstrar o grau de relevância de uma informação, dependendo da área de atuação, iremos apresentar o PCI DSS. O Padrão de Segurança de Dados (DSS) do Setor de Cartões de Pagamento (PCI) foi desenvolvido para incentivar e aprimorar a segurança dos dados do portador do cartão e facilitar a ampla adoção de medidas de segurança de dados consistentes no mundo todo. A norma foi elaborada para ser utilizada pelos avaliadores que realizam análises *in loco* para comerciantes e prestadores de serviços que devem comprovar a conformidade com o PCI DSS.

Os requisitos do PCI DSS se aplicam a todos os componentes do sistema que estejam incluídos ou conectados no ambiente dos dados do portador do cartão. O ambiente de dados do portador do cartão integra a rede que possui os dados do portador do cartão ou dados de autenticação confidencial, incluindo componentes de rede, servidores e aplicativos.

- Os componentes de rede podem incluir firewalls, chaves, roteadores, pontos de acesso wireless, mecanismos de rede e outros mecanismos de segurança;
- Os servidores podem incluir, Web, banco de dados, autenticação, e-mail, proxy, NTP (*network time protocol*) e DNS (*domain name server*);
- Os aplicativos podem incluir, todos os aplicativos adquiridos e personalizados, incluindo os que sejam internos e externos (Internet).

Segue abaixo o quadro com uma visão geral dos 12 requisitos exigidos pelo PCI DSS.

PCI Padrão de Segurança de Dados do PCI – Visão Geral Alto Nível	
Construir e Manter uma Rede Segura	
Requisito 1:	Instalar e manter uma configuração de firewall para proteger os dados do portador do cartão
Requisito 2:	Não usar padrões disponibilizados pelo fornecedor para senhas do sistema e outros parâmetros de segurança
Proteger os Dados do Portador do Cartão	
Requisito 3:	Proteger os dados armazenados do portador do cartão
Requisito 4:	Codificar a transmissão dos dados do portador do cartão em redes abertas e públicas
Manter um Programa de Gerenciamento de Vulnerabilidades	
Requisito 5:	Usar e atualizar regularmente o software antivírus
Requisito 6:	Desenvolver e manter sistemas e aplicativos seguros
Implementar Medidas de Controle de Acesso Rigorosas	
Requisito 7:	Restringir o acesso aos dados do portador do cartão de acordo com a necessidade de divulgação dos negócios
Requisito 8:	Atribuir um ID exclusivo para cada pessoa que tenha acesso a um computador
Requisito 9:	Restringir o acesso físico aos dados do portador do cartão
Monitorar e Testar as Redes Regularmente	
Requisito 10:	Acompanhar e monitorar todos os acessos com relação aos recursos da rede e aos dados do portador do cartão
Requisito 11:	Testar regularmente os sistemas e processos de segurança
Manter uma Política de Segurança de Informações	
Requisito 12:	Manter uma política que aborde a segurança das informações

Quadro 1 - Padrão de Segurança de Dados do PCI – Fonte: Security Standards Council (Jul,2009)

1.3.1. Informações de aplicabilidade do PCI DSS

O quadro abaixo mostra um exemplo dos dados comuns do portador de cartão em sua autenticação, ilustrando a permissão do armazenamento de cada elemento, e se existe a necessita de proteção do mesmo.

	Elemento de dados	Armazenamento permitido	Proteção necessária	PCI DSS nec. 3.4
Dados do portador do cartão	O número da conta principal (PAN)	Sim	Sim	Sim
	O nome do portador do cartão [1]	Sim	Sim [1]	Não
	Código de serviço [1]	Sim	Sim [1]	Não
	Data de vencimento [1]	Sim	Sim [1]	Não
Dados de autenticação confidenciais [2]	Dados da tarja magnética completa [3]	Não	N/D	N/D
	CAV2/CVC2/CVV2/CID	Não	N/D	N/D
	PIN/Bloqueio de PIN	Não	N/D	N/D

Quadro 2 – Informações de aplicabilidade PCI DSS – Fonte: Security Standards Council (Jul,2009)

Os elementos de dados devem ser protegidos se forem armazenados em conjunto com o PAN, essa proteção deve ser feita com base nos requisitos do PCI DSS para proteção geral do ambiente de dados do portador do cartão.

Outras legislações relacionadas à proteção de dados do consumidor, privacidade, roubo de identidade ou segurança de dados podem exigir uma proteção específica desses dados ou a divulgação adequada das práticas da empresa se os dados pessoais do cliente estiverem sendo coletados durante o curso dos negócios, porém este tratamento não se aplica ao PCI DSS se o PAN não for armazenado, processado ou transmitido.

1.3.2. Localização dos dados do portador do cartão e dos dados de autenticação confidencial

Os dados confidenciais de autenticação são formados pelos dados da tarja magnética, que são compostos por códigos, valores de validação do cartão e dados do PIN. O armazenamento dos dados é proibido, devido o grande valor que os mesmos possuem, pois pessoas mal-intencionadas podem gerar cartões de pagamento falsos e criar transações fraudulentas.

As figuras abaixo demonstram o local dos dados do portador do cartão e dos dados confidenciais de autenticação.

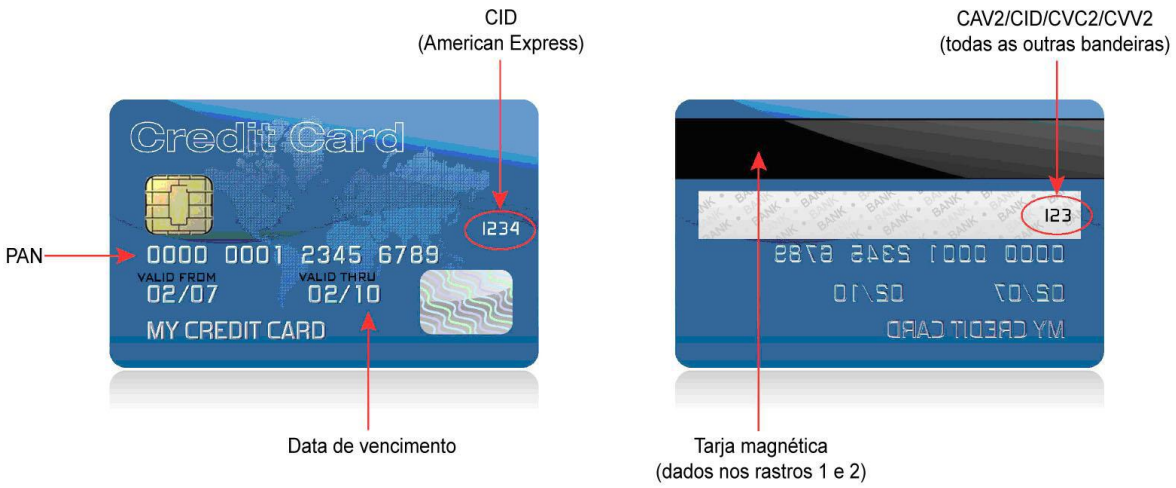

Figura 2 Cartão com a posição das informações do proprietário e informações confidenciais (Jul,2009)

- **Tarja Magnética** – Os dados codificados na fita magnética são utilizados para autorização durante a transação com o cartão. Esses dados também podem ser encontrados na imagem da tarja magnética, no chip ou em algum outro lugar do cartão. As entidades não podem reter esses dados após a autorização da transação. Os únicos elementos dos dados da tarja que podem ser retidos são o número da conta principal, o nome do portador do cartão, a data de vencimento e o código de serviço;
- **Código de validação do Cartão** - O cartão possui de três a quatro dígitos impressos à direita do painel de assinatura ou na frente do cartão de pagamento, estes números são usados para verificar transações com cartão não presente;
- **PIN -** Número de identificação pessoal inserido pelo portador do cartão durante uma transação com o cartão.

1.3.3. Requisito 3 – Proteger os dados armazenados do portador do cartão

Conforme citamos no quadro 1 – Padrão de Segurança de Dados do PCI, o PCI possui 12 requisitos essenciais para seu funcionamento, mas em nosso trabalho daremos foco apenas para o requisito 3, requisito que se refere a proteger os dados do portador do cartão.

Neste requisito as medidas de proteção como criptografia, truncamento e mascaramento são componentes essenciais da proteção de dados do portador do cartão. Caso um invasor consiga burlar outros controles de segurança da rede e obtiver acesso aos dados criptografados, sem as chaves criptográficas adequadas, os dados estarão ilegíveis e inutilizáveis.

Listaremos abaixo as melhores práticas para assegurar a proteção dos dados armazenados do portador do cartão.

- Manter o mínimo de armazenamento de dados do portador do cartão. Desenvolver uma política de retenção e descarte de dados;
- Não armazenar os dados de autenticação confidencial após a autorização, mesmo que estejam criptografados;

- Não armazenar o conteúdo completo de qualquer rastro da tarja magnética localizada na parte posterior do cartão, em um chip ou outro local;
- Não armazenar o código ou valor de verificação do cartão, este número possui de três a quatro dígitos impressos na frente ou atrás do cartão de pagamento, este numero é utilizado para verificar as transações do cartão;
- Mascarar o PAN quando exibido, pois a exibição do PAN completo em locais como telas de computador, recibos de cartão de pagamento, faxes ou extratos em papel podem fazer com que esses dados sejam obtidos por indivíduos não autorizados e usados de forma fraudulenta;
- Não armazenar o PIN ou o bloco de PIN criptografado. Caso ocorra o roubo dessa informação, indivíduos mal-intencionados podem executar transações de débito protegidas por senha nos caixas eletrônicos;
- *Hashing* de direção única com base na criptografia robusta. Funções de *hash* de direção única (como SHA-1) baseadas em uma criptografia robusta podem ser usadas para deixar os dados do portador do cartão ilegíveis. As funções de hashing são adequadas quando não houver necessidade de recuperar o número original, pois é irreversível;
- *Tokens* de índice e *pads* devem ser armazenados de forma segura. Os tokens de índice e pads também podem ser usados para tornar os dados do portador do cartão ilegíveis;
- As chaves criptográficas usadas para criptografar os dados do portador do cartão dever ser muito bem protegidas, para que não possam ser roubada e utilizada para decodificar os dados;
- As chaves criptográficas antigas que não são mais utilizadas devem ser destruídas de forma a não serem recuperadas. Caso seja necessário mantê-las para usar com dados arquivados e criptografados, elas deverão ser muito bem protegidas;
- O conhecimento compartilhado e o controle duplo das chaves de criptografia são utilizados para eliminar a possibilidade de uma pessoa ter acesso à chave inteira. Este procedimento é utilizado em sistemas manuais de criptografia por

chave, ou quando o gerenciamento de chaves não for implementado pelo produto da criptografia;

- As soluções de criptografia adotadas não devem levar em conta nem aceitar a substituição de chaves vindas de fontes não autorizadas ou de processos inesperados.

Para diminuir o risco de vazamento de informações (o que normalmente se resulta em fraude), a indústria de cartões de pagamento se preocupa e investe em segurança. A norma PCI DSS demonstra esta preocupação. Quando o dado está armazenado para uso, o mesmo deve ser mantido criptografado, quando não mais necessário o dado deve ser descartado, tornando a sua recuperação impossível. O mesmo quando se trata do cartão, nele estão contidos os dados altamente confidenciais e devem ser descartados de forma que evite a reconstrução da informação. No capítulo dois iremos apresentar as melhores formas de destruição das informações conforme o tipo de mídia (física (cartões) ou lógica (dados armazenados em sistema informatizados)).

1.4. MasterCard logical security requirements for card personalization bureaus

A *MasterCard Logical Security* possui requisitos de segurança de dados para os fornecedores e vendedores de cartões que oferecem produtos para cartões MasterCard. Essas exigências constituem a base da auditoria anual de segurança lógica e física , exigidas pelo programa de certificação da Global MasterCard.

Os requisitos de segurança lógica desta norma foram criados para enfrentar as ameaças à confidencialidade dos dados de personalização durante a transferência de dados, acesso, armazenamento e destruição, além de todos os aspectos relacionados com a gestão de chaves.

A incorporação de chips é a principal preocupação da segurança lógica, pois os requisitos LSP (*Logical Security Program*) são atualmente limitados ao chip de identificação dos produtos, a fim de monitorar a utilização de produtos que têm demonstrado o cumprimento de segurança aplicáveis (CAST) e o programa de qualidade (CQM).

Nos últimos anos, a preocupação com a segurança lógica gerou novas normas propiciando assim novas direções, devido o surgimento de novas tecnologias e a preocupação com as novas formas de ataque aos dados confidenciais, pois caso as ameaças não sejam devidamente tratadas, existe um risco crescente para o sistema de pagamento, para os emitentes e para os titulares de cartões.

1.4.1. Processo de auditoria

Como parte de sua auditoria de segurança lógica, os vendedores credenciados são convidados a responder a uma série de questões relacionadas aos seus processos e procedimentos, onde um auditor credenciado pela MasterCard analisará respostas descritas nos formulários acompanhado por um membro da empresa. Ao concluírem o relatório de auditoria, os detalhes de apoio serão encaminhados para a MasterCard e uma cópia do relatório é deixada com a empresa auditada.

1.4.2. Resultado de auditoria

Os relatórios de auditoria podem conter várias conclusões de não conformidade em relação aos requisitos solicitados na norma, quando isso ocorre a empresa é obrigada a desenvolver um plano de ação para corrigir eventuais conclusões. As ações planejadas para resolver cada constatação, devem ser explicitamente declaradas, juntamente com a data alvo quando a ação corretiva deve ser concluída. Geralmente, a não conformidade deve ser resolvida em um prazo de três meses após conclusão do trabalho de auditoria, mas este prazo pode variar dependendo da situação encontrada, pois quando a não conformidade for de entendimento grave que possa trazer um alto risco, este prazo pode diminuir.

Na figura abaixo podemos observar o sistema dos cartões auditados nas empresas certificadas pela MasterCard.

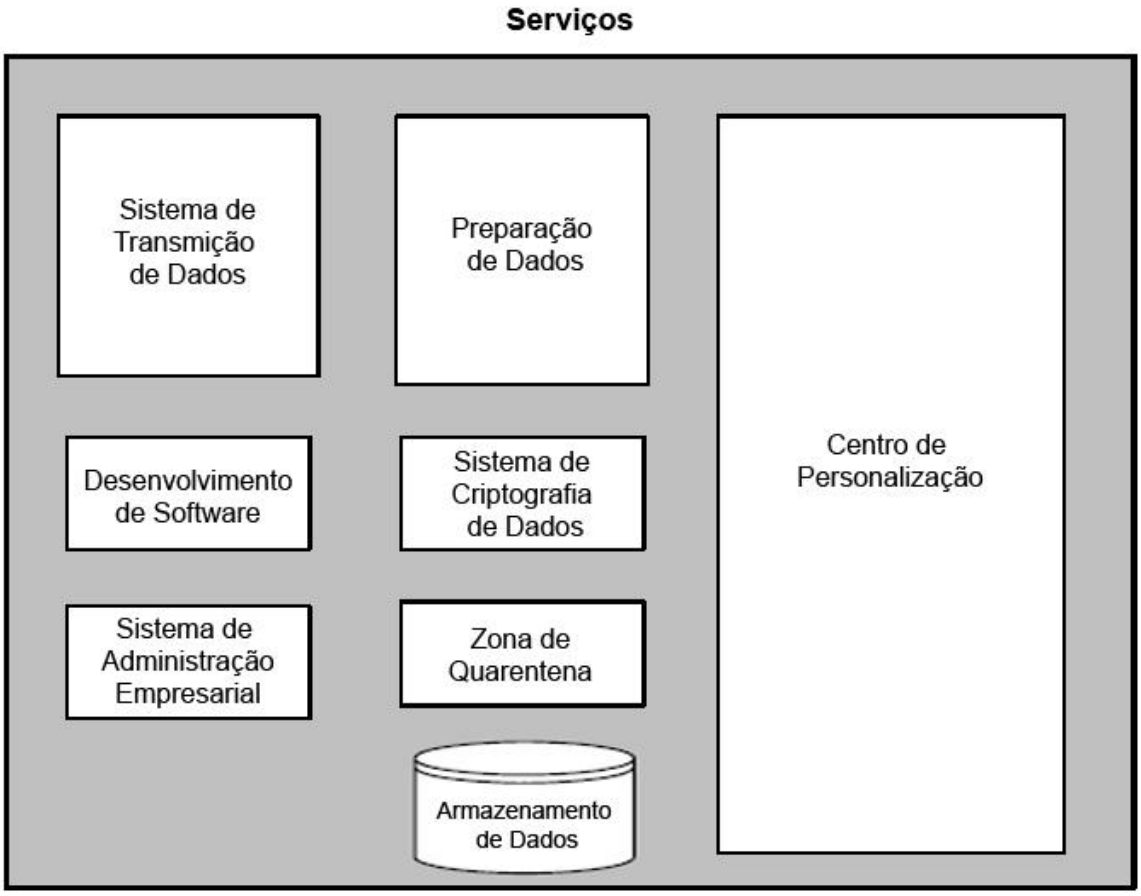

Figura 3 Modelo do sistema de funcionamento da Fabrica de cartões – Fonte: MasterCard Logical Security Requirements for Card Personalization Bureaus (Jun,2007)

1.4.3. Sistema de transmissão de dados

Os dados eletrônicos personalizados são enviados através de um formulário por links dedicados em um canal de comunicação público ou através da internet, para garantir a segurança dos dados os mesmos devem ser criptografados. O sistema de transmissão de dados no âmbito da empresa irá se comunicar com o emitente para a recepção de dados criptografados.

1.4.4. Sistema de criptografia de dados

Esta função fala sobre a decifragem dos dados de entrada e da criptografia de dados que são transferidos entre as instalações de fábrica. Para realizar este trabalho é necessário um Hardware de Segurança (HSM), onde encontram-se as chaves criptográficas necessárias para realizar as funções criptográficas. Em alguns casos, o sistema de criptografia de dados pode ser fortemente associado

com os nós de transporte de dados, pois podemos utilizar uma rede virtual privada [VPN], que já possui uma conexão criptografada fechada através de um firewall. Em outros casos, os dois podem ser fisicamente separados.

1.4.5. Zona de quarentena

A zona de quarentena é a área onde os dados de outras fábricas são isolados, o acesso aos dados são estritamente controlados.

1.4.6. Preparação de dados

A facilidade de preparação de dados é onde os dados de personalização estão preparados para a produção. Os dados podem ser decifrados, agrupados, reformatados, ou preparados para o uso de equipamento de produção dos cartões.

A facilidade de preparação de dados pode ser uma função autônoma, ou podem ser parte integrante do centro de personalização.

1.4.7. Centro de personalização

A personalização refere-se coletivamente aos processos que envolvem a transferência, por escrito, ou de codificação de qualquer tipo de sistema de pagamento, emitente ou do portador de cartão de dados específico para um cartão de pagamento.

- Personalização da gravura ou o cartão com informações do titular do cartão;
- Codificação da tarja magnética com os dados fornecidos pelo emitente;
- Escrita ou a transferência de dados emitente ou do portador de cartão específico para um chip incorporado ou embutido no cartão.

O termo “centro de personalização” refere-se ao ambiente seguro onde a personalização é feita.

O centro de personalização possui todos os equipamentos necessários para a produção do cartão, seu acesso é estritamente limitado ao pessoal autorizado, todas as atividades que ocorrem dentro do centro de personalização estão sujeitos a procedimentos e controles rigorosos. Sempre que o equipamento

utilizado, o mesmo está ligado na forma de uma rede, essa rede deve ser isolada de outros sistemas da Fábrica de Cartões.

1.4.8. Sistema de transmissão de dados

Em uma fábrica de cartões muitos departamentos são compostos por setores com instalações separadas, ou até mesmo setores em países distintos. Nestes casos, os dados de personalização deverão ser transferidos entre instalações seguras da empresa. A transmissão de dados é assumida como eletrônicos. No entanto, o transporte de dados Nível 2 ou Nível 3 pode ser realizado em mídia física (como o CD-ROM ou fita magnética).

A transferência dos dados pode ser de muitos para um, um para muitos ou muitos para muitos, independente do tipo de topologia, os mecanismos de transferência de dados devem ser estruturados e devem obedecer os requisitos de segurança exigidos pela MasterCard.

Segue abaixo uma figura que ilustra a arquitetura de um sistema de transmissão de dados, onde a caixa tracejada delimita o âmbito de aplicação desta função.

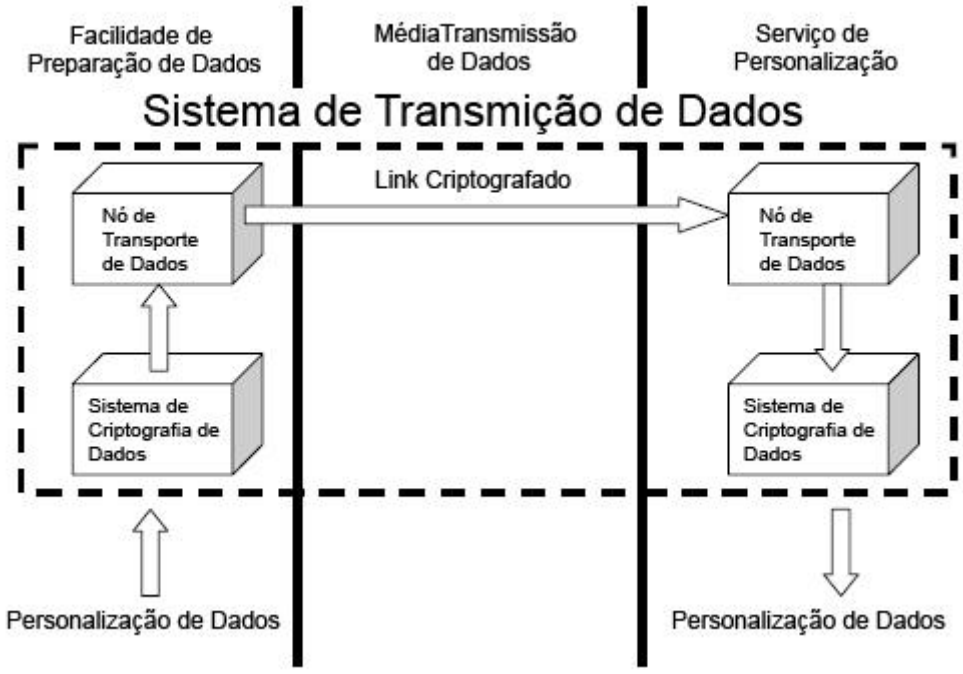

Figura 4 Modelo de transmissão de Dados - cartões – Fonte: MasterCard Logical Security Requirements for Card Personalization Bureaus (Jun, 2007)

1.4.9. Desenvolvimento de software

Esta função vai estar presente onde a fábrica de cartões desenvolve o seu próprio software para processar, transferir ou manipular os dados de personalização.

Os softwares de concepção e desenvolvimento devem seguir os procedimentos definidos, para garantir a segurança das informações no ambiente de produção, o acesso às informações deve ser estritamente controlada.

1.4.10. Sistema de administração empresarial

Os sistemas de negócios e administração são sistemas semelhantes ao de folha de pagamento, estoque e processamento de pedidos, estes sistemas permitem que a fábrica de carões possa gerir seus negócios com mais facilidade e agilidade.

Embora normalmente não participam com personalização de cartões, estes sistemas normalmente suportam conexões à redes externas e estão dentro do escopo da auditoria.

1.4.11. Armazenamento de dados

Esta função fornece um meio seguro para armazenar dados sensíveis, antes ou depois da personalização do cartão. Os requisitos de segurança se aplicam a qualquer tipo dado Nível 2 e Nível 3, que encontra-se armazenado em mídia. Segue abaixo a lista com alguns requisitos de segurança:

- Definir os procedimentos de auditoria e de segurança que controlam o acesso, manuseio e uso de todos os meios de armazenamento;
- Criar um registro que documente o acesso e a responsabilização por todos os meios de armazenamento. O registro deve conter a data da última utilização e do usuário autorizado;
- Fitas e discos magnéticos devem ser apresentados de uma forma ordenada;
- Quando não está em uso, todas as fitas devem ser mantidas em suas embalagens;
- Criptografar todos dados Nível 2 e Nível 3 armazenados na mídia de backup;

- Todas as mídias de armazenamento como memórias, fitas, discos e ambores, devem ser devidamente assinaladas e tratadas;
- Deve-se usar etiquetas invioláveis em todos os suportes que contém dados de nível 3.

1.4.12. Desclassificação e destruição de dados

Os requisitos de destruição de dados nesta se aplicam a dados em uma mídia que está no final do seu período de utilização. A desclassificação se aplica aos meios de comunicação que está sendo reutilizado em um ambiente menos seguro, onde os procedimentos padrão de eliminação de dados podem permitir a recuperação dos dados (normalmente porque a supressão remove apenas os ponteiros endereço sem destruir fisicamente os dados dentro da mídia).

Os dados armazenados em mídia, como fitas magnéticas que são reutilizados no mesmo ambiente de segurança elevado e sujeitos a medidas de segurança de dados originais podem ser apagados em vez de destruir. Estes requisitos se aplicam a qualquer Nível 2 ou Nível 3 de dados que são apagados, destruídos ou desclassificados. Segue abaixo a lista com alguns requisitos de segurança para a destruição de dados confidenciais:

- Definir e implementar procedimentos para a exclusão, a destruição e a desclassificação de todos os Níveis 2 e 3 de dados;
- Todos os dados do portador do cartão (chip utilizado para a personalização ou codificação de tarja magnética, incluindo backups) devem ser apagados no prazo de 30 dias a contar da conclusão da personalização do cartão;
- É necessário a existência de log de auditoria à prova de falsificação, com a data de recebimento dos dados do portador do cartão, a data que foi concluída a personalização e o prazo da retenção de dados;
- Para a destruição de quaisquer dados nível 2: A destruição manual deve ser realizada sob controle dual;
- A exclusão automática deve ser sujeita a procedimentos de verificação que fornecem a confirmação de que os dados foram destruídos;

- A destruição de dados de nível 3 deve ser realizada sob controle duplo, e um registro mantido e assinado confirmando o que foi destruído, e quando;
- Todos os métodos utilizados para a destruição de dados devem fornecer confiança razoável, garantindo que os dados que foram destruídos não possam mais serem recuperados;
- Se o nível de classificação de dados foi alterado para um nível mais baixo, então você deve definir um procedimento para garantir que a mídia de armazenamento tenha sido efetivamente apagada ou neutralizada antes de ser transferido para um novo uso. (Isto inclui a alteração do estatuto para um nível de segurança mais baixo ou mudar o destino da mídia);
- Este procedimento deve exigir o apagamento completo ou desmagnetização de mídia de armazenamento usada anteriormente;
- É necessário implementar processos para garantir que os CDs regraváveis e DVDs que contêm Nível 2 e Nível 3 de dados não possam ser reclassificados para o nível de segurança mais baixo ou ser reatribuído a um uso diferente.

1.4.13. Varredura de vulnerabilidades

Em geral, as empresas de personalização possuem ambientes totalmente isolados, onde o transporte dos dados é realizado em links dedicados, garantindo que os dados não serão expostos a ameaças de redes externas. No entanto, existem algumas empresas que buscam reduzir os custos de comunicação utilizando as opções públicas, expondo os dados à ameaças externas que derivam da Internet e outras redes públicas.

O objetivo do escaneamento de vulnerabilidades é ajudar a proteger os dados do cartão de serem acessadas por pessoas externas não autorizadas. Portanto, se em quaisquer circunstâncias, as transferências dos dados de um cartão da empresa ocorrer pela Internet, esta conexão estará sujeita as exigências de varredura de vulnerabilidades, pois todos os computadores que estão acessíveis a partir da Internet devem seguir os requisitos.

No nosso entendimento, a norma de segurança lógica da MasterCard é mais robusta que o PCI DSS, abrange com mais detalhes aspectos de segurança da informação e descarte/desclassificação da informação. A partir do próximo

capítulo iremos apresentar os tipos de mídias e a melhor forma de descarte da informação, além de demonstrar ferramentas de uso livre para descarte de informações em meios eletrônicos de forma segura. Que podem ser usadas para o descarte seguro de informações do portador de cartões, exigido pelo PCI e pela MasterCard.

2. MÍDIAS E O PRINCÍPIO DA GRAVAÇÃO.

Desde os primórdios a comunicação é uma necessidade do homem, como diz o artigo “Do Papel ao PDA” da revista BP Magazine, a comunicação se fazia pela conversa e palavras ditas ao léu. Com o passar do tempo o ser humano descobriu a necessidade de registrar o que se conversava o que acontecia no dia-a-dia da sociedade, daí então surgiu a escrita 5000 anos atrás. Desde então não param de surgir formas de se registrar seus negócios, suas histórias, a existência do ser humano. Como diz o artigo da revista BP Magazine “O registro de informações evoluiu das ancestrais plaquetas de argila, passando pelos papiros egípcios repletos de hieróglifos, pelo pergaminho, pelos milhares de rolos de texto guardados – e depois perdidos – na mítica Biblioteca de Alexandria, chegando ao códice, aos livros de horas medievais, ao texto impresso com tipos móveis de Gutenberg, às várias formas de impressão que advieram a partir daí, até chegar aos escritos internáuticos, ao computador e à palavra cibernética. A humanidade empreendeu uma longa viagem durante os séculos para chegar a era da tecnologia.”

Nos dias atuais, com o surgimento da informática, utilizamos novas técnicas para elaborar e armazenar documentos, não precisamos mais escrever diretamente no papel, os documentos podem ser criados e armazenados no próprio computador ou em dispositivos de armazenamento como veremos a seguir.

Com base no estudo de MONTE e LOPES (2004), abaixo temos alguns suportes de informações com tecnologias variadas para armazenamento e como estas funcionam:

2.1. Mídias óticas

- ***Compact Disc Read Only Memory - (CDROMs)*** – Em português significa Disco Compacto só para Leitura, são geralmente utilizados para armazenar softwares de instalação, porém sua capacidade é inferior ao DVD. São fabricados nos tamanhos de 14, 12 e 5¼ polegadas, e sua capacidade de

armazenamento varia de 650MB a 700MB. O grande problema desses discos é que os fabricantes não possuem uma norma padronizadora de tecnologia, onde a maior parte dos equipamentos de leitura/gravação e discos sejam de tecnologia proprietária, fazendo a capacidade dos discos mudar de acordo com fabricantes e com o seu tamanho. Podem apresentar diferentes colorações: esverdeadas, azuis ou amareladas, por exemplo.

Figura 5 CDROM
Fonte: Cultura Geek Alti1040 (2009)

O CD contém uma longa linha de sulcos escritos de uma forma helicoidal no disco, seu extremo corresponde '1's binários. Cada sulco tem aproximadamente 0.5 mícron de largura e 0.83 mícron de comprimento, sua pista está separada da outra por 1.6 mícron. São gravados do centro para o exterior e sua parte mais interna não contêm dados, pois os dados são armazenados numa região anelada compreendida entre os valores de 4,6 cm e 11,7 cm de diâmetro.

- ***Digital Versatile Disc* (*DVD*)**– Sua aparência física lembra muito com um CD, utiliza o mesmo princípio de armazenamento, porém sua capacidade de armazenamento é superior em até 7 (sete) vezes. Usa menores deformações microscopias que refletem o raio laser na superfície refletora.

Figura 6 DVDROM
Fonte: Cultura Geek Alti1040 (2009)

- ***Blu-ray Disc (BD)*** - Seu nome deriva do fato de adotar um feixe de luz laser de cor violeta (λ = *405 nm*) em vez do infravermelho usado pelo CD (λ = *780 nm*) ou do vermelho de DVD (λ = *650 nm*) comuns. Geralmente utilizado para vídeo de alta definição e armazenamento de dados de alta densidade. O BD é o sucessor do DVD, sua capacidade de armazenamento varia de 25 a 50 *Gigabytes* permitindo assim armazenar filmes até 1080p Full HD de até 4 horas sem perdas na qualidade.

Figura 7 Blu-Ray

Fonte: Cultura Geek Alti1040 (2010)

Quando se faz um comparativo entre mídias, podemos observar qual possui o menor comprimento de onda, que permite reduzir as marcas que desviam o raio laser, pois essas precisam ser da ordem do comprimento de onda da luz, possibilitando assim um aumento da capacidade em discos de dimensões semelhantes.

A figura abaixo mostra comparativamente o laser vermelho focalizado em um CD, em um DVD-Vídeo (com comprimento de onda menor, ainda na cor vermelha) e o laser azul em disco do tipo Blu-ray:

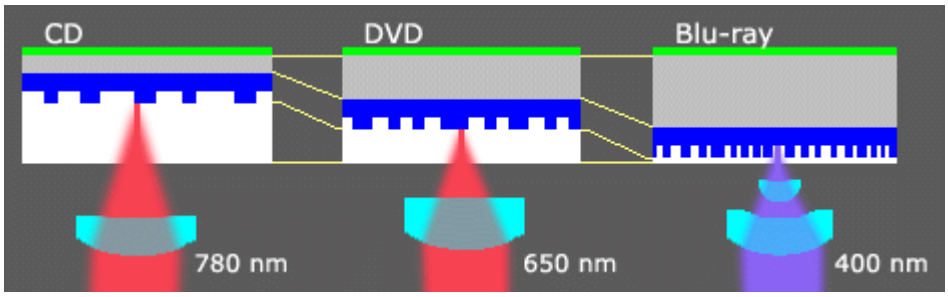

Figura 8 Comparativo entre CDROM, DVDROM e Blu-Ray

Fonte: Fazendo Vídeo (2009)

Os CDs e DVDs possuem lasers de gravação e leitura com comprimento entre 780 e 650 nanômetros, no entanto, com o uso de um laser com comprimento de ondas mais curtas de 400 nanômetros, é possível gravar pontos muito menores nos discos, aumentando assim sua densidade. Esta tecnologia é utilizada em mídias Blu-Ray.

Seguindo a lógica acima, quanto maior a capacidade de armazenamento da mídia, menor deve ser a fragmentação para a destruição da mídia, conforme mencionado no capítulo de destruição física.

2.2. Mídias magnéticas

- **Disco Rígido** - Popularmente chamado de *Winchester* ou *HD,* são unidades de disco que possuem uma grande variedade de tamanhos para armazenamento de dados. Geralmente são utilizadas para a instalação de sistemas operacionais e para armazenamentos de arquivos que necessitam de constantes consultas.

Figura 9 Disco Rígido
Fonte: Morimoto (2000)

A superfície dos discos magnéticos de um HD é dividida em trilhas e setores. Cada trilha recebe um endereçamento próprio e elas são divididas nos setores, que são pequenos trechos de 512 bytes onde os dados ficam armazenados. Como um HD é formado por até 4 discos e os braços de leitura não são independentes, todos os braços movem para a mesma trilha em todos os discos. Com isso as trilhas passam a se chamar cilindros, pois o braços vão ler a mesma trilha em cada um dos discos.

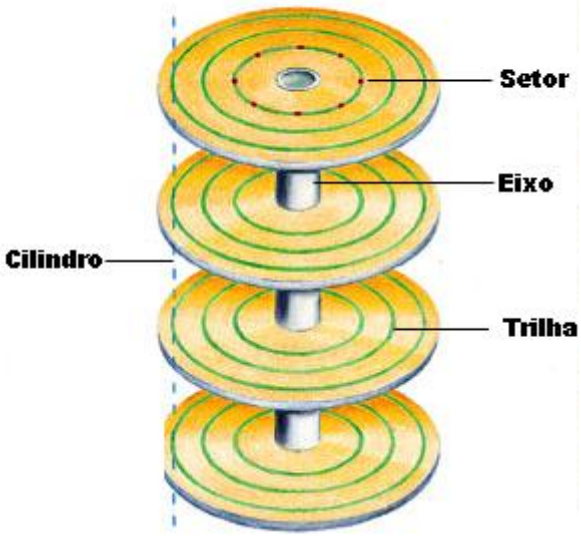

Figura 10 Setores, trilhas e cilindros
Fonte: Morimoto (2000)

Os primeiros discos rígidos utilizavam a mesma tecnologia de mídia magnética usadas em disquetes, chamada ***COATED MEDIA***, que além de permitir uma baixa densidade de gravação, durava pouco tempo em funcionamento.

Os discos atuais utilizam mídia laminada (*Plated mídia*), uma mídia mais densa, de qualidade muito superior, que permite a enorme capacidade de armazenamento dos discos modernos.

A cabeça de leitura e gravação é composta por um dispositivo de gravação e outro de leitura. O dispositivo de gravação é como um eletroímã que utiliza a eletricidade para criar o campo magnético que é utilizado na gravação.

Já o dispositivo de leitura faz o processo oposto, ele passa pelos bits gravados captando o campo magnético emitido através de um processo de indução (HDs antigos) ou resistência (HDs atuais). Além disso, para não interferir no processo de leitura dos campos, o dispositivo de leitura é protegido por um escudo eletromagnético, permitindo a leitura apenas do campo que está sendo lido.

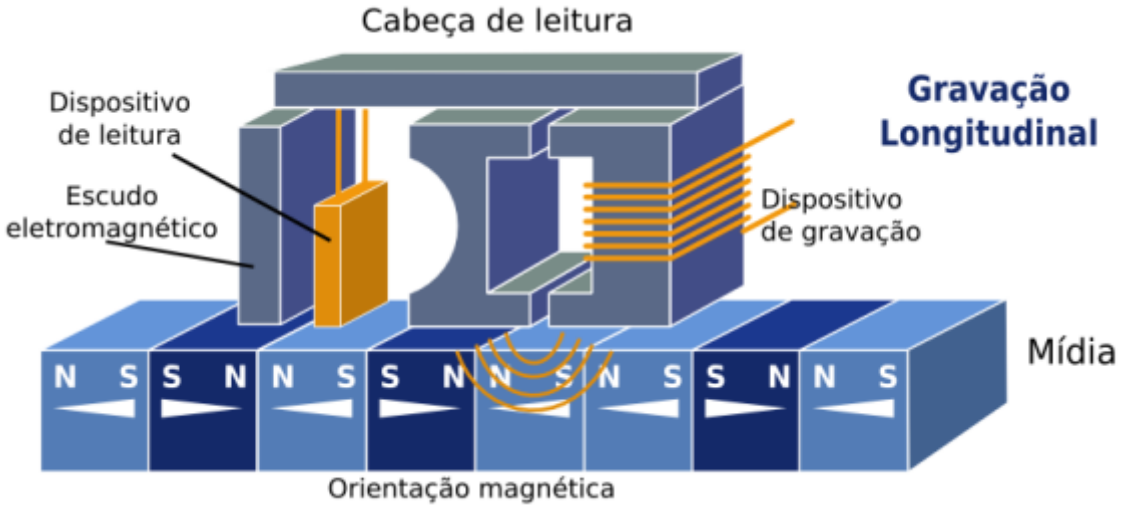

Figura 11 Gravação Longitudinal

Fonte: Morimoto (2000)

Um problema que surgiu com o passar do tempo foi o espaço físico para a gravação magnética, o que se tornou um obstáculo para o aumento da capacidade de armazenamento. A partir de certo ponto, a área de gravação (Chamada de *magnetic element*) torna-se tão pequena que a orientação magnética dos bits pode ser alterada pela própria energia térmica do ambiente em que está.

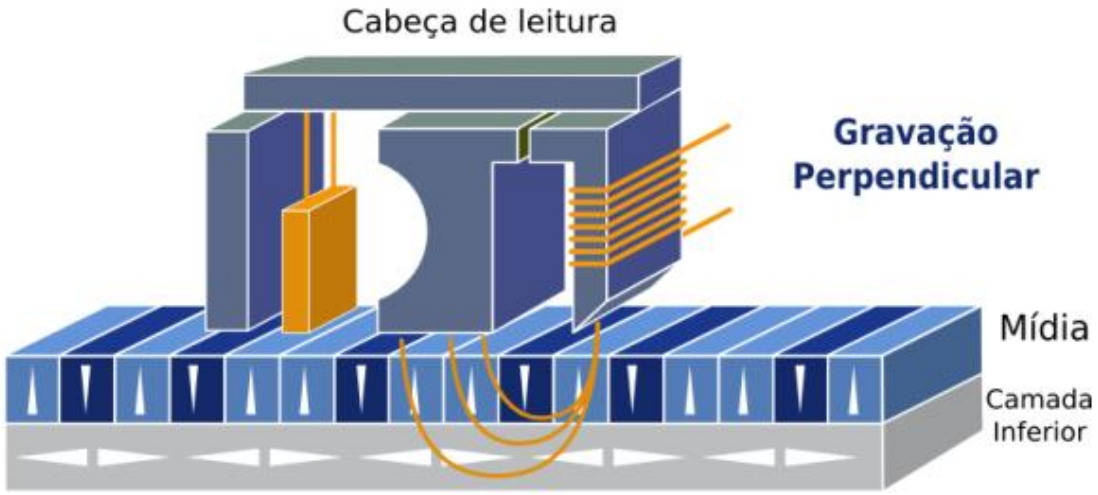

Figura 12 Gravação Longitudinal 2

Fonte: Morimoto (2000)

A Tecnologia de Gravação utilizada nos HDs até a primeira metade de 2007 é chamada Gravação Longitudinal, onde a orientação magnética dos bits é determinada na horizontal. Com esta tecnologia ficou cada vez mais difícil

aumentar a capacidade, sem que a gravação se torne insistente, acelerou-se a migração para a tecnologia de gravação perpendicular, onde a orientação magnética passa a ser na vertical, aumentando bastante a capacidade de armazenamento.

- **Disquete -** É um disco de mídia magnética removível, para armazenamento de dados. O termo equivalente em inglês é *floppy-disk*, significando disco flexível. Pode ter o tamanho de 3,5 polegadas com capacidade de armazenamento de 720 KB (*DD* = *Double Density*) até 5,76 MB (*EDS* = *Extra Density Super*), embora o mais comum atualmente seja 1,44 MB (*HD* = *High Density*), ou 5,25 polegadas com armazenamento de 160 KB (*Single Side* = *Face Simples*) até 1,2 MB.

Figura 13 Disquete
Fonte: Obtido através de Fotografia (2010)

- **Fitas Magnéticas** – São tiras plásticas contínuas cobertas por material magnético, são removíveis, possuem resistência mecânica, apresentam homogeneidade magnética e grande capacidade de armazenamento, geralmente são utilizadas como backup de dados.

  Este dispositivo possui cabeçotes em posições fixas com um eletroímã que magnetiza o meio magnético, após receber uma corrente elétrica no sentido correspondente ao cabeçote de leitura, este mecanismo faz com que as fitas girem para que o cabeçote possa acessar a fita.

  As fitas magnéticas são atualmente divididas em tipos, tipo I, II ou III. Essa divisão é realizada através do fator de coercividade (a medida do campo magnético reverso necessário para zerar a magnetização da fita).

FITA TIPO I – Possui a coercividade abaixo de 350 oersteds (unidade medida da força magnetizante para produzir uma força magnética desejada através uma superfície).

FITA TIPO II - Possui um fator coercividade entre 350 e 750 oersteds.

FITA TIPO III - Comumente referida como uma fita de alta energia (fita de 4 ou 8mm são exemplos) possui fator coercividade entre 750 e 1700 oersteds.

- **Fitas em carretel (Tape Reel) – Tipo III:** São fitas magnéticas, geralmente com 12,7 mm de largura, espessura de 0, 048 mm e comprimento de 194 a 780 m. A informação é registrada em pontos magnetizáveis ao longo de sete ou nove pistas, possui densidade de dados variando de 200 a 6250 bpi (bits por polegada);

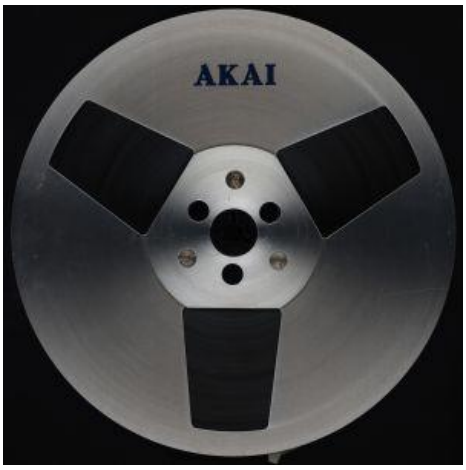

Figura 14 Fita Carretel
Fonte: Stock.Xchng (2010)

- **Cartucho de fita (*Tape Cartridge*) – TIPO II:** é uma fita magnética encapsulada em um cartucho plástico ou metálico, semelhante às fitas de áudio e vídeo. O encapsulamento serve de proteção para o meio de armazenamento de dados barato, comparando a outros meios e possui grande capacidade de armazenamento (vários gigabytes). Normalmente, são apresentados dois valores para a capacidade de armazenamento das fitas: é a capacidade de armazenamento sem compressão dos dados e o outro, a capacidade após a compressão dos dados.

Figura 15 Tape Cartridge
Fonte: Tape and Media (2010)

- **Fitas Half-inch – TIPO III:** são fitas magnéticas com 12,65 mm de largura, relativamente baratas, mas que necessitam de drives caros.

  Exemplo: **DLT (Digital Linear Tape)**, com capacidade de 20 GB até 80 GB, dimensão 105,8 X 105,4 mm.

Figura 16 Fita Half-Inch (DLT)
Fonte: 1 Giga (2010)

- **Fitas Quarter-inch Cartridge (QIC**) **– Tipo III**: são fitas magnéticas com ¼ de largura, relativamente baratas e que suportam altas taxas de transferências de dados. Estão entre as fitas mais populares para backup em computadores pessoais. Exemplo: **Travan**, com capacidade de 400 MB até 20 GB e dimensão de cartuchos de 76,2 X 50,8 mm.

Figura 17 Fita Quarter-Inch Cartridge (Travan)
Fonte: Webdados (2010)

- **Fitas 8 mm Helical-scan – TIPO III:** são fitas magnéticas com 8 mm de largura que usam a mesma tecnologia das fitas de videocassete. Exigem drives relativamente caros e possuem baixas taxas de transferências.

  Exemplo: **VXA**, com capacidade de 24 GB até 160 GB e dimensão de cartuchos de 95 X 62,5 mm.

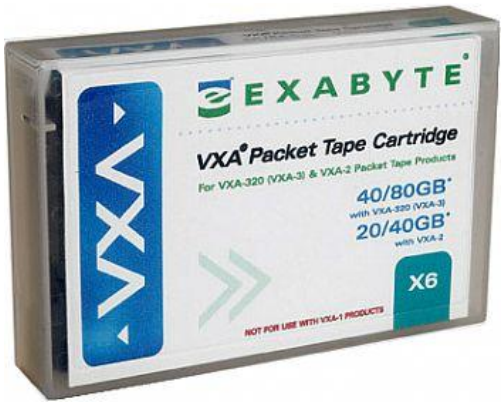

Figura 18 Fita 8 mm Helical-Scan (VXA)
Fonte: Tech CD (2010)

- **Fitas 4 mm DAT – TIPO I:** são fitas magnéticas com 4 mm de largura, foram criadas pela SONY, em 1987. Essas fitas necessitam de drives relativamente caros e possuem baixas taxas de transferências. Elas utilizam o formato **DDS (Digital Data Storage)** para armazenar os dados.

  Exemplo: **DAT DDS 1,** com capacidade de 4 GB, com dimensões dos cartuchos de 73 X 54 mm.

Figura 19 Fita 4 mm (DAT)
Fonte: Sul Mídia (2010)

- **Fita cassete – TIPO I:** é um padrão de fita para gravação de áudio lançado oficialmente em 1963, invenção da empresa holandesa Philips. A fita era basicamente constituída por dois carretéis, a fita magnética e todo o mecanismo de movimento são alojados em uma caixa plástica, isto facilitava o manuseio e a utilização, permitindo que a fita fosse colocada ou retirada em qualquer ponto da reprodução ou gravação sem a necessidade de ser rebobinada como as fitas de rolo. Com um tamanho de 10 cm x 7 cm, a caixa plástica permitia uma enorme economia de espaço em relação às fitas tradicionais.

Figura 20 Fita K7
Fonte: Flickr (2010)

2.3. Memórias

- **Cartão de Memória (*Memória Flash*) -** dispositivo de armazenamento móvel utilizado para transportar arquivos, geralmente são utilizados em câmeras digitais, telefones celulares, mp3 players e notebooks, sua funcionalidade é

semelhante à memória RAM de um computador, mas suas propriedades fazem com que os dados não sejam perdidos com a falta de energia, porém ao se tratar de um dispositivo móvel, existe o risco de perda das informações armazenadas com a perda do cartão, trazendo assim prejuízos incalculáveis dependo do tipo de informação armazenada.

Figura 21 Cartão de Memória
Fonte: Xoppi (2010)

- ***Pen-Drive* (*Flash Drive*)** - dispositivo de armazenamento móvel utilizado para transportar arquivos, sua conexão é realizada através da porta USB tipo A. A facilidade de manuseio e grande capacidade do dispositivo o torna um dos equipamentos móveis mais utilizados, porém semelhante ao cartão de memória, a perda do mesmo pode trazer prejuízos incalculáveis dependo do tipo de informação armazenada.

Figura 22 Pen Drive
Fonte: Pelfusion (2010)

- ***Dynamic Random Access Memory (DRAM)*** - é um tipo de memória de acesso aleatório que armazena cada bit de dados em um capacitor separado dentro de um circuito integrado. Ao contrário de memória flash a DRAM é uma

memória volátil, ou seja, ela perde seus dados quando a alimentação é removida.

Esse tipo de memória geralmente é utilizado em consoles de vídeo game (Playstation, Xbox 360 e Wii), laptop, notebook e computadores da estação de trabalho.

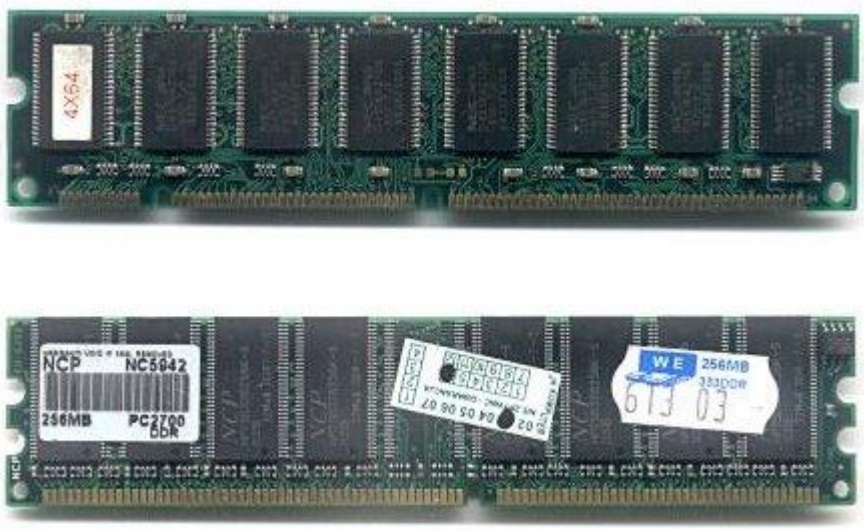

Figura 23 Memória DRAM
Fonte: Amit Bhawani (2010)

- ***Electronically Alterable Programmable Read Only Memory (EAPROM)*** - memória só de leitura, normalmente conhecida pela sigla ROM, utilizada como meios de armazenamento em computadores e outros dispositivos eletrônicos. Como os dados armazenados na memória ROM não podem ser modificados (pelo menos não muito rápido e fácil), é usado principalmente para distribuir firmware, software que está intimamente ligado a um hardware específico.

  Em seu sentido mais estrito, refere-se apenas ROM máscara (o mais antigo tipo de ROM de estado sólido), que é fabricado com os dados desejados permanentemente armazenados nele e, portanto, nunca pode ser modificado. No entanto, os tipos mais modernos, como flash EPROM e EEPROM podem ser apagados e reprogramados várias vezes, eles ainda são descritos como "memória só de leitura (ROM). Seu processo de reprogramação é pouco frequente, relativamente lento e muitas vezes não permitem o acesso aleatório, escreve às posições de memória de forma individual.

Figura 24 Memória EPROM
Fonte: Ice Fusion (2010)

- ***Magnetic Bubble Memory*** - é um tipo de memória de computador não-volátil que usa uma camada fina de um material magnético para armazenar pequenas áreas magnetizadas, conhecida como bolhas ou domínios, cada bolha armazena um bit de dados. Essa tecnologia começou em 1970, mas falhou comercialmente devido a queda de preços dos discos rígidos nos anos 1980.

Figura 25 Memória Magnetic Bubble
Fonte: Sina Sihon (2010)

- ***Magnetic core memory*** - memória de núcleo magnético é uma forma primitiva de memória de acesso aleatório. Ele usa um pequeno anel magnético, através do qual os fios são encadeados para armazenar informações, através da polaridade do campo magnético que eles contêm. Essa memória é muitas vezes chamada de memória principal ou informalmente de núcleo.

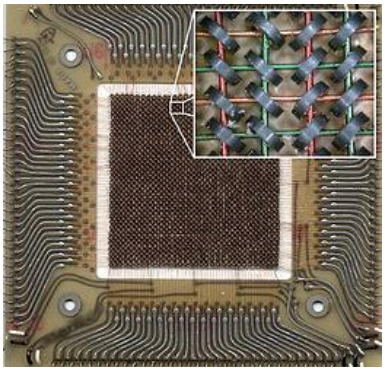

Figura 26 Memória magnetic Core
Fonte: Computer History (2010)

- ***Static Random Access Memory (SRAM)*** - é uma memória de semicondutor, onde a palavra *static* indica que, ao contrário da RAM dinâmica (DRAM), não precisam ser periodicamente atualizadas. A SRAM utiliza circuito biestável, mas é ainda volátil, no sentido convencional de que os dados são perdidos quando a memória não é alimentada.

Figura 27 Memória Static Random Access
Fonte: Perangkat Komputer (2010)

2.4. Outras mídias de armazenamento

- **Cartão de Pagamentos** - é utilizado para fazer pagamentos eletrônicos. É formado por um cartão de plástico que contém o nome do portador, número do cartão e data de validade, além de, no verso, ter um campo para assinatura do cliente o número de segurança (CVV2) e a tarja magnética (geralmente preta). A maioria dos cartões de crédito possuem forma e tamanho padronizados, como especificado pelo padrão ISO.

Figura 28 Cartão de Credito
Fonte: Zazzle (2010)

- **Fita Perfurada –** Os meios perfurados foram os primeiros meios de armazenamento de dados utilizados nos sistemas de computação (baseados nos princípios criados por Jacquard em 1805).

  Os dados eram armazenados em papéis perfurados, não havendo possibilidade de alteração, a não ser se os papéis fossem perfurados novamente. A leitura era realizada por dispositivos que possuíam escovas metálicas e discos metálicos. Nos furos, havia contato entre eles e a detecção dos dados.

  Os meios perfurados podiam ser cartões perfurados (cartolina retangular) ou fitas perfuradas (fita continua de papel, nos quais a posição da perfuração indicava o dado armazenado). Os cartões perfurados necessitavam de unidades de perfuração e unidades de leitura. Já as fitas perfuradas possuíam um único dispositivo que realizava as duas operações. Esses tipos de sistemas foram utilizados até bem recentemente.

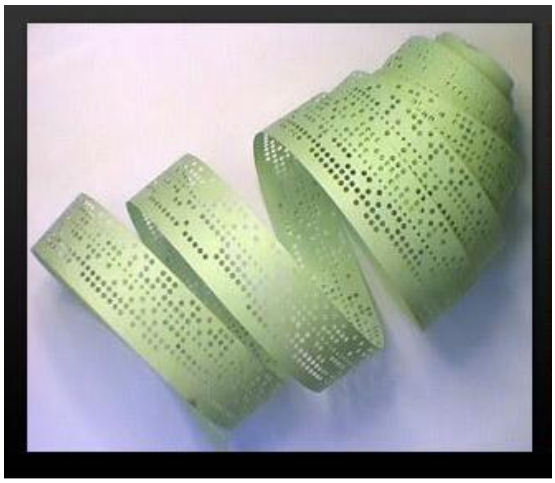

Figura 29 Fita Perfurada
Fonte: Áudio List (2010)

Como apresentando, a quantidade de mídias para armazenamento de informações é bem extensa, mas podemos subdividir basicamente em quatro tipos pelas suas características:

- **Magnéticas**: Discos Rígidos, Fitas Magnéticas;
- **Óticos**: CDs, DVDs, *Blu Rays*;
- **Memórias sólidas**: Qualquer tipo de *Memory Disk* e *PenDrive;*
- **Físicas**: Pedaço de Papel, Agenda, Livro, etc.

Trataremos no próximo capítulo qual o método adequado para o descarte seguro, dependendo das características de cada tipo de mídia.

3. MÉTODOS PARA DESCARTE SEGURO DE DADOS

Com a classificação da informação e com o ciclo de vida da informação, temos uma base para determinar o quão crítica é a informação e com os tipos de mídias mais utilizados, mostrados no capítulo anterior, podemos dar mais atenção para o descarte seguro das informações críticas e suas mídias. Este capítulo demonstra quais as formas utilizadas para o descarte seguro de dados, isto é, descarte de forma com que as informações não possam ser recuperadas. Este descarte pode ser lógico ou físico, no caso da necessidade do descarte físico, iremos explanar sobre o que fazer com os resíduos gerados, existe hoje diversas empresas que dão um destino correto a eles, conforme normas e licenças da CETESB e certificadas por outros órgãos como ISO 14000.

O termo “saneamento dos dados” é utilizado quando é necessária a total destruição dos dados de uma mídia (HD, CD, Fita Magnética, etc., conforme vimos no subcapítulo anterior) impossibilitando a recuperação das informações contidas nela.

No caso dos dados armazenados em discos rígidos de computadores, quando um dado é removido através de um simples delete ou uma forma rápida de exclusão de algum sistema operacional ou de gerenciamento de arquivos (Windows Explorer, linha de comando do MS-DOS, Gerenciados de fitas backup, etc.), ele não é excluído da mídia onde estava, apenas é apagado o ponteiro (índice) onde constava que aquele dado existia em um determinado setor da mídia. Para sua real eliminação este dado deve ser sobrescrito diversas vezes, impossibilitando a sua leitura, ou até mesmo utilizar outros métodos como desmagnetizar ou destruir completamente a mídia (fragmentação, pulverização, incineração).

Mas não só em computadores, informações importantes são armazenadas, a Agência Nacional de Segurança dos Estados Unidos (NSA) disponibiliza guias e documentações que ajudam a entender de que forma devemos definir a forma de destruição dos dados, dependendo da informação e dependendo da mídia onde a informação está armazenada.

A NSA basicamente divide em dois tipos de mídias:

- **Cópia Impressa:** É a representação física da informação como, impressão em papel, fax e fitas de impressão, placas entre outras formas semelhantes.
- **Eletrônica:** É representada por bit e bytes contidos em discos rígidos, memórias RAM, memórias ROM, discos, dispositivos de armazenamento (*pen drive, memory cards*, etc.), computadores, equipamentos de rede entre outros.

Segundo o guia de saneamento da NSA, as cópias impressas são as mídias menos controladas, estas informações são muitas vezes encontradas em lixeiras e locais de reciclagem.

Como as mídias e suas tecnologias estão sempre em evolução, a NSA afirma que, é preciso ter foco na informação gravada na mídia para definir a melhor forma de Saneamento.

Ainda segundo o guia, o saneamento pode ser dividido em quatro categorias:

Eliminação: Ato de descartar as mídias sem nenhum outro tipo de saneamento, isto é mais comum em descarte de papéis sem informações que causem algum dano organizacional, financeiro, pessoal ou qualquer outro dano;

Apagar: Apagar a informação é o nível de saneamento de mídia que deve proteger a confidencialidade da informação e um ataque comum, feito através de comandos de teclado. Ao apagar a informação ela não deve ser recuperada por nenhuma ferramenta de recuperação de dados. O mais comum é a sobrescrita da informação com métodos como Gutmann e DoD.M5220.22M;

Purging: Este nível consiste em proteger a informação contra ataques avançados (ataques de laboratório). Em discos rígidos padrão ATA, fabricados após o ano de 2001, este nível é possível através da desmagnetização do disco por um desmagnetizador, este deve gerar um campo magnético que seja capaz de apagar os dados. Além de ser uma forma mais rápida para sanear dados em discos com grande quantidade de informações gravadas, também pode ser utilizado para desmagnetizar disquetes e fitas magnéticas;

Destruição: Destruição da mídia é a última forma de saneamento. Após este processo ela não mais poderá ser utilizada. Dentre os métodos de destruição estão: desintegração, incineração, pulverização e derretimento.

Explanaremos sobre alguns métodos que se enquadram nos tipos de saneamento descritos. Mas antes reforçamos um ponto do Manual da NSA “A chave para decidir como gerenciar a mídia na organização é primeiro considerar a informação, e então a mídia (...) isso conduzira a uma decisão de como lidar com a mídia”.

Então antes de pensar na forma de descarte ou saneamento de uma mídia, pense primeiro na informação que precisa ser descartada.

3.1. Método Gutmann

O método Gutmann, criado por Peter Gutmann, 2001, método utilizado na destruição de dados em disco rígido. Determina-se que para a eliminação segura dos dados em um disco rígido é necessário sobre escrever o bloco do disco várias vezes com padrões aleatórios e em diferentes frequências para que o campo magnético oscile e o mais rápido possível e não deixe vestígios magnéticos.

Tabela 1 – Descrição dos passos utilizados para sanear um disco

Passo	Binário	Hexadecimal
1	(Random)	(Random)
2	(Random)	(Random)
3	(Random)	(Random)
4	(Random)	(Random)
5	01010101 01010101 01010101	55 55 55
6	10101010 10101010 10101010	AA AA AA
7	10010010 01001001 00100100	92 49 24
8	01001001 00100100 10010010	49 24 92
9	00100100 10010010 01001001	24 92 49
10	00000000 00000000 00000000	00 00 00
11	00010001 00010001 00010001	11 11 11
12	00100010 00100010 00100010	22 22 22
13	00110011 00110011 00110011	33 33 33
14	01000100 01000100 01000100	44 44 44
15	01010101 01010101 01010101	55 55 55
16	01100110 01100110 01100110	66 66 66
17	01110111 01110111 01110111	77 77 77
18	10001000 10001000 10001000	88 88 88
19	10011001 10011001 10011001	99 99 99
20	10101010 10101010 10101010	AA AA AA
21	10111011 10111011 10111011	BB BB BB
22	11001100 11001100 11001100	CC CC CC
23	11011101 11011101 11011101	DD DD DD
24	11101110 11101110 11101110	EE EE EE
25	11111111 11111111 11111111	FF FF FF
26	10010010 01001001 00100100	92 49 24
27	01001001 00100100 10010010	49 24 92
28	00100100 10010010 01001001	24 92 49
29	01101101 10110110 11011011	6D B6 DB
30	10110110 11011011 01101101	B6 DB 6D
31	11011011 01101101 10110110	DB 6D B6
32	(Random)	(Random)
33	(Random)	(Random)
34	(Random)	(Random)
35	(Random)	(Random)

Fonte: (Petter Gutmann,1996)

Conforme a tabela acima, o sistema que utilizar o método de Gutmann deverá, nos quatro primeiros passos, sobrescrever o bloco com dados randômicos, após isso do quinto ao trigésimo primeiro passo, o bloco deverá receber os dados especificados em cada passo e do trigésimo segundo ao trigésimo quinto, novamente o sistema deverá sobrescrever o bloco com dados randômicos.

Este é o mais robusto, pois tem mais passos a serem executados, com isso também é o mais lento. É recomendável quando as informações são de extrema importância ou com poucos bytes.

3.2. Método VSITR

Este método foi criado com base na política de classificação de Tecnologia da informação (*Verschlusssachen-IT-Richtlinien* - VSITR) criado pelo Departamento Alemão de Segurança da Informação (BSI - *Bundesamt für Sicherheit in der Informationstechnik*), um método utilizado na destruição de dados em disco rígido, propondo que para a remoção segura das informações, cada bloco seja sobrescrito em sete passos:

- Passo 1:
  - Sobrescreve todos os blocos com 0's (zeros);
- Passo 2:
  - Sobrescreve todos os blocos com 1's (uns);
- Passo 3:
  - Sobrescreve todos os blocos com 0's (zeros);
- Passo 4:
  - Sobrescreve todos os blocos com 1's (uns);
- Passo 5:
  - Sobrescreve todos os blocos com 0's (zeros);
- Passo 6:
  - Sobrescreve todos os blocos com 1's (uns);
- Passo 7:
  - Sobrescreve todos os blocos com 0's (zeros).

Este método é utilizado nas principais ferramentas do mercado e é considerado seguro e um pouco menos lento que o método de Gutmann.

3.3. Método DOD 5220.22M

Muitas informações da internet dão este método como uma norma do departamento de defesa dos Estados Unidos, mas na verdade é uma técnica que utiliza alguns passos da matriz de saneamento da agência de defesa da segurança do departamento de Defesa dos Estados Unidos.

US DoD 5220.22-M (8-306./E,C & E) (7 passes)

Este método executará o procedimento **“e”**, **“c”** e depois o **“e”** novamente (vide Matriz de Saneamento Anexo A):

- **e** – Cada dado sobrescrito deve residir na memória por um período maior que o dado anterior residia.
- **c** – Sobrescrever todos os locais endereçáveis com um único caractere utilizando uma ferramenta de sobrescrita aprovada.
- **e** – Cada dado sobrescrito deve residir na memória por um período maior que o dado anterior residia.

US DoD 5220.22-M (8-306./E) (3 passes)

Este método executará apenas o procedimento:

- **e** – Cada dado sobrescrito deve residir na memória por um período maior que o dado anterior residia.

Consideramos que este método, que é utilizado pelo departamento de defesa dos Estados Unidos, está no mesmo nível do VSITR em termos de velocidade e execução do descarte seguro. Ele também é encontrado nas principais ferramentas do mercado.

3.4. Desmagnetizar

Um desmagnetizador é extremamente efetivo na limpeza de qualquer mídia magnética (disco rígido, disquete e fita magnética) e com o uso desse equipamento é possível retorná-los a seu estado inicial, sem nenhuma informação.

Segundo a NSA (NATIONAL SECURITY AGENCY), Agência de Segurança dos Estados Unidos, dispositivos de armazenamento magnético são definidos por sua coercividade que é medida em Oe (*Oersteds*). A NSA divulga uma lista com os equipamentos de desmagnetização que são avaliados conforme o

requerimento para a destruição dos dados armazenados em dispositivos magnéticos.

Figura 30 Desmagnetizadores TIPO I,II e III
Fonte: Data Securityinc

3.4.1. Fitas magnéticas

Segundo o Guia de Saneamento de Dados da NSA, fitas magnéticas podem ser apagadas utilizando desmagnetizadores de fita tipo I, II ou III aprovados. A NSA divulga uma lista chamada *Evaluated Products List – Degausser* (http://www.nsa.gov/ia/government/index.cfm) onde são listados os equipamentos aprovados para desmagnetizar fitas magnéticas.

Abaixo um quadro que demonstra os tipos de desmagnetizadores e o tipo de mídia que é apagada por ele.

Se o desmagnetizador é:	Então o Nível de Coercividade é:	Isto saneará as seguintes Mídias			
		Tipo I	Tipo II	Tipo IIA	Tipo III
Tipo I	0-350 Oe	S	C	C	C
Tipo II	351-750 Oe	S	S	C	C
Tipo II Estendido	751-1000 Oe	S	S	S	C
Tipo III	1001-1700 Oe e Acima	S	S	S	S

Quadro 3 – Tipo de Desmagnetizador e nível de coercividade
Fonte: NSA – NISPOM (2008)

S – A mídia está totalmente saneada e pode ser descartada ou reutilizada.

C – A mídia é considerada limpa e retém as informações originais.

3.4.2. Discos magnéticos (disco rígido)

Para efetuar a desmagnetização de um disco, é preciso saber qual a coercividade necessária para anular a magnetização presente no disco. A NSA

divulga uma lista chamada *Evaluated Products List – Degausser*, nela existe informações sobre dispositivos que realizam desmagnetização e suas potências e também um quadro demonstrando quais as potências necessárias para desmagnetizar diversos dispositivos de armazenamento magnético, conforme quadro abaixo:

Dispositivo de Armazenamento Magnético	**Oe**
9-Track Reel-to-Reel Computer tape	300
TK50, TK70	350
3480, 3490E	520
SLR1, SLR2, TR-1, DC2120, DC6150, DC6525	550
SLR3, SLR4, SLR5, TR-3, DC9100, DC9120, ID-1, SLR24, SLR32, TR-4, ADR30, ADR50, ADR2-120	900
Mammoth 8mm, AIT-1 8mm, VXA-1 8mm	1320
M2 Mammoth2 8mm, VXA-2 8mm 230m	1350
AIT-2 8mm	1380
AIT-3 8mm, AIT-4 8mm, S-AIT-1 ½”	1400
Redwood SD-3	1515
DLTtape III, DLTtape IIIXT	1540
DD-2 19mm	1550
DTF-1	1579
DDS1: 4mm60m, 4mm90m	1590
D8: 8mm 112m, 8mm 160m	1600
MagstarMP: 3570-B, 3570-C, 3570-C/XL, Magstar: 3590, 3590-E, STK-9840, STK-T9940	1625
TR-5, SLR40, SLR50, SLR60, SLR100, TR-7 (Travan 40 GB), SLR75, SLR140	1650
DDS2 4mm 120m	1750
DLTtape IV, DLTtape VS1, NCTP, DD-2QD (Quad Density) 19mm, LTO-Ultrium1	1850
SuperDLTtape1	1900
LTO-Ultrium2	2150
DDS3 4mm 125m	2250
DTF-2	2300
DDS4 4mm 150m, DAT-72 4mm 170m	2350
Enterprise 3592, STK-T10000 (T10K)	2500
Super DLTtape II	2600
DLTtape S4, LTO-Ultrium3	2650
LTO-4	2710
5 ¼” 360KB DD Minidisk	300
3.5” 720KB DD Microdisk, 5 ¼” 1.2MB HD Minidisk	650
3.5” 1.44MB HD Microdisk	720
SuperDisk 120MB	1500
Zip 100 MB Disk	1550
Zip 250 MB Disk, Zip 750 MB Disk	2250

Quadro 4 – Relação entre Coercividade e a mídia
Fonte: NSA - Evaluated Products List – Degausser (2009)

Para desmagnetização de discos rígidos, a NSA disponibiliza um gráfico que mostra a potência necessária de coercividade conforme o ano de fabricação,

quanto mais novo, maior a potência necessária. Os discos rígidos são separados em Longitudinais e Perpendiculares:

- Longitudinal: a superfície magnética do disco fica organizada de forma horizontal (paralela) ao plano do disco.
- Perpendicular: a superfície magnética do disco é organizada de forma vertical (perpendicular) ao plano do disco.

Os discos Longitudinais foram os fabricados até o ano de 2006, após este ano começaram a ser produzidos os discos perpendiculares devido à falta de espaço físico para armazenamento dos bits. Os dois tipos ficaram no mercado por algum tempo ainda.

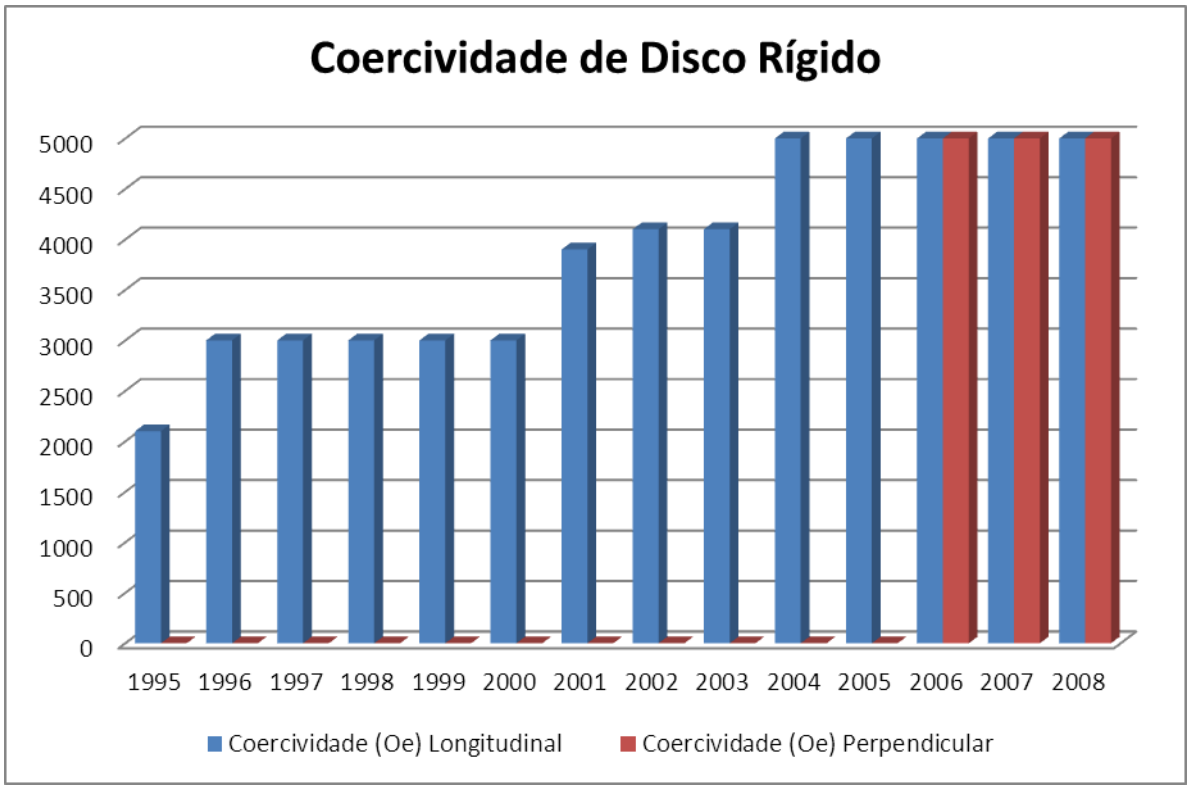

Gráfico 1. – Relação entre Coercividade e a mídia
Fonte: NSA - Evaluated Products List – Degausser (2009)

O custo para a compra de um desmagnetizador varia conforme a potência, o tamanho e a especificação que o mesmo atende. No site *Data Devices International* existe uma grande gama de aparelhos para as mais variadas funções. Os preços variam de U$ 95,00 a U$ 41.900,00, fora manutenção.

Para empresas que não tem uma demanda que justifique a compra de um equipamento deste, esta mesma empresa trabalha com o serviço de desmagnetização, com o custo de U$ 10,00 por cartucho de fita magnética ou U$ 25,00 por disco rígido. Outras empresas como Data Security Inc e Verity Systems também vendem desmagnetizadores, mas os custos não estão disponíveis no site, apenas após contato com um representante.

3.5. Destruição física.

Em casos em que a desmagnetização e o saneamento de dados não forem aceitos por normas vigentes, como forma de destruição de dados classificados como secretos ou confidenciais, restará então a destruição física do meio onde o dado está armazenado. O departamento de defesa dos Estados Unidos propõe um modelo de destruição de dados na recomendação DoD 5220.22M, onde afirma que caso os dados sejam secretos as mídias de armazenamento devem ser incineradas, pulverizadas ou desintegradas.

- Pulverização: quebrar a mídia até ela ser totalmente reduzida a pó.
- Incineração: queimar a mídia até ela ser totalmente reduzida a cinzas.
- Desintegração: aplicar ácido na superfície do disco.

  Estes métodos são destinados para a total destruição da mídia e devem ser executados por uma empresa prestadora de serviço de destruição de metais ou de incineração com as normas para a execução destas atividades de forma eficaz e segura.

- Fragmentar: Despedaçar a mídia em pedaços pequenos.

  Este método pode ser utilizado em mídias flexíveis como papéis e disquetes. O fragmento gerado por este método deve ser de um tamanho suficiente que não seja possível a recuperação da informação.

- Manufatura reversa: Segundo Akiko Ribeiro (2009), este processo consiste em descaracterizar o produto (monitores, placas, Discos Rigidos, entre outros eletrônicos) visando a reciclagem de suas matérias primas e uma destinação final aos materiais não recicláveis.

Este método, apesar de não estar explicito no DOD5220.22M, pode ser considerado, pois primeiramente é feita a separação das peças internas, conforme suas matérias primas e após isto é executada a trituração destas peças.

Para todos os métodos citados, em nossa visão, devem ser tomadas algumas precauções de segurança. Antes do envio deste material para empresas de gerenciamento de resíduos, recomendamos o uso de ferramenta de sobrescrita e a assinatura de um termo de confidencialidade com a empresa.

Foram realizadas pesquisas de preços com empresas do setor de gerenciamento de resíduos e a empresa TWM Ambiental foi a empresa com o custo mais baixo pesquisado, ela cobra para incineração de discos rígido e fitas magnéticas R$ 3,00 por quilo do material, fora o transporte. Valores atuais.

De todos os métodos de descarte físicos apresentados a manufatura reversa, na nossa visão, é a forma que menos agride o ambiente além de ter um melhor custo benefício. Este método separa as matérias primas e recicla o que é possível e descarta o que não é, tem um custo de R$ 1,30 por quilo, a partir de 312 quilos de material. Menos do que isso é cobrado o valor fechado, R$ 400,00. Valores atuais.

A seguir, apresentaremos algumas preocupações ambientais que empresas devem ter com os resíduos gerados.

3.6. Preocupações ambientais com os resíduos gerados.

As questões referentes ao ambiente têm se tornado uma preocupação crescente, devido à diminuição da qualidade de vida e aos riscos oferecidos à saúde humana. Carletto e Bazzo (2007) caracterizam esses problemas como contaminações do ar, água e solo, esgotamento dos recursos naturais, uso intensivo de produtos químicos e perda da biodiversidade. Isto indica que novas tecnologias e o intenso desenvolvimento dos setores agrícola e industrial são os principais responsáveis por estes desastres sócio-ambientais.

É necessária a busca de empresas especializadas e com as certificações e licenças de órgãos que regulam empresas que interferem no meio ambiente,

para a realização da destruição física de meios que contenham dados confidenciais.

Abaixo alguns itens necessários às empresas em São Paulo:

- CETESB
  - **Licença de Instalação de Unidade de Incineração**: Documento expedido pela CETESB que permite a instalação da fonte poluidora em local determinado, desde que as disposições legais sejam cumpridas. Alguns fatores como, características do local e critérios ambientais são analisados.
  - **Licença de operação de Unidade de Incineração**: documento que autoriza o funcionamento da fonte poluidora, que antes deve receber a Licença de Instalação. Esta licença não será expedida em caso de exigências da Licença de Instalação não serem cumpridas ou a atividade em questão não ser correspondente à solicitada na Licença de Instalação.
- Alvará de Vigilância sanitária.
- Alvará da Secretaria de Estado da Habitação
- Certificado ISO 14000
  - Este certificado identifica que a empresa possui um Sistema de Gestão Ambiental e procedimentos demonstrando que a empresa está comprometida com o meio ambiente.

Para facilitar a busca por pontos para descarte de lixos eletrônicos, a Secretaria Estadual do meio Ambiente e o Instituto Sérgio Mota lançaram o site E-Lixo Maps (http://www.e-lixo.org/). Através deste site você consegue saber qual é o ponto de descarte de lixo eletrônico mais próximo, basta informar o seu CEP.

Antes de entregar o seu material para empresas de descarte, estude os métodos que a mesma adota para o descarte e exija a assinatura de um termo de sigilo.

3.7. Situações de maior atenção com o descarte.

Devemos ter uma maior atenção em algumas situações em que as informações podem ser descartadas sem a devida preocupação, em estudo de OLTSIK e BIGGAR (2006), uma empresa que armazene dados sigilosos em estações de

trabalho teria como obrigação excluir de forma segura todos os dados quando submetidos a:

- **Fim de aluguel**: Quando um contrato de aluguel de equipamento se esgotar, é necessário apagar todas as informações contidas em suas mídias antes de serem devolvidas ao fornecedor.
- **Fim da vida útil**: Antes de desfazerem de equipamentos obsoletos, é necessária a eliminação das informações. Muitas vezes esses equipamentos são recolocados no mercado, possibilitando que pessoas não autorizadas tenham acesso às informações.
- **Uso para outro objetivo:** Quando uma estação de trabalho é realocada, por exemplo, de um setor a outro, a sua confidencialidade pode ser comprometida. Por isso é necessário garantir que os dados sejam efetivamente removidos.
- **Quebra/conserto:** Quando a estação apresenta algum problema, ou a mídia em que estejam contidos dados importantes falha, é importante a destruição da informação para que empresas terceirizadas ou outros setores não tenham acesso a conteúdos confidenciais.
- **Terceirização:** A medida de remoção completa dos dados em um ambiente terceirizado também é importante, pois garante a confidencialidade dos dados mesmo após o fim de um contrato ou até mesmo no caso de uma realocação.

Conforme estudo de GARFINKEL e SHELAT (2003), mesmo existindo várias ferramentas no mercado para descartar dados com segurança, sem que eles possam ser recuperados, no mercado ainda é encontrado diversos discos usados contendo informações que poderiam ser confidenciais, abaixo algumas citações dos autores para esta negligência com os dados:

- **Falta de conhecimento:** O responsável pelos arquivos não tem o conhecimento da forma como funciona um sistema de arquivos;
- **Falta de preocupação com o problema:** O Problema é conhecido pela pessoa, mas é tratado com descaso;

- **Falta de preocupação com os dados:** O problema é conhecido pela pessoa, ela está ciente da importância que os dados têm, porém não se importa com a confidencialidade destes dados;
- **Não saber mensurar o problema:** O responsável pelas informações, ao entregar seu disco para alguém, ele não acredita que o seu disco será vasculhado por este alguém;
- **Pressa:** Ao tentar apagar suas informações, a pessoa acaba não realizando todos os procedimentos para assegurar que estas informações foram completamente apagadas;
- **Falta de ferramentas:** A pessoa não possui ferramentas apropriadas para realizar um descarte completo das informações;
- **Incompetência:** O indivíduo possui as ferramentas, porém não tem a competência necessária de realizar os procedimentos;
- **Erros nas ferramentas:** A ferramenta escolhida para o descarte seguro dos dados, por alguma razão, apresenta algum erro, e este erro às vezes acaba passando despercebido pelo utilizador da ferramenta;
- **Falha de Hardware:** Durante a remoção dos arquivos, o computador pode apresentar alguma falha de hardware, obrigando a troca do disco, tornando esse procedimento bastante demorado. Ou o utilizador pensa que o defeito está no disco, quando na verdade não está.

É importante notar que os autores tocam em pontos rotineiros dentro de uma empresa e que muitas vezes passam despercebidos. Por isso é importante a implantação de divulgação de procedimentos, contendo instruções de descarte de informações de forma segura, que minimizem o risco de vazamento de informações através de mídias (principalmente Discos Rígidos) descartadas ou retiradas do local seguro.

Com isso segue um quadro relacionando o tipo de mídia e o método de descarte que pelo nosso estudo, entendemos ser o melhor:

Tipo	Método primário	Método secundário	Método terciário	É possível reutilizar a mídia?
Mídias Magnéticas	Sobrescrita (Gutmann, VSITR, DOD)	Desmagnetizar	Destruição Física (Incineração, Fragmentação, Pulverização)	Sim, some se utilizado os métodos primário e secundário
Mídias Óticas	Destruição Física (Incineração, Fragmentação, Pulverização)	Não Disponível	Não Disponível	Não
Memórias	Sobrescrita (Gutmann, VSITR, DOD)	Destruição Física (Incineração, Fragmentação, Pulverização)	Não Disponível	Sim, somente se utilizado o método primário
Papéis	Destruição Física (Incineração, Fragmentação, Pulverização)	Não Disponível	Não Disponível	Não

Quadro 5 – Tipo de mídia e o melhor método

Agora que foram apresentados os principais meios de descarte, demonstraremos no próximo capítulo um estudo de caso com ferramentas gratuitas e de fácil localização na internet. Estas ferramentas possuem os principais métodos apresentados para descarte de informações em meios magnéticos através da sobrescrita de dados.

Os métodos de desmagnetização e destruição física das mídias não serão apresentados no estudo de caso a seguir.

4. ESTUDO DE CASO

Neste capítulo demonstraremos um estudo de caso, onde realizaremos o descarte de arquivos em um disco rígido através de ferramentas de sobrescrita de dados e recuperação em mídias digitais. Com isso demonstraremos um dos métodos do nosso trabalho para o melhor entendimento da forma como informações são apagadas das mídias digitais. Os softwares escolhidos foram o Eraser, software desenvolvido pela própria empresa Eraser, o software Recuva, desenvolvido pela empresa Piriform e o software Glary Utilities, desenvolvido pela empresa Glary Soft . A escolha pela utilização destes softwares foi pelo fato de serem softwares gratuitos e de fácil localização na internet e por possuírem os métodos apresentados no trabalho.

4.1. Software Eraser

Sempre que um dado é apagado ele não é removido fisicamente do disco rígido, apenas é apagado o índice com a localização da área onde ele se encontra. Caso a área do disco onde o dado se encontrava for reescrita pelo sistema com algum outro dado, o dado anterior será realmente removido. É com base neste conceito que as ferramentas de recuperação de dados funcionam, tudo depende do fato de já ter sido escrita ou não uma informação nesse local.

Conforme o manual de usuário do *Active Eraser,* a forma de atuação do Eraser é escrever diversas vezes nas zonas de forma aleatória, tornando assim impossível a recuperação original do dado, mesmo recorrendo a métodos mais complexos que envolvem a manipulação de campos magnéticos nos pratos dos discos. O método que adotamos para realizar este estudo de caso foi o método de Gutmann, um dos métodos descritos em nosso trabalho, onde as zonas do disco rígido foram reescritas em 35 passos.

O que distingue o Eraser de outras ferramentas é a possibilidade de agendamento de tarefas na eliminação permanente dos dados, desde a eliminação sempre que iniciamos o PC até ao agendamento periódico numa base diária ou semanal.

4.2. Software Recuva

Como citamos anteriormente, quando apagamos um arquivo do disco rígido, ele não é removido realmente, apenas o índice que levava a este arquivo é apagado, isso permite que softwares como o RECUVA possa realizar a recuperação deles. Além de recuperar arquivos deletados o software permite também o descarte seguro destes arquivos deletados, reescrevendo diversas vezes o setor em que o arquivo foi encontrado.

Conforme o capítulo 3 deste documento, as mídias óticas armazenam os dados através do feixe de laser que queima sua superfície, por isso o RECUVA não recupera informações neste tipo de mídia (CDs, DVDs e outros suportes ópticos), podemos utilizá-lo somente em discos rígidos, cartões de memória e pen drives por se tratarem de armazenamento em meio magnético ou sólido.

4.3. Software Glary Utilities

O Software Glary Utilities é uma ferramenta mais completa que os softwares ERASER e RECUVA, na questão de manutenção do Sistema Operacional, pois possui alternativas para Limpar o Registro, Corrigir Atalho, Remover Programa e Otimizar Memória, porém no quesito do descarte seguro das informações possui somente o método Dod. 5220.22-M. Conforme descrito anteriormente, o software não pode ser utilizado em mídias como CDs, DVDs e outros suportes ópticos.

As informações foram retiradas do site do fabricante *Glary Soft.*

4.4. Estudo de caso 1 – Descarte de dados através do software Eraser

Segue abaixo o demonstrativo de nossa atividade através das evidências coletadas, onde na figura demonstramos uma estrutura de pasta e arquivos que serão removidos através da ferramenta Eraser.

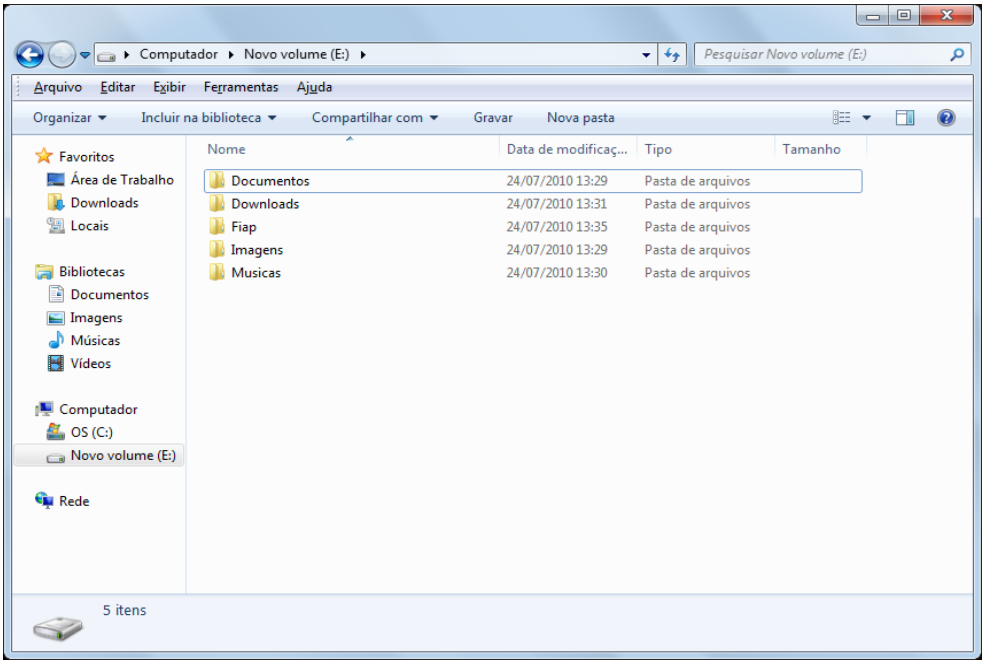

Figura 31 – Estudo de Caso 1 – Estrutura de pastas e arquivos – Obtido em análise realizado com o Software

Iniciaremos o procedimento de remoção permanente das informações, através do agendamento de uma tarefa dentro do software Eraser.

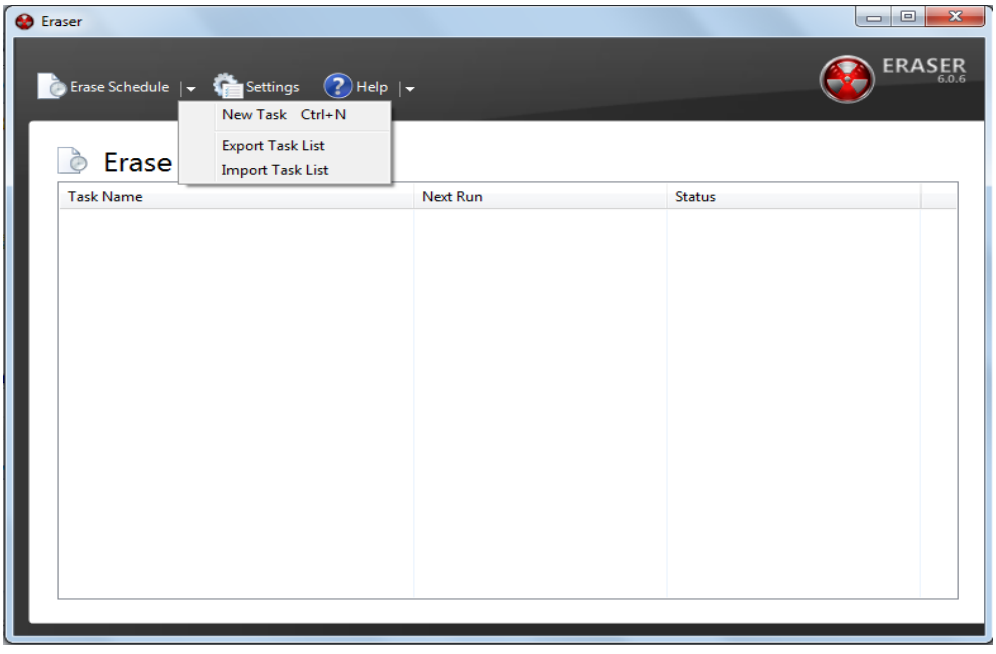

Figura 32 – Estudo de Caso 1 – Iniciando o processo de destruição dos dados – Obtido em análise realizada com software

Para realizarmos o processo, é preciso selecionar o volume onde encontra-se os dados que serão removidos de forma segura, garantindo o seu descarte permanente, clicaremos no **OK** para continuar o procedimento.

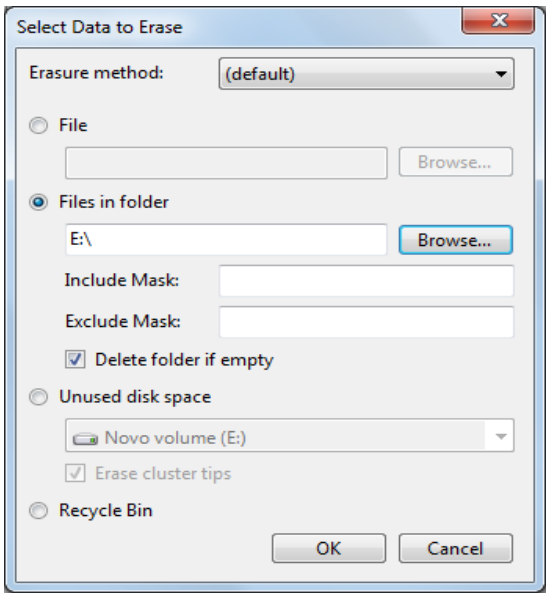

Figura 33 – Estudo de Caso 1 – Selecionando o volume para a destruição - Obtido em análise realizada com software

Para escolher o método de destruição é necessário entrar no menu de configurações **(Settings)**, onde escolhemos o método de Gutmann, um dos métodos descritos em nosso trabalho onde irá reescrever a área do disco em 35 passos.

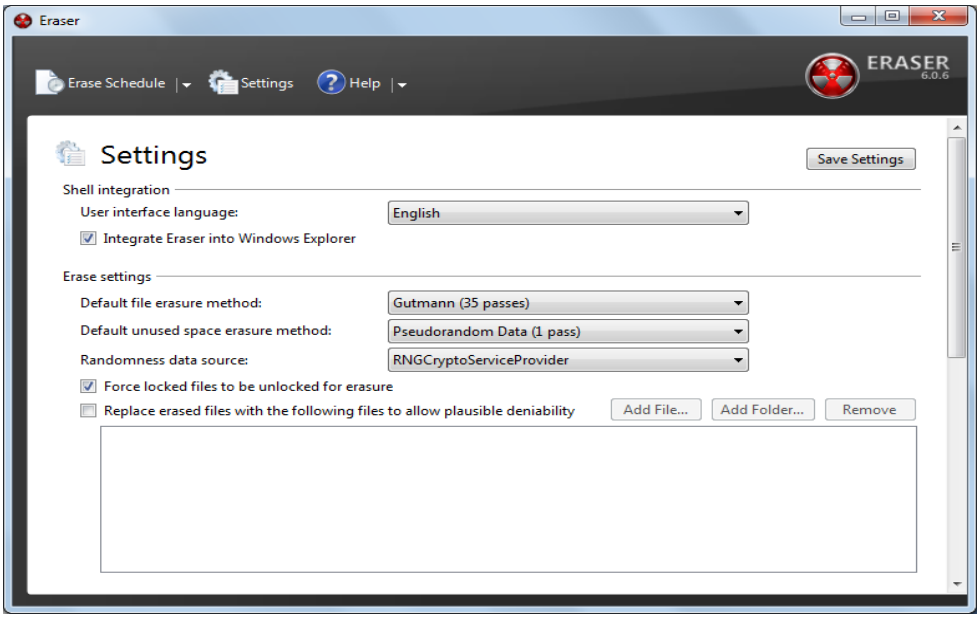

Figura 34 – Estudo de Caso 1 – Escolhendo o método de Destruição - Obtido em análise realizada com software

Após a escolha do volume e método, o software realizará o descarte permanente das informações, conforme a figura abaixo.

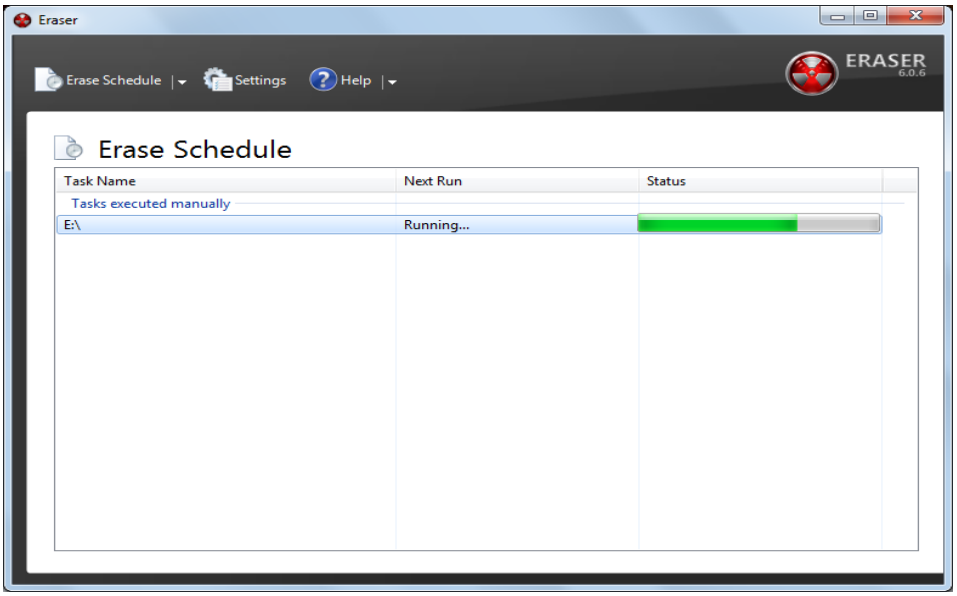

Figura 35 – Estudo de Caso 1 – Execução da ferramenta - Obtido em análise realizada com software

Observamos, conforme figura abaixo, que os dados do volume selecionados foram removidos.

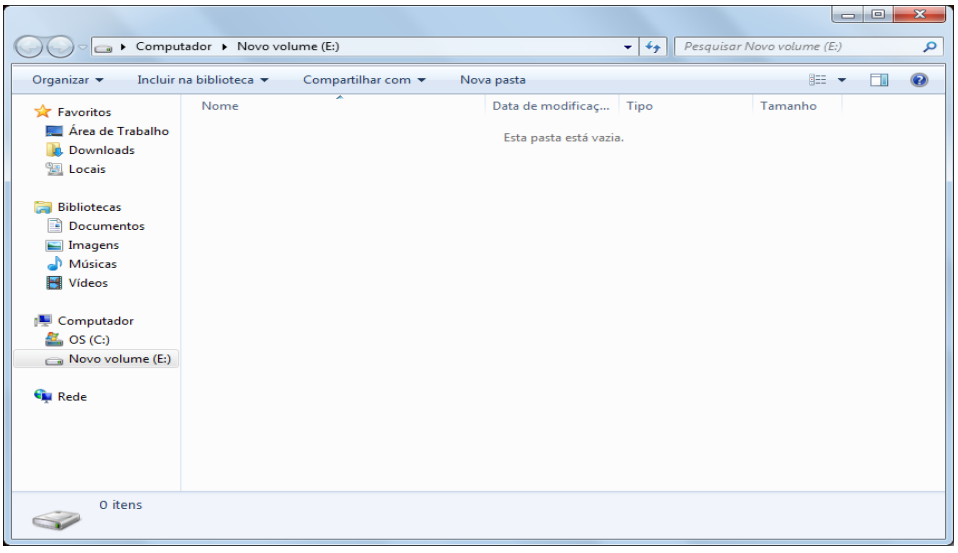

Figura 36 – Estudo de Caso 1 Remoção da Estrutura de pastas e arquivos - Obtido em análise realizada com software

Após o descarte dos dados através do software Eraser, vamos tentar recuperá-los através do software Recuva. Para realizar uma varredura completa na partição do disco rígido, é necessário selecionar o volume e clicar no botão **Verificar**.

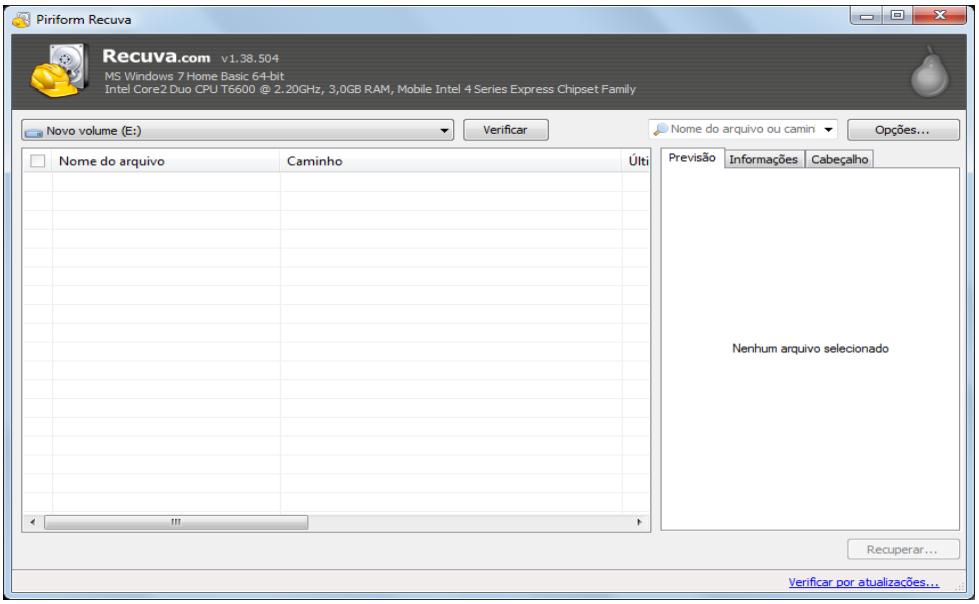

Figura 37 – Estudo de Caso 1 – Tentativa de recuperação de arquivos - Obtido em análise realizada com software

Após o término do procedimento, é possível verificar que o software vasculhou um disco rígido de 4 Gb e não encontrou nenhum arquivo possível de recuperação.

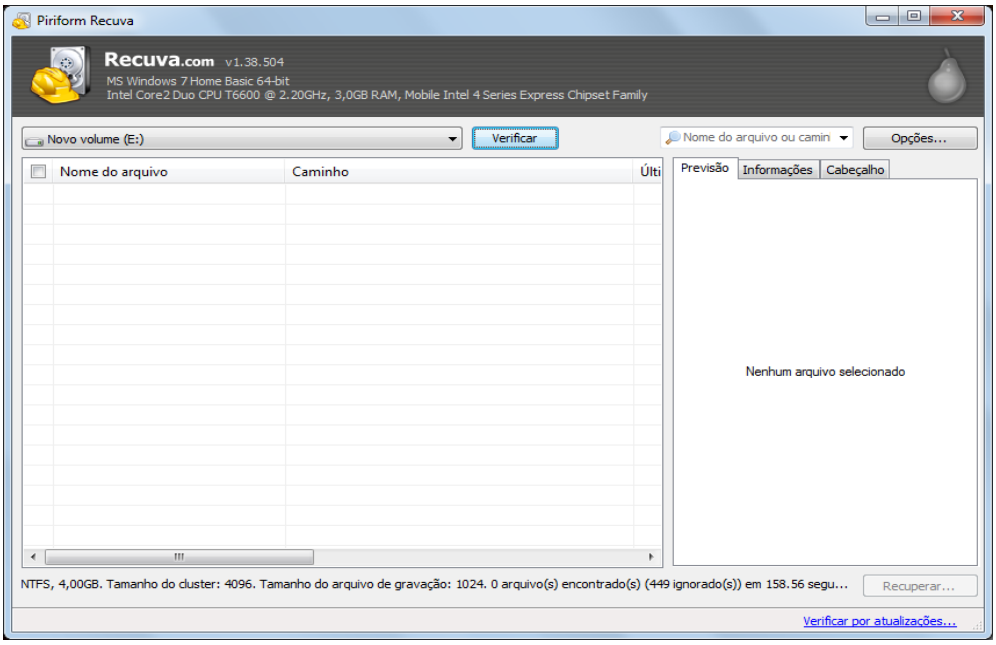

Figura 38 – Estudo de Caso 1 – Resultado da restauração do software Recuva - Obtido em análise realizada com software

4.5. Estudo de caso 2 – Descarte de dados através de um simples delete do Sistema Operacional Windows

Segue abaixo o demonstrativo de nossa atividade através das evidências coletadas, onde na figura demonstramos uma estrutura de pasta e arquivos que serão removidos através de remoção do SO Windows com as teclas *shift+delete*.

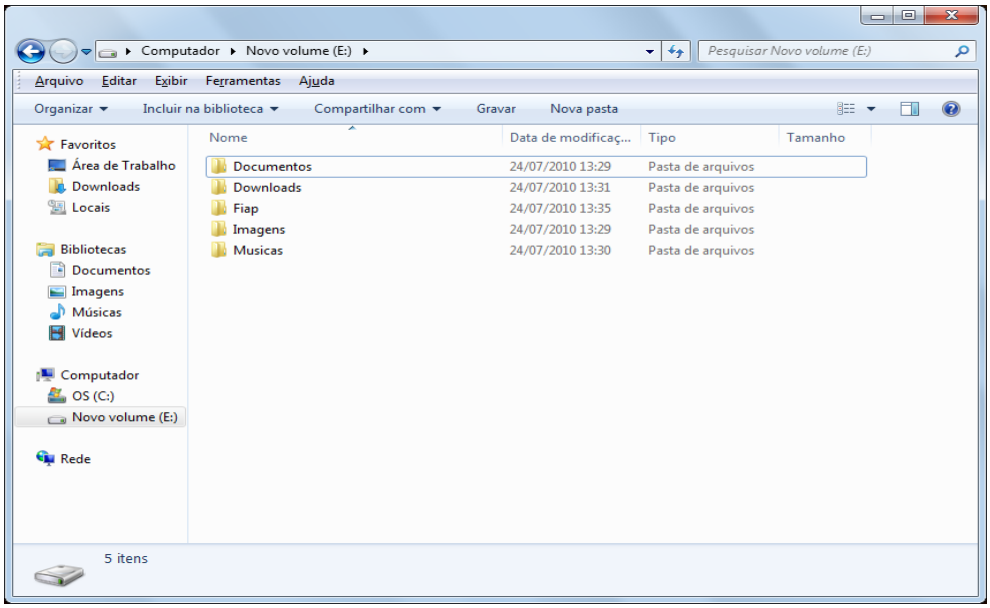

Figura 39 – Estudo de Caso 2 – Estrutura de Pastas e Arquivos - Obtido em análise realizada com software

Antes do Sistema Operacional executar o descarte da informação, ele pede a confirmação da remoção da informação de forma permanente.

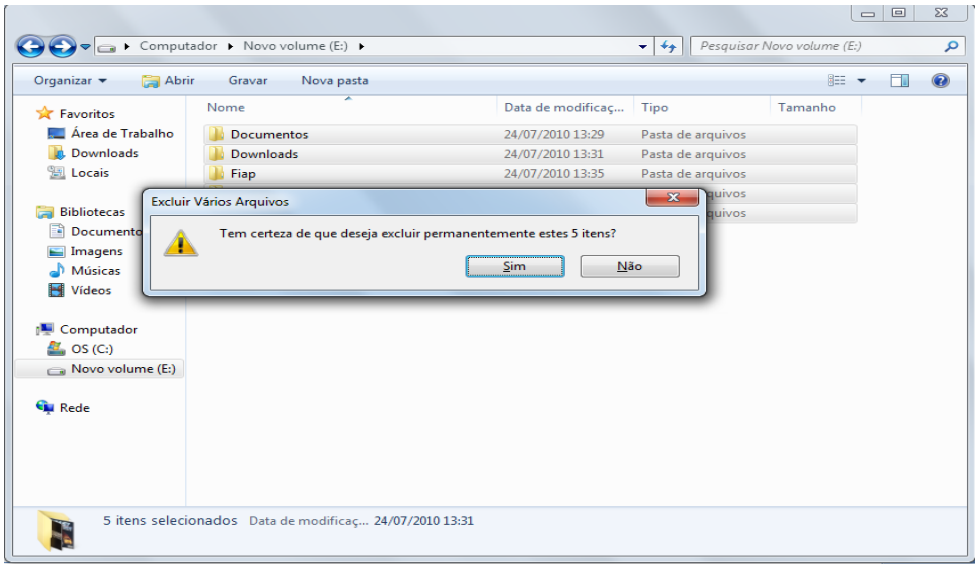

Figura 40 – Estudo de Caso 2 – Removendo a estrutura de Pastas e Arquivos através do delete - Obtido em análise realizada com software

Após o comando de delete permanente do Windows, observamos conforme a figura abaixo, que os dados não encontram-se mais no volume.

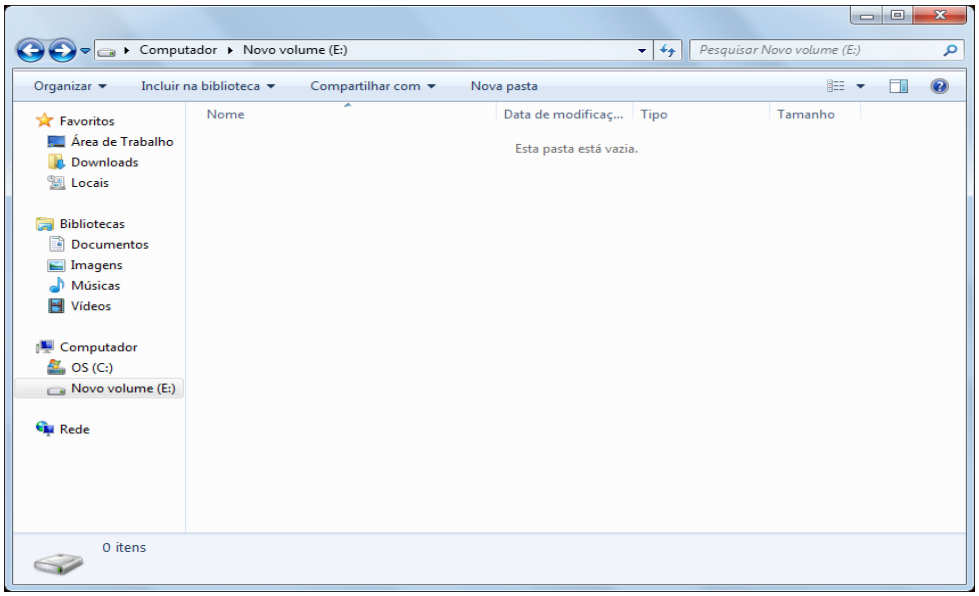

Figura 41 – Estudo de Caso 2 – Remoção da Estrutura de pastas e arquivos - Obtido em análise realizada com software

A seguir analisaremos a partição do disco rígido com o software Recuva na tentativa de recuperarmos os arquivos eliminados. Para realizar o procedimento, selecionaremos o volume E: e clicaremos no botão **Verificar**.

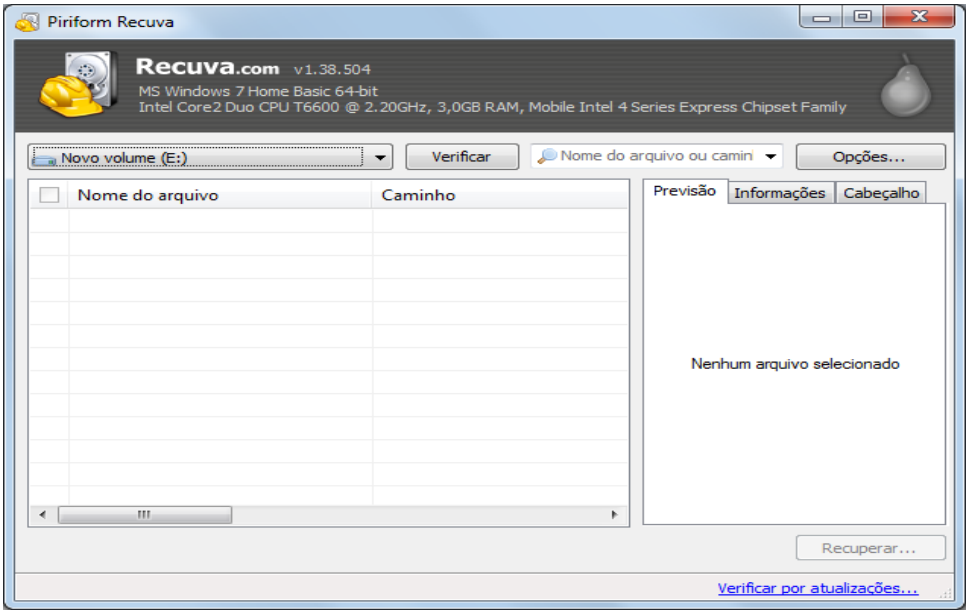

Figura 42 – Estudo de Caso 2 – Tentativa de recuperação do Software Recuva - Obtido em análise realizada com software

Ao executarmos a verificação do software Recuva, observamos conforme figura abaixo que diversos arquivos foram encontrados.

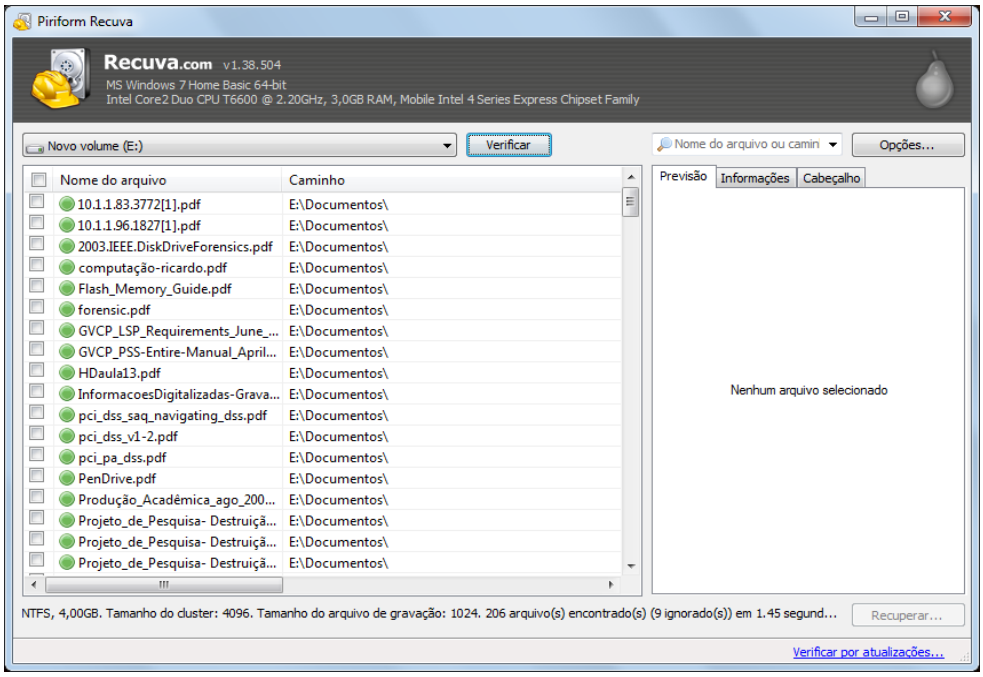

Figura 43 – Estudo de Caso 2 - Arquivos encontrados após analise do Software Recuva - Obtido em análise realizada com software

Para restaurarmos os arquivos encontrados, é necessário selecioná-los e com o botão direito do mouse clicar na opção **Recuperar Marcados** apontando o destino para sua posição original.

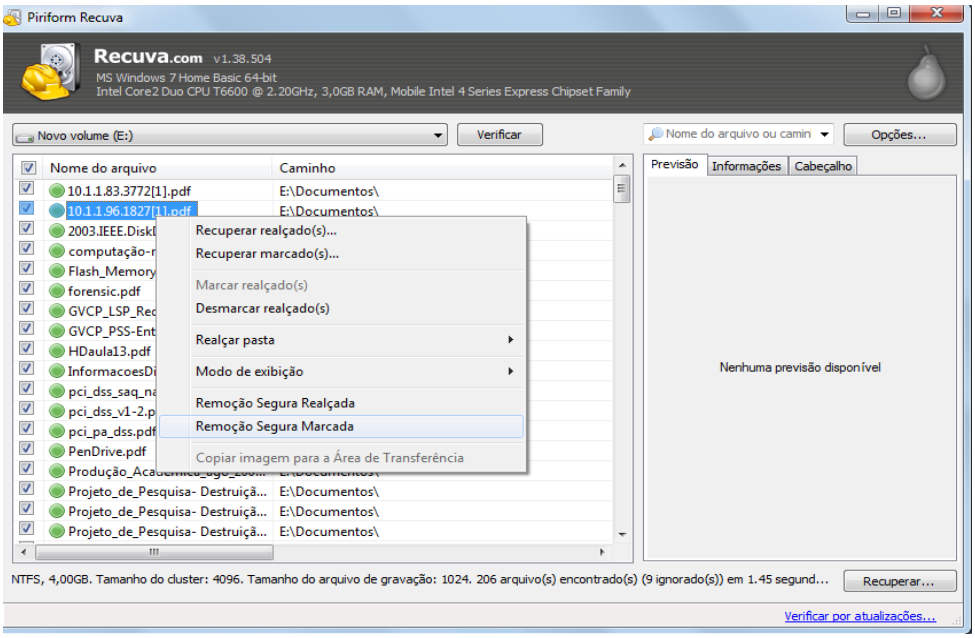

Figura 44 – Estudo de Caso 2 – Restauração de arquivos através do Software Recuva - Obtido em análise realizada com software

Após realizar o procedimento de recuperação do software Recuva, observamos conforme figura abaixo, que os dados foram recuperados em sua estrutura original.

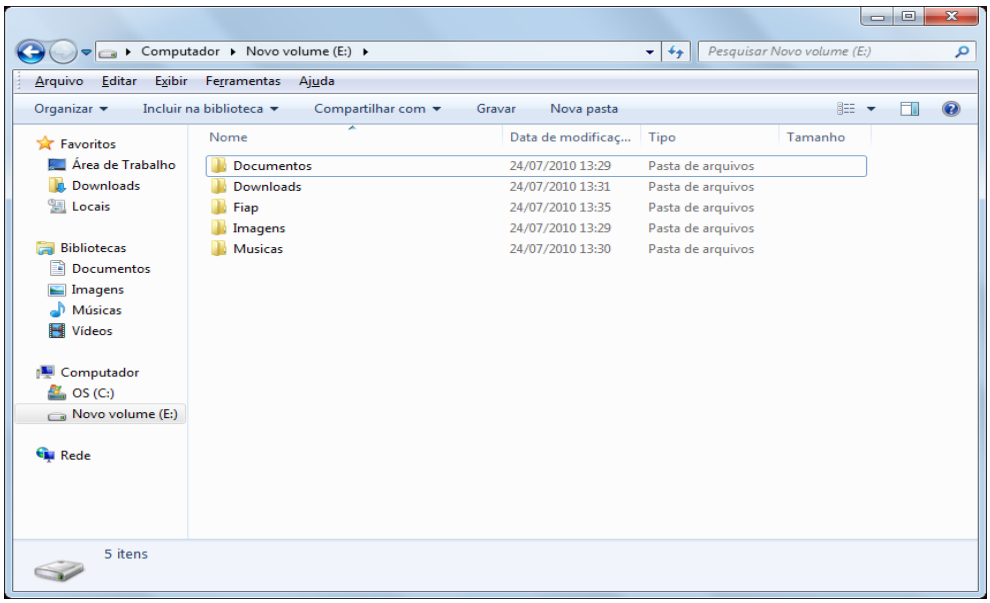

Figura 45 – Estudo de Caso 2 – Estrutura de pastas e arquivos restaurados com o Software Recuva - Obtido em análise realizada com software

4.6. Estudo de caso 3 – Descarte de dados através de um simples delete, e análise com o software Recuva para sua destruição

Segue abaixo o demonstrativo de nossa atividade através das evidências coletadas, onde na figura demonstramos uma estrutura de pasta e arquivos que serão removidos através do SO Windows pressionando as teclas *shift+delete*.

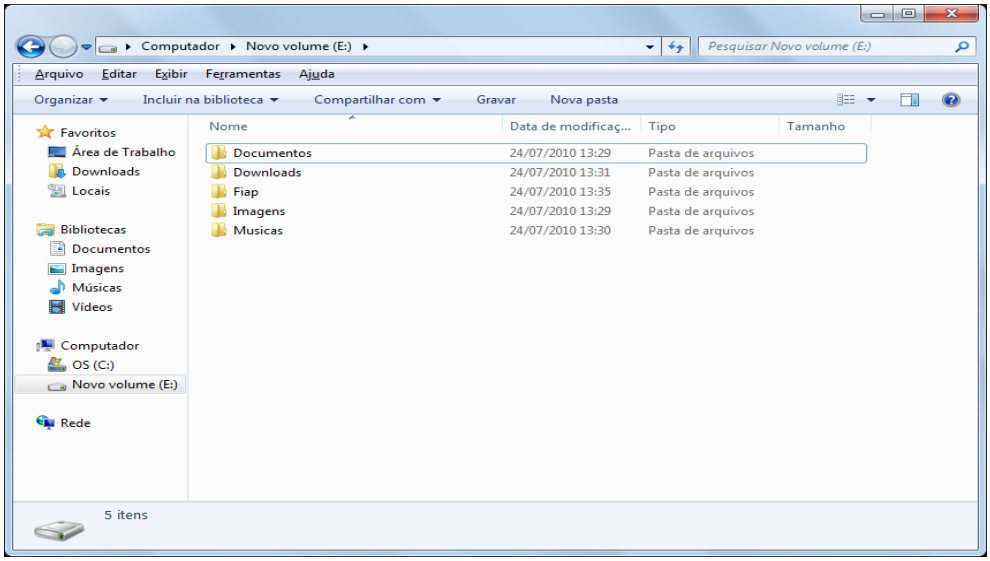

Figura 46– Estudo de Caso 3 – Estrutura de pastas e arquivos - Obtido em análise realizada com software

Antes do Sistema Operacional executar o descarte da informação, ele pede a confirmação dizendo que irá remover a informação de forma permanente.

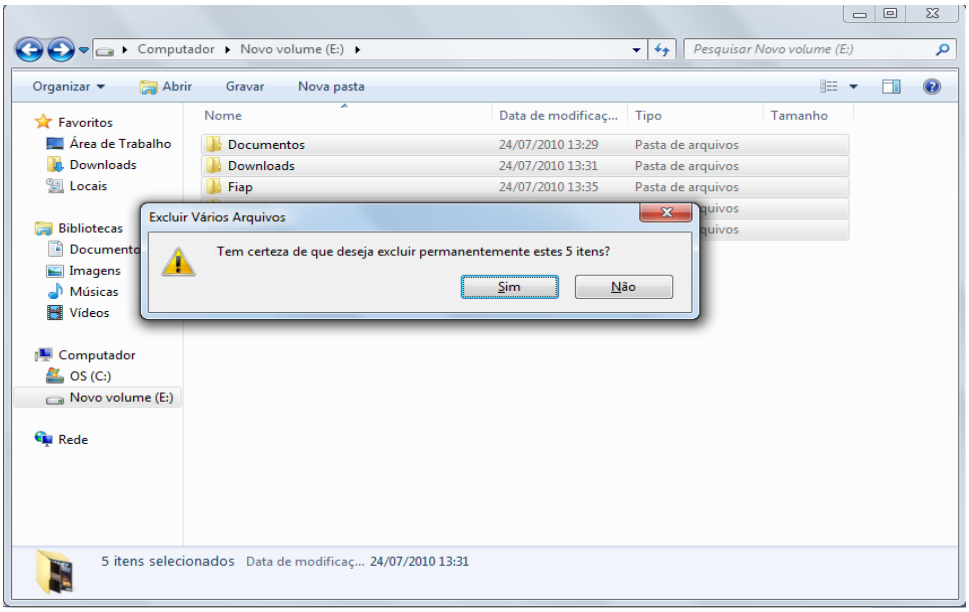

Figura 47 – Estudo de Caso 3 – Removendo a estrutura de Pastas e Arquivos através do delete - Obtido em análise realizada com software

Após o comando de delete permanente do Windows, é possível observar conforme figura abaixo, que os dados foram removidos do disco rígido.

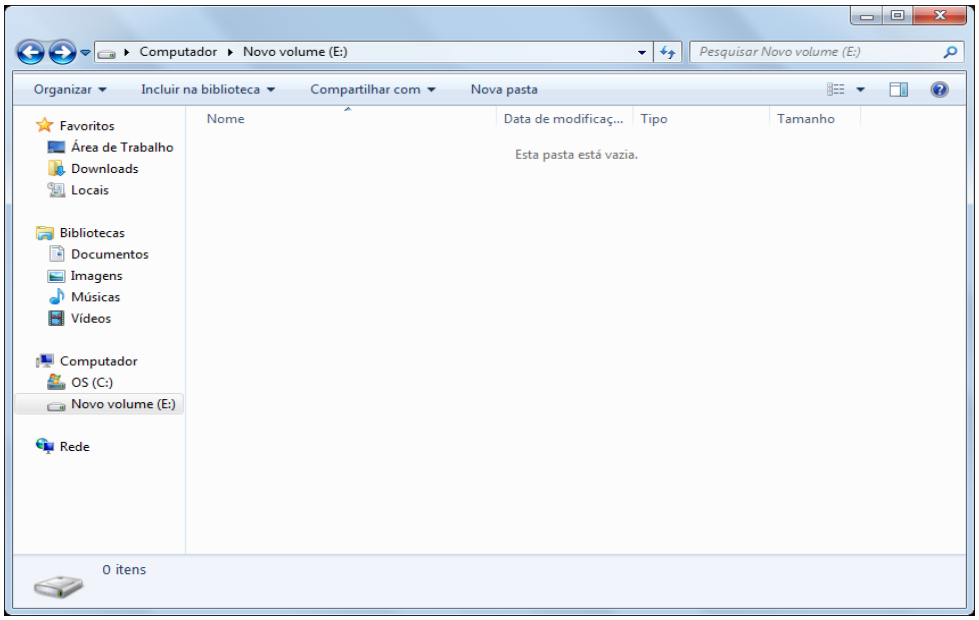

Figura 48 Estudo de Caso 3 – Remoção da Estrutura de pastas e arquivos - Obtido em análise realizada com software

A seguir analisaremos a partição do disco rígido com o software Recuva na tentativa de recuperarmos os arquivos removidos, selecionaremos o volume E: e clicaremos no botão **Verificar**.

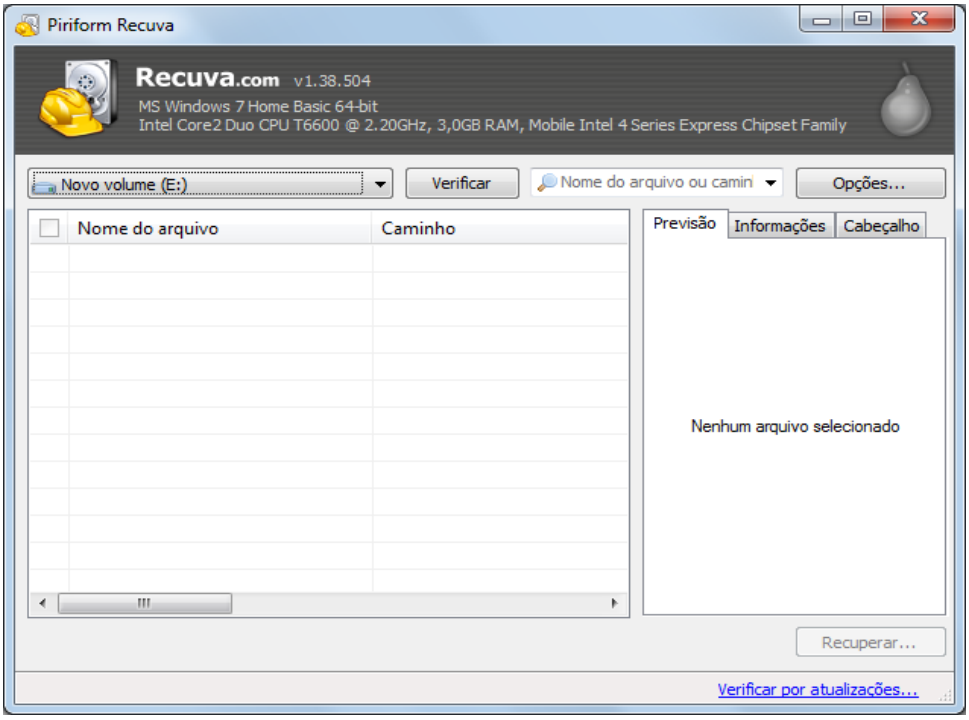

Figura 49 – Estudo de Caso 3 – Verificação para encontrar arquivos removidos - Obtido em análise realizada com software

Após a execução da verificação do software Recuva, observamos conforme figura abaixo, que diversos arquivos foram encontrados.

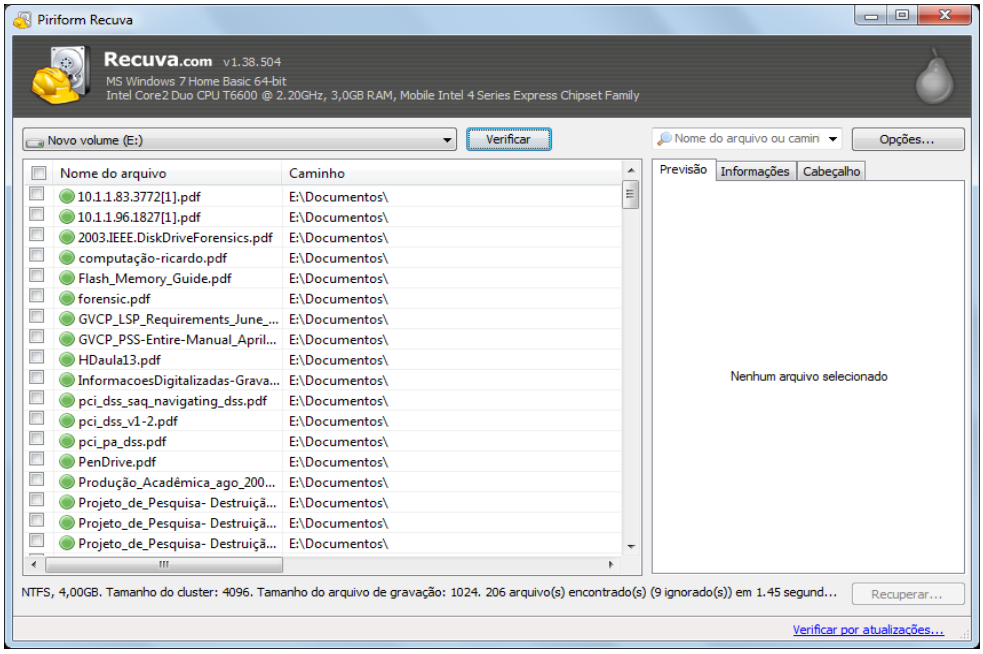

Figura 50. – Estudo de Caso 3 – Arquivos encontrados - Obtido em análise realizada com software

Ao clicarmos no botão “**Opções...**” é possivel selecionar uma técnica para a destruição segura dos dados. Para este estudo escolhemos o método de Gutmann que irá reescrever os dados em 35 passos, conforme apresentado neste trabalho.

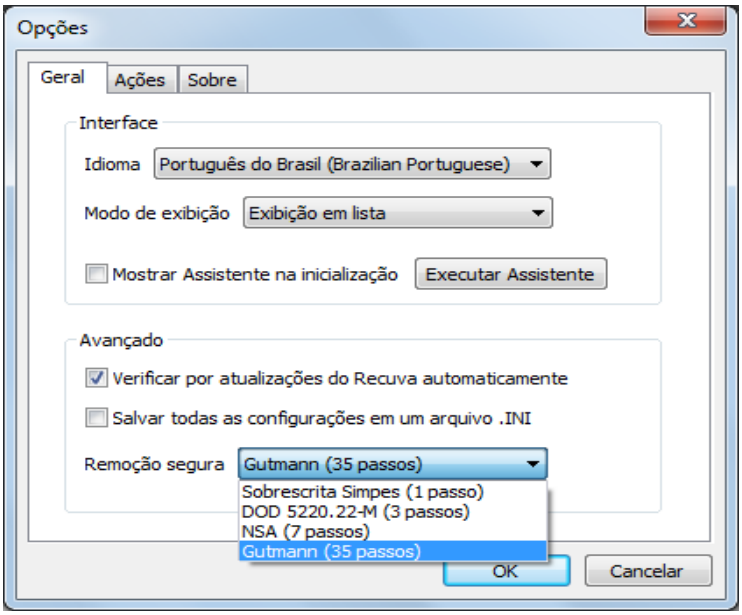

Figura 51 – Estudo de Caso 3 – Configura método de destruição - Obtido em análise realizada com software

Para a destruição de todos os dados, selecionamos todos os arquivos e clicando com o botão direito do mouse selecionamos a opção **Remoção Segura Marcada**.

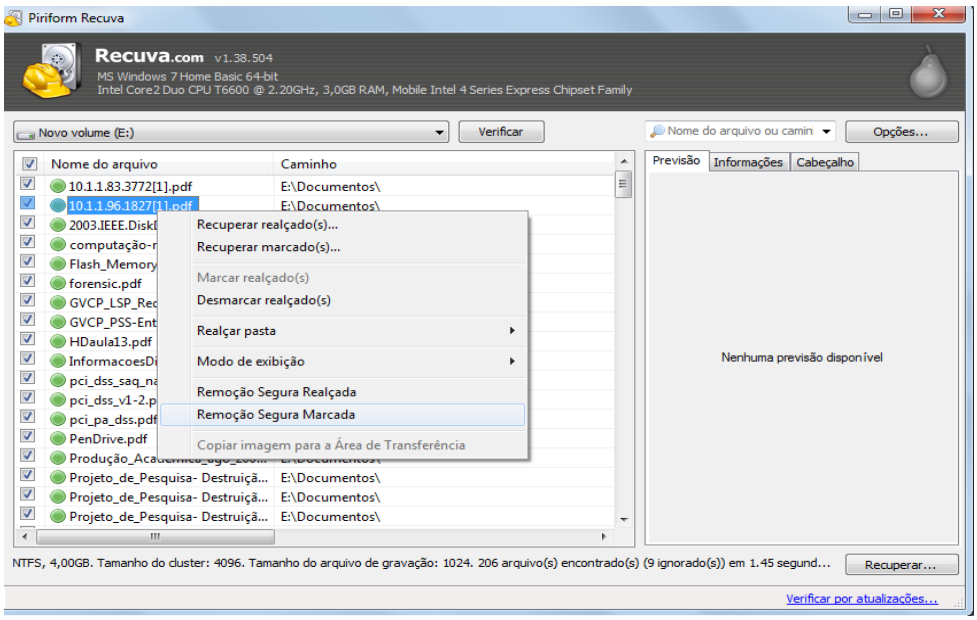

Figura 52 – Estudo de Caso 3 – Destruição de arquivos encontrados - Obtido em análise realizada com software

Após a execução do processo uma janela de conclusão é exibida, demonstrando a quantidade de arquivos que foram removidos de forma permanente.

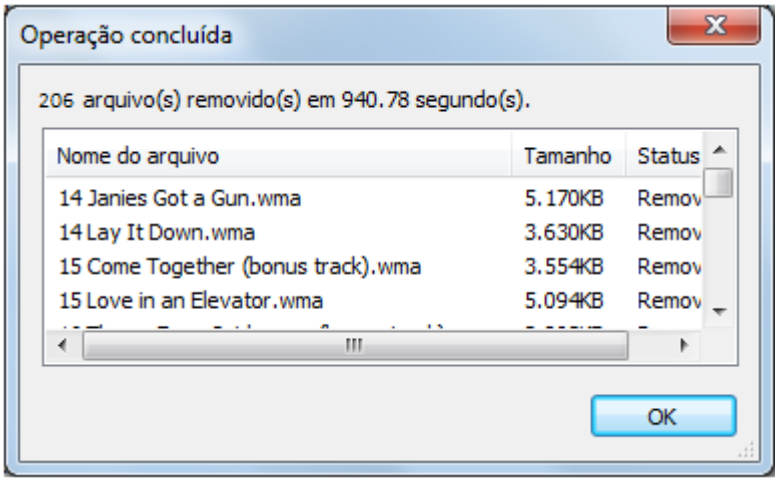

Figura 53 – Estudo de Caso 3 – Destruição de dados concluída - Obtido em análise realizada com software

Para verificarmos se realmente os dados foram removidos permanentemente, executamos a ferramenta Recuva, na tentativa de encontrar os arquivos novamente, porém nenhum dado foi encontrado.

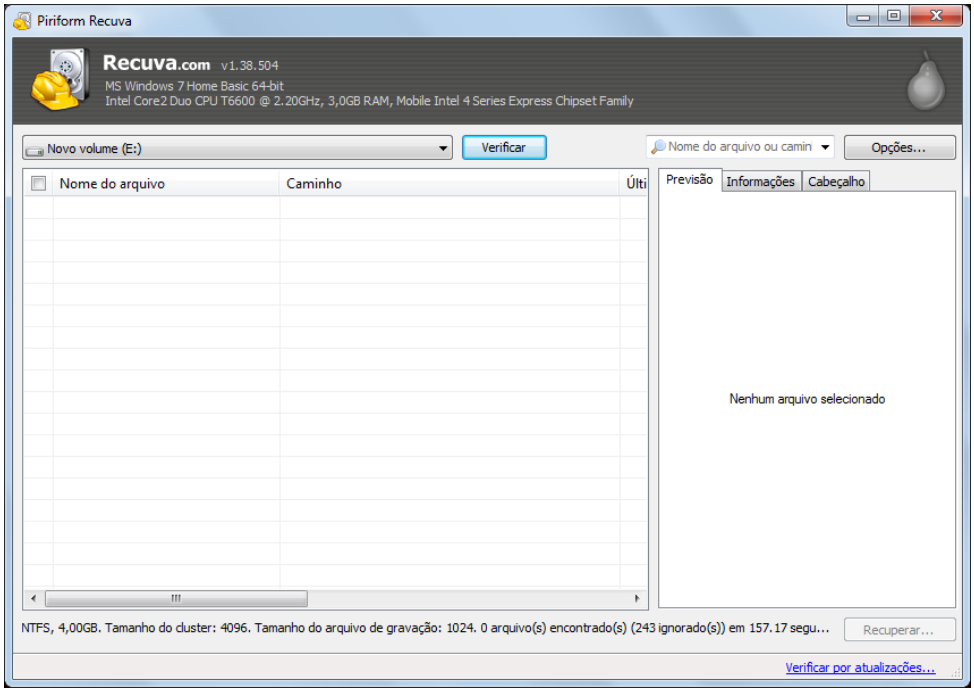

Figura 54 Estudo de Caso 3 – Tentativa de recuperação de dados - Obtido em análise realizada com software

4.7. Estudo de caso 4 – Descarte de dados através do software Glary Utilities

Segue abaixo o demonstrativo de nossa atividade através das evidências coletadas, onde na figura demonstramos uma estrutura de pasta e arquivos que serão removidos através do software Glary Utilities.

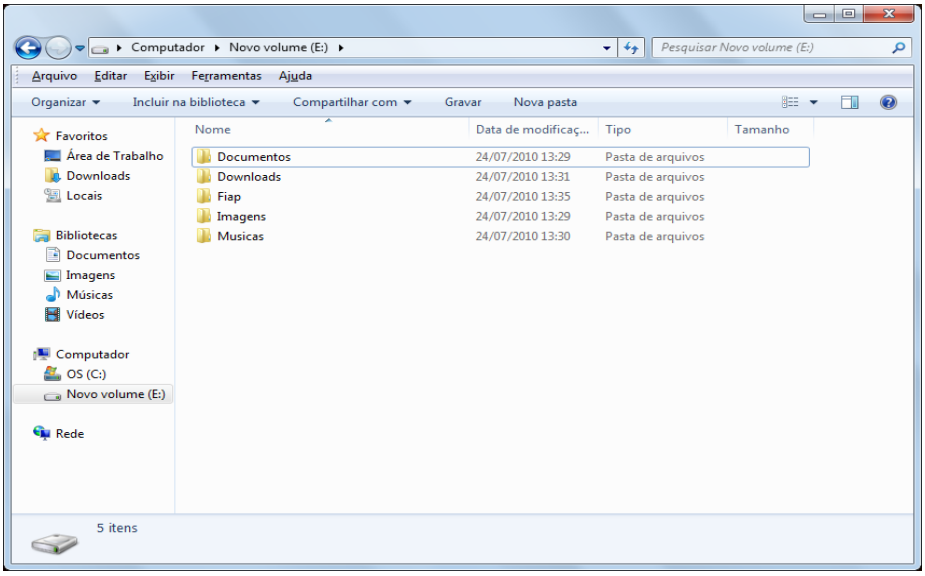

Figura 55 – Estudo de Caso 4 – Estrutura de pastas e arquivos – Obtido em análise realizado com o Software

Iniciaremos o procedimento de remoção permanente das informações, dentro do software Glary Utilities no menu **Segurança**, clicando na opção **Apagar Arquivos**.

Figura 56 – Estudo de Caso 4 – Iniciando o processo de destruição dos dados – Obtido em análise realizado com o Software

Para realizarmos o processo, é preciso selecionar a estrutura de pastas e arquivos que serão removidos de forma segura, clicando no botão **Add Pasta**. A figura abaixo, apresenta o método de Dod 5220.22-M.

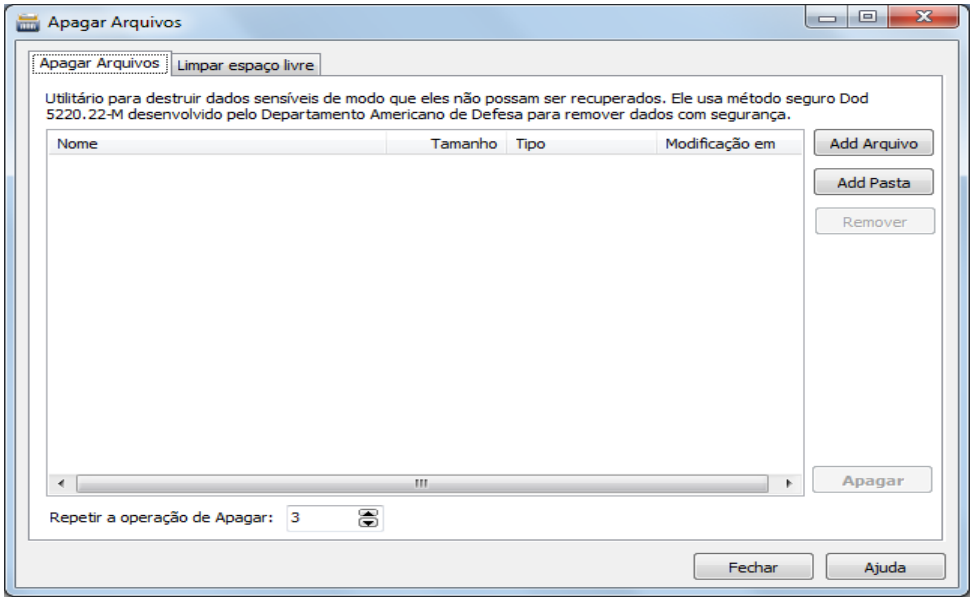

Figura 57 – Estudo de Caso 4 – Selecionando as pastas para a destruição - Obtido em análise realizada com software

Na figura abaixo, observamos as pastas selecionadas para o descarte permanete, para confirmar o procedimento clicamos no botão **Apagar**.

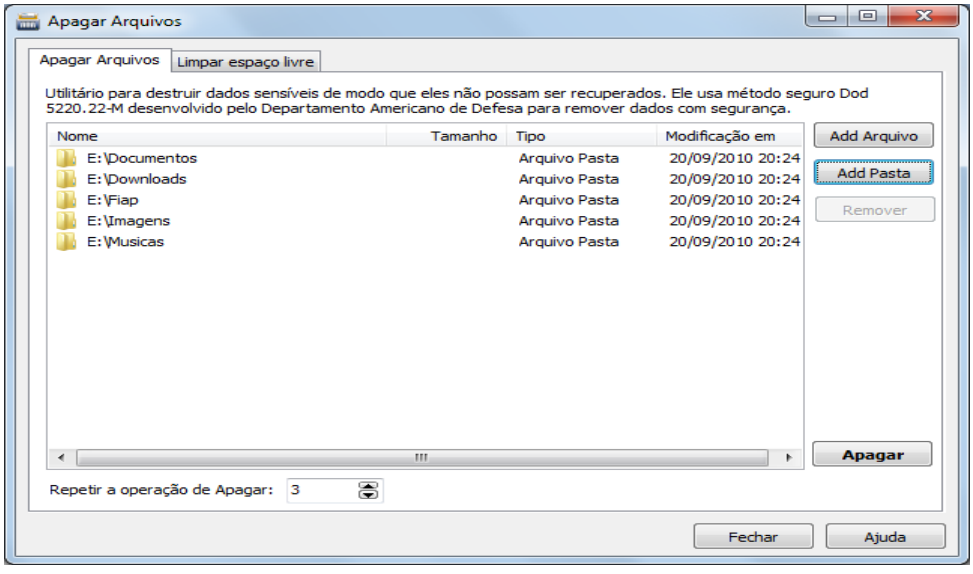

Figura 58 – Estudo de Caso 4 – Executando a destruição das informações - Obtido em análise realizada com software

Ao término do processo de remoção permanente dos dados é possível observar conforme figura abaixo, que a estrutura foi completamente removida do disco rígido.

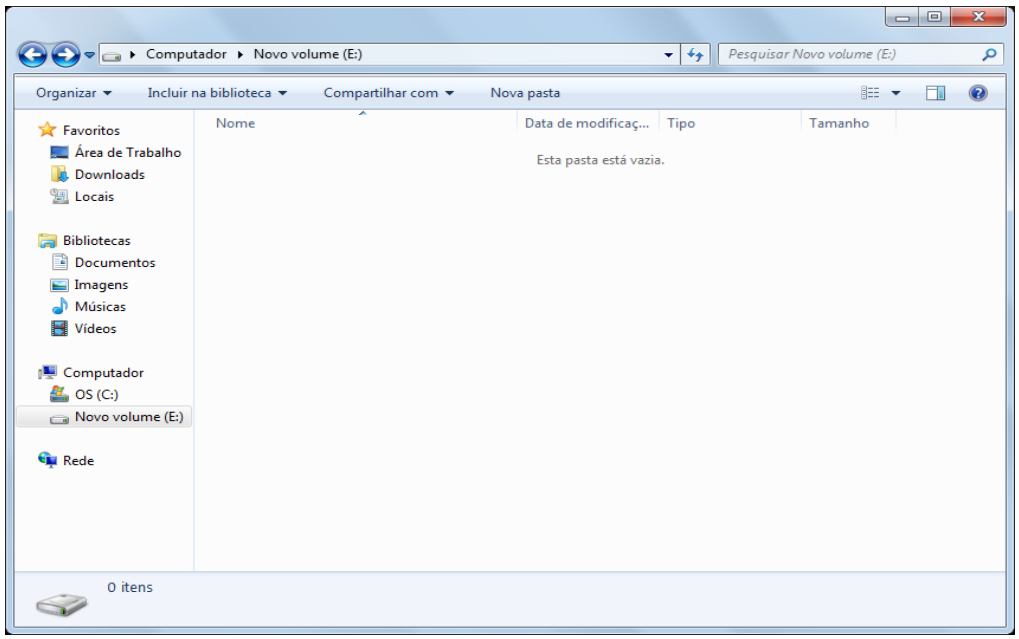

Figura 59 – Estudo de Caso 4 - Remoção da Estrutura de pastas e arquivos - Obtido em análise realizada com software

A seguir analisaremos a partição do disco rígido com o software Recuva na tentativa de recuperarmos os arquivos removidos, selecionaremos o volume E: e clicaremos no botão **Verificar**.

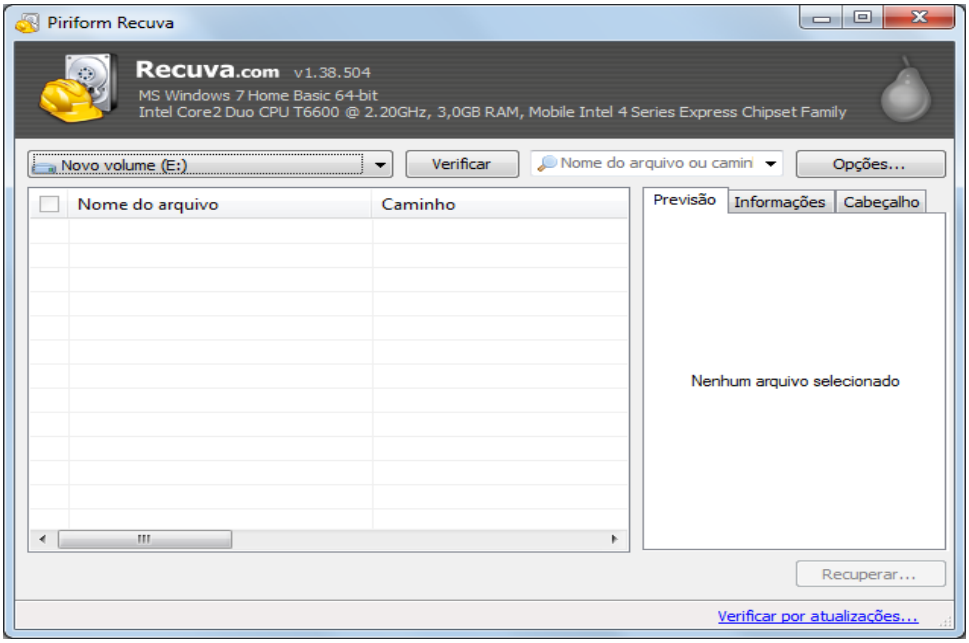

Figura 60 – Estudo de Caso 4 - Verificação para encontrar arquivos removidos - Obtido em análise realizada com software

Após a execução da ferramenta, observamos conforme figura abaixo, que nenhum arquivo foi encontrado.

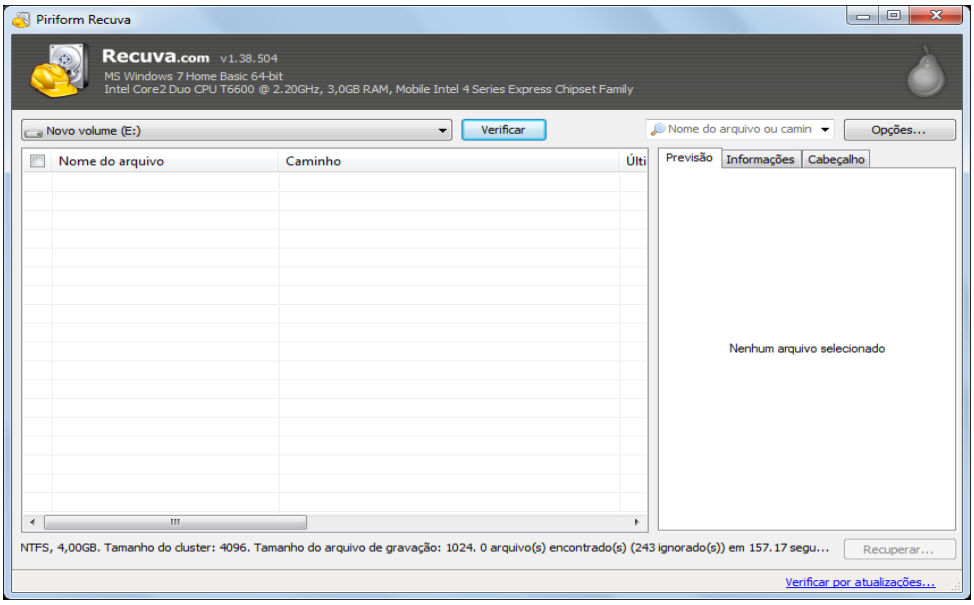

Figura 61 – Estudo de Caso 4 - Arquivos encontrados - Obtido em análise realizada com software

4.8. Estudo de caso 5 – Descarte de dados através do processo de Formatação

Segue abaixo o demonstrativo de nossa atividade através das evidências coletadas, onde na figura demonstramos uma estrutura de pasta e arquivos que serão removidos através do comando Formatar do SO Windows.

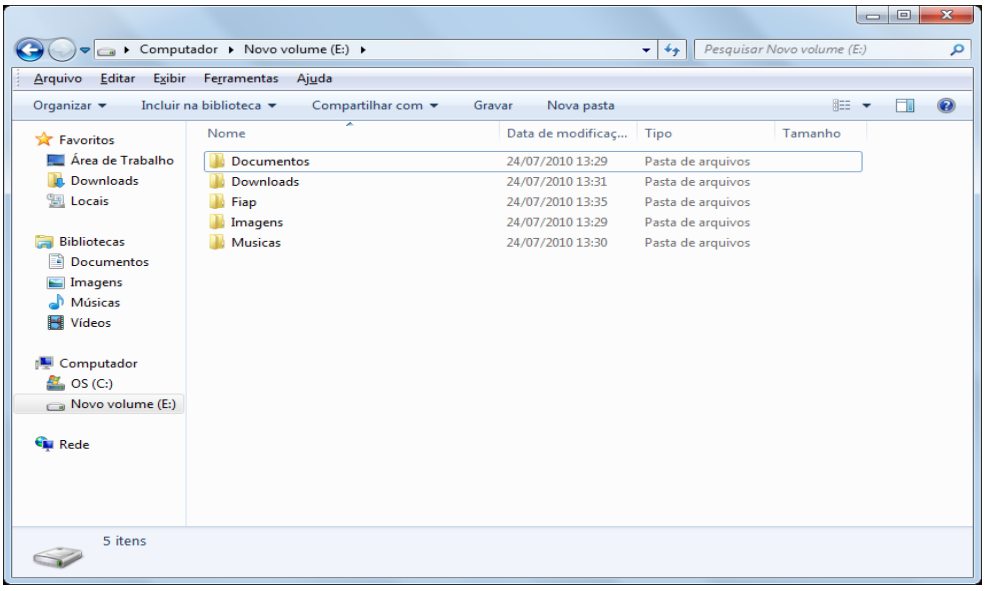

Figura 62 – Estudo de Caso 5 – Estrutura de pastas e arquivos – Obtido em análise realizado com o software

Para iniciarmos o processo de formatação do volume E:, é preciso clicar com o botão direito do mouse no volume e selecionando a opção **Formatar**.

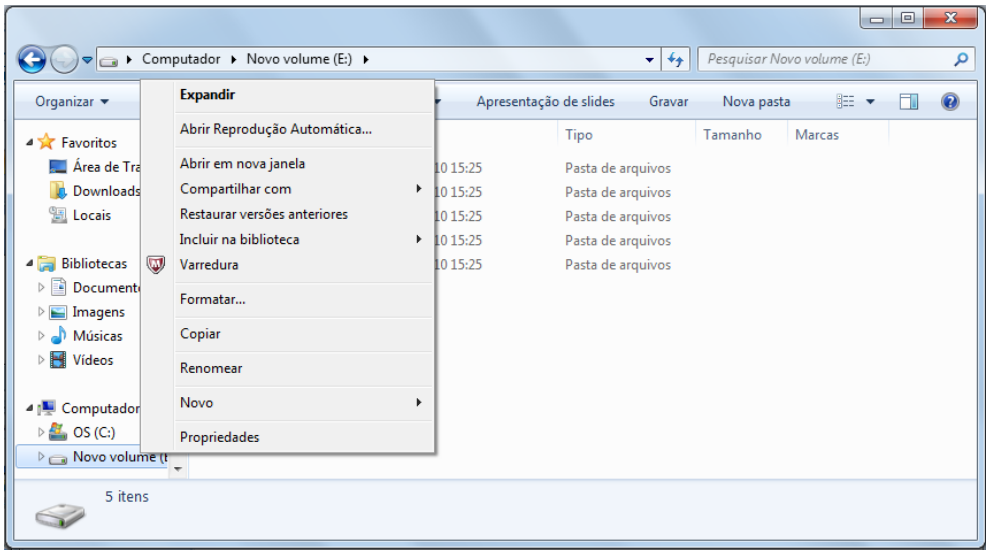

Figura 63 – Estudo de Caso 5 – Formatando o volume E – Obtido em análise realizado com o software

Na formatação do volume é possível escolher o sistema de arquivos, utilizaremos o sistema de arquivos NTFS.

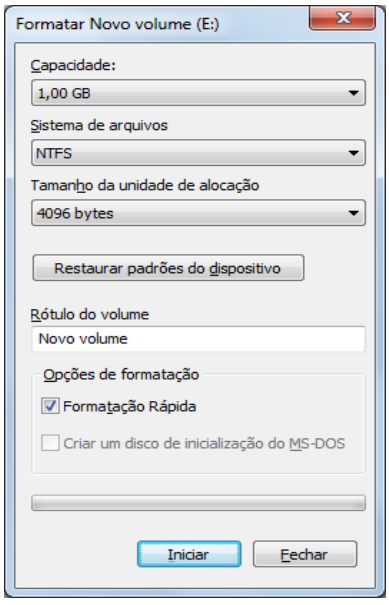

Figura 64 – Estudo de Caso 5 – Selecionando o tipo de Formatação – Obtido em análise realizado com o software

Antes do Sistema Operacional executar a formatação, ele pede a confirmação dizendo que a formatação apagará todos os dados do disco.

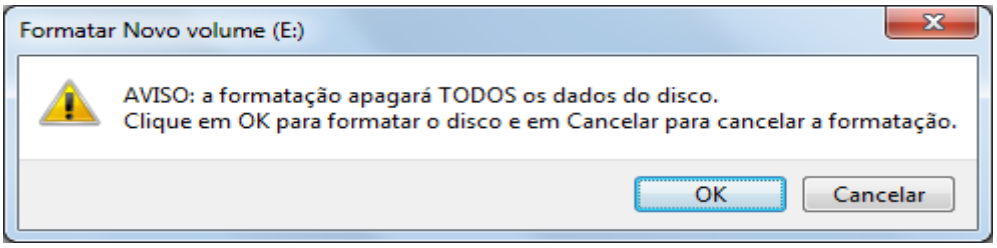

Figura 65 – Estudo de Caso 5 – Aviso da perda de dados – Obtido em análise realizado com o software

Ao término do processo de formatação do disco, observamos conforme figura abaixo, que os dados foram removidos.

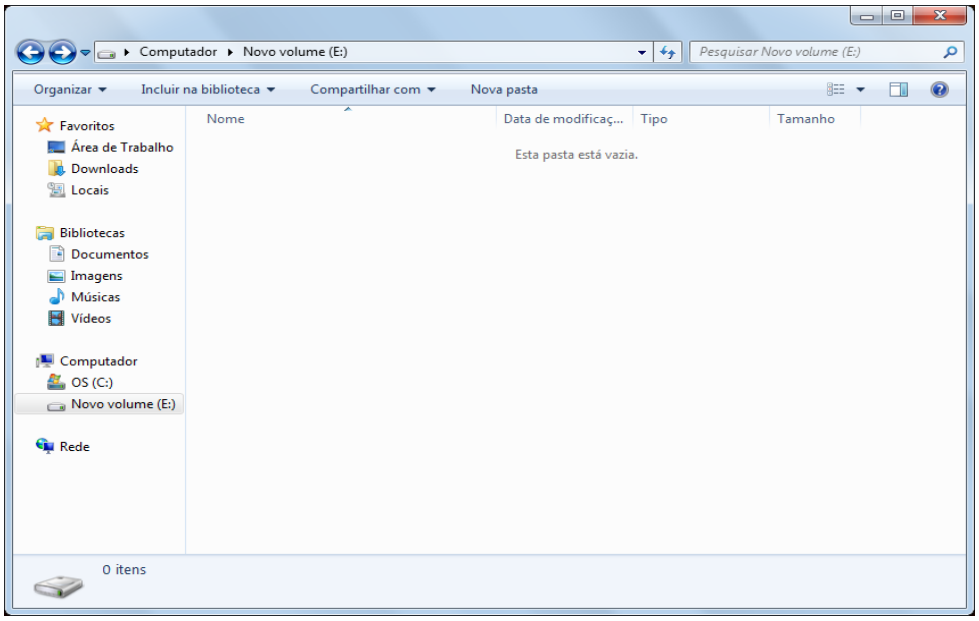

Figura 66 Estudo de Caso 5 – Resultado da formatação do volume E - Obtido em análise realizada com software

A seguir analisaremos a partição do disco rígido com o software Recuva na tentativa de recuperarmos os arquivos removidos pela formatação, selecionaremos o volume E: e clicaremos no botão **Verificar**.

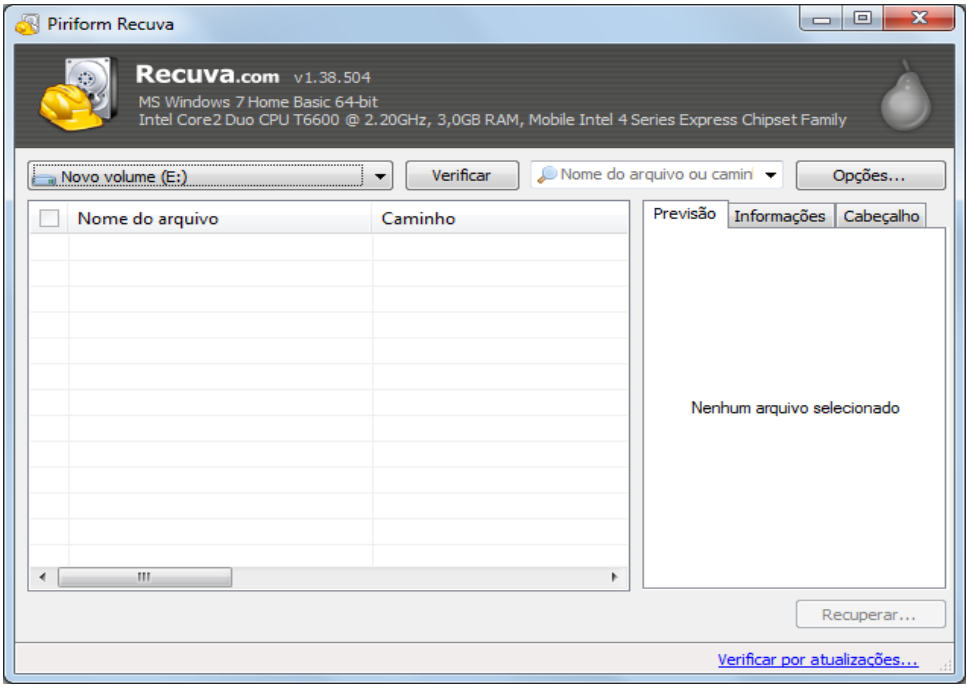

Figura 67 – Estudo de Caso 5 - Verificação para encontrar arquivos removidos - Obtido em análise realizada com software

Ao executarmos a verificação do software Recuva, observamos que diversos arquivos foram encontrados.

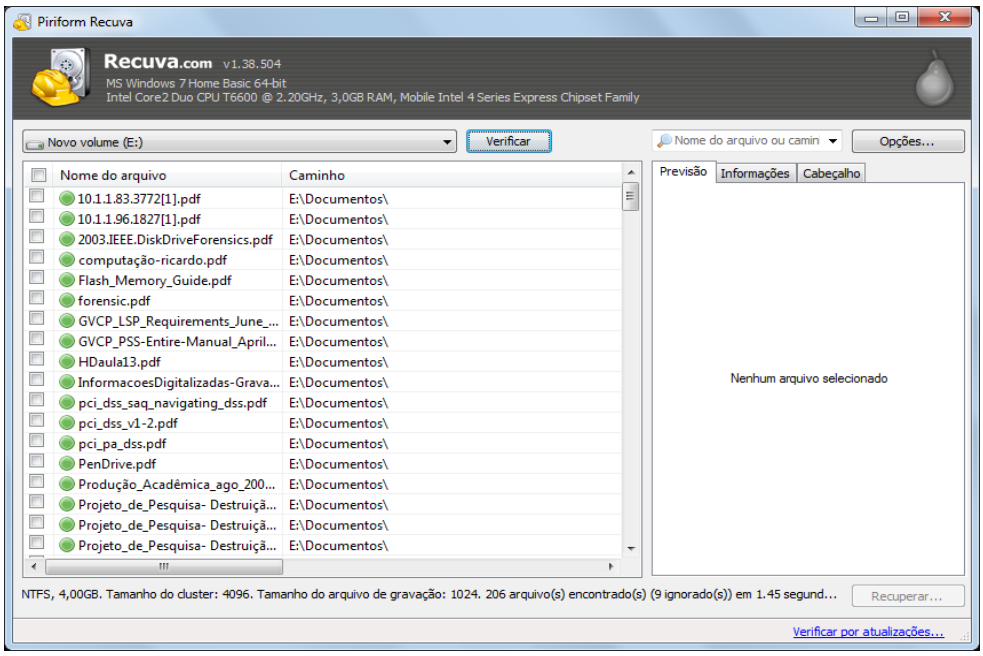

Figura 68 – Estudo de Caso 5 - Arquivos encontrados após a formatação- Obtido em análise realizada com software

Para a recuperação dos dados é necessário selecionar todos os arquivos e com o botão direito do mouse clicar na opção **Recuperar Marcados**, indicando um novo volume para a restauração, pois neste caso o software não permitiu o local original.

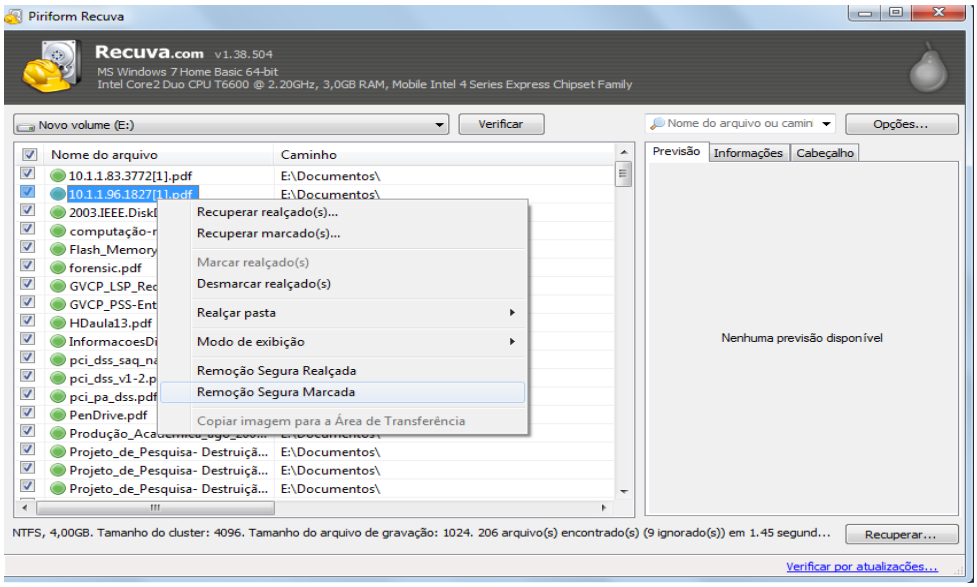

Figura 69 – Estudo de Caso 5 - Processo de recuperação dos arquivos encontrados - Obtido em análise realizada com software

Após a realização do procedimento, observamos que a recuperação dos dados foi realizada com sucesso, porém o software não conseguiu restaurar os arquivos com o nome original e também não conseguiu restaurar a estrutura de pastas, porém o conteúdo do arquivo permanece acessível.

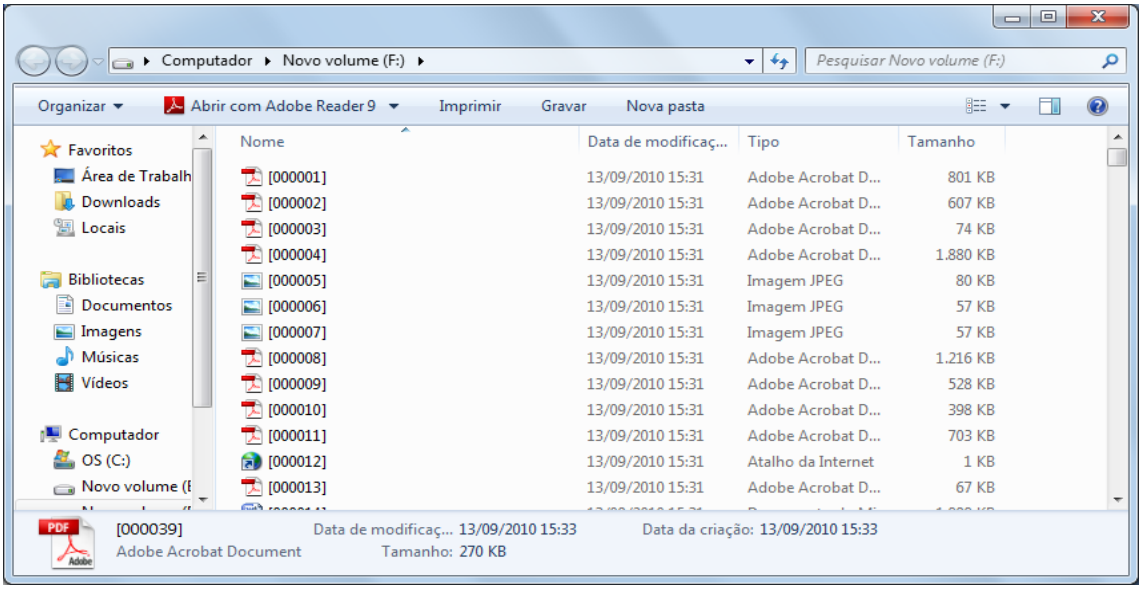

Figura 70 – Estudo de Caso 5 – Restauração de dos arquivos encontrados - Obtido em análise realizada com software

4.9. Sumarização Estudos de caso

Com os estudos, percebemos que o descarte seguro de dados é muito importante, pois um simples delete ou uma formatação de volume, não assegura que as informações foram descartadas por completo.

Descreveremos uma tabela comparativa com os softwares utilizados e as formas de destruição que foram demonstradas nos estudos de Caso relatados acima.

Formas de Destruição	Versão	Método Utilizado	Destruição	Recuperação
SOFTWARE ERASER	6.0.6	Gutmann 35 Passos	Conseguiu realizar o descarte completo das informações, impossibilitando sua recuperação.	Não possui função de recuperação.
SOFTWARE RECUVA	1.38.504	Gutmann 35 Passos	Conseguiu realizar o descarte completo das informações, impossibilitando sua recuperação.	Conseguiu recuperar os arquivos, quando não destruídos de forma segura.
SOFTWARE GLARY UTILITIES	2.28.0.1011	DOD 5220.22-M	Conseguiu realizar o descarte completo das informações, impossibilitando sua recuperação.	Conseguiu recuperar os arquivos, porém não foi utilizado no estudo de caso.
DELETE DO WINDOWS	Não Disponível	Não Disponível	Não conseguiu realizar o descarte completo das informações, possibilitando sua recuperação.	Os dados foram recuperados com o software RECUVA
FORMAT DO WINDOWS	Não Disponível	Não Disponível	Não conseguiu realizar o descarte completo das informações, possibilitando sua recuperação.	Os dados foram recuperados com o software RECUVA

Quadro 6 – Comparativo das Técnicas utilizadas nos estudos de Caso

Este estudo de caso teve foco em descarte lógico de informações contidas em discos rígidos. Consideramos o software Eraser melhor pela sua usabilidade e

sua ferramenta de agendamento. Mas não descartamos a utlização dos demais softwares estudados, dependendo da necessidade. Um exemplo é se for necessária a análise de arquivos já descartados mas forma não segura como delete e formatação do SO Windows, neste caso o Recuva é uma boa solução pois, ele analisa o disco em busca destes arquivos, e caso encontre os arquivos deletados ele os descarta definitivamente. Com isso, fica a cargo do leitor analisar a sua necessidade e determinar qual a melhor ferramenta para a sua necessidade.

CONCLUSÃO

Neste trabalho buscamos apresentar a melhor forma de gerenciamento das informações para seu descarte seguro através de ferramentas adequadas ao meio de armazenamento.

Na questão de gerenciamento das informações, uma empresa que busque proteger este ativo tão valioso que é a informação, nós recomendamos fortemente a busca de apoio na família de normas ISO 27000, principalmente as normas ISO 27001 e ISO 27002. Nelas são difundidos conceitos do SGSI (Sistema de Gestão de Segurança da Informação) e o PDCA que em português quer dizer planejar, fazer, verificar e agir que é o modelo de execução para implantação de uma boa gestão de segurança. Além de apresentar controles importantes para uma boa metodologia de gestão da informação, que são:

- Política de segurança;
- Organização da segurança da informação;
- Gestão dos ativos;
- Recursos humanos e segurança;
- Segurança física e ambiental;
- Controle de acesso;
- Descarte e reutilização;
- Ciclo de vida da informação;
- Classificação da informação.

Estes controles devem ser implantados antes de se pensar em descarte das informações.

Na nossa visão são necessários numa organização documentos que regem as diretrizes de gestão dos ativos, controle de acesso, organização e de conscientização das pessoas quanto à necessidade de descarte seguro conforme a classificação da informação.

Outras normas como o PCI e o MasterCard logical security requirements for card personalization bureaus, são mais focadas em questões financeiras do segmento de pagamento com cartões, dão ênfase a monitoração das informações sigilosas em todo seu ciclo de vida, focando muito o descarte seguro destas.

Na questão do descarte das informações é muito importante analisar qual o tipo da mídia de armazenamento para utilizar o método de descarte que atenda a necessidade. Conforme o que foi apresentado neste estudo, recomendamos as seguintes ações:

- **Discos rígidos e memórias sólidas para reutilização**: Em casos de necessidade de descarte de informações em mídias magnéticas que não serão descartadas fisicamente, podem ser utilizados os métodos de sobrescrita apresentados neste estudo como Gutmann, DOD 5220.22-M, VSITR. Recomendamos após a utilização de um dos métodos de descarte o uso de uma ferramenta de recuperação para teste da eficácia do descarte.
- **Discos rígidos e fitas magnéticas não reutilizáveis**: Em casos de mídias magnéticas danificadas que contenham informações sigilosas recomendamos a contratação de uma empresa especializada em desmagnetização, incineração ou trituração. No caso das duas últimas formas de destruição pode ser considerado a uso de manufatura reversa, que irá separar as peças conforme sua matéria prima e triturá-las para reciclagem ou incinerar para descarte de matérias não recicláveis.
- **Memória sólida não reutilizável**: Em casos de pen-drives, cartões de memórias e outros dispositivos que utilizam memórias sólidas, nós recomendamos a trituração ou incineração após uma manufatura reversa.
- **Mídias óticas, fitas perfuradas e papel**: nestas formas de armazenamento de informações, recomendamos o método de descarte por destruição física, através de incineração, fragmentação, pulverização ou desintegração.

Levantamos custos para descarte de mídias de armazenamento com algumas empresas do setor de gerenciamento de resíduos. Recomendamos fortemente o uso de manufatura reversa para mídias de armazenamento compostas por diversas matérias primas (ex: HDs, Fitas, Disquetes, etc.) devido ao seu custo benefício. Nos dias de hoje, onde ações relacionadas ao meio ambiente estão cada vez mais ganhando importância no âmbito social, manufatura reversa aparece como uma boa prática para um marketing social da empresa e para destruição das informações confidenciais. De qualquer forma ainda recomendamos, quando possível, a utilização de outro método de descarte como sobrescrita ou desmagnetização. Para

demais mídias compostas por apenas uma matéria prima, o uso de manufatura reversa é não necessário.

No estudo de caso realizado, demonstramos que quando não ocorre o descarte seguro das informações, sempre existe a possibilidade de recuperação.

Utilizando somente métodos de sobrescrita em disco rígido, conseguimos um bom resultado de eliminação segura. Demonstramos que a formatação e o delete através do sistema operacional Windows são ineficazes no descarte seguro de informação, e os softwares Eraser e Glary Utílities foram eficazes. Para esta constatação utilizamos o software Recuva na tentativa de recuperação das informações.

A área de gestão de segurança da informação deve apoiar iniciativas de gestão e classificação das informações através de divulgação de políticas e procedimentos pertinentes para descarte seguro de informação.

Para estudos futuros, recomendamos o maior aprofundamento em questões de:

- Descarte de materiais tecnológicos com foco ambiental;
- Novos métodos de descarte através de sobrescrita de dados;
- Constante estudo de descarte de informações em novas mídias que surgirão com evolução natural da tecnologia;
- Estudo da capacitação das empresas de gestão de resíduos tecnológicos em relação gestão de confidencialidade de informações de seus clientes.

REFERÊNCIAS

SÊMOLA, Marcos. **Gestão da Segurança da Informação – Uma visão Executiva**. Editora Campus. Rio de Janeiro, 2003.

CROSBY, Philip B. **Qualidade é Investimento**. José Olympio Editora. 5ª Edição, Rio de Janeiro, 1992.

MARTIN, James. **Engenharia da Informação – Introdução**. Editora Campus. Rio de Janeiro, 1991.

FELICIANO NETO, Acácio; FURLAN, José Davi e HIGO, Wilson. **Engenharia da Informação – Metodologia, Técnicas e Ferramentas**. Editora McGraw-Hill. São Paulo, 1988.

WADLOW, Thomas. **Segurança de Redes**. Editora Campus. Rio de Janeiro, 2000.

REZENDE, Denis Alcides e ABREU, Aline França. **Tecnologia da Informação Aplicada a Sistemas de Informação Empresariais**. Editora Atlas. São Paulo, 2000.

BORAN, Sean. **IT Security Cookbook**, 1996. Disponível em: http://www.boran.com/security/. Acessado em: 15/06/2010.

MONTE, Antônio Carlos e LOPES, Luis Felipe. **A Qualidade dos Suportes de Armazenamento de Informações.** Visual Books, ano 2004.

MORIMOTO, Carlos E.. **Hardware, o Guia Definitivo.** GDH Press e Sul Editores, ano 2007

TORRES, Gabriel. **Hardware**. Axcel books, 4ª Edição.

OLTSIK, Jon e BIGGAR, Heidi. **White Paper: Segurança centrada nas informações e eliminação de dados**, Junho de 2006. Disponível em: http://brazil.emc.com/collateral/analyst-reports/esg-wp-emc-security-jul-06.pdf. Acessado em: 23/05/2010

BPMagazine. **Do papel ao PDA**, 2006. Disponível em: http://www.bpsolutions.com.br/bpmaga/edicao12/14_17_tecnologia.pdf , Acessado em: 22/06/2010

GARFINKEL, Simone. **Anti-Forensics: Techniques, Detection and Countermeasures**, 2007. Disponível em: http://www.simson.net/clips/academic/2007.ICIW.AntiForensics.pdf, Acessado em: 23/05/2010

Normas ABNT. Disponível em: http://www.abntcatalogo.com.br/, Acessado em 20/09/2010

GARFINKEL, Simon ; SHELAT, Abhi. **Remembrance of Data Passed: A Study of Disk Sanitization Practices**, 2003. Disponível em: http://www.simson.net/clips/academic/2003.IEEE.DiskDriveForensics.pdf, acessado em: 23/05/2010

GUTMANN, Peter. **Secure Deletion of Data from Magnetic and Solid-State Memory**, 1996. Disponível em: http://www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html, Acessado em: 29/05/2010

HOUSLEY, Russ; POLK, Tim. **Planning for PKI -** Best practices guide for deploying public key infrastructures. John Wiley and Sons, 2001

Revista Brasileira de Ensino de Física, v. 32, n. 1, 1504. **Estudando campos magnéticos e histerese com um anel de Rowland,** 2010**.** Disponivel em: http://www.sbfisica.org.br/rbef/indice1.php?vol=32&num=1. Acessado em 29/05/2010

National Security Agency. **Degausser Evaluated Products List**, 2007. Disponível em: http://www.nsa.gov/ia/_files/government/MDG/NSA_CSS_Storage_Device_Declassification_Manual.pdf, Acessado em: 15/06/2010

Associação Brasileira de Normas Técnicas. **ABNT Catalogo.** Disponível em: http://www.abntcatalogo.com.br, Acessado em: 15/06/2010

Defense Security Service. **ODAA Process Guide for C&A of Classified Systems under NISPOM**, 2008 Disponível em: http://www.dss.mil/isp/odaa/documents/odaa_process_guide_revised050908.pdf Acessado em: 15/06/2010

National Institute of Standards and Technology. **Guidelines for Media Sanitization,** 2006. Disponível em: http://csrc.nist.gov/publications/nistpubs/800-88/NISTSP800-88_rev1.pdf. Acessado em: 15/06/2010

Glary Soft. Disponível em http://www.glarysoft.com/products/utilities/glary-utilities/. Acessado em: 15/06/2010

National Industrial Security Program. **DoD 5220.22-M,** 2006. Disponível em: http://www.dss.mil/isp/odaa/documents/nispom2006-5220.pdf. Acessado em: 15/06/2010

Active Eraser. **Ultmante Data Security Tool:** User´s Manual, 2003. Disponível em: http://www.active-eraser.com/downloads/hdderaser.pdf, acessado em: 15/06/2010.

Recuva Quick Start. Disponivel em: http://docs.piriform.com/recuva/recuva-quick-start, acessado em 15/06/2010.

CETSB, **Licenciamento Ambiental,** http://www.cetesb.sp.gov.br/licenciamentoo/index.asp

DAUM, Magnus & LUCKS, Stefan. **Hash Collisions**. Disponível em: http://th.informatik.uni-mannheim.de/people/lucks/HashCollisions/, Acessado em 18/06/2010.

Schneier, Bruce. **Cryptanalysis of SHA-1.** Disponível em: *http://www.schneier.com/blog/archives/2005/02/cryptanalysis_o.html*, Acessado em 23/06/2010.

Marcus Ranun. **One-Time-Pad.** Disponível em: http://www.ranum.com/security/computer_security/papers/otp-faq/, Acessado em 24/06/2010

Two-Factor Authentication Token. Disponível em: http://www.insight.co.uk/files/whitepapers/Two-factor%20authentication%20(White%20paper).pdf , Acessado em 25/06/2010

Modelo PDCA aplicado para processos SGSI – Fonte: ISO 27001. Disponível em: www.iso.org acessado em 27/06/2010

Conselho de padrões de Segurança LLC do PCI. **Navegando pelo PCI DSS:** Entendendo o porquê dos requisitos, 2008. Disponível em: http://pt.pcisecuritystandards.org/_onelink_/pcisecurity/en2pt/doc/pci_dss_saq_navigating_dss.pdf acessado em 24/06/2010

MasterCard. MasterCard Logical Security Requirements for Card Personalization Bureaus, Editora: MasterCard Worldwide. O'Fallon, 2007.

Cultura Geek Alti**, CDROM.** Disponível em: http://alt1040.com/2009/12/los-cinco-grandes-perdedores-durante-la-decada-de-los-00s acessado em 02/04/2010

Cultura Geek Alti**, DVDROM.** Disponível em: http://alt1040.com/2009/12/los-cinco-grandes-perdedores-durante-la-decada-de-los-00s acessado em 02/04/2010

Cultura Geek Alti**, Blu-Ray**. Disponível em: http://alt1040.com/2010/07/el- blu-ray-no-tiene-quien-le-escriba acessado em 02/04/2010

Fazendo Vídeo, **Comparativo entre CDROM, DVDROM e Blu-Ray**. Disponível em: http://www.fazendovideo.com.br/vtfor2.asp acessado em 02/04/2010

Tech Fuels Technology savvy fórum **, Disco Rígido.** Disponível em: http://www.techfuels.com/optical-drives/4512-seagate-200-gb-sata-hard-disk-drive.html acessado em 02/04/2010

Somali Software**, Setores, trilhas e cilindros**. Disponível em: http://www.somalisoftware.com/aqoonta/pc/cash14-aad.shtml acessado em 02/04/2010

GDH Press**, Gravação Longitudinal**. Disponível em: http://www.gdhpress.com.br/hardware/leia/index.php?p=cap5-4 acessado em 05/05/2010

GDH Press**, Gravação Longitudinal 2**. Disponível em: http://www.gdhpress.com.br/hardware/leia/index.php?p=cap5-4) acessado em 05/05/2010

Lock System Informática, **Disquete**. Disponível em: http://www.locksys.com.br/produtos1.html acessado em 08/05/2010

Stock.Xchng , **Fita Carretel.** Disponível em: http://www.sxc.hu/photo/95464 acessado em 08/05/2010

Tape and Mídia, **Tape Cartridge**. Disponível em: http://www.tapeandmedia.com/detail.asp?product_id=18P7535 acessado em 08/05/2010

1 Giga, **Fita Half-Inch (DLT)**. Disponível em: http://www.1giga.com.br/popup_image.php?pID=228 acessado em 08/05/2010

Webdados, **Fita Quarter-Inch Cartridge (Travan)**. Disponível em: http://loja.webdados.pt/index.php?action=lista&id_tipo=503 acessado em 10/05/2010

Tech CD, **Fita 8 mm Helical - Scan (VXA)**. Disponível em: http://www.techcd.com.br/loja/mostra.asp?id=40007 acessado em 24/06/2010

Sul Mídia, **Fita 4 mm (Dat)**. Disponível em: http://www.sulmidia.com.br/produto/405/fita-dat-2040-gb-150-mt-sony-dds4.html acessado em 24/06/2010

Flickr, **Fita K7**. Disponível em: http://www.flickr.com/photos/minebilder/89489349/ acessado em 24/06/2010

Xoppi, **Cartão de Memória**. Disponível em: http://www.xoppi.com/fotoAmpliar.php?id=32198&idE=136652 acessado em 24/06/2010

Pelfusion **, Pen Drive**. Disponível em: http://pelfusion.com/tutorials/35-useful-adobe-illustrator-tutorials-for-3d-artwork/ acessado em 24/06/2010

Amit Bhawani**, Memória DRAM**. Disponível em: http://www.amitbhawani.com/blog/what-is-dimm/, acessado em 24/06/2010

Ice Fusion**, Memória EPROM**. Disponível em: http://www.icefusion.com.br/programacao/54-dicas/75-comando-fgetcsv-php, acessado em 24/06/2010

Sina Sihon**, Memória Magnetic Bubble**. Disponível em: http://www.sinasohn.com/cgi-bin/clascomp/bldhtm.pl?computer=shp5000 , acessado em 24/06/2010

Computer History, **Memória Magnetic Core**. Disponível em: http://www.computerhistory.org/semiconductor/timeline/1970-DRAM.html, acessado em 24/06/2010

Perangkat Komputer**, Memória Static Randon Access**. Disponível em: http://devilcomputer.blogspot.com/2009/11/sram-static-random-access-memory.html, acessado em 24/06/2010

Zazzle, **Cartão de Credito**. Disponível em: http://www.zazzle.com.br/empresa+cartoes+visitas acessado em 24/06/2010.

Áudio List**, Fita Perfurada**. Disponível em: http://audiolist.org/forum/kb.php?mode=article&k=263 acessado em 24/06/2010.

Data Securityinc, **Desmagnetizadores TIPO I, II e III**. Disponível em: http://www.datasecurityinc.com/degausser/products.html acessado em 24/06/2010.

Data Devices International, **Degaussers, Degaussing Equipment and More.** Disponivel em http://www.datadev.com/degausser-data-security-main.html acessado em 28/07/2010.

Akiko Ribeiro, **1° Seminário Estadual de Resíduos Tecnológicos: Manufatura Reversa.** 2009 Disponivel em: http://www.residuoselectronicos.net/archivos/noticias/seminariocearajunio09/presentaciones/AkikoRibeiroOXIL_SeminarioResiduosTecnologicos_Cearajunio2009.pdf Acessado em: 20/07/2010

GLOSSÁRIO

Coercividade – é a medida do campo magnético reverso necessário para zerar a magnetização após o magneto estar saturado.

Hash/Hashing - São funções que tomam como entrada um número arbitrário de bits e produzem uma saída de tamanho fixo.

Mícron – Unidade de medida onde 1 mícron equivale a 1 milésimo de milímetro.

Nanômetro – Unidade de medida onde 1 milímetro é dividido por um milhão.

OECD – *Organisation for Economic Co-operation and Development*

Oersteds - Unidade medida da força magnetizante para produzir uma força magnética desejada através de uma superfície.

PAD – Chave com sequências aleatórias de criptografia, utilizada na criptografia OPT (One Time Pad).

PDCA – Modelo descrito na norma ISO 27001, quer dizer *Plan* (Planejar), *Do* (Fazer), *Check* (Checar) e *Act* (Agir).

SHA – É uma família de algoritmos que está relacionada com funções criptográficas, seu significado é Secure Hash Algorithm. A função mais usada da família é a SHA-1, considerada o sucessor do MD5.

Token - São dispositivos de segurança para autenticação, geralmente são utilizados como complemento ou como substituição de uma senha.

ANEXO A

DSS matriz de saneamento e limpeza

O Departamento de Defesa dos Estados Unidos (NSA) disponibiliza uma matriz de saneamento, limpeza e descarte de mídias comuns. Segue abaixo um quadro e sua forma de leitura para a destruição dos dados.

Mídia	**Apagar**					**Sanear**														
Fita Magnética																				
Tipo I	a						b									l					
Tipo II	a						b									l					
Tipo III	a						b									l					
Disco Magnético																				
Bernoulli	a	C					b									l					
Disquete	a	C					b									l					
Disco Rígido Não Removível		C				a			d							l					
Disco Rígido Removível	a	C				a			d							l					
Discos Ópticos																				
Leitura e Grava varias vezes		C														l					
Apenas leitura																l	m				
Grava uma vez e le varias vezes																l	m				
Memória																				
Dynamic Random Access Memory (DRAM)		C	g					c					g				l					
Electronically Alterable Programmable Read Only Memory (EAPROM)				H											i		l					
Electronically Erasable PROM (EEPROM)				H							F						l					
Erasable Programmable ROM (EPROM)					j			**c**								**k**	l					k em seguida c
Flash EPROM (FEPROM)				H				**c**						**h**			l					h em seguida c
Programmable ROM (PROM)		C															l					
Magnetic Bubble Memory		C				a		c									l					
Magnetic Core Memory		C				a			d								l					
Magnetic Plated Wire		C						**c**			**e**						l					**c** e **e**
Magnetic Resistive Memory		C															l					
Non-Volatile RAM (NOVRAM)		C						c									l					
Read Only Memory (ROM)																	l					
Synchronous DRAM (SDRAM)		C	g					c					g				l					
Static Random Access Memory (SRAM)		C	g					c					g				l					
Outras Mídias																				
Fita de Vídeo																	l					
Filme																	l					
Equipamento																				
Monitor			g																	p		
Impressora de impacto			g										g							o		o e então g
Impressora a Laser			g										g						n			n e então g

Quadro 3 – Matriz de Saneamento e Limpeza

Fonte: Departamento de Defesa dos Estados Unidos NISPOM (2008)

Quando aparecer uma letra **sem** estar em negrito, quer dizer que uma única destas opções completará o procedimento: ex. NOVRAN: execute o procedimento c ou l que esta memória estará saneada. Onde houver letras em negrito, quer dizer que os

procedimentos deverão ser combinados para serem completos e na última coluna estará qual é ordem em que o procedimento deverá ser executado.

Abaixo os procedimentos a serem executados e suas respectivas letras:

a – Desmagnetizar com desmagnetizador tipo I, II ou III

b – Desmagnetizar com o mesmo tipo (I, II ou III) de desmagnetizador.

c – Sobrescrever todos os locais endereçáveis com um único caractere utilizando uma ferramenta de sobrescrita aprovada.

d – Sobrescrever todos os locais endereçáveis com um caractere, isto complementa, então utilize caracteres aleatórios.

e – cada dado sobrescrito deve residir na memória por um período maior que o dado anterior residia.

f – Sobrescrever todos os locais com um padrão de dados aleatórios, em seguida com zeros binários e finalmente com binários 1 utilizando uma ferramenta aprovada para sobrescrita.

g – Remover toda a força elétrica para incluir a bateria.

h – Realize o total apagamento do chip conforme o padrão de fabricação.

i – Realize o procedimento **h,** em seguida **c**, num total de três vezes.

j – Realize um apagamento com ultravioleta conforme recomendações de fabricação

k – Realize o procedimento **j**, mas incremente o tempo por três.

l – Destruição

m – Destruição é apenas necessária se conter informações classificadas (confidências, internas, etc.).

n – Imprimir uma página (Pode ser teste de fonte) quando o ciclo de impressão não se completar (ex. Atolamento de papel ou falha de energia). Descarte do produto não classificado se um exame visual não revelar qualquer informação classificada.

o – As fitas de impressão devem ser destruídas, as placas limpas.

p – Inspecionar e/ou testar a superfície da tela para evidência de informações queimadas na tela, se apresentarem informações, a tela deve ser destruída.