

2.3 PROCEDIMENTOS PARA HASH

A função criptográfica hash é um algoritmo utilizado para garantir a integridade de um documento eletrônico, de modo que um perito técnico possa comprovar que não houve alteração neste documento desde a época em que este foi transformado. Assim, uma simples alteração neste documento acarretará uma alteração do resumo hash original, desconstituindo assim a prova de integridade do depósito do programa de computador.

A transformação do programa de computador em resumo digital hash será feita pelo titular do direito utilizando algoritmos públicos hash, e esta informação irá compor o formulário eletrônico e-Software quando do pedido de registro.

RECOMENDA-SE O USO DE ALGORITMO SHA-512 OU ALGORITMO MAIS RECENTE PARA A OBTENÇÃO DO RESUMO DIGITAL HASH.

Alguns destes algoritmos também são encontrados em ambiente Linux. Por exemplo, para rodar o algoritmo SHA-512 no Linux, basta executar a seguinte linha de comando: sha512 sem nome do arquivo.

Substitua a expressão nome_do_arquivo pelo nome do arquivo de origem, incluindo a

extensão (ex.: código_fonte.pdf).

Outra possibilidade para gerar o hash é utilizando um comando nativo do Microsoft

Windows. Para o Windows 7, siga os passos abaixo:

1) Copie o arquivo a partir do qual deseja gerar o resumo hash para a Área de Trabalho

(Desktop);

2) Clique no botão “Iniciar” no canto inferior esquerdo da tela;

3) No campo de pesquisa, digite a palavra “cmd” e tecle “Enter”;

4) Na janela aberta (Prompt de comando), digite o seguinte comando:

cd Desktop

5) Tecle “Enter”;

6) Insira, agora, a linha de comando abaixo: (exemplo)

CertUtil -hashfile nome SHA512 | find /i /v "sha512" | find /i /v "certutil" > temp.txt

substituindo a palavra nome pelo nome do arquivo de origem, incluindo a extensão (ex.:

código_fonte.pdf), e tecla "Enter";

7) Por fim, copie e cole no prompt de comando as duas linhas de código abaixo:

```
powershell -Command "(gc temp.txt) -replace ' ', '' | Out-File resumo_hash.txt"
```

```
taskkill /IM notepad.exe
```

8) Abra o arquivo-texto gerado na Área de Trabalho (Desktop), nomeado "resumo_hash.txt". O resumo hash contido neste arquivo é exatamente o trecho que

Função hash	Resumo hash	Tamanho do resumo hash
MD5	9e107d9d372bb6826bd81d3542a419d6	32
SHA-1	2fd4e1c67a2d28fced849ee1bb76e7391b93eb12	40
SHA-224	730e109bd7a8a32b1cb9d9a09aa2325d2430587ddbc0c38bad911525	56
SHA-256	d7a8fbb307d7809469ca9abcb0082e4f8d5651e46d3cdb762d02d0bf37c9e592	64
SHA-512	07E547D9586F6A73F73FBAC0435ED76951218FB7D0C8D788A309D785436BBB642E93A25 2A954F23912547D1E8A3B5ED6E1BFD7097821233FA0538F3DB854FEE6	128

Tabela 1 - Exemplos de resumos hash

deve ser copiado e colado no formulário de consulta de software.