Notas de Aula de Arquitetura e Organização de Computadores

BIOS e UEFI

BIOS

Chip de BIOS do tipo DIP (Dual In Parallel), encontrado em placas-mãe antigas, **BIOS**, em computação ***Basic Input/Output System*** (Sistema Básico de Entrada/Saída). O BIOS é um programa de computador gravado em *firmware* executado por um computador quando ligado. Ele é responsável pelo suporte básico de acesso ao hardware, como iniciar a carga do sistema operacional

Origem do termo

O termo apareceu pela primeira vez no sistema operacional CP/M, descrevendo a parte do sistema carregada durante a inicialização, que lidava diretamente com o hardware (máquinas CP/M normalmente tinham apenas um simples boot loader na ROM). A maioria das versões do DOS tem um arquivo "IBMBIO.COM" ou "IO.SYS" que são análogos ao disco CP/M BIOS.

Onde se localiza

Chip de BIOS do tipo PLCC (Plastic Leaded Chip Carrier), encontrado em placas-mãe modernas. O BIOS é armazenado num chip ROM (*Read-Only Memory*) que pode ser do tipo Mask-ROM e PROM nas placas-mãe produzidas até o início da década de 1990, e Flash ROM (memória flash) nas placas mais recentes. Na memória ROM da placa-mãe existem mais dois programas chamados Setup (usado para configurar alguns parâmetros do BIOS), e POST (Power On Self Test) (uma seqüência de testes ao hardware do computador para verificar se o sistema se encontra em estado operacional).

Funcionamento

MBR (Master Boot Record) é lida pelo BIOS, que interpreta a tabela de partição e em seguida carrega um programa chamado *Bootstrap*, que é o responsável pelo carregamento do Sistema Operacional, no setor de boot da partição que dará o boot. O MBR e a tabela de partição ocupam apenas um setor de uma trilha, o restante dos setores desta trilha não são ocupados, permanecendo vazios e inutilizáveis, servindo como área de proteção do MBR.

Entre outras funções o papel mais importante do BIOS é o carregamento do S. Op.. Quando o computador é ligado e o microprocessador tenta executar sua primeira instrução, ele tem que obtê-la de algum lugar. Não é possível obter essa instrução do sistema operacional, pois esse se localiza no disco rígido, e o microprocessador não pode se comunicar com ele sem que algumas instruções o digam como fazê-lo. É o BIOS o responsável por fornecer essas instruções.

Sequência de funcionamento

Quando o computador é ligado, o BIOS opera na seguinte sequência:

1. Verifica as informações armazenadas em uma prquena parte da RAM, que se localiza em um chip fabricado com tecnologia CMOS. A memória CMOS armazena informações relativas a configuração de hardware, que podem ser alteradas de acordo as mudanças do sistema. Essas informações são usadas pelo BIOS modificar ou complementar sua programação padrão, conforme necessário.
2. POST (Power-On Self-Test ou Autoteste de Partida), que são os diagnósticos e testes realizados nos componentes físicos (Disco rígido, processador, etc). Os problemas são comunicados ao usuário por uma combinação de sons (bipes) numa determinada seqüência e se possível, exibidos na tela. O manual do fabricante permite a identificação do problema descrevendo a mensagem que cada seqüência de sons representa.
3. Ativação de outros BIOS possivelmente presentes em dispositivos instalados no computador (ex. discos SCSI e placas de vídeo).
4. Descompactação para a memória principal. Os dados, armazenados numa forma compactada, são transferidos para a memória, e só aí descompactados. Isso é feito para evitar a perda de tempo na transferência dos dados.
5. Leitura dos dispositivos de armazenamento, cujos detalhes e ordem de inicialização são armazenados na CMOS. Se há um sistema operacional instalado no dispositivo, em seu primeiro sector (o Master Boot Record) estão as informações necessárias para o BIOS encontrá-la (este sector não deve exceder 512 bytes).

Existem pequenos trechos de softwares chamados de *Manipuladores de Interrupção* que atuam como tradutores entre os componentes de hardware e o sistema operacional. Um exemplo dessa tradução é quando é pressionada uma tecla no teclado, o evento associado ao sinal é enviado para o manipulador de interrupção do teclado que é enviado a CPU que trata e envia esse evento para o sistema operacional. Os drivers de dispositivos são outros trechos de software que identificam e atuam como interface entre os componentes básicos de hardware como o teclado, mouse, disco rígido.

Bateria

Bateria de Lítio CR2032 3V

A bateria interna do tipo Lítio (bateria de lítio) CR2032 tem a função de manter as informações da *Flash-ROM* (EEPROM) armazenadas enquanto o computador está desligado (somente em placas-mãe antigas, nas atuais sua principal função é manter o relógio interno funcionando). A bateria de lítio é dotada de três volts de potência para que mantenha funcionando sem atrasar o relógio e outros componentes como as informações gravadas na BIOS.

Inicialização do Computador

Ao ligar o computador, o 1º software lido é o BIOS. Durante a sequência de inicialização, o BIOS efetua operações para deixar o computador pronto a ser usado. Depois de verificar a configuração na CMOS e carregar os manipuladores de interrupção, o BIOS determina se a placa gráfica está operacional. Então o BIOS verifica se é 1ª inicialização (cold boot) ou de uma reinicialização (reboot).

Esta verifica as portas PS/2 ou portas USB à procura de um teclado ou um mouse. Procura igualmente por um barramento PCI e, caso encontre algum, verifica todas as placas PCI instaladas. Se o BIOS encontrar algum erro durante o início (POST), haverá uma notificação ao utilizador em forma de bipes e mensagens. Após tudo isto são apresentados detalhes sobre o sistema:

- Processador
- Unidades (drives) de disco flexível e disco rígido

- Memória
- Versão e data do BIOS

Recursos

Na maioria dos BIOS é possível especificar em qual ordem os dispositivos de armazenamento devem ser carregados. Desta forma é possível, por exemplo, carregar uma distribuição do sistema operacional Linux que funciona diretamente do CD antes do sistema operacional instalado no HD

Alguns BIOS também permitem a escolha entre diversos sistemas operacionais instalados, mas isto geralmente é feito com um software de terceiros (*boot loader*).

Atualização ou Upgrade

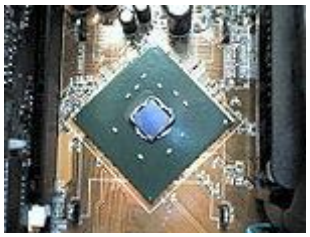
De um modo geral nas placas-mãe o BIOS pode ser atualizado, e os fabricantes disponibilizam arquivos para essa finalidade. A atualização pode resolver problemas de funcionamento de periféricos, ou mesmo erros da versão anterior do BIOS. Ela altera 3 programas da memória ROM (BIOS, POST, Setup) e é uma operação de risco requerendo cuidado para não haver danos na placa-mãe.

Há vários problemas que podem acontecer nas atualizações, alguns deles são: arquivos corrompidos, falta de informações para a solicitação do software correto, ou ainda a falta de energia elétrica. Ocorrendo problemas o S.Op. poderá não iniciar, deixando a placa-mãe inoperante.

O upgrade do chip deve ser feito quando for realmente necessário. Os fabricantes do *firmware* são: American Megatrends, Award, General Software, Insyde Software, e Phoenix Technologies.

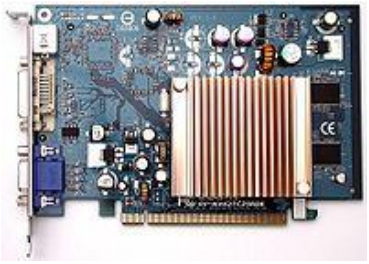
Chipset

Chipset é um *chip* (ou conjunto de *chips*) responsável pelo controle de diversos dispositivos de entrada e saída como o barramento de comunicação do processador, o acesso à memória, o acesso ao HD, periféricos *on-board* e *off-board*, comunicação do processador com a memória RAM e entre outros componentes da placa-mãe. Geralmente, é dividido em southbridge e northbridge.

• O **northbridge** faz a comunicação do processador com as memórias, através do barramento de comunicação externa do processador, e com os barramentos de alta velocidade AGP e PCI Express. Faz o trabalho mais pesado, requer um dissipador de calor devido ao seu aquecimento elevado.	• O **southbridge** geralmente é responsável pelo controle de dispositivos de entrada ou saída (I/O) como as interfaces IDE que ligam os HDs, os drives de CD-ROM, drives de DVD-ROM ao processador. Controlam as interfaces SATA. Cuidam do controle de dispositivos *on-board* como o som.
 Northbridge da placa-mãe ASUS P4P800-E	 Southbridge da placa-mãe ASUS P4P800-E

Slots de expansão

placa de rede 100Mbit tipo PCI da NIC



Algumas tecnologias foram desenvolvidas para dar maior flexibilidade aos computadores pessoais uma vez que cada cliente pretende utiliza-lo para um fim específico. O barramento **PCI** ou ***Peripheral Component Interconnect*** é uma tecnologia para conectar diferentes periféricos na Placa-mãe. Veja maiores detalhes no artigo Peripheral Component Interconnect.

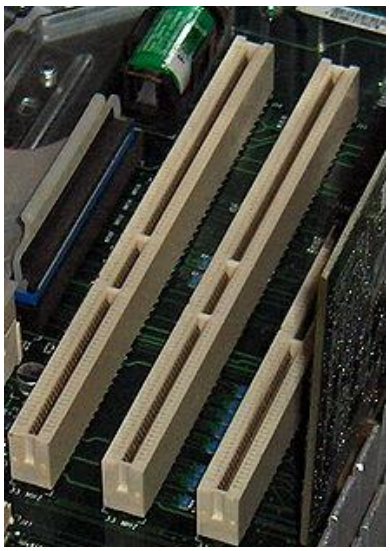
O barramento **AGP** ou ***Accelerated Graphics Port*** foi uma tecnologia de barramento usada principalmente por placas de vídeo. As placas AGP excedem um pouco em tamanho as placas PCI. A tecnologia AGP foi substituída pelo barramento PCI Express. A tecnologia PCI Express conta com um recurso que permite o uso de uma ou mais conexões seriais.

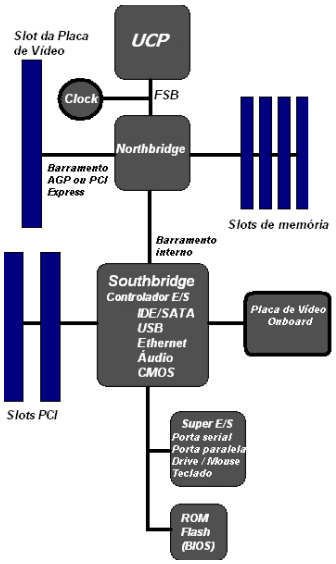
Controladores

- ***On-board***: como o próprio nome diz, o componente *on-board* vem diretamente conectado aos circuitos da placa mãe, funcionando em sincronia e usando capacidade do processador e memória RAM quando se trata de vídeo, som, modem e rede. Tem como maior objetivo diminuir o preço das placas ou componentes mas, em caso de defeito o dispositivo não será recuperável. São exemplos de circuitos *on-board*: vídeo, modem, som e rede.
- ***Off-board***: são os componentes ou circuitos que funcionam independentemente da placa mãe e por isso, são separados, tendo sua própria forma de trabalhar e não usando o processador, geralmente, quando vídeo, som, modem ou rede, o dipositivo é "ligado" a placa-mãe usando os *slots* de expansão para isso, têm um preço mais elevado que os dispositivos *on-board*, sendo quase que totalmente o contrário em todos os aspectos do tipo *on-board*, ou seja, praticamente todo o processamento é realizado pelo próprio *chipset* encontrado na placa do dispositivo.

Slot

Slot é um termo em inglês para designar ranhura, fenda, conector, encaixe ou espaço.





Sua função é ligar os perifericos ao barramento e suas velocidades são correspondentes as do seus respectivos barramentos. Nas placas-mãe são encontrados vários slots para o encaixe de placas (vídeo, som, modem e rede por exemplo). Alguns exemplos de slots: ISA, PCI, AGP e PCI Express.

Configurando o Setup do BIOS

O Setup:

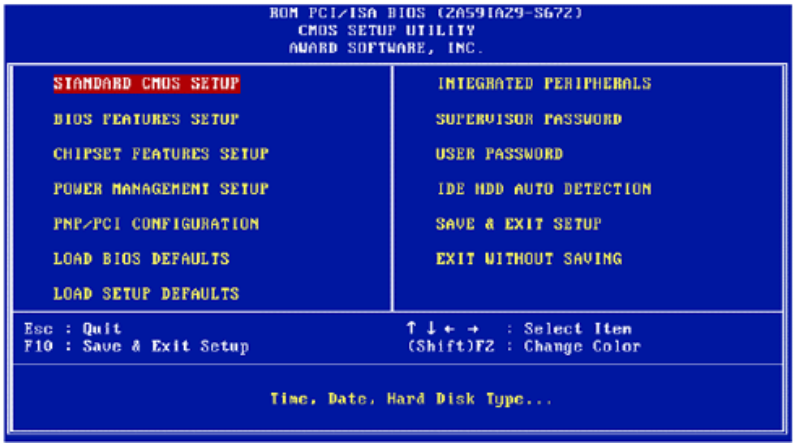
O Setup contém todas as informações para que o sistema reconheça os componentes instalados no computador: se qualquer dispositivo não for identificado ou localizado pelo BIOS, ocorrerá problemas para fazê-lo funcionar no sistema operacional.

As informações da identificação e localização dos componentes ficam gravadas no CMOS *Complementay Metal Oxide Semicondutor*, que é uma memória RAM embutida no chip do BIOS.

Para acessar o Setup do computador, quando o mesmo é ligado aparecerá uma mensagem semelhante a esta: “Pressione a tecla <**Del**> para rodar o Setup”. Pressione-a e aparecerá esta tela: (este é um Setup do fabricante do BIOS chamado “Award”, sendo que cada placa-mãe tem uma versão de Setup, variando os fabricantes e versões.)

1. **Standard CMOS Setup**: Configurações do HD, drive de disquetes, drives de CD-ROM, data e hora. Aqui também poderá ativar UDMA (em setup's de BIOS AMI) e no caso de BIOS "Award" UDMA é configurado na opção abaixo:

2. **BIOS Features Setup - *Advanced CMOS Setup*** - Aqui é encontrado informações de sequência de Boot além de configuração de caches, quantidade de memória RAM e algumas opções do BIOS, entre muitas outras (mais abaixo são apresentados as melhores configurações). Algumas opções podem aparecer com nomes diferentes, dependendo da marca e do modelo do BIOS.



2.1 Virus Warning - Ativando esta opção ele irá monitorar gravações no MBR (Master Boot Recording) do HD. O setor MBR é o responsável pela inicialização, sendo que ele irá indicar onde está o sistema (em C:\ ou D:\, por exemplo). Caso seja detectada alguma tentativa de gravação no setor de boot, o BIOS irá parar o sistema (sendo que não irá passar desta etapa, a não ser que autorize a gravação no setor MBR), interrompendo a gravação e exibindo na tela uma mensagem de alerta (perguntando se deve autorizar ou não a gravação). Deixe "*Enable*" para prevenir vírus no computador (é altamente recomendável um bom Anti-Vírus instalado no computador sendo que a maioria deles pode detectar vírus de boot).

2.2 CPU Internal cachê: *CPU Level 1 cache, L1 cache* - Esta opção permite habilitar ou desabilitar o *cache* interno do processador (cache L1). Desabilite-o se estiver muitos problemas graves com seu computador, mas o sistema irá ficar extremamente lento. É altamente recomendável ativar esta opção e ela está ativada por padrão.

2.3 CPU External cachê: *CPU Level 2 cache, L2 cache* - Esta opção permite habilitar ou desabilitar o *cache* externo do processador (cache L2). Desabilite-o se ocorrer muitos problemas de travamento do seu computador, mas o sistema irá ficar extremamente lento. É altamente recomendável ativar esta opção. Alguns processador não possuem esta opção (o que deixa o computador também um pouco lento).

2.4 1st Boot Sequence – Define-se qual será a primeira opção de Boot: deixe em "IDE-0".

2.5 2nd Boot Sequence – Define-se qual será a segunda opção de Boot: deixe em "Floppy".

2.6 Try other Boot Devices - Aqui se define quais serão as outras formas de Boot: deixe em "Disable" pois geralmente as outras opções acima darão o Boot.

2.7 Boot UP Num Lock Status - Esta opção serve apenas para determinar se a tecla Num Lock permanecerá ligada (**on**) ou desligada (**off**) quando o micro for inicializado.

2.8 System BIOS Shadow, Video Bios Shadow - Ativando estas opções, será feita uma cópia do conteúdo do BIOS principal e do BIOS da placa de vídeo na RAM. A memória RAM é muito mais rápida do que a memória ROM do BIOS e o Boot será levemente mais rápido.

3. **Chipset Features Setup: Advanced Chipset Setup** - Esta seção armazena opções de desempenho da memória RAM e da memória *cache*, placa de vídeo e modem. Pode-se fazer OC (*Overclock*) na memória RAM (algo que só é recomendável em poucas situações).

4. **PNP/PCI Configuration** - Contém opções para configurar manualmente os endereços de IRQ e DMA ocupados pelos dispositivos externos: são os famosos Plugs&Play. A maioria dos periféricos atuais são Plug&Play.
5. **Power Management Setup** - Aqui se pode configurar opções de modos de economia de energia como desligamento automático do seu monitor, teclado e HD depois de certo tempo de inatividade. Estas opções podem ser feitas pelo Windows em "Painel de Controle/Gerenciamento de Energia" e por isso usualmente não há necessidade de alterar as configurações no próprio Setup.
6. **Integrated Peripherals: Features Setup** - Tudo que se adiciona ao computador é configurado nesta opção: aqui pode-se desabilitar qualquer um dos dispositivos da placa mãe, incluindo as portas IDE, a porta do drive de disquetes, portas IEE1324 (as famosas portas Fireware), portas USB, portas de impressoras, portas seriais etc., RAID, SATA (nova tecnologia das placas mães de transferências de dados) além de configurar algumas outras opções e os endereços de IRQ ocupados por estes dispositivos.
7. **IDE HDD Auto Detection: Detect IDE Master/Slave, Auto IDE** - Ao instalar um disco rígido novo, não se esqueça de usar esta opção para que o Bios detecte o HD automaticamente: se ele ainda não reconhecer, entre em "Standard CMOS Setup" e configure-o manualmente.
8. **User PASSWORD** - Aqui se coloca senha tanto para tentativa de entrada no sistema quanto no setup.
9. **Load BIOS Default** – Aqui se pode *resetar* o BIOS para as suas configurações default.
10. **Load SETUP Defaults**- Aqui se pode *resetar* o SETUP do BIOS: isto irá definir que o computador carregue apenas as opções necessárias para que o computador funcione.

Arquivo de Etiqueta: BIOS

Boot Seguro e UEFI

Unifed Extensible Firmware Interface (UEFI) ou, Interface Unificada de Firmware Extensível, é uma especificação desenhada para substituir o subsistema BIOS (Basic Input Output System) que se encontra presente em todos os computadores. A BIOS é uma peça essencial para coisas tão elementares como instalar um sistema operativo quando ainda não existe nenhum SO instalado.

A necessidade de evolução da BIOS nasceu, tal como quase tudo na indústria, de limitações da plataforma anterior, como por exemplo o limite de endereçamento direto de memória, o aspeto gráfico ou questões de atualização. Esta evolução começou quando a Microsoft indexou a obtenção do logotipo de certificação a uma funcionalidade designada de "Secure Boot" que se começou a falar sobre UEFI.

Neste artigo é explicado o que é o Boot Seguro e como é que o mesmo funciona.

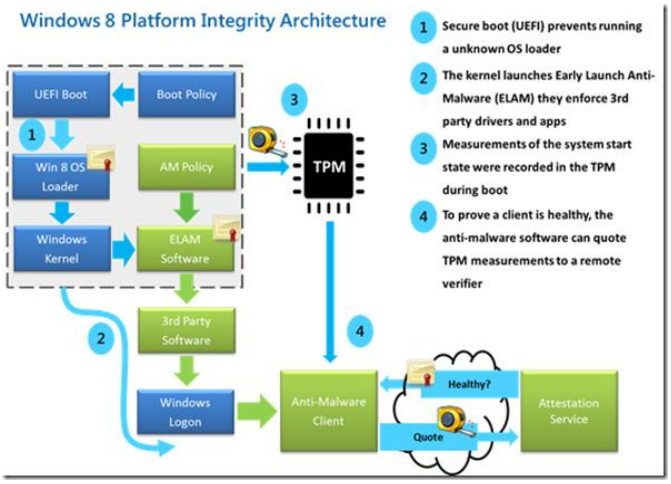


Imagem 1 – Arquitetura integridade da plataforma Windows 8

Arranque Seguro (Safe Boot)

O Arranque Seguro foi desenvolvido para impedir malware de se infiltrar na máquina antes do próprio sistema operativo iniciar a sequência de arranque. Se um malware for capaz de se carregar antes do sistema operativo arrancar, o mesmo passa a ter a capacidade de contornar e evitar qualquer medida de segurança e ao mesmo tempo tornar-se invisível (*recomendo leitura do artigo Rootkits*).

O processo de Arranque Seguro segue o princípio das assinaturas onde apenas o software assinado e aprovado pode ser executado. Se uma peça de software, seja ela sistema operativo, ROMs ou firmware, não se encontrar assinada e aprovada a execução da mesma é recusada.

Imagem 2 – Percurso de arranque com a BIOS no modo Legado

A primeira peça a ser assinada e autorizada é o Gestor de Arranque do Windows que desta forma impede a partir daquele momento a execução de qualquer outro software antes dele que não se encontre devidamente assinado e autorizado.

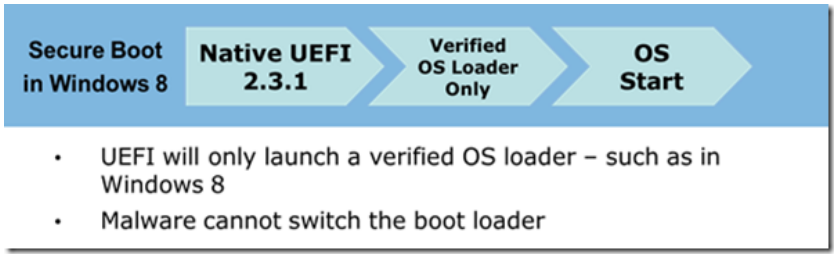


Imagem 3 – Percurso de Arranque Seguro com via UEFI

Modo de funcionamento

Internamente o UEFI está dividido em três áreas: Uma que contém a lista de signatários e assinaturas das aplicações autorizadas, conhecida por “db”, uma outra área com o oposto, ou seja, com a lista de signatários não confiáveis ou revogados e aplicações não autorizadas, conhecida por “dbx”, e por último uma área que é usada para atualizar a lista de assinaturas autorizadas e revogadas, conhecida por “KEK”.

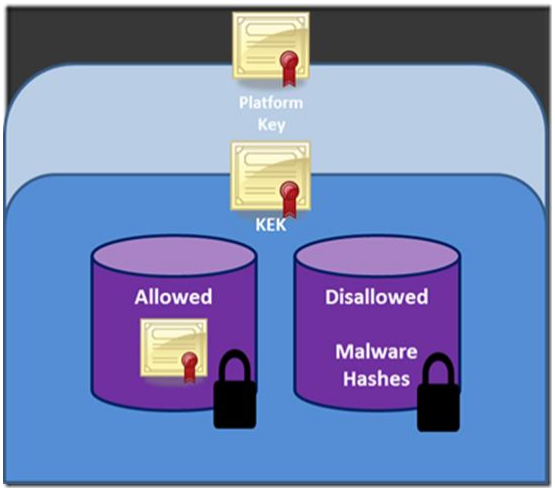


Imagem 4 – Bases de dados de segurança para os certificados

Depois de o computador ser ligado, as bases de dados de assinaturas são comparadas com a chave de plataforma. Se o firmware não for confiável, o firmware UEFI tem de iniciar o processo de recuperação específico do fabricante para restaurar um firmware confiável. Se houver um problema

com o Gestor de Arranque do Windows, o firmware tentará usar uma cópia de segurança do Gestor de Arranque do Windows. Se isto também falhar, o firmware tem de iniciar o processo de remediação específico do fabricante. Após o início da execução do Gestor de Arranque do Windows, se houver um problema com os controladores ou com o núcleo NTOS, é carregado o Ambiente de Recuperação do Windows (Windows RE), para que seja possível recuperar a imagem destes controladores ou do núcleo. Em seguida, o Windows carrega o software antimalware. Finalmente, o Windows carrega os outros controladores do núcleo e inicializa os processos em modo de utilizador.

Aspetos negativos do Boot Seguro

Uma das questões levantadas por esta implementação está relacionada com o fato de uma vez o Windows 8 instalado na máquina apenas versões futuras do sistema operacional Windows poderão ser instaladas. Se tentar numa máquina com UEFI/Windows 8 instalar um Linux vai verificar que o mesmo não é possível porque o arranque do boot loader do Linux não vai ser autorizado a arrancar.

Da mesma forma que é possível impedir outros boot loaders de arrancarem é possível instrumentar o arranque seguro para por exemplo impedir a instalação do Windows Server numa máquina que tenha sido vendida com o propósito de correr apenas o Windows 8.

Para aumentar o grau de complexidade deste tema podemos ainda adicionar os seguintes fatos:

- Para se poder gerar chaves válidas, o boot loader precisa ser assinado por uma CA de confiança este processo é simples numa empresa que produza código fechado mas difícil de se conseguir com código aberto como é o caso do Linux.
- A maior parte dos fabricantes não incluíram nas placas mães a funcionalidade de desligar o Arranque Seguro fazendo com que seja na maior parte dos casos um processo irreversível.

Como determinar se o Windows está dando Boot em modo BIOS ou UEFI

Existem diversas técnicas para determinar que modo uma instalação do Windows está a usar para arrancar. Abaixo listo apenas dois desses métodos.

Método #1

1. Executar o comando “msinfo32”
2. Na janela “Informações de sistema” o valor do campo “Modo de BIOS” indica o modo de arranque do Windows

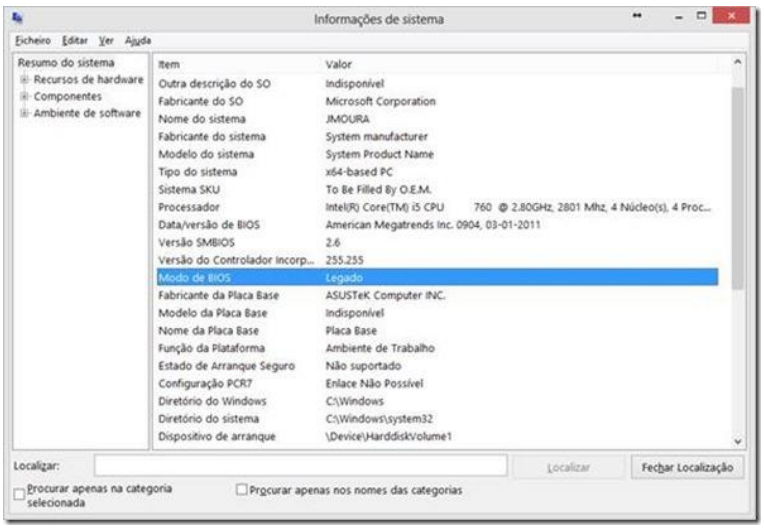


Imagem 5 – Janela Informações de Sistema mostrando que a BIOS se encontra em modo Legado

Método #2

1. Executar o comando “notepad C:\Windows\Panther\setupact.log”
2. No Bloco de Notas pesquisar por “Detected boot environment”

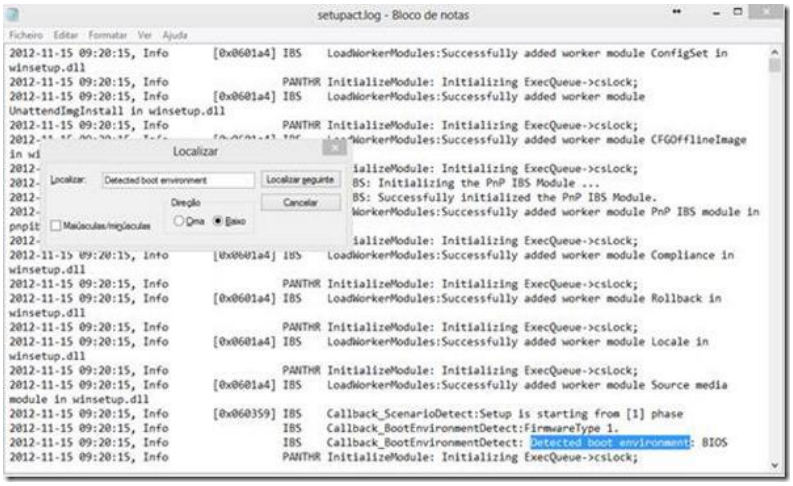


Imagem 6 – Entrada do ficheiro setupact.log mostrando que a BIOS se encontra em modo Legado

Microsoft mostra detalhes do menu de boot do Windows 8

Boot rápido demais do Windows 8 pode virar um problema.

A Microsoft fez várias otimizações para deixar a inicialização do Windows 8 mais rápida e isso acabou se tornando um problema. Imagine que se esteja querendo entrar no modo de segurança do Windows para corrigir algum problema com drivers ou softwares mal feitos. No Windows 7 e anteriores, basta teclar F8 e navegar pelo menu seguro. No Windows 8, o processo é o mesmo, mas será preciso ser mais ágil.

Em computadores com SSD e placa mãe UEFI, o tempo para apertar F8 antes que o Windows 8 inicie é de menos de 200 milissegundos. De acordo com a Microsoft, uma pessoa rápida consegue pressionar repetidamente uma tecla a cada 250 milissegundos – ou seja, quatro teclas por segundo. A tentativa de acessar o setup da placa mãe teclando Delete também seria frustrante.

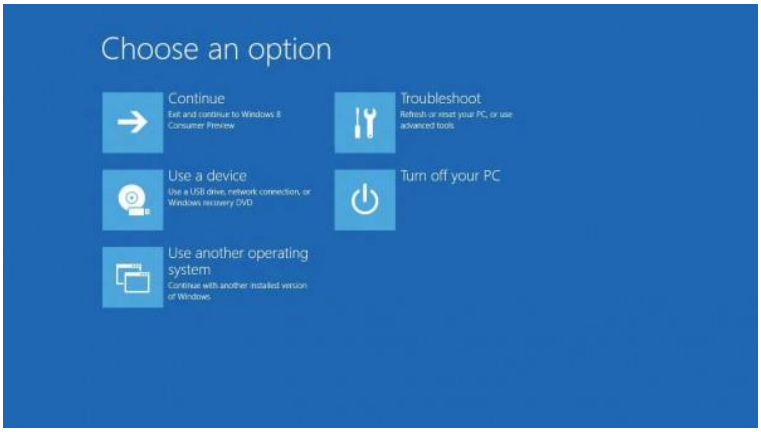


Imagem 7 – Não falaram se é possível bootar o Ubuntu direto desse menu.

Para resolver o problema, Chris Clark, um dos responsáveis pela experiência de usuário dos produtos da Microsoft, apresentou detalhes do novo gerenciador de boot do Windows 8, que traz opções de sobra para recuperar o sistema e pode ser acessado mesmo quando o processo de inicialização do Windows já tiver começado

As novidades são bem úteis. Ao se iniciar o Windows 8 por engano, é possível desligá-lo instantaneamente ou dar boot em outro sistema, como o Windows 7. Além disso, usuários com placa mãe UEFI podem clicar (ou tocar) numa opção do menu e dar boot por meio de um pendrive ou DVD de recuperação do Windows, por exemplo.

Uma seção de opções avançadas traz várias ferramentas para reparar o Windows, desde a restauração do sistema direto do menu de boot até um botão para acessar as configurações da placa mãe. Também será possível utilizar uma ferramenta de reparação automática, acessar o prompt de comando e restaurar uma imagem do Windows.

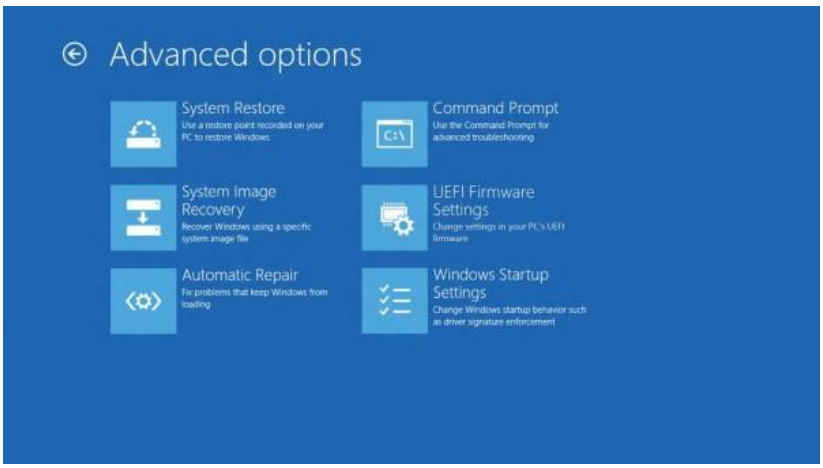


Imagem 8 – Restauração de imagem sem DVD de recuperação, até que enfim!

A BIOS da inicialização do sistema está presente a tanto tempo em nossas vidas que raramente pensamos em uma forma diferente de inicializarmos a nossa máquina. Com décadas de existência, nenhuma proposta teve força ou popularidade suficiente para derrubar a conhecida tela preta que vemos toda vez que ligamos o PC. Pelo menos até agora.

Intel e HP trabalham desde os anos 1990 no EFI (Extensible Firmware Interface – Interface de Firmware Extendida) que é uma forma mais avançada e versátil de dar "boot" no computador, e ao chegar na versão 1.1 teve seu nome atualizado para UEFI (Unified EFI) e foi entregue ao *Unified EFI Forum* que incorporou inúmeros recursos como criptografia, interface avançada para o usuário e autenticação via rede.

O resultado é uma experiência de uso bastante aprimorada, com novas funcionalidades e uma aparência muito mais intuitiva do que a clássica BIOS oferece. Como é possível observar na imagem abaixo, é possível utilizar o mouse para navegar pelas opções do UEFI e ter muito mais controle sobre todas as partes do hardware, permitindo que o usuário comum consiga fazer o que desejar sem precisar recorrer a um expert em computação, ou mesmo correr o risco de queimar o equipamento

Uma das grandes reclamações da maioria dos usuários é que - independentemente da configuração da máquina - o sistema necessita de muito tempo para ligar, onde grande parte dele é devido à baixa performance da BIOS, que acrescenta de 10 a 15 segundos no tempo total. Em computadores equipados com UEFI é possível realizar um boot completo em até oito segundos, tempo ainda menor se o PC estiver equipado com uma SSD.

Duas críticas muito recorrentes ao UEFI se referem à segurança (devido ao grande poder que o chip tem sobre o hardware e o sistema operacional) e ao aparecimento de bugs imprevisíveis, pois se trata de uma tecnologia nova. Por mais que a BIOS seja limitada, já está bastante amadurecida e seus bugs não são apenas previsíveis como fáceis de consertar.

Normalmente os usuários se preocupam com esses dois pontos, mas pode ser uma história parecida com a dos SSDs, que a princípio eram vistos com desconfiança, porém hoje são a melhor alternativa para quem procura alto desempenho.

O que é UEFI?

Aplica-se ao Windows 8.1, ao Windows RT 8.1

UEFI é uma interface de firmware padrão para PCs, projetada para substituir o **BIOS**. Esse padrão foi criado por mais de 140 empresas de tecnologia como parte do consórcio UEFI, incluindo a Microsoft. Ele foi projetado para aprimorar a interoperabilidade do software e lidar com as limitações do BIOS. Estas são algumas das vantagens do firmware UEFI:

- Segurança aprimorada para ajudar a proteger o processo de pré-inicialização contra ataques do tipo **bootkit**.
- Tempos de inicialização mais rápidos e retomada da hibernação.
- Suporte para unidades com mais de 2,2 TB.

- Suporte para drivers de dispositivos modernos com firmware de 64 bits que o sistema pode usar para lidar com mais de 17,2 GB de memória durante a inicialização.
- Capacidade de usar BIOS com hardware UEFI.

UEFI faz o mesmo trabalho que o BIOS, mas com uma diferença básica: ela armazena todos os dados sobre inicialização e início em um arquivo . efi, em vez de armazená-las no firmware.

UEFI tem um menu de configuração detalhado, mais útil do que a **BIOS** tradicional. **UEFI** suporta inicialização segura, evitando que o PC seja danificado por malware. **UEFI** é executado no modo de 32 ou 64 bits e o espaço de endereço endereçável é aumentado com base na **BIOS**, o processo de inicialização é muito mais rápido.

A **UEFI** fornece uma interface "limpa" entre o Sistema Operacional e o "firmware" da máquina durante o período de inicialização e fornecerá suporte a um mecanismo independente da arquitetura para inicializar placas controladoras de dispositivos.

Como habilitar o modo UEFI na BIOS?

Para inicializar para UEFI ou BIOS:

1. Inicialize o computador e pressione a tecla do fabricante para abrir os menus. Chaves comuns usadas: Esc, Delete, F1, F2, F10, F11 ou F12. ...
2. Ou, se o Windows já estiver instalado, na tela Entrar ou no menu Iniciar, selecione Power () > manter Shift ao selecionar Reiniciar.

Quais as vantagens do sistema em UEFI?

Aplica-se ao Windows 8.1, ao Windows RT 8.1

Estas são algumas das **vantagens** do firmware **UEFI**: Segurança aprimorada para ajudar a proteger o processo de pré-inicialização contra ataques do tipo bootkit. Tempos de inicialização mais rápidos e retomada da hibernação. Suporte para unidades com mais de 2,2 terabytes (TB).

UEFI x BIOS: Qual a diferença?

As siglas UEFI: Unified Extensible Firmware Interface e BIOS: Basic Input/Output System.

Procedimento de boot

Em primeiro lugar, sei que estamos desviando do assunto, mas prometo que isso vai ajudar com alguns conceitos mais tarde.

Como é feito o boot no computador: descrição passo a passo:

1. Deve-se pressionar o botão de ligar/desligar do seu laptop ou desktop.
2. A CPU inicia, mas precisa de algumas instruções para funcionar (lembre-se: a CPU sempre precisa fazer algo). Como a memória principal está vazia neste momento, a CPU se restringe às instruções de carregamento do chip do firmware da placa-mãe e começa a executar essas instruções.
3. O código do firmware faz um Power On Self Test (POST, ou autoteste de inicialização), inicializa o hardware restante, detecta os periféricos conectados (mouse, keyboard, pen drive etc.) e verifica se todos os dispositivos conectados estão funcionando bem. Pode-se ouvir um "bipe" que os desktops normalmente usavam quando o POST tinha êxito.
4. Por fim, o código do firmware analisa todos os dispositivos de armazenamento e procura por um carregador de boot (geralmente localizado no primeiro setor de uma unidade de disco). Se o carregador de boot é encontrado, o firmware entrega a ele o controle do computador.

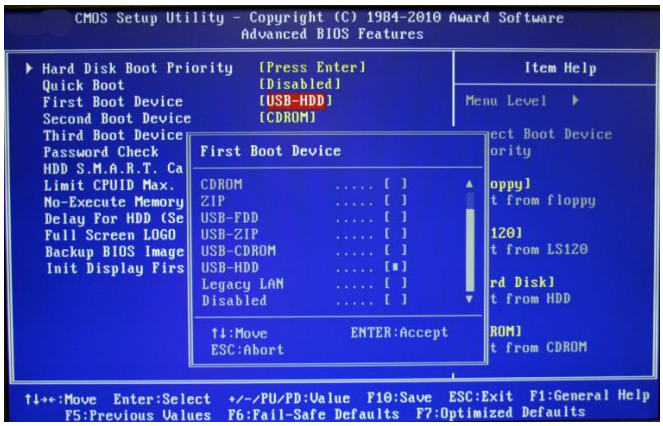
Um pouco mais sobre esse tópico para fins deste artigo.

1. Agora que o carregador de boot está carregado, sua tarefa é carregar o resto do sistema operacional. O GRUB é um desses carregadores de boot. Ele é capaz de carregar sistemas operacionais do tipo UNIX e de carregar em sequência o SO Windows. O carregador de boot está disponível somente no primeiro setor de uma unidade de disco, que tem 512 bytes. Dada a complexidade dos sistemas operacionais modernos, alguns desses carregadores de

boot tendem a fazer carregamento em diversos estágios, onde o carregador de boot principal carrega o carregador de boot do segundo estágio em um ambiente no qual ele não está restrito aos 512 bytes.

2. O carregador de boot em seguida carrega o kernel na memória. Sistemas operacionais do tipo UNIX, então, rodam o processo init (o processo principal, a partir do qual os outros processos são derivados/executados) e finalmente inicializa os níveis de execução.
3. No Windows, o wininit.exe é carregado junto de alguns processos, como o services.exe, para o controle de serviços, o lsass.exe, para a segurança local e a autoridade (semelhante aos níveis de execução) e o lsm.exe, para o gerenciamento da sessão local.
4. Depois de tudo isso, e após alguns outros drivers serem inicializados, a Interface Gráfica de Usuário (GUI) é carregada e que é visualizada a tela de login.
5. Essa foi uma visão bastante geral do processo de boot. Se estiver interessado em sistemas operacionais, eu recomendo que leia mais sobre o assunto em osdev.net (em inglês).

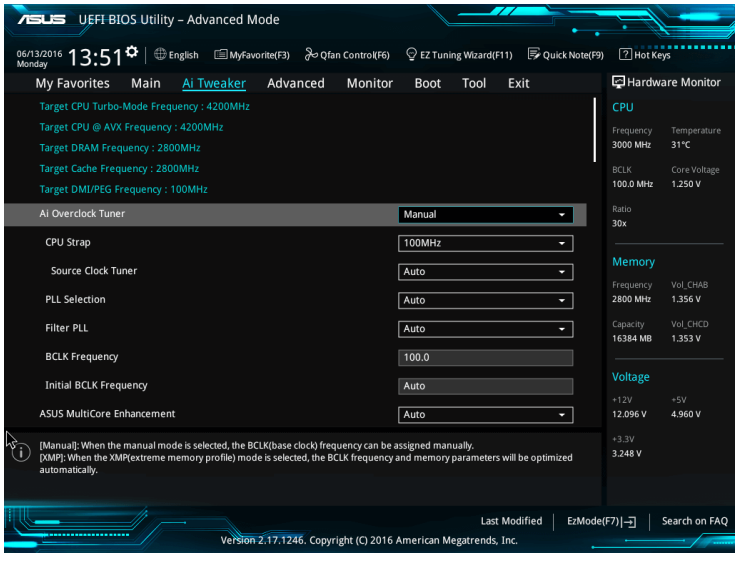
BIOS:



BIOS no firmware parte sobre o procedimento de boot, ele é armazenado em uma EPROM, o que permite ao fabricante lançar as atualizações com facilidade.

Ele fornece muitas funções auxiliares que permitem a leitura dos setores de boot das unidades de armazenamento conectadas e imprimir coisas na tela. Pode-se ter acesso ao BIOS durante as fases iniciais do procedimento de boot pressionando, normalmente, del, F2 ou F10.

UEFI:



A UEFI faz o mesmo trabalho que o BIOS, mas com uma diferença básica: ela armazena todos os dados sobre inicialização e início em um arquivo .efi, em vez de armazená-las no firmware.

Esse arquivo .efi é armazenado em uma partição especial chamada EFI System Partition (ESP) no disco rígido. Essa partição ESP também contém o carregador de boot.

A UEFI foi projetada para vencer as várias limitações do antigo BIOS, incluindo:

1. A UEFI da suporte a tamanhos de unidade de até 9 zetabytes, enquanto o BIOS dá suporte a apenas 2,2 terabytes.
2. A UEFI fornece tempo de inicialização mais rápido.
3. A UEFI tem suporte a unidades discreto, enquanto o BIOS tem o suporte a unidades armazenado em sua ROM. Desse modo, atualizar o firmware do BIOS é um pouco difícil.
4. A UEFI oferece segurança, por exemplo, com o “Secure Boot”, que evita que o computador faça boot a partir de aplicações não autorizadas/não assinadas. Isso ajuda a evitar os rootkits, mas também dificulta o boot dual, já que trata o outro SO como uma aplicação não assinada. No momento, apenas o Windows e o Ubuntu são SOs assinados (fique à vontade para informar o autor caso ele esteja errado).
5. A UEFI roda em modo de 32 ou de 64 bits, enquanto o BIOS roda em modo de 16 bits. Por isso, a UEFI consegue fornecer uma GUI (de navegação com o mouse), diferente do BIOS, que somente permite a navegação com o teclado.

Não precisando da UEFI

Apesar de todos os computadores modernos já virem equipados com a UEFI por padrão, há motivos para os quais se escolheria o BIOS em vez da UEFI. São eles:

1. Sendo um iniciante e não se importa com brincar com qualquer tipo de firmware, o BIOS.
2. Se possuir pelo menos de 2 TB por disco rígido ou partição, pode utilizar o BIOS.
3. O BIOS permite rodar vários sistemas operacionais sem alterar configurações. Isso pode ser um problema de segurança sob a ótica moderna, mas, ao menos, não incomoda o usuário.
4. O BIOS fornece informações do sistema ao sistema operacional. Assim, se o seu SO estiver rodando em modo de 16 bits, ele não precisa escrever código para interagir com o hardware, podendo usar métodos fornecidos diretamente pelo BIOS. Do contrário, se o SO estiver em modo de 32 ou de 64 bits, será preciso fornecer suas próprias sub-rotinas para interagir com o hardware.
5. E se você é alguém que prefere um teclado e UI baseada em texto em vez da navegação com o mouse em uma GUI, o BIOS é para você.

O UEFI leva em conta essas limitações e provê um modo legado. Nele, pode-se executar tudo como se estivesse em um firmware do BIOS. Lembre-se, porém, que a Intel anunciou que deixaria de dar suporte ao BIOS tradicional desde 2020.

Referências

http://ojmoura.wordpress.com/tag/bios/

http://tecnoblog.net/102028/boot-windows-8-rapido/

http://canaltech.com.br/o-que-e/hardware/O-que-e-UEFI/#ixzz2imt5Q5fQ

http://windows.microsoft.com/pt-br/windows-8/what-uefi