

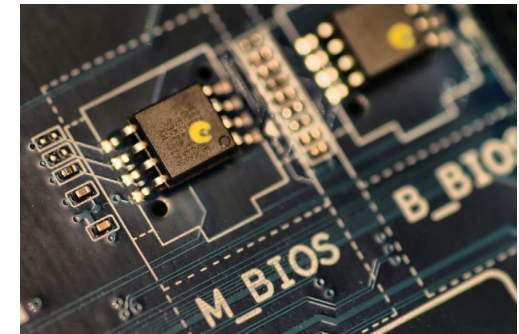
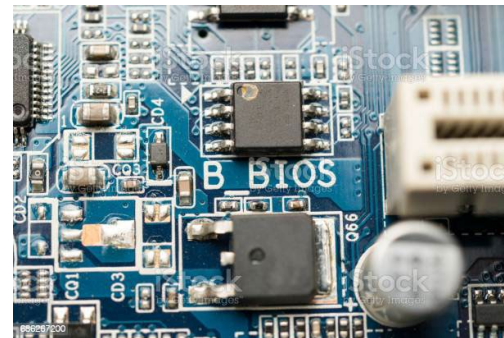
— Laboratório de Hardware

BIOS e UEFI

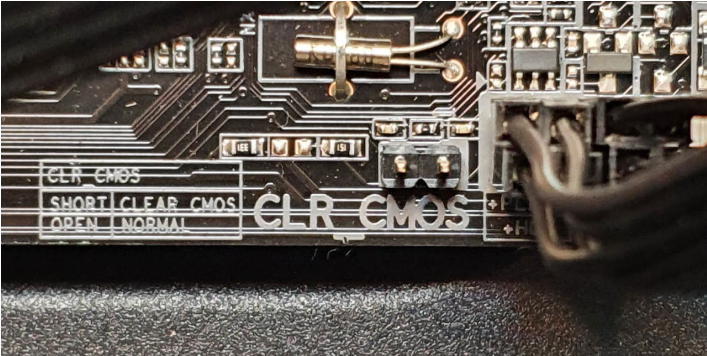
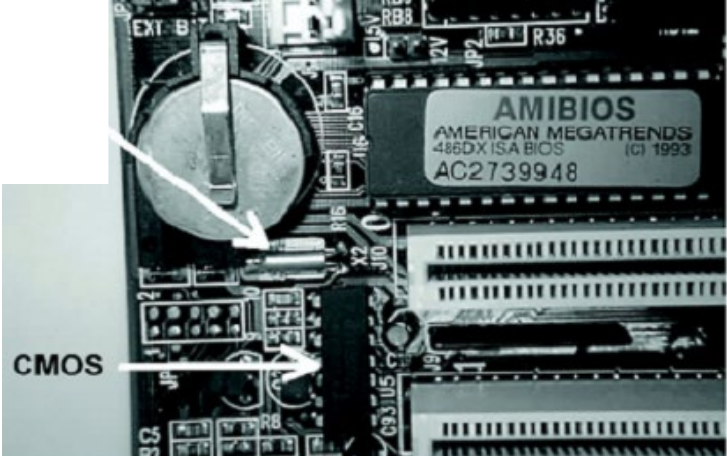
BIOS – Conceitos Iniciais

- BIOS (Basic Input Output System)
 - Sistema Básico de Entrada e Saída, é a primeira camada de software do computador, sendo um pequeno sistema encarregado de reconhecer o hardware, realizar o boot (inicialização) e prover informações básicas para o funcionamento do sistema. O sistema da BIOS é personalizado para cada modelo de placa-mãe.
 - Originalmente, o firmware BIOS era armazenado em um chip EEPROM na placa mãe do PC.
- Setup da BIOS
 - É um programa que permite configurar várias opções acerca do Hardware associado à placa-mãe, bem como opções relacionadas ao desempenho do sistema, senhas e etc. Uma configuração mal feita pode acarretar em um decréscimo significativo no desempenho do computador
- CMOS (Complementary Metal Oxide Semiconductor)
 - Pequena Memória do tipo RAM, com aproximadamente 128 Bytes de capacidade que armazena modificações feitas no Setup da BIOS. Por se tratar de memória ROM, a BIOS não permite atualizações diretamente em seu chip.
 - Por ser tipo RAM, é volátil e seu conteúdo se mantém graças a alimentação elétrica fornecida por uma bateria. A bateria deve ser trocada de tempos em tempos e, nesse momento, o Setup da BIOS deverá ser reconfigurado.
 - Para resetar as configurações salva no CMOS, basta remover a bateria da placa-mãe por alguns instantes ou fazer uma operação definida na placa-mãe como CLEAR CMOS, que pode ser fechar um pequeno curto circuito que desvia a alimentação elétrica do CMOS por alguns instantes ou reconfigurar um jumper que, também, desvia a alimentação elétrica do CMOS.

BIOS - Apresentação



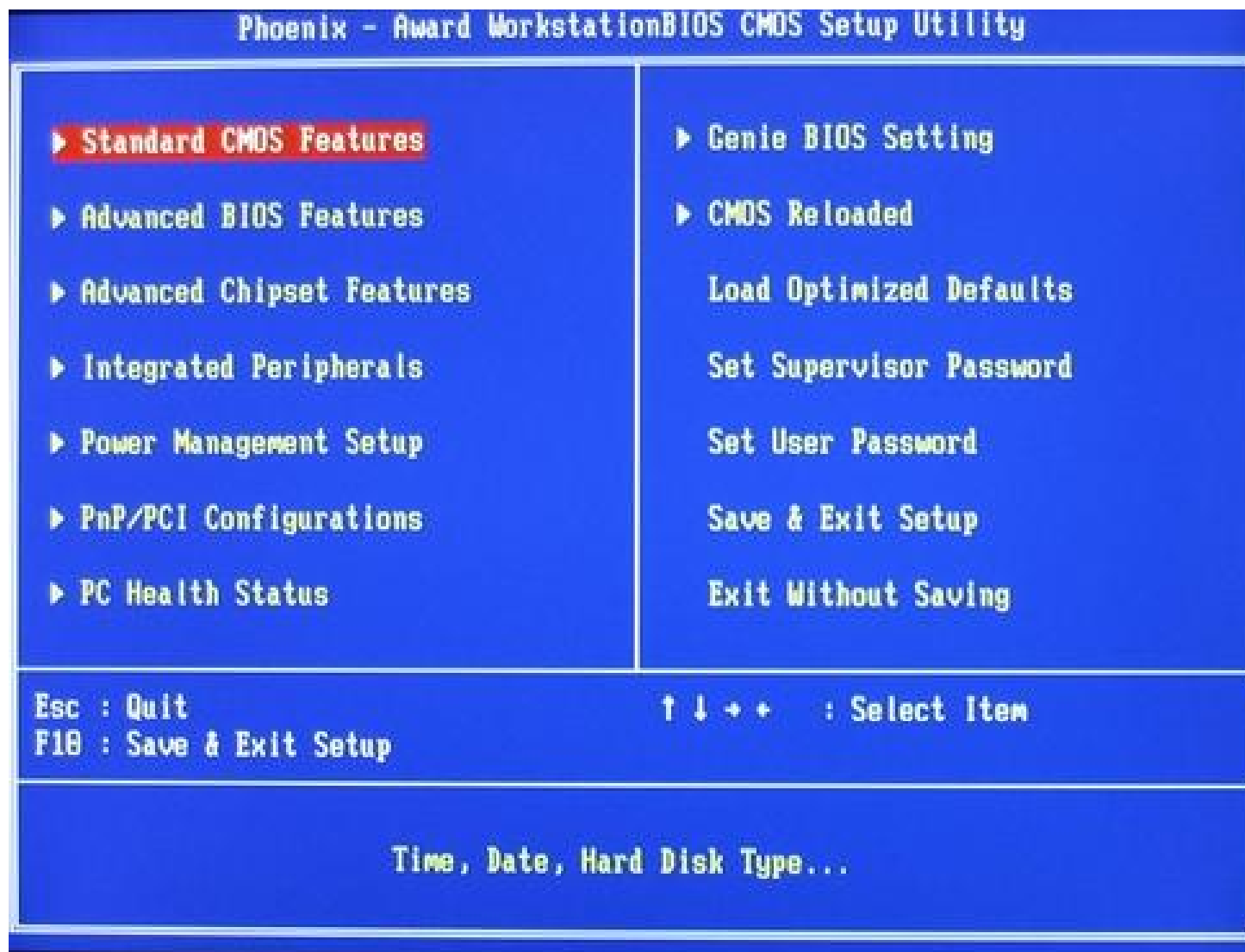
CMOS - Apresentação



OR



Setup da BIOS - Apresentação



Setup da BIOS - Apresentação

PhoenixBIOS Setup Utility							
Main	Advanced	Security	Boot	Exit			
System Time:	[11]:29:50]						
System Date:	[06/13/2012]						
Legacy Diskette A:	[1.44/1.25 MB 3½"]						
Legacy Diskette B:	[Disabled]						
▶ Primary Master	[None]						
▶ Primary Slave	[None]						
▶ Secondary Master	[VMware Virtual ID]						
▶ Secondary Slave	[None]						
▶ Keyboard Features							
System Memory:	640 KB						
Extended Memory:	523264 KB						
Boot-time Diagnostic Screen:	[Disabled]						
				Item Specific Help			
				<Tab>, <Shift-Tab>, or <Enter> selects field.			
F1	Help	↑↓	Select Item	-/+	Change Values	F9	Setup Defaults
Esc	Exit	↔	Select Menu	Enter	Select ▶ Sub-Menu	F10	Save and Exit

Boot

- Processo de inicialização do computador (Boot)
 1. Pressiona-se o botão de ligar/desligar do computador.
 2. A CPU inicia, mas precisa de algumas instruções para funcionar (a CPU sempre precisa fazer algo). Como a memória principal está vazia neste momento, a CPU se restringe às instruções de carregamento do chip da BIOS e começa a executar essas instruções.
 3. O código da BIOS faz um Power On Self Test (POST) que é um 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. Se estabelecia como padrão, soar um “bip” quando o POST tinha êxito.
 - a. Caso um erro de hardware acontecesse, uma sequência de bips, exclusivo para cada falha, soava.
 4. Exibe-se um sumário da análise feita pela BIOS com todos os componentes identificados e, quando aplicável, suas capacidades. Dependendo da configuração era bem rápido.
 - a. Sobreposto, em algumas placas-mãe, por um logo
 5. Por fim, o código da BIOS 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, a BIOS entrega a ele o controle do computador.

POST - Apresentação

 Award Modular BIOS v6.00PG
 Copyright (C) 1984-2011, Award Software, Inc.

GA-990FXA-UD5 F7e

Processor : AMD FX(tm)-8150 Eight-Core Processor
<CPUID:00600F12 Patch ID:0623>

Memory Testing : 4079MB OK

Memory information: **DDR3 1066**

IDE Channel 0 Master : KINGSTON SNVP325SZ12BGB AGYA0Z0Z

IDE Channel 0 Slave : None

IDE Channel 1 Master : None

IDE Channel 1 Slave : None

IDE Channel 2 Master : None

IDE Channel 2 Slave : None

IDE Channel 4 Master : None

IDE Channel 4 Slave : None

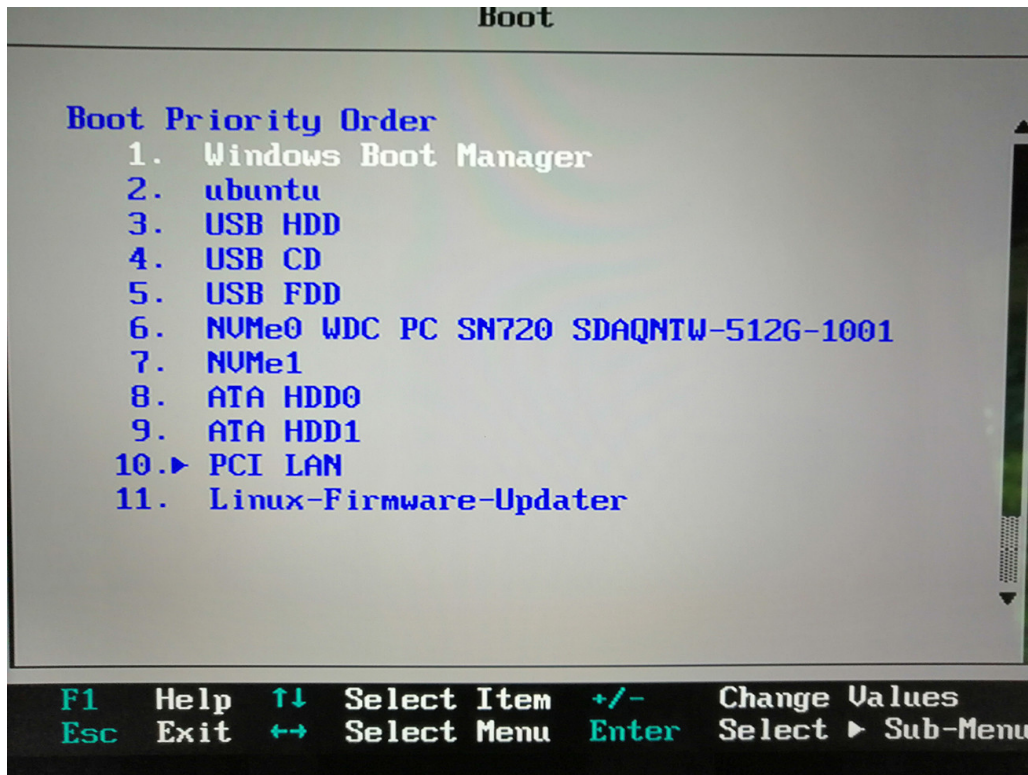
IDE Channel 6 Master : None

IDE Channel 6 Slave : None

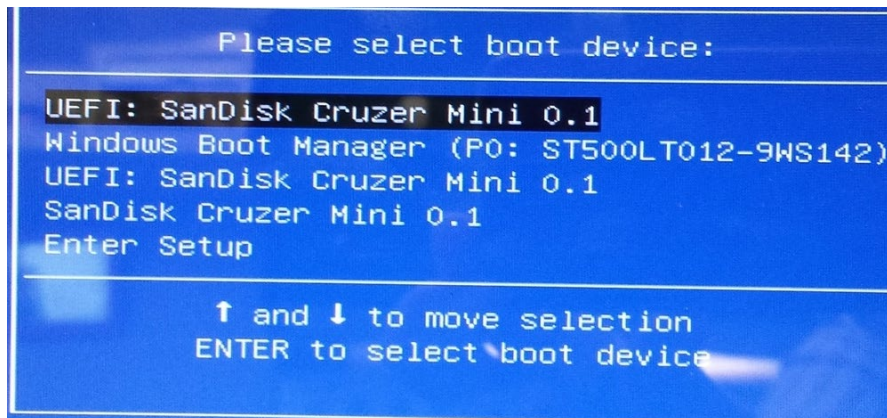
Prepare to Enter Setup...

11/16/2011-RD990-SB950-7A66FG04C-00

POST – Seleccionar Disco



BIOS – Boot Order



Pós POST – Boot Device Select

Atualização (Upgrade) de BIOS

- Na maioria das placas mãe o BIOS pode ser atualizado, e os fabricantes disponibilizam arquivos para essa finalidade.
- A atualização pode resolver problemas de funcionamento ou compatibilidade de periféricos, ou mesmo erros da versão anterior do BIOS. A atualização altera três programas que estão dentro da memória ROM (BIOS, POST, Setup), é uma operação de risco e requer muito 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,
 - Falta de energia elétrica.
 - Se ocorrer algum problema o sistema poderá não iniciar, deixando a placa-mãe muitas vezes inoperante (Brick).
- A atualização ou o upgrade do chip somente deve ser feito quando for realmente necessário.
- Os principais fabricantes deste firmware são: American Megatrends (AMI), Award, General Software, Insyde Software, e Phoenix Technologies.
- As BIOS geralmente são de código fechado e isso pode causar alguns problemas para quem se preocupa com a segurança do computador ou quer trocar sua placa wifi para outra de marca diferente (que geralmente a BIOS bloqueia). Para isso, existe o projeto libreboot, que permite a substituição de uma BIOS privativa por uma implementação de uma BIOS livre para alguns servidores, desktops e notebooks.

Bios Upgrade - Apresentação

BIOS Update Utility

- Latitude On OROM : X03

A010 UPDATE (Dell System Latitude E4310)

- System BIOS : A10

- Embedded Controller : A10

- Intel Ignition Engine : 6.0.21.1188

- Intel Ignition Engine Update : 6.0.21.1188

- Intel Management Engine Update : 6.2.20.1035

- Legacy Video OROM : X14

- Legacy DCI Video OROM : X28

- Legacy RAID OROM : X09

- Latitude On OROM : X03

- Intel AntiTheft : 2.0.24

Do you wish to continue (y/n)? y

Your system will restart automatically.

Preparing to Update



UEFI - Unified Extensible Firmware Interface

- Interface Unificada de Firmware Extensível, é uma especificação que define uma interface de software entre o sistema operacional e o firmware (sistema) da plataforma.
- UEFI substitui a interface de firmware do Sistema de Entrada/Saída Básico (BIOS), presente em todos os computadores pessoais compatíveis com o IBM PC.
- Na prática, a maioria das imagens UEFI fornecem suporte legado para os serviços do BIOS. UEFI pode suportar diagnósticos remotos e reparação de computadores, mesmo sem outro sistema operacional instalado.
- A especificação original EFI (Extensible Firmware Interface) foi desenvolvida pela Intel. Algumas de suas práticas e formatos de dados espelham aqueles do Windows.
- A motivação original para o EFI veio durante o início do desenvolvimento do primeiro sistema Intel-HP Itanium em meados de 1990. As limitações do PC BIOS (modo 16-bits, espaço de endereçamento de 1MB, dependências de hardware PC AT, etc.) foram vistas como claramente inaceitáveis para a grande plataforma de servidores visada como alvo. Os esforços iniciais para resolver esses problemas foram inicialmente chamados Intel Boot Initiative e foi depois renomeado para Extensible Firmware Interface (EFI).
- Em julho de 2005, a Intel cessou o desenvolvimento da especificação EFI quando esta chegou à versão 1.10, e contribuiu para o Unified EFI Forum, que desenvolveu a especificação com o nome Unified Extensible Firmware Interface (UEFI). A especificação EFI original é de propriedade da Intel, que fornece exclusivamente licenças para produtos EFI, mas a especificação UEFI é de propriedade do Fórum.
- A versão 2.1 da especificação UEFI foi lançada em 7 de janeiro de 2007. Foi adicionado criptografia, autenticação de rede e a Arquitetura de Interface de Usuário (Infraestrutura de Interface Humana no UEFI). A última especificação UEFI, a versão 2.10, foi aprovada em agosto de 2022.

UEFI - Unified Extensible Firmware Interface

- Mesmo com pequenas melhorias, a interface da BIOS evoluiu muito pouco. Some-se a isso o fato de que o software não acompanhou as mudanças tecnológicas de PC desde o tempo do MS-DOS.
- Outra questão da BIOS tradicional são suas limitações. O software só consegue ser executado no modo de processador de 16 bits e tem apenas 1 MB de espaço para rodar. Além disso, a BIOS inicializa somente em unidades de 2.1 TB ou menos.
- Em contrapartida, o UEFI pode ser executado no modo de 32 bits ou 64 bits. O firmware ainda pode inicializar em unidades a partir de 2.2 TB. Ele também tem mais espaço de endereçamento, permitindo realizar um boot completo de sistema em até oito segundos — ou menos, se o PC for equipado com um SSD.
 - A UEFI dá suporte a tamanhos de unidade de até 9 Zetabytes.
- O UEFI ainda tem como vantagens o fato de poder ser armazenado na memória flash da placa-mãe ou em um disco rígido. Contudo, vale destacar que o UEFI pode ter interfaces variadas de acordo com a fabricante do computador.
- Configurações antigas, que possuem BIOS, não podem ser atualizadas para este formato, no entanto, atualmente, a grande maioria dos computadores já possuem o UEFI instalado em substituição à BIOS.

UEFI - Recursos

- Secure boot
 - Pode tornar o processo de inicialização seguro por meio da prevenção de carregamento de drivers ou carregadores de SO que não são assinados com uma assinatura digital aceitável.
- Compatibility Support Module (CSM)
 - O Compatibility Support Module (CSM), em português Módulo de Suporte à Compatibilidade, é um componente do firmware UEFI que fornece compatibilidade legada do BIOS por meio da emulação de um ambiente BIOS, permitindo que sistemas operacionais legados e algumas option ROMs que não suportam UEFI ainda sejam usados.
- Serviços
 - O EFI define boot services, que incluem suporte a consoles de texto e gráficos em vários dispositivos, barramentos, serviços de bloco e de arquivos, e runtime services, assim como data e hora.
- Gerenciador de boot
 - Um Gerenciador de boot EFI é também usado para selecionar e carregar o sistema operacional, removendo a necessidade de um mecanismo de boot loader (o boot loader do SO é uma aplicação EFI).

UEFI - Recursos

- Drivers de dispositivo
 - Em adição aos drivers de dispositivos padrões específicos da arquitetura, a especificação EFI provê para um ambiente de drivers de dispositivo independente do processador, chamado EFI Byte Code ou EBC.
 - Alguns tipos de drivers de dispositivo (não EBC) específicos para a arquitetura podem ter interfaces para uso pelo sistema operacional. Isso permite ao SO confiar ao EFI o suporte básico aos gráficos e à rede enquanto os drivers específicos são carregados.
- Suporte a Disco
 - Em adição ao esquema de partição do PC padrão, Master boot record (MBR), o EFI adiciona suporte para uma tabela de partição GUID (GPT), que não sofre das mesmas limitações. A especificação EFI não inclui uma descrição para um sistema de arquivos; implementações da EFI tipicamente suportam FAT32 como seus sistemas de arquivos

UEFI - Recursos

- O Shell EFI
 - A comunidade EFI criou um Shell open source que permite, ao invés de inicializar diretamente em um SO completo, um boot no Shell EFI. O shell é uma aplicação EFI; ele pode residir diretamente dentro da ROM da plataforma, ou num dispositivo para o qual os drivers estão na ROM.
 - O Shell pode ser usado para executar outras aplicações EFI, como setup, a instalação do SO, utilitários de diagnóstico ou configuração, e atualizações da flash do sistema; ele pode também ser usado para tocar CDs ou DVDs sem ter que iniciar um sistema operacional completo, contanto que uma aplicação EFI com as características apropriadas seja escrita. Extensões
- Extensões
 - Extensões ao EFI podem ser carregadas de virtualmente qualquer dispositivo de armazenamento não volátil ligado ao computador. Por exemplo, um OEM (Fabricante do Equipamento) pode vender sistemas com uma partição EFI em um HD que adicionariam características adicionais para o firmware EFI padrão armazenado na ROM da placa mãe.

UEFI - Suporte

- O sistema Linux é capaz de usar o EFI em tempo de boot desde do início de 2000, usando o carregador de boot ELILO.
 - Tem suporte ao GRUB2
- HP-UX tem usado EFI como mecanismo de boot nos sistemas IA-64 desde 2002. OpenVMS tem usado em produtos comerciais desde janeiro de 2005.
- O Microsoft Windows Server 2003 para IA-64, Windows XP 64-bit Edition, e Windows 2000 Advanced Server Limited Edition, todos para a família Intel Itanium de processadores, suportam EFI, um requisito das plataformas pela especificação DIG64.
 - Desde o Windows 8, o suporte a firmwares não-UEFI foi retirado
- A Apple Computer adotou o EFI para a linha dos Macintosh baseados em Intel.
 - Em um Mac baseado em Intel sem o chip Apple T2 Security, a raiz de confiança do firmware da UEFI é o chip onde o firmware está armazenado. As atualizações do firmware da UEFI são assinadas digitalmente pela Apple e verificadas pelo firmware antes da atualização do armazenamento.
- É possível fazer a atualização do firmware UEFI diretamente pelo sistema operacional, com aplicações disponibilizadas pelo desenvolvedor do chip.
 - Apesar de ser mais seguro, ainda é recomendado apenas em situações de grande necessidade

UEFI - Atualização

- O sistema Linux é capaz de usar o EFI em tempo de boot desde do início de 2000, usando o carregador de boot ELILO.
 - Tem suporte ao GRUB2
- HP-UX tem usado EFI como mecanismo de boot nos sistemas IA-64 desde 2002. OpenVMS tem usado em produtos comerciais desde janeiro de 2005.
- O Microsoft Windows Server 2003 para IA-64, Windows XP 64-bit Edition, e Windows 2000 Advanced Server Limited Edition, todos para a família Intel Itanium de processadores, suportam EFI, um requisito das plataformas pela especificação DIG64.
 - Desde o Windows 8, o suporte a firmwares não-UEFI foi retirado
- A Apple Computer adotou o EFI para a linha dos Macintosh baseados em Intel.
 - Em um Mac baseado em Intel sem o chip Apple T2 Security, a raiz de confiança do firmware da UEFI é o chip onde o firmware está armazenado. As atualizações do firmware da UEFI são assinadas digitalmente pela Apple e verificadas pelo firmware antes da atualização do armazenamento.

UEFI - Apresentação

ASUS UEFI BIOS Utility - EZ Mode Exit/Advanced Mode

11:12
Friday [04/06/2012]

P8277-U DELUXE
BIOS Version : 0906
CPU Type : Intel(R) Core(TM) i7-2700K CPU @ 3.50GHz Speed : 3500 MHz
Total Memory : 8192 MB (DDR3 1600MHz)

Temperature

CPU	+93.2°F/+34.0°C
MB	+98.6°F/+37.0°C

Voltage

CPU	1.102V	5V	5.080V
3.3V	3.360V	12V	12.384V

Fan Speed

CPU_FAN	1291RPM	CPU_OPT_FAN	N/A
CHA_FAN1	N/A	CHA_FAN2	N/A

System Performance

Quiet | Performance | Energy Saving | Normal

Boot Priority

Use the mouse to drag or keyboard to navigate to decide the boot priority.

Shortcut (F3) Advanced Mode (F7) Boot Menu (F8) Default (F5)

UEFI - Apresentação

GIGABYTE | UEFI DualBIOS 00:45:16 SUN

Voltage

CPU Vcore 1.054V

Fan Speed

CPU Fan Speed 1000

Temperature

CPU Temperature 45.0

CPU Status

CPU Core Frequency 3400MHz

CPU Core Ratio 31

CPU Vcore 1.054V

CPU VRIN 1.154V

CPU VCCIOA 1.000V

CPU VAXG 0.800V

CPU Temperature 45.0C

CPU Fan Speed 1000RPM

CPU OPT Fan Speed 1000RPM

Memory Status

DDR Frequency 2133MHz

DRAM Voltage (CH A/B) 1.350V

Memory Channel A 11-10-13-10

Memory Channel B 11-10-13-10

Home Performance System BIOS Features Peripherals Power Management Save & Exit

Performance

CPU Base Clock

Host/PCIe Clock

Processor Base Clock

Host Clock Value

CPU Clock Ratio

CPU Frequency

System Memory Multiplier

Memory Frequency

CPU Vcore

CPU Vcore Offset

DRAM Voltage

PCH Core

System Status

Host Clock 3400MHz

System Temperature 45.0C

PCH Temperature 45.0C

1st System Fan Speed 1000RPM

2nd System Fan Speed 1000RPM

3rd System Fan Speed 1000RPM

4th System Fan Speed 1000RPM

5th System Fan Speed 1000RPM

Setup User Options

Main Menu	Sub Menu	Options
Performance	Frequency	Performance Boost
System	Memory	CPU Base Clock
BIOS Features	Voltage	Host/PCIe Clock Frequency
Peripherals	PC Health Status	Processor Base Clock(Gear)
Power Management	Miscellaneous	Host Clock Value
Save & Exit	Advanced CPU Core Features	Processor Graphics Clock
	Channel A Timing Settings	CPU Upgrade
	Channel B Timing Settings	CPU Clock Ratio
	3D Power Control	CPU Frequency
	CPU Core Voltage Control	Advanced CPU Core Features
	Chipset Voltage Control	
	DRAM Voltage Control	

Select Your Option: [OK] [Cancel]


Model Name	Z370-Gaming 7	CPU ID	80080AC1
BIOS Version	F15	Update Revision	80080007
BIOS Date	04/11/2017	Total Memory Size	8192MB
BIOS ID	BALLBO01		
CPU Name	Intel(R) Core(TM) i7-7700K CPU @ 3.60GHz		

Apply

Enter:Select ← ↑ ↓ → :Move Cursor Shift+← → :Main Menu Ctrl+← → :Sub Menu F1 :Help F2 :Classic Mode F3 :Resolution

UEFI - Apresentação

v 2.0.27.1

 **HP Firmware Update and Recovery**

Please select

Update
Update the firmware on this device (restart required).

Create Recovery USB flash drive
Create an HP firmware Recovery USB flash drive to recover another HP device.

[README](#) [Show Contents](#)

BIOS/UEFI - Exemplo

- BIOS - [LINK](#)
- UEFI - [LINK](#)