

MANUAL DO USUÁRIO

POSITIVO MASTER

Ferramenta de Sanitização de Mídia



IDENTIFICAÇÃO DA INTERFACE

Existem versões distintas desta ferramenta, as ferramentas apresentam as mesmas características técnicas, mas com interfaces distintas. Compare a aparência da sua ferramenta com as imagens a seguir para identificar qual versão está utilizando.

O objetivo deste manual é auxiliar o usuário a utilizar a ferramenta de formatação existente na BIOS de equipamentos Positivo Master selecionados, elencando o passo-a-passo e descrevendo as opções disponíveis.

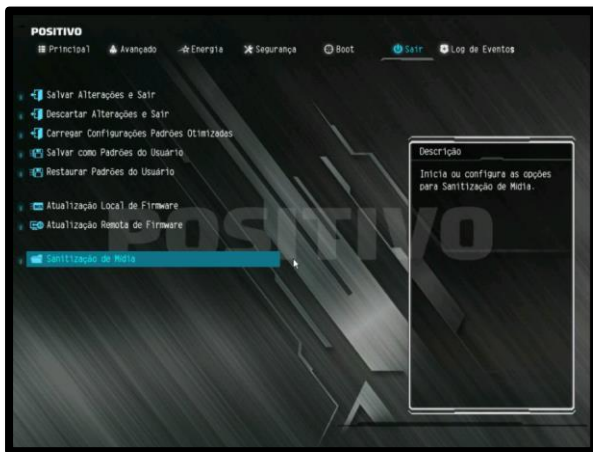
As ferramentas seguem as recomendações da norma NIST SP 800-88 Rev.1 denominada “Guides for Media Sanitization” que estabelece orientações práticas para o método de sanitização apropriado de acordo com o nível de confidencialidade da informação contida no equipamento.

INTERFACE 1

USO DA FERRAMENTA 1 - PASSO A PASSO

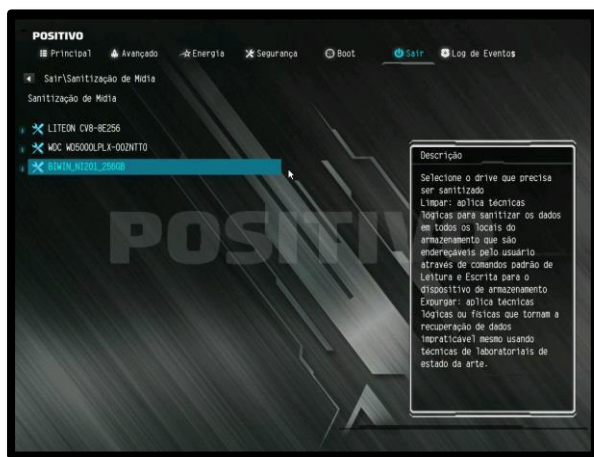
Ao ingressar nas opções de configuração da BIOS do equipamento, siga as orientações descritas abaixo para acionar a ferramenta de sanitização de mídia:

1. Para acionamento da ferramenta, selecionar a opção “Sair” na barra de menu superior e em seguida, a opção “Sanitização de Mídia” conforme figura abaixo:

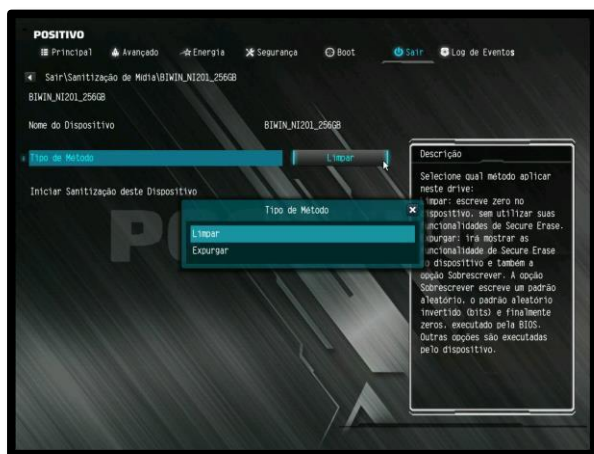


2. Ao ser acionada a opção “Sanitização de Mídia”, será apresentada a lista de dispositivos de armazenamento instalados no equipamento que foram reconhecidos pelo sistema. Selecionar da lista o dispositivo que será apagado e pressione a tecla <ENTER>.

(A imagem a seguir é apenas ilustrativa. A sua lista de dispositivos será diferente, de acordo à sua configuração específica).



3. Depois de selecionado o dispositivo a ser apagado, será possível selecionar o método a ser aplicado.



A opção “Limpar” é a mais simples e escreve “00” em todos os setores do disco.

Já a opção “Expurgar” é mais flexível e oferece até 3 opções de comandos disponíveis (Sobrescrever, Apagamento Seguro e Formatar). Este método envia a solicitação ao firmware do dispositivo de armazenamento para a execução do comando. Por isso, as opções exatas dependerão do dispositivo de armazenamento específico instalado em seu equipamento.

A opção “Sobrescrever” leva bastante tempo para completar e, em geral, é mais lenta que o método “Limpar”. O tempo de execução dependerá da característica e implementação do firmware do dispositivo de armazenamento específico.

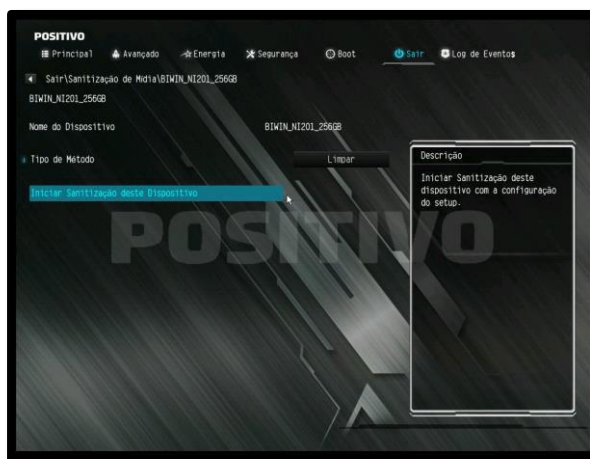
A opção “Apagamento Seguro” exige que a senha do Usuário ou senha Mestre do dispositivo de armazenamento esteja configurada e seja digitada para permitir a operação. Esta opção permite dois modos de operação, Normal ou Melhorado, definidos de acordo ao estabelecido na recomendação NIST SP 800-88 r1 (https://csrc.nist.gov/glossary/term/secure_erase_command). Caso a senha do dispositivo de armazenamento não tenha sido configurada, a tentativa de execução desta opção retornará uma mensagem de erro.

A opção “Formatar” somente estará disponível se o dispositivo de armazenamento selecionado for padrão NVMe. Esta opção permite até 3 configurações adicionais dependendo do firmware do dispositivo NVMe instalado e selecionado: “Nenhum”, “Dados do Usuário” e “Criptográfico”.

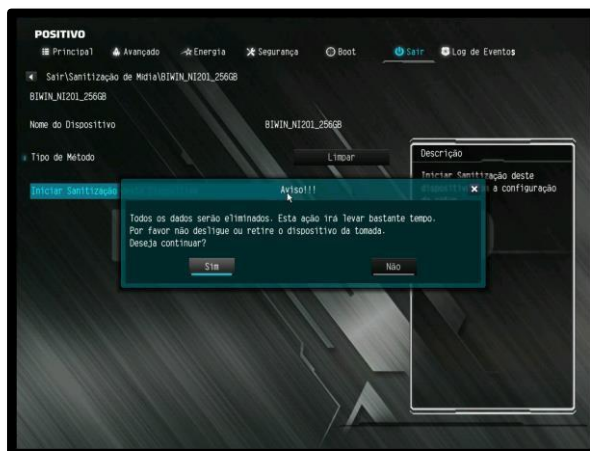
A configuração adicional “Nenhum” elimina os dados de forma **não segura**, marcando a mídia como não utilizada, mas mantendo os dados inalterados. Já a configuração adicional “Dados dos Usuários” sobrescreve e apaga todos os dados do dispositivo. Por fim, a configuração adicional “Criptográfico” torna os dados existentes inacessíveis ao apagar a chave de encriptação atual (somente possível no caso do dispositivo de armazenamento ter sido criptografado).

Mais detalhes destas opções podem ser obtidos em <https://www.intel.com/content/dam/www/public/us/en/documents/technology-briefs/ssd-technical-advisory.pdf> (informações em inglês).

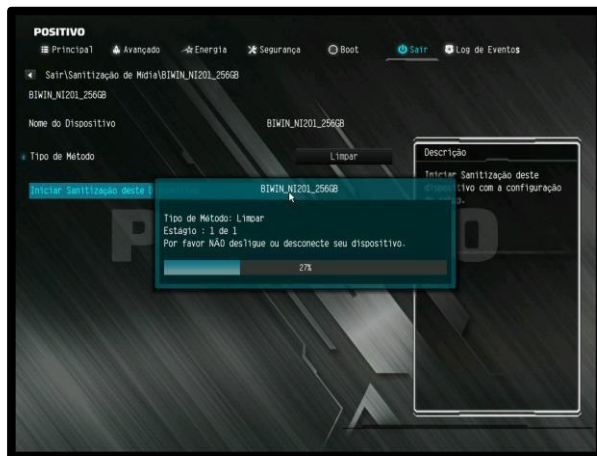
4. Depois de escolhido o Método e suas respectivas opções, selecionar “Iniciar Sanitização deste Dispositivo” e apertar <ENTER>:



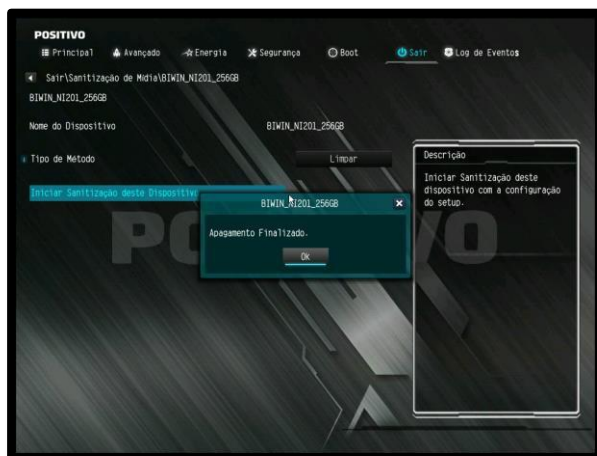
5. Como a operação é irreversível, uma tela de AVISO aparecerá pedindo confirmação antes de prosseguir, para evitar o uso acidental:



6. A execução do procedimento poderá ser acompanhada na tela seguinte:



7. Quando o procedimento for encerrado, aparecerá a seguinte mensagem na tela:



ORIENTAÇÕES E RECOMENDAÇÕES

Como explicado anteriormente, nem todas as opções serão visíveis a todos os usuários pois várias delas dependem de recursos e capacidades do dispositivo de armazenamento instalado no equipamento.

O tempo necessário para a conclusão do procedimento poderá variar significativamente, dependendo da opção selecionada, podendo levar várias horas.

- Para apagar dispositivo de armazenamento **M.2 NVMe** de forma eficiente e rápida, recomenda-se utilizar a opção:

Expurgar -> Formatar -> Criptográfico ou Expurgar -> Formatar -> Dados do Usuário

- Para dispositivos de armazenamento M.2 SATA, SSD SATA ou HDD SATA, o comando “Formatar” não estará disponível. Nesse caso, recomenda-se utilizar a opção:

Expurgar -> Apagamento Seguro -> Usuário -> Melhorado

Caso as opções recomendadas não estejam disponíveis para o seu dispositivo selecionado, utilize os outros métodos.

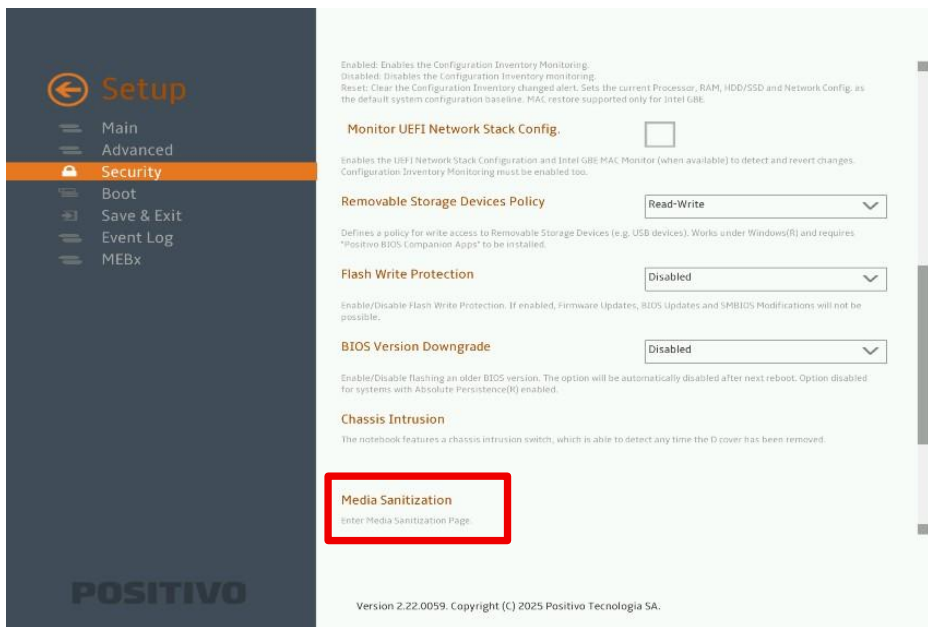
INTERFACE 2

USO DA FERRAMENTA 2 - PASSO A PASSO

1. Durante a inicialização do sistema, pressione F2 para acessar o BIOS.

Ao ingressar nas opções de configuração da BIOS do equipamento, siga as orientações descritas abaixo para acionar a ferramenta de sanitização de mídia:

2. Selecione a aba **Security**.
3. Selecione a opção **Media Sanitization**.



4. Selecione a unidade de armazenamento desejada.
Será apresentada a lista de dispositivos de armazenamento instalados no equipamento que foram reconhecidos pelo sistema. Selecionar o dispositivo desejado.

Obs: A imagem a seguir é apenas ilustrativa, a lista de dispositivos pode ser diferente e varia de acordo com o modelo adquirido.



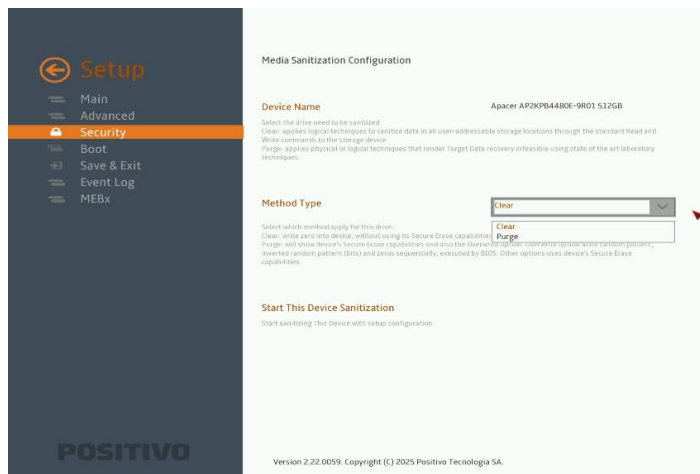
5. Selecione o método a ser aplicado.

Clear

A opção “Clear” é a mais simples e escreve “00” em todos os setores do disco.

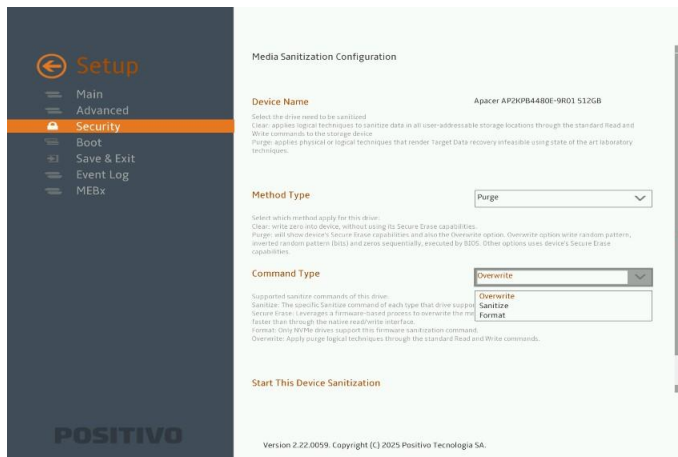
Purge

Oferece diferentes comandos. Este método envia a solicitação ao firmware do dispositivo de armazenamento para a execução do comando. Por isso, as opções exatas habilitadas por esse modo dependerão do dispositivo de armazenamento específico instalado em seu equipamento.



6. Selecione o tipo de comando

- Sanitize: O comando Sanitize específico de cada tipo que a unidade suporta.
 - Secure Erase: Utiliza um processo baseado no firmware para sobrescrever a memória mais rapidamente do que pela interface padrão de leitura/gravação.
 - Format: Apenas unidades NVMe suportam este comando de sanitização via firmware.
- Overwrite: Aplica técnicas de limpeza lógica por meio dos comandos padrão de Leitura e Gravação.



Obs 1: A opção “Format” somente estará disponível se o dispositivo de armazenamento selecionado for padrão NVMe. Esta opção permite até 3 configurações adicionais dependendo do firmware do dispositivo NVMe instalado e selecionado: “Nenhum”, “Dados do Usuário” e “Criptográfico”.

Obs 2: A configuração adicional “Nenhum” elimina os dados de forma não segura, marcando a mídia como não utilizada, mas mantendo os dados inalterados. Já a configuração adicional “Dados dos Usuários” sobrescreve e apaga todos os dados do dispositivo. Por fim, a configuração adicional “Criptográfico” torna os dados existentes inacessíveis ao apagar a chave de criptografia atual (somente possível no caso do dispositivo de armazenamento ter sido criptografado).

Mais detalhes destas opções podem ser obtidos em

<https://www.intel.com/content/dam/www/public/us/en/documents/technology-briefs/ssd-technical-advisory.pdf> (informações em inglês).

7. Sanitize Method

- **Crypto Erase:** A exclusão dos dados ocorre através da destruição ou substituição da chave criptográfica usada para criptografar os dados armazenados
- **Block Erase:** Exclusão dos dados através do envio de comandos de apagamento direto ao controlador de memória.
- **Overwrite Erase:** Os dados são substituídos por padrões específicos de bits (como zeros, uns ou padrões aleatórios) usando comandos de escrita padrão

← Setup

≡ Main

≡ Advanced

🔒 Security

≡ Boot

≡ Save & Exit

≡ Event Log

≡ MEBx

POSITIVO

Device Name

Apacer AP2KP84480E-9R01 512GB

Select the drive need to be sanitized.
Clear: applies logical techniques to sanitize data in all user-addressable storage locations through the standard Read and Write commands to the storage device.
Purge: applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

Method Type

Purge

Select which method apply for this drive:
Clear: write zero into device, without using its Secure Erase capabilities.
Purge: will show device's Secure Erase capabilities and also the Overwrite option. Overwrite option write random pattern, inverted random pattern (bits) and zeros sequentially, executed by BIOS. Other options uses device's Secure Erase capabilities.

Command Type

Sanitize

Suggested sanitize commands of this drive:
Sanitize: The specific Sanitize command of each type that drive supports for purge technique.
Secure Erase: Leverages a firmware-based process to overwrite the media. This command typically executes substantially faster than through the native read/write interface.
Format: Only WtE drives support this firmware sanitization command.
Overwrite: Apply purge logical techniques through the standard Read and Write commands.

Sanitize Method

Block Erase

Crypto Erase, Block Erase, Overwrite Erase

Version 2.22.0059. Copyright (C) 2025 Positivo Tecnologia SA.

8. Secure Erase Setting

- **User Data:** Remove todos os dados do espaço de usuário (dados armazenados pelo sistema ou pelo usuário) usando comandos internos do firmware (como ATA Secure Erase ou NVMe Format).
- **Cryptographic:** Esse modo realiza a Crypto Erase, ou seja, a chave de criptografia usada para proteger os dados é destruída ou substituída. Os dados permanecem fisicamente no dispositivo, mas se tornam inacessíveis e irrecuperáveis.

The screenshot displays the 'Setup' menu on the left with 'Security' selected. The main area shows the 'Secure Erase' configuration for a device named 'Apacer AP2KP64480E-9R01 512GB'. The 'Method Type' is set to 'Purge' and the 'Command Type' is set to 'Format'. Under 'Secure Erase Setting', the 'User Data' option is selected, indicating that user data will be erased. The interface includes detailed descriptions for each option and a footer with the version number 2.22.0059 and copyright information for Positivo Tecnologia SA.

Setup

- Main
- Advanced
- Security**
- Boot
- Save & Exit
- Event Log
- MEBx

POSITIVO

Device Name Apacer AP2KP64480E-9R01 512GB

Select the drive need to be sanitized
Clear: applies logical techniques to sanitize data in all user-addressable storage locations through the standard Read and Write commands, to the storage device.
Purge: applies physical or logical techniques that render Target Data recovery infeasible using state of the art laboratory techniques.

Method Type

Select which method apply for this drive:
Clear: write zero into device, without using its Secure Erase capabilities.
Purge: will show device's Secure Erase capabilities and also the Overwrite option. Overwrite option write random pattern, directed random pattern (bits) and zeros sequentially, executed by BIOS. Other options uses device's Secure Erase capabilities.

Command Type

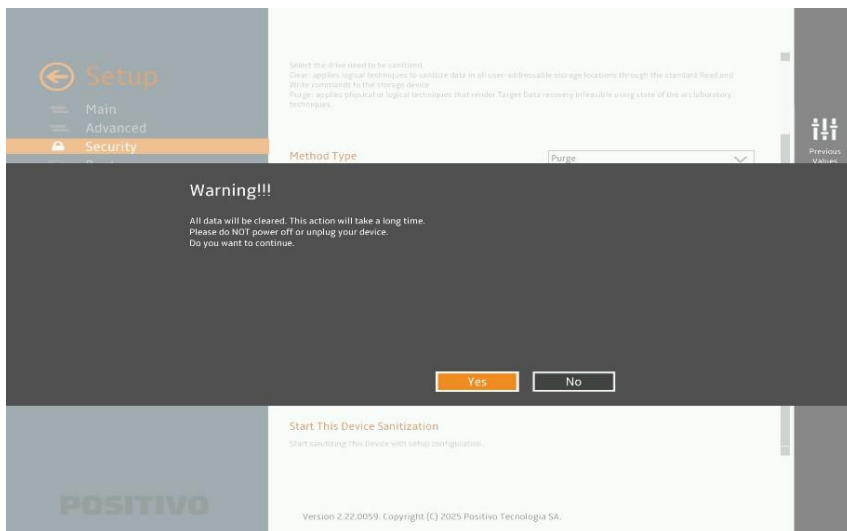
Supported sanitize commands of this drive:
Sanitize: The specific Sanitize command of each type that drive supports for purge technique.
Secure Erase: Leverages a firmware-based process to overwrite the media. This command typically executes substantially faster than through the native read/write interface.
Format: Only for the drive, support this firmware sanitization command.
Overwrite: Apply purge logical techniques through the standard Read and Write commands.

Secure Erase Setting

User Data: All user data shall be erased.
Cryptographic: All user data shall be erased cryptographically.

Version 2.22.0059. Copyright (C) 2025 Positivo Tecnologia SA.

9. Confirme o início da operação. Como a operação é irreversível, uma tela de AVISO aparecerá pedindo confirmação antes de prosseguir, para evitar o uso acidental. O tempo do procedimento varia de acordo com o tamanho da unidade e parâmetros selecionados. O computador não deve ser desligado.



Como explicado anteriormente, nem todas as opções serão visíveis a todos os usuários pois várias delas dependem de recursos e capacidades do dispositivo de armazenamento instalado no equipamento.

O tempo necessário para a conclusão do procedimento poderá variar significativamente, dependendo da opção selecionada, podendo levar várias horas.

- a. Para apagar dispositivo de armazenamento **M.2 NVMe** de forma eficiente e rápida, recomenda-se utilizar a opção:

Expurgar -> Formatar -> Criptográfico ou Expurgar -> Formatar -> Dados do Usuário

- b. Para dispositivos de armazenamento M.2 SATA, SSD SATA ou HDD SATA, o comando “Formatar” não estará disponível. Nesse caso, recomenda-se utilizar a opção:

Expurgar -> Apagamento Seguro -> Usuário -> Melhorado

Caso as opções recomendadas não estejam disponíveis para o seu dispositivo selecionado, utilize os outros métodos.



Preservação Ambiental

A conscientização ambiental faz parte da cultura de cada pessoa, faça a sua parte. Recomenda-se que seu equipamento antigo e em desuso não seja descartado no lixo comum. Para saber como colaborar, entre em contato através dos canais ao lado:



recicle@positivo.com.br



4002 6440
(capitais e grandes centros)
0800 644 7500
(demais regiões)



www.meupositivo.com.br/tiverde

POSITIVO

www.positivoempresas.com.br

©2025 - Positivo Tecnologia. Todos os direitos reservados. Este documento é de propriedade da Positivo Tecnologia, não podendo ser reproduzido, transmitido, transcrito, total ou parcialmente, sem autorização prévia por escrito da mesma. Seu conteúdo possui caráter técnico-informativo. A Positivo Tecnologia reserva-se o direito de realizar as alterações que julgar necessárias em seu conteúdo sem prévio aviso. Todos os nomes de empresas e produtos citados são marcas registradas de seus respectivos proprietários. Fotos meramente ilustrativas e as cores podem variar conforme o modelo. Componentes sujeitos à alteração sem prévio aviso.



Os termos HDMI e HDMI High-Definition Multimedia Interface, e o logotipo HDMI são marcas ou marcas registradas da HDMI Licensing Administrator, Inc. nos Estados Unidos e em outros países.