Dell EMC PowerEdge R6525

Guía de referencia de BIOS y UEFI

Número de parte: E67S
Tipo reglamentario: E67S001
Agosto de 2022
Rev. A08

DELL Technologies

Notas, precauciones y avisos

NOTA: Una NOTA indica información importante que le ayuda a hacer un mejor uso de su producto.

PRECAUCIÓN: Una PRECAUCIÓN indica la posibilidad de daños en el hardware o la pérdida de datos, y le explica cómo evitar el problema.

AVISO: Un mensaje de AVISO indica el riesgo de daños materiales, lesiones corporales o incluso la muerte.

© 2019 - 2022 Dell Inc. o sus subsidiarias. Todos los derechos reservados. Dell, EMC y otras marcas comerciales son marcas comerciales de Dell Inc. o sus filiales. Es posible que otras marcas comerciales sean marcas comerciales de sus respectivos propietarios.

Tabla de contenido

1

Aplicaciones de administración previas al sistema operativo

Puede administrar la configuración básica y las características de un sistema sin necesidad de iniciar el sistema operativo mediante el uso del firmware del sistema.

Opciones que se utilizan para administrar las aplicaciones previas al sistema operativo

Puede utilizar cualquiera de las siguientes opciones para administrar las aplicaciones previas al sistema operativo:

- Configuración del sistema
- Dell Lifecycle Controller
- Boot Manager (Administrador de inicio)
- Entorno de ejecución previa al inicio (PXE)

Temas:

Configuración del sistema

Mediante la opción **Configuración del sistema**, puede configurar los ajustes del BIOS, los ajustes de iDRAC y los ajustes del dispositivo del sistema.

Puede acceder a la configuración del sistema mediante cualquiera de las siguientes interfaces:

- Interfaz gráfica de usuario: para acceder al tablero de iDRAC, haga clic en **Configuración** y, a continuación, haga clic en **Configuración del BIOS**.
- Explorador de texto: el navegador se habilita mediante Console Redirection (Redirección de consola).

Para ver **Configuración del sistema**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema**.

NOTA: Si el sistema operativo comienza a cargar antes de presionar F2, espere a que el sistema termine de iniciar, reinícielo e intente nuevamente.

Los detalles de la pantalla **Menú principal de la configuración del sistema** se describen a continuación:

Tabla 1. Menú principal de configuración del sistema

Opción	Descripción
BIOS del sistema	Permite configurar los ajustes del BIOS.
Configuración de iDRAC	Permite establecer la configuración de la iDRAC. La configuración de la iDRAC es una interfaz para establecer y configurar los parámetros de la iDRAC utilizando UEFI (Unified Extensible Firmware Interface). Puede habilitar o deshabilitar diversos parámetros de la iDRAC mediante la utilidad de configuración de la iDRAC. Para obtener más información sobre esta utilidad, consulte la *Guía del usuario de Integrated Dell Remote Access Controller* en www.dell.com/poweredgemanuals.

Tabla 1. Menú principal de configuración del sistema (continuación)

Opción	Descripción
Configuración del dispositivo	Permite configurar ajustes para dispositivos como controladoras de almacenamiento o tarjetas de red.

BIOS del sistema

Para ver la pantalla **BIOS del sistema**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema**.

Tabla 2. Detalles de BIOS del sistema

Opción	Descripción
Información del sistema	Proporciona información sobre el sistema, como el nombre de modelo, la versión del BIOS y la etiqueta de servicio.
Configuración de la memoria	Muestra información y opciones relacionadas con la memoria instalada.
Configuración del procesador	Muestra información y opciones relacionadas con el procesador, como la velocidad y el tamaño de la memoria caché.
Configuración de SATA	Muestra las opciones que permiten activar o desactivar los puertos y la controladora SATA integrada.
Configuración de NVMe	Muestra las opciones que permiten cambiar la configuración de NVMe. Si el sistema contiene las unidades NVMe que desea configurar en un arreglo RAID, debe establecer este campo y el campo **SATA integrado** en el menú **Configuración de SATA** en el modo de **RAID**. Es posible que también deba cambiar el valor **Boot Mode (Modo de inicio)** a **UEFI**. De lo contrario, debe configurar este campo en **Non-RAID (no RAID)**.
Configuración de inicio	Muestra las opciones que permiten especificar el modo de inicio (BIOS o UEFI). Permite modificar los ajustes de arranque UEFI y BIOS.
Configuración de red	Muestra las opciones para administrar la configuración de red y los protocolos de inicio de UEFI. Se administra la configuración de la red heredada en el menú **Configuración del dispositivo**. **NOTA:** La configuración de red no es compatible con el modo de arranque del BIOS.
Dispositivos integrados	Especifica las opciones para administrar puertos y controladoras de dispositivos integrados, y especifica las opciones y funciones relacionadas.
Comunicación serie	Especifica las opciones para administrar los puertos serie, y especifica las opciones y funciones relacionadas.
Configuración del perfil del sistema	Muestra las opciones que permiten cambiar la configuración de administración de energía del procesador y la frecuencia de la memoria.
Seguridad del sistema	Muestra las opciones que se utilizan para configurar los ajustes de seguridad del sistema, como la contraseña del sistema, la contraseña de configuración, la seguridad del módulo de plataforma de confianza (TPM) y el inicio seguro de UEFI. También administra el botón de encendido del sistema.
Control de SO redundante	Establece la información del sistema operativo redundante para el control de dicho sistema.
Otros ajustes	Muestra opciones que permiten cambiar la fecha y hora del sistema.

Información del sistema

Para ver la pantalla **Información del sistema**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Información del sistema**.

Tabla 3. Detalles de Información del sistema

Opción	Descripción
System Model Name (Nombre del modelo del sistema)	Especifica el nombre de modelo del sistema.
System BIOS Version (Versión del BIOS del sistema)	Especifica la versión del BIOS instalada en el sistema.
System Service Tag (Etiqueta de servicio del sistema)	Especifica la etiqueta de servicio del sistema.
System Manufacturer (Fabricante del sistema)	Especifica el nombre del fabricante del sistema.
System Manufacturer Contact Information (Información de contacto del fabricante del sistema)	Especifica la información de contacto del fabricante del sistema.
System CPLD Version (Versión de CPLD del sistema)	Especifica la versión actual del firmware del dispositivo lógico programable complejo (CPLD) del sistema.
Versión de cumplimiento de normas de UEFI	Especifica el nivel de cumplimiento de normas de UEFI del firmware del sistema.
Versión de AGESA	Especifica la versión de código de referencia de AGESA.
Versión de SMU	Especifica la versión del firmware de SMU.
Versión de DXIO	Especifica la versión del firmware de DXIO.

Configuración de memoria

Para ver la pantalla **Configuración de memoria**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Configuración de memoria**.

Tabla 4. Detalles de Configuración de memoria

Opción	Descripción
System Memory Size	Especifica el tamaño de la memoria en el sistema.
Tipo de memoria del sistema	Especifica el tipo de memoria instalado en el sistema.
System Memory Speed	Especifica la velocidad de memoria del sistema.
Voltaje de memoria del sistema	Especifica el voltaje de memoria del sistema.
Video Memory	Muestra el tamaño de la memoria de vídeo.
Prueba de memoria del sistema	Especifica si las pruebas de la memoria del sistema se ejecutan durante el inicio del sistema. Las dos opciones disponibles son **Habilitada** y **Deshabilitada**. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Demora de actualización de DRAM	Permitir que la **Controladora de memoria de la CPU** demore la ejecución de los comandos de **Actualización** puede mejorar el rendimiento de algunas cargas de trabajo. Al minimizar el tiempo de demora, se garantiza que la controladora de memoria ejecute el comando de **ACTUALIZACIÓN** en intervalos regulares. Para los servidores basados en Intel, esta configuración solo afecta a sistemas configurados con DIMM que utilizan DRAM de densidad de 8 Gb. De manera predeterminada, esta opción es establecida en **Mínimo**.
Modo de funcionamiento de la memoria	Especifica el modo de funcionamiento de la memoria. Esta opción está disponible y establecida en **Modo de optimizador** de manera predeterminada.
Estado actual del modo de funcionamiento de la memoria	Especifica el estado actual del modo de funcionamiento de la memoria.

Tabla 4. Detalles de Configuración de memoria (continuación)

Opción	Descripción
Intercalado de memoria	Habilita o deshabilita la opción de intercalado de memoria. Las dos opciones disponibles son **Automática** y **Deshabilitada**. Esta opción está establecida en **Auto** (Automática) de manera predeterminada.
Registro de errores corregible	Habilita o deshabilita el registro de errores corregible. Esta opción está establecida en **Habilitada** de manera predeterminada.
Autorreparación de DIMM (reparación posterior al paquete) en un error de memoria incorregible	Habilita o deshabilita la reparación posterior al paquete (PPR) en un error de memoria incorregible. Esta opción está establecida en **Habilitada** de manera predeterminada.

Configuración del procesador

Para ver la pantalla **Configuración del procesador**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Configuración del procesador**.

Tabla 5. Detalles de Configuración del procesador

Opción	Descripción
Procesador lógico	Cada núcleo de procesador admite hasta dos procesadores lógicos. Si esta opción se establece en **Habilitada**, el BIOS muestra todos los procesadores lógicos. Si esta opción se establece en **Deshabilitada**, el BIOS solo muestra un procesador lógico por núcleo. Esta opción está establecida en **Habilitada** de manera predeterminada.
Tecnología de virtualización	Permite habilitar o deshabilitar la tecnología de virtualización del procesador. Esta opción está establecida en **Habilitada** de manera predeterminada.
Compatibilidad con IOMMU	Habilita o deshabilita la compatibilidad con IOMMU. Es necesario para crear una tabla ACPI IVRS. Esta opción está establecida en **Habilitada** de manera predeterminada.
Protección de DMA del kernel	Cuando esta opción se establece como Habilitada, el uso de IOMMU, el BIOS y el sistema operativo habilitará la protección de acceso directo a la memoria para dispositivos periféricos compatibles con DMA. Habilite la **Compatibilidad con IOMMU** para utilizar esta opción. Esta opción está establecida en **Deshabilitada** de manera predeterminada. Cuando se habilita esta opción mediante el uso de Tecnología de virtualización, el BIOS y el sistema operativo habilitan la protección contra el acceso directo a la memoria en los dispositivos periféricos compatibles con DMA. Habilite la Tecnología de virtualización para utilizar esta opción.
Precapturador de HW de flujo L1	Habilita o deshabilita el precapturador de hardware de flujo L1. Esta opción está establecida en **Habilitada** de manera predeterminada.
Precapturador de HW de flujo L2	Habilita o deshabilita el precapturador de hardware de flujo L2. Esta opción está establecida en **Habilitada** de manera predeterminada.
Precapturador del intervalo L1	Habilita o deshabilita el precapturador del intervalo L1. Esta opción está establecida como **Habilitada** de manera predeterminada, ya que optimiza la carga de trabajo general.
Precapturador de región de L1	Habilita o deshabilita el precapturador de la región de L1. Esta opción está establecida como **Habilitada** de manera predeterminada, ya que optimiza la carga de trabajo general.
Precapturador arriba abajo de L2	Habilita o deshabilita el precapturador arriba abajo de flujo de L2. Esta opción está establecida como **Habilitada** de manera predeterminada, ya que optimiza la carga de trabajo general.

Tabla 5. Detalles de Configuración del procesador (continuación)

Opción	Descripción
Enumeración de núcleos de MADT	Especifica la enumeración de núcleos de MADT. Esta opción está establecida en **Lineal** de manera predeterminada.
Nodos de NUMA por conector	Especifica la cantidad de nodos de NUMA por conector. Esta opción está establecida en **1** de manera predeterminada.
CCX como dominio de NUMA	Habilita o deshabilita CCX como dominio de NUMA. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Cifrado de memoria seguro (SME)	Permite habilitar o deshabilitar las funciones de cifrado seguro de AMD, como **SME** y la **Virtualización segura cifrada (SEV)**. También determina si se pueden habilitar otras funciones de cifrado seguro, como **TSME** y **SEV-SNP**. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
ASID SEV no ES mínima	Determina la cantidad de ID de espacio de dirección disponibles para virtualización cifrada segura no ES y ES. Esta opción está establecida en **1** de manera predeterminada.
Paginación anidada protegida (SNP)	Habilita o deshabilita el **SEV-SNP**, un conjunto de protección de seguridad adicionales. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Cobertura de memoria SNP	Esta opción selecciona el modo de operación de la memoria de paginación anidada (SNP) y de la tabla de asignación inversa (RMP). La RMP se utiliza para garantizar una asignación uno a uno entre las direcciones físicas del sistema y las direcciones físicas huéspedes.
Cifrado de memoria seguro transparente (TSME)	Activa o desactiva el **TSME**. **TSME** es un cifrado de memoria continua que no requiere compatibilidad con el SO ni con el hipervisor. Esta opción está establecida en **Deshabilitada** de manera predeterminada. • Si el SO admite **SME**, no habilite este campo. • Si el hipervisor es compatible con **SEV**, no habilite este campo. La activación de **TSME** afecta el rendimiento de la memoria del sistema.
REP MOVSB/STOSB mejorado	Habilita o deshabilita la compatibilidad con REP MOVSB/STOSB mejorado. Esta configuración puede afectar el rendimiento según la aplicación que se esté ejecutando en el servidor. Esta opción está establecida en **Deshabilitada** de manera predeterminada. **NOTA:** Esta opción solo está disponible para el procesador AMD EPYC 7003.
REP MOVSB rápido y corto	Habilita o deshabilita la compatibilidad con REP MOVSB rápido y corto. Esta configuración puede afectar el rendimiento según la aplicación que se esté ejecutando en el servidor. Esta opción está establecida en **Deshabilitada** de manera predeterminada. **NOTA:** Esta opción solo está disponible para el procesador AMD EPYC 7003.
Transmisión de REP-MOV/STOS	Habilita o deshabilita la compatibilidad con la transmisión de REP MOVISTOS. Esta configuración puede afectar el rendimiento según la aplicación que se esté ejecutando en el servidor. Esta opción está establecida en **Deshabilitada** de manera predeterminada. **NOTA:** Esta opción solo está disponible para el procesador AMD EPYC 7003.
TDP configurable	Permite volver a configurar los niveles de alimentación de diseño térmico (TDP) del procesador con base en las capacidades de alimentación y entrega térmica del sistema. TDP se refiere a

Tabla 5. Detalles de Configuración del procesador (continuación)

Opción	Descripción
	la cantidad máxima de potencia que el sistema de refrigeración necesita para disipar el calor. Esta opción está establecida en **Máximo** de manera predeterminada. **NOTA:** Esta opción solo está disponible en ciertas SKU de los procesadores, y la cantidad de niveles alternativos también varía.
Modo x2APIC	Activa o desactiva el modo x2APIC. Esta opción está establecida en **Habilitada** de manera predeterminada. **NOTA:** Para la configuración de dos CPU de 64 núcleos, el modo x2APIC no es intercambiable si hay 256 subprocesos activados (configuración del BIOS: todos los CCD, núcleos y procesadores lógicos activados).
Cantidad de CCD por procesador	Controla el número de CCD habilitados en cada procesador. Esta opción está establecida en **Todos** de manera predeterminada.
Cantidad de núcleos por CCD	Especifica la cantidad de núcleos por CCD. Esta opción está establecida en **Todos** de manera predeterminada.
Velocidad de núcleo de procesador	Muestra la frecuencia máxima de núcleo del procesador.
Procesador n	**NOTA:** Según el número de CPU instaladas, puede haber hasta n procesadores en la lista. La siguiente configuración aparece en cada procesador instalado en el sistema:

Tabla 6. Detalles del procesador n

Opción	Descripción
Familia-Modelo-Versión	Muestra la familia, el modelo y la versión del procesador según la definición de AMD.
Marca	Especifica el nombre de la marca.
Caché de nivel 2	Muestra el tamaño total de la memoria caché L2.
Caché de nivel 3	Muestra el tamaño total de la memoria caché L3.
Cantidad de núcleos	Muestra la cantidad de núcleos por procesador.
Microcódigo	Especifica la versión del microcódigo del procesador.

Configuración de SATA

Para ver la pantalla **Configuración de SATA**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Configuración de SATA**.

Tabla 7. Detalles de la Configuración de SATA

Opción	Descripción
SATA integrado	Permite establecer la opción de SATA integrado en **Apagado**, **Modo de AHCI** o **Modos de RAID**. Esta opción está establecida en **AHCI Mode** (Modo de AHCI) de manera predeterminada. **NOTA:** 1. Es posible que también deba cambiar el valor Boot Mode (Modo de inicio) a UEFI. De lo contrario, debe establecer este campo a modo no RAID.

Tabla 7. Detalles de la Configuración de SATA (continuación)

Opción	Descripción
	2. No hay compatibilidad con el sistema operativo de Ubuntu y ESXi bajo el modo de RAID.
Bloqueo de congelación de seguridad	Envía el comando **Security Freeze Lock (Bloqueo de congelación de seguridad)** a las unidades SATA integradas durante la POST. Esta opción solo corresponde al Modo de AHCI. Esta opción está establecida en **Habilitada** de manera predeterminada.
Caché de escritura	Permite habilitar o deshabilitar el comando para las unidades SATA integradas durante la POST. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Puerto n	Establece el tipo de unidad del dispositivo seleccionado. Para los modos **AHCI** o **RAID**, la compatibilidad con el BIOS siempre está habilitada. **Tabla 8. Puerto n** **Opciones** / **Descripciones** **Modelo** — Muestra el modelo de unidad del dispositivo seleccionado. **Tipo de unidad** — Muestra el tipo de unidad conectada al puerto SATA. **Capacidad** — Especifica la capacidad total de la unidad. Este campo no está definido para dispositivos de medios extraíbles, como las unidades ópticas.

Configuración de NVMe

Para ver la pantalla **Configuración de NVMe**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Configuración de NVMe**.

Tabla 9. Detalles de la configuración de NVMe

Opción	Descripción
Modo NVMe	Esta opción establece el modo de la unidad NVMe. Si el sistema contiene las unidades de NVMe que desea configurar en un arreglo RAID, debe establecer este campo y el campo de SATA integrado en el menú de configuración de SATA al modo de RAID. Es posible que también deba cambiar la configuración del modo de arranque a UEFI. Esta opción está establecida en **Sin RAID** de manera predeterminada.
Controlador de NVMe del BIOS	Las unidades NVMe calificadas por Dell siempre utilizan el controlador UEFINVMe integrado en Dell EROS. Cuando esta opción se establece en "Todas las unidades", el controlador del BIOS también se utilizará con cualquier unidad NVMe en el sistema que Dell no haya calificado. Esta opción está establecida en **Controladores calificados de Dell** de manera predeterminada. **NOTA:** Cuando esta opción se establece en "Todas las unidades" y hay unidades NVMe no calificadas por Dell, usted tiene una configuración que no se ha validado, lo que puede provocar un comportamiento inesperado.

Configuración de inicio

Puede utilizar la pantalla **Boot Settings** (Configuración de arranque) para establecer el modo de inicio en **BIOS** o **UEFI**. También le permite especificar el orden de inicio.

- **UEFI**: La interfaz de firmware extensible unificada (Unified Extensible Firmware Interface o UEFI) es una nueva interfaz entre sistemas operativos y firmware de plataformas. La interfaz está compuesta por tablas de datos con información relativa a la plataforma y

llamadas de servicio de tiempo de ejecución y de inicio, disponibles para el sistema operativo y su cargador. Los siguientes beneficios están disponibles cuando **Boot Mode (Modo de inicio)** se configura en **UEFI**:

- Compatibilidad para particiones de unidad superiores a 2 TB.
- Seguridad mejorada (p. ej., inicio seguro de UEFI).
- Menos tiempo para iniciar.

NOTA: Para ejecutar el inicio desde unidades NVMe, debe usar solamente el modo de inicio de UEFI.

- **BIOS**: el **Modo de inicio del BIOS** es el modo de inicio heredado. Se conserva para mantener la compatibilidad con versiones anteriores.

Para ver la pantalla **Configuración de inicio**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Configuración de inicio**.

Tabla 10. Detalles de Configuración de inicio

Opción	Descripción
Modo de inicio	Permite establecer el modo de inicio del sistema. Si el sistema operativo admite UEFI, puede utilizar esta opción para UEFI. Estableciendo este campo en BIOS se permitirá la compatibilidad con sistemas operativos que no sean de UEFI. Esta opción está establecida en **UEFI** de manera predeterminada. **PRECAUCIÓN: El cambio de modo de inicio puede impedir que el sistema se inicie si el sistema operativo no se ha instalado en el mismo modo de inicio.** **NOTA:** Establecer este campo en UEFI deshabilita el menú **Configuración de inicio del BIOS**.
Reintento de secuencia de inicio	Permite habilitar o deshabilitar la función **Reintento de secuencia de inicio**. Si esta opción está configurada como **Activada** y el sistema no se inicia, el sistema intentará de nuevo la secuencia de inicio después de 30 segundos. Esta opción está establecida en **Habilitada** de manera predeterminada.
Conmutación por error de la unidad de disco duro	Habilita o deshabilita la conmutación por error de la unidad de disco duro. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Inicio de USB genérico	Habilita o deshabilita el marcador de posición de inicio de USB genérico. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Marcador de posición de la unidad de disco duro	Habilita o deshabilita el marcador de posición de la unidad de disco duro. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Limpiar todas las variables y el orden de Sysprep	Si se configura en **Ninguno**, el BIOS no hará nada. Cuando se configura en **Sí**, el BIOS elimina las variables de Sysprep #### y SysPrepOrder. Esta opción es una opción de onetime, se restablecerá a ninguno cuando se eliminen variables. Esta configuración solo está disponible en el **modo de inicio de UEFI**. De manera predeterminada, esta opción está establecida en **Ninguno**.
Configuración de inicio de UEFI	Especifica la secuencia de inicio de UEFI. Permite habilitar o deshabilitar las opciones de inicio de UEFI. **NOTA:** Esta opción controla el orden de inicio de UEFI. La primera opción de la lista se intentará primero. **Tabla 11. Configuración de inicio de UEFI** **Opción** / **Descripción** **Secuencia de inicio de UEFI** — Permite cambiar el orden de los dispositivos de inicio. **Boot Options Enable/Disable (Habilitar/deshabilitar opciones de inicio)** — Permite seleccionar los dispositivos de inicio habilitados o deshabilitados.

Selección del modo de inicio del sistema

System Setup (Configuración del sistema) permite especificar uno de los siguientes modos de inicio para instalar el sistema operativo:

- El modo de inicio UEFI (el valor predeterminado) es una interfaz de inicio mejorada de 64 bits.

  Si ha configurado el sistema para que se inicie en modo UEFI, este reemplaza al BIOS del sistema.

1. En el **Menú principal de configuración del sistema**, haga clic en **Configuración de inicio** y seleccione **Modo de inicio**.
2. Seleccione el modo de arranque de UEFI al que desea que se inicie el sistema.

   PRECAUCIÓN: El cambio de modo de inicio puede impedir que el sistema se inicie si el sistema operativo no se ha instalado en el mismo modo de inicio.
3. Una vez que el sistema se inicia en el modo especificado, instale el sistema operativo desde ese modo.

NOTA: Para poder instalarse desde el modo de inicio UEFI, un sistema operativo debe ser compatible con UEFI. Los sistemas operativos DOS y de 32 bits no son compatibles con UEFI y sólo pueden instalarse desde el modo de inicio BIOS.

NOTA: Para obtener la información más reciente sobre sistemas operativos compatibles, visite www.dell.com/ossupport

Cambio del orden de inicio

Sobre esta tarea

Es posible que deba cambiar el orden de inicio si desea iniciar desde una llave USB o una unidad óptica. Las siguientes instrucciones pueden variar si ha seleccionado **BIOS** para **Boot Mode (Modo de inicio)**.

NOTA: El cambio de la secuencia de arranque de la unidad solo es compatible en el modo de arranque del BIOS.

Pasos

1. En la pantalla **Menú principal de configuración del sistema**, haga clic en **BIOS del sistema** > **Configuración de arranque** > **Configuración de arranque de UEFI** > **Secuencia de arranque de UEFI**.
2. Utilice las teclas de dirección para seleccionar un dispositivo de inicio y utilice las teclas + y - para desplazar el orden del dispositivo hacia abajo o hacia arriba.
3. Haga clic en **Exit (Salir)** y, a continuación, haga clic en **Yes (Sí)** para guardar la configuración al salir.

   NOTA: También puede habilitar o deshabilitar los dispositivos de orden de arranque, según sea necesario.

Configuración de red

Para ver la pantalla **Configuración de red**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Configuración de red**.

NOTA: Para obtener información sobre la configuración de rendimiento de red de Linux, consulte la *Guía de ajuste de red Linux para servidores basados en procesador AMD EPYC* en AMD.com.

NOTA: La configuración de red no es compatible con el modo de arranque del BIOS.

Tabla 12. Detalles de Configuración de red

Opción	Descripción
Configuración de PXE de UEFI	Permite controlar la configuración del dispositivo PXE de la UEFI.
Dispositivo de PXE n(n = 1 a 4)	Activa o desactiva el dispositivo. Si esta opción está habilitada, se crea una opción de inicio de PXE de UEFI para el dispositivo.
Configuración del dispositivo de PXE n(n = 1 a 4)	Permite controlar la configuración del dispositivo PXE.
Configuración de UEFI HTTP	Permite controlar la configuración del dispositivo HTTP de UEFI.
Dispositivo HTTP n(n = 1 a 4)	Activa o desactiva el dispositivo. Si esta opción está habilitada, se crea una opción de inicio de HTTP de UEFI para el dispositivo.
HTTP Device n Settings (Configuración de n de dispositivos HTTP) (n = 1 a 4)	Permite controlar la configuración del dispositivo HTTP.
Configuración de UEFI iSCSI	Permite controlar la configuración del dispositivo iSCSI.

Tabla 13. Detalles de Configuración del dispositivo de PXE n

Opción	Descripción
Interfaz	Especifica la interfaz de NIC utilizada para el dispositivo PXE.
Protocolo	Especifica el protocolo utilizado para el dispositivo PXE. Esta opción está establecida en **IPv4** o **IPv6**. De manera predeterminada, esta opción está configurada como **IPv4**.
Vlan	Habilita la Vlan para el dispositivo PXE. Esta opción está establecida en **Habilitar** o **Deshabilitar**. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
ID de Vlan	Muestra la ID de Vlan para el dispositivo PXE
Prioridad de Vlan	Muestra la prioridad de Vlan para el dispositivo PXE.

Tabla 14. Detalles de Configuración del dispositivo n de HTTP

Opción	Descripción
Interfaz	Especifica la interfaz de NIC utilizada para el dispositivo HTTP.
Protocolo	Especifica el protocolo que se utiliza para el dispositivo HTTP. Esta opción está establecida en **IPv4** o **IPv6**. De manera predeterminada, esta opción está configurada como **IPv4**. Las siguientes opciones estarán disponibles cuando protocolo esté configurado como IPv6: **Configuración automática**: activación/desactivación de la configuración automática de IPv6 para este dispositivo HTTP. **Dirección IPv6**: dirección de unidifusión IPv6 para este dispositivo HTTP. **Longitud del prefijo**: longitud del prefijo IPv6 (0-128) para este dispositivo HTTP.
Vlan	Habilita la Vlan para el dispositivo HTTP. Esta opción está establecida en **Habilitar** o **Deshabilitar**. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
ID de Vlan	Muestra la ID de Vlan para el dispositivo HTTP
Prioridad de Vlan	Muestra la prioridad de Vlan para el dispositivo HTTP.
DHCP	Habilita o deshabilita DHCP para este dispositivo HTTP. Esta opción está ajustada como **Enable (Habilitada)** de forma predeterminada.
Dirección IP	Especifica la dirección IP del dispositivo HTTP.
Máscara de subred	Especifica la máscara de subred para el dispositivo HTTP.
Gateway	Especifica la gateway para el dispositivo HTTP.
Información de DNS a través de DHCP	Habilita o deshabilita la información de DNS de DHCP. Esta opción está ajustada como **Enable (Habilitada)** de forma predeterminada.
DNS primario	Especifica la dirección IP del servidor DNS principal para el dispositivo HTTP.
DNS secundario	Especifica la dirección IP del servidor DNS secundario para el dispositivo HTTP.
URI	Obtiene la URI del servidor DHCP Si no está especificada

Tabla 15. Detalles de la pantalla Configuración de iSCSI de UEFI

Opción	Descripción
Nombre de iniciador de iSCSI	Especifica el nombre del iniciador iSCSI en formato IQN.
Dispositivo 1 iSCSI	Habilita o deshabilita el dispositivo iSCSI. Cuando está deshabilito, se crea una opción de inicio de UEFI para el dispositivo iSCSI automáticamente. Está establecida en **Deshabilitada** de manera predeterminada.
Configuración de dispositivo 1 de iSCSI	Permite controlar la configuración del dispositivo iSCSI.

Tabla 16. Detalles de la pantalla Configuración de dispositivo de ISCSI 1

Opción	Descripción
Conexión 1	Habilita o deshabilita la conexión de iSCSI. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Conexión 2	Habilita o deshabilita la conexión de iSCSI. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Valores de configuración 1	Permite controlar la configuración de la conexión de iSCSI.
Valores de configuración 2	Permite controlar la configuración de la conexión de iSCSI.
Orden de conexión	Permite controlar el orden en que se intentarán las conexiones de iSCSI.

Dispositivos integrados

Para ver la pantalla **Dispositivos integrados**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Dispositivos integrados**.

Tabla 17. Detalles de Dispositivos integrados

Opción	Descripción
Puertos USB accesibles para el usuario	Configure los puertos USB accesibles para el usuario. Seleccionar **Encender solo los puertos posteriores** deshabilita los puertos USB frontales; seleccionar **Apagar todos los puertos** deshabilita todos los puertos USB, frontales y posteriores; seleccionar **Apagar todos los puertos (dinámicamente)** deshabilita todos los puertos USB frontales y posteriores durante la POST. De manera predeterminada, esta opción está establecida en **Apagar todos los puertos**. Cuando los puertos USB accesibles para el usuario se establecen en **Apagar todos los puertos (dinámicamente)**, la opción **Habilitar solo los puertos frontales** está habilitada. • **Habilitar solo los puertos frontales**: habilita o deshabilita los puertos USB frontales durante el tiempo de ejecución del sistema operativo. El teclado y el mouse USB seguirán funcionando en ciertos puertos USB durante el proceso de arranque, según la selección. Después de que termine el proceso de arranque, los puertos USB se habilitarán o deshabilitarán según el ajuste.
Puerto USB interno	Habilita o deshabilita el **puerto USB interno**. De manera predeterminada, esta opción está establecida en **Encendido** o **Apagado**. De manera predeterminada, esta opción está establecida en **Encendido**.
Puerto USB de iDRAC Direct	El puerto USB de iDRAC Direct es administrado por iDRAC exclusivamente sin visibilidad de host. De manera predeterminada, esta opción está establecida en **Encendido** o **Apagado**. Si se establece en **Apagada**, iDRAC no detecta todos los dispositivos USB instalados en este puerto administrado. De manera predeterminada, esta opción está establecida en **Encendido**.
Controladora RAID integrada	Activa o desactiva la controladora RAID interna. Esta opción está establecida en **Habilitada** de manera predeterminada.
NIC1 y NIC2 integradas	Habilita o deshabilita las opciones **NIC1 y NIC2 integradas**. Si se establece en **Deshabilitada (sistema operativo)**, es posible que la NIC aún esté disponible para el acceso de red compartido por la controladora de administración integrada. Configure la opción **NIC1 y NIC2 integrada** mediante las utilidades de administración de NIC del sistema.
Controladora de video integrada	Activa o desactiva el uso de la controladora de video integrada como la pantalla principal. Si se establece en **Habilitada**, la controladora de video incorporada será la pantalla principal, incluso si complemento de tarjetas de gráficos están instalados. Cuando se establece en **Deshabilitada**, se utilizará una tarjeta gráfica suplementaria como la pantalla principal. El BIOS se muestra el resultado tanto para la principal de vídeo adicional y el vídeo incorporada durante la prueba POST y entorno previo al

Tabla 17. Detalles de Dispositivos integrados (continuación)

Opción	Descripción
	inicio. El video integrado se desactivará justo antes del inicio del sistema operativo. Esta opción está establecida en **Habilitada** de manera predeterminada. **NOTA:** Cuando haya varias tarjetas de gráficos adicionales instaladas en el sistema, la primera tarjeta detectada durante la enumeración de PCI se selecciona como video primario. Es posible que tenga que volver a ordenar las tarjetas en las ranuras para controlar qué tarjeta es el vídeo primario.
Estado actual de la controladora de video integrada	Muestra el estado actual de la controladora de video integrada. La opción **Estado actual de la controladora de video integrada** es un campo de solo lectura. Si la controladora de video integrada es la única funcionalidad de pantalla en el sistema (es decir, no hay ninguna tarjeta gráfica adicional instalada), la controladora de video integrada se utiliza automáticamente como la pantalla principal, incluso si la configuración de **Controladora de video integrada** está establecida en **Deshabilitada**.
Frecuencia de LCLK compleja de la raíz 0x00	Establece la frecuencia de LCLK para la dirección del bus 0x00.
Frecuencia de LCLK compleja de la raíz 0x20	Establece la frecuencia de LCLK para la dirección del bus 0x20.
Frecuencia de LCLK compleja de la raíz 0x40	Establece la frecuencia de LCLK para la dirección del bus 0x40.
Frecuencia de LCLK compleja de la raíz 0x60	Establece la frecuencia de LCLK para la dirección del bus 0x60.
Frecuencia de LCLK compleja de la raíz 0x80	Establece la frecuencia de LCLK para la dirección del bus 0x80.
Frecuencia de LCLK compleja de la raíz 0xA0	Establece la frecuencia de LCLK para la dirección del bus 0xA0.
Frecuencia de LCLK compleja de la raíz 0xC0	Establece la frecuencia de LCLK para la dirección del bus 0xC0.
Frecuencia de LCLK compleja de la raíz 0xE0	Establece la frecuencia de LCLK para la dirección del bus 0xE0.
Bus de I/O recomendado de PCIe	Cuando se establece en **Activado**, puede proporcionar la dirección de bus (en decimales) para elegir el dispositivo final para el bus de I/O recomendado. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
I/O recomendada mejorada	Cuando se establece en **Activada**, la velocidad de LCLK para el complejo raíz donde está activada la I/O preferida se establecerá automáticamente en 600 MHz (593 MHz efectivos).
Habilitación global de SR-IOV	Permite habilitar o deshabilitar la configuración del BIOS de los dispositivos de virtualización de I/O de una raíz (SR-IOV). Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Puerto de tarjeta SD interna	Activa o desactiva el puerto de tarjeta SD interno del módulo SD doble interno (IDSDM). De manera predeterminada, esta opción está establecida en **Encendido**.
Redundancia de la tarjeta SD interna	Configura el modo de redundancia del módulo SD doble interno (IDSDM). En el modo de **Duplicación**, los datos se escriben en ambas tarjetas SD. Cuando una de las tarjetas falla y se reemplaza, los datos de la tarjeta activa se copian en la tarjeta fuera de línea durante el inicio del sistema Cuando la redundancia está **Deshabilitada**, solo la tarjeta SD principal es visible para el sistema operativo. Esta opción está establecida en **Duplicación** de manera predeterminada.
Tarjeta SD interna principal	De manera predeterminada, la tarjeta SD principal está seleccionada como tarjeta SD 1. Si la tarjeta SD 1 no está presente, la controladora selecciona la tarjeta SD 2

Tabla 17. Detalles de Dispositivos integrados (continuación)

Opción	Descripción
	como tarjeta SD principal. Esta opción está establecida en **Tarjeta SD 1** de manera predeterminada.
Temporizador de vigilancia del SO	Si el sistema no responde, este temporizador de vigilancia ayuda a recuperar el sistema operativo. Cuando esta opción está establecida en **Habilitada**, el sistema operativo inicializa el temporizador. Cuando esta opción está establecida en **Deshabilitada** (el valor predeterminado), el temporizador no tendrá ningún efecto en el sistema.
Límite de región de memoria asignada para I/O	Controla dónde se asigna la MMIO. La opción **1 TB** está diseñada para sistemas operativos específicos que no son compatibles con MMIO mayor a 1 TB. Esta opción está establecida en **8 TB** de manera predeterminada. La opción predeterminada es la dirección máxima compatible con el sistema y recomendada en la mayoría de los casos.
Deshabilitación de ranura	Permite activar o desactivar las ranuras de PCIe disponibles en el sistema. La función Deshabilitación de ranura controla la configuración de las tarjetas PCIe instaladas en la ranura especificada. La deshabilitación de las ranuras solo se debe utilizar cuando la tarjeta periférica instalada impida arrancar el sistema operativo o provoque retrasos en el inicio del sistema. Si la ranura está desactivada, la ROM de opción y el controlador UEFI están desactivados. Solamente las ranuras que se encuentran presentes en el sistema están disponibles para control. **Ranura n**: habilita o deshabilita, o bien deshabilita únicamente el controlador de arranque para la ranura de PCIe n. Esta opción está establecida en **Habilitada** de manera predeterminada.
Bifurcación de ranura	**Configuración de bifurcación de descubrimiento de ranura** permite la **Bifurcación predeterminada de plataforma** y el **Control de bifurcación manual**. El valor predeterminado está establecido en **Bifurcación predeterminada de plataforma**. Se puede acceder al campo de bifurcación de ranura cuando se establece en **Control de bifurcación manual**, y aparece en color gris cuando se establece en **Bifurcación predeterminada de plataforma**.

Serial Communication (Comunicación en serie)

Para ver la pantalla **Comunicación en serie**, encienda el sistema, presione F2 y haga clic en **Menú principal de configuración del sistema** > **BIOS del sistema** > **Comunicación en serie**.

NOTA: El puerto serial es opcional para el sistema PowerEdge R6525. La opción de comunicación en serie solo corresponde si el puerto serie COM está instalado en el sistema.

Tabla 18. Detalles de Comunicación en serie

Opción	Descripción
Serial Communication (Comunicación en serie)	Permite seleccionar los dispositivos de comunicación en serie (dispositivo en serie 1 y dispositivo en serie 2) en el BIOS. También se puede habilitar la redirección de consola del BIOS y especificar la dirección de puerto. Esta opción está establecida en **Automática** de manera predeterminada.
Dirección de puerto serial	Permite establecer la dirección del puerto para los dispositivos de serie. Esta opción está establecida en **Dispositivo en serie 1=COM2, dispositivo en serie 2=COM1** de manera predeterminada. **NOTA:** Solo puede utilizar el dispositivo serie 2 para la función de comunicación en serie en la LAN. Para utilizar la redirección de consola mediante SOL, configure la misma dirección de puerto para la redirección de consola y el dispositivo serie. **NOTA:** Cada vez que se inicia el sistema, el BIOS sincroniza la configuración del MUX serie guardada en iDRAC. La configuración del MUX serie se puede modificar independientemente en iDRAC. La carga de la configuración

Tabla 18. Detalles de Comunicación en serie (continuación)

Opción	Descripción
	predeterminada del BIOS desde la utilidad de configuración del BIOS no siempre revierte la configuración del MUX serie a la configuración predeterminada del dispositivo en serie 1.
External Serial Connector (Conector serie externo)	Permite asociar el conector en serie externo a **Dispositivo en serie 1**, **Dispositivo en serie 2** o al **Dispositivo de acceso remoto**. Esta opción está establecida en **Dispositivo en serie 1** de manera predeterminada. **NOTA:** Solo Dispositivo serie 2 se puede utilizar para Comunicación en serie en la LAN (SOL). Para utilizar la redirección de consola mediante SOL, configure la misma dirección de puerto para la redirección de consola y el dispositivo serie. **NOTA:** Cada vez que se inicia el sistema, el BIOS sincroniza la configuración del MUX serie guardada en iDRAC. La configuración del MUX serie se puede modificar independientemente en iDRAC. La carga de la configuración predeterminada del BIOS desde la utilidad de configuración del BIOS no siempre revierte esta configuración a la configuración predeterminada del dispositivo en serie 1.
Failsafe Baud Rate (Velocidad en baudios a prueba de errores)	Permite especificar la velocidad en baudios a prueba de errores para la redirección de consola. El BIOS intenta determinar la velocidad en baudios automáticamente. Esta velocidad en baudios a prueba de errores solo se utiliza si falla el intento y no se debe cambiar el valor. De manera predeterminada, esta opción está configurada como **115200**.
Tipo de terminal remoto	Establece el tipo de terminal de consola remota. Esta opción está establecida en **VT100/VT220** de manera predeterminada.
Redirection After Boot (Redirección después del inicio)	Permite habilitar o deshabilitar la redirección de la consola del BIOS cuando se carga el sistema operativo. Esta opción está establecida en **Habilitada** de manera predeterminada.

Configuración del perfil del sistema

Para ver la pantalla **Configuración del perfil del sistema**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Configuración del perfil del sistema**.

Tabla 19. Detalles de Configuración del perfil del sistema

Opción	Descripción
Perfil del sistema	Permite establecer el perfil del sistema. Si configura la opción System Profile (Perfil del sistema) en un modo distinto a **Custom (Personalizado)**, el BIOS configura automáticamente el resto de las opciones. Solo se pueden cambiar el resto de opciones si el modo establecido es **Custom (Personalizado)**. Esta opción está establecida en **Rendimiento por vatio (sistema operativo)** de manera predeterminada. Otras opciones incluyen **Rendimiento** y **Personalizado**. **NOTA:** Todos los parámetros en pantalla de la configuración del perfil del sistema se encuentran disponibles solo cuando la opción **System Profile (Perfil del sistema)** está establecida en **Custom (Personalizado)**.
Administración de energía de la CPU	Permite establecer la administración de energía de la CPU. Esta opción está establecida en **OS DBPM** (DBPM del sistema operativo) de manera predeterminada. Otra opción incluye **Máximo rendimiento**.
Frecuencia de memoria	Configura la velocidad de la memoria del sistema. Puede seleccionar **Máximo rendimiento** o una velocidad específica. Esta opción está establecida en **Máximo rendimiento** de manera predeterminada.
Turbo Boost	Permite habilitar o deshabilitar el funcionamiento en modo Turbo Boost del procesador. Esta opción está establecida en **Habilitada** de manera predeterminada.

Tabla 19. Detalles de Configuración del perfil del sistema (continuación)

Opción	Descripción
Estados C	Permite habilitar o deshabilitar el funcionamiento del procesador en todos los estados de alimentación disponibles. Los estados C permiten que el procesador ingrese en un estado de bajo consumo cuando está inactivo. Cuando se establece en **Habilitado** (controlado por el sistema operativo) o en **Autónomo** (si hay compatibilidad con el control por hardware), el procesador puede funcionar en todos los estados de alimentación disponibles para ahorrar energía, pero podría aumentar la latencia de memoria y el jitter de frecuencia. Esta opción está establecida en **Habilitada** de manera predeterminada.
Escritura de datos CRC	Cuando se establece en **Habilitado**, se detectan y se corrigen los problemas de bus de datos de DDR4 durante las operaciones de 'escritura'. Se necesitan dos ciclos adicionales para la generación de bits de CRC que impacta en el rendimiento del sistema. Es de solo lectura, a menos que Perfil del sistema se establezca en **Personalizado**. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Comprobación automática del estado de la memoria	Permite establecer el modo de comprobación automática del estado de la memoria. Esta opción está establecida en **Standard** (Estándar) de manera predeterminada.
Velocidad de actualización de memoria	Establece la velocidad de actualización de la memoria en 1x o 2x. Esta opción está establecida en **1x** de manera predeterminada.
Administración de energía de enlace L1 ASPM PCI	Habilita o deshabilita la administración de energía del vínculo L1 ASPM de la PCI. Esta opción está establecida en **Habilitada** de manera predeterminada.
Control deslizante de determinismo	Establece el determinismo del sistema por **Determinismo de alimentación** o **Determinismo de rendimiento**. Esta opción está establecida en **Determinismo de alimentación** de manera predeterminada.
Modo de eficiencia optimizado	El modo de eficiencia optimizado maximiza el rendimiento por vatio mediante la reducción oportuna de la frecuencia/alimentación. Habilita o deshabilita el modo de eficiencia optimizado.
Deshabilitación de mejora de rendimiento del algoritmo (ApbDis)	Habilita o deshabilita la deshabilitación de mejora de rendimiento del algoritmo (ApbDis). Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Velocidad máxima de XGMI	Este campo especifica la velocidad máxima de XGMI del procesador.
Administración de ancho de enlace dinámico (DLWM)	Reduce el ancho de enlace de xGMI entre los conectores de x16 a x8 (valor predeterminado), cuando no se detecta tráfico en el vínculo. De manera predeterminada, esta opción es establecida en **No forzado**.

Seguridad del sistema

Para ver la pantalla **Seguridad del sistema**, encienda el sistema, presione F2 y haga clic en **Menú principal de configuración del sistema** > **BIOS del sistema** > **Seguridad del sistema**.

Tabla 20. Detalles de Seguridad del sistema

Opción	Descripción
CPU AES-NI	Mejora la velocidad de las aplicaciones mediante el cifrado y descifrado con Advanced Encryption Standard Instruction Set (Conjunto de instrucciones de estándar de cifrado avanzado) y está establecida en Habilitado de manera predeterminada. Esta opción está establecida en **Habilitada** de manera predeterminada.
Contraseña del sistema	Permite establecer la contraseña del sistema. Esta opción está establecida en **Habilitada** de forma predeterminada y es de solo lectura si el puente de la contraseña no está instalado en el sistema.
Contraseña de configuración	Permite establecer la contraseña de configuración. Esta opción es de solo lectura si el puente de contraseña no está instalado en el sistema.
Estado de contraseña	Bloquea la contraseña del sistema. De manera predeterminada, esta opción está establecida en **Desbloqueado**.

Tabla 21. Información de Seguridad del TPM 1.2

Opción	Descripción
Seguridad del TPM	**NOTA:** El menú TPM solo está disponible cuando el módulo TPM está instalado. Le permite controlar el modo de información del módulo de plataforma segura (TPM). De manera predeterminada, la opción **Seguridad del TPM** está establecida en **Desactivado**. Solo puede modificar los campos estado del TPM y activación del TPM si el campo **Estado del TPM** está establecido en **Encendido con medidas previas al arranque** o **Encendido sin medidas previas al arranque**. Si la opción TPM 1.2 está instalada, la opción **Seguridad de TPM** está establecida en **Apagada**, **Encendida con medidas previas al arranque** o **Encendida sin medidas previas al arranque**. Si la opción de TPM 2.0 está instalada, la opción **Seguridad del TPM** se establece en **Activado** o **Desactivado**. De manera predeterminada, esta opción está establecida en **Desactivada**.
Información de TPM	Permite cambiar el estado operativo del TPM. Esta opción está establecida en **Sin cambios** de forma predeterminada.
Firmware del TPM	Indica la versión de firmware del TPM.
Estado de TPM	Especifica el estado del TPM.
Comando TPM	Controla el Módulo de plataforma segura (TPM). Cuando se establece en **Ninguno**, no se envía ningún comando en el TPM. Si se establece en **Activado**, el TPM se habilitará y se activará. Si se establece en **Desactivado**, el TPM se deshabilitará y se desactivará. Cuando esta opción se establece en **Borrar**, se borra todo el contenido del TPM. De manera predeterminada, esta opción está establecida en **Ninguno**.

Tabla 22. Información de Seguridad del TPM 2.0

Opción	Descripción
Información de TPM	Permite cambiar el estado operativo del TPM. Esta opción está establecida en **Sin cambios** de forma predeterminada.
Firmware del TPM	Indica la versión de firmware del TPM.
Jerarquía de TPM	Habilita, deshabilita o borra las jerarquías de almacenamiento y aprobación. Si se configura en **Habilitado**, las jerarquías de aprobación y almacenamiento se pueden usar. Si se configura en **Deshabilitado**, las jerarquías de aprobación y almacenamiento no se pueden usar. Si se configura en **Borrar**, se borra cualquier valor de las jerarquías de aprobación y almacenamiento y, luego, se restablece la opción en **Habilitado**.
Configuración avanzada de TPM	Especifica detalles de la configuración avanzada del TPM

Tabla 23. Detalles de Seguridad del sistema

Opción	Descripción
Medición dinámica de la raíz de confianza (DRTM) de AMD	Habilitar/deshabilitar la Medición dinámica de la raíz de confianza (DRTM) de AMD Para habilitar AMD DRTM, se deben habilitar las siguientes configuraciones: 1. TPM2.0 debe estar habilitado y el algoritmo hash debe establecerse en SHA256. 2. Se debe habilitar el SME transparente (TSME). 3. La protección de acceso directo a la memoria debe estar habilitada.
Botón de encendido	Habilita y deshabilita el botón de encendido de la parte frontal del sistema. Esta opción está establecida en **Habilitada** de manera predeterminada.
Recuperación de alimentación de CA	Permite establecer la reacción del sistema después de que se restablezca la alimentación de CA del sistema. De manera predeterminada, esta opción está establecida en **Última**.
Demora de recuperación de alimentación de CA	Permite establecer la demora para que el sistema se encienda después de restaurar la alimentación de CA al sistema. De manera predeterminada, esta opción está establecida en **Inmediato**.

Tabla 23. Detalles de Seguridad del sistema (continuación)

Opción	Descripción
Demora definida por el usuario (60 s a 600 s)	Establece el valor de **User Defined Delay (Retraso definido por el usuario)** cuando está seleccionada la opción **User Defined (Definido por el usuario)** para **AC Power Recovery Delay (Retraso de recuperación de alimentación de CA)**.
Acceso de variable de UEFI	Proporciona diversos grados de variables UEFI de garantía. Cuando está establecida en **Estándar** (valor predeterminado), las variables UEFI son accesibles en el sistema operativo por la especificación UEFI. Cuando se establece en **Controlled (Controlado)**, las variables UEFI seleccionadas están protegidas en el entorno y las nuevas entradas de inicio UEFI se ven obligadas a estar en el extremo de la orden de inicio actual.
Arranque seguro	Habilita el arranque seguro, donde el BIOS autentica cada imagen de inicio previo usando los certificados de la política de inicio seguro. De manera predeterminada, el arranque seguro está establecido en **Deshabilitado**.
Política de arranque seguro	Cuando la política de arranque seguro está establecida en **Estándar**, el BIOS utiliza las claves y los certificados del fabricante del sistema para autenticar las imágenes previas al arranque. Cuando la política de inicio seguro está establecida en **Personalizada**, el BIOS utiliza las claves y los certificados definidos por el usuario. La política de inicio seguro está establecida en **Estándar** de manera predeterminada.
Modo de arranque seguro	Configura la manera en que el BIOS utiliza la política de inicio seguro objetos (PK, KEK, db, dbx). Si el modo actual se establece en **Modo implementado**, las opciones disponibles son **Modo de usuario** y **Modo implementado**. Si el modo actual se establece en **Modo de usuario**, las opciones disponibles son **Modo de usuario**, **Modo de auditoría** y **Modo implementado**.
Resumen de política de arranque seguro	Muestra la lista de certificados y hashes que el inicio seguro utiliza para autenticar las imágenes.
Configuración de la política personalizada de arranque seguro	Configura la política personalizada de arranque seguro. Para activar esta opción, establezca la política de inicio seguro para opción personalizada.

Tabla 24. Modo de arranque seguro

Opciones	Descripciones
Modo de usuario	En **Modo de usuario**, PK debe estar instalada y verificación de la firma DEL BIOS realiza en programación intenta actualizar los objetos de directiva. El BIOS permite transiciones programadas no autenticadas entre los modos.
Modo implementado	El **Modo implementado** es el modo más seguro. En **Modo implementado**, PK debe estar instalado y el BIOS realiza verificación de la firma en programación intenta actualizar los objetos de directiva. El **Modo implementado** restringe las transiciones de modo programático.
Modo de auditoría	En **Modo de auditoría**, PK no está presente. El BIOS no autentica mediante programación las actualizaciones de los objetos de directiva, y las transiciones entre los modos. El BIOS verifica la firma en las imágenes previas al arranque y registra los resultados en la tabla de información de ejecución de imagen, pero ejecuta las imágenes pasen o no la verificación. El **Modo de auditoría** es útil para determinar, mediante programación, un conjunto que funcione de objetos de política.

Asignación de contraseña del sistema y de configuración

Requisitos previos

Asegúrese de que el puente de contraseña esté habilitado. El puente de contraseña habilita o deshabilita las características de la contraseña del sistema y la contraseña de configuración. Para obtener más información, consulte la sección de configuración del puente de la tarjeta madre del Sistema.

NOTA: Si la configuración del puente de contraseña está deshabilitada, se eliminan las contraseñas actuales del sistema y de configuración, y no necesitará proporcionar la contraseña del sistema para iniciarlo.

Pasos

1. Para entrar a la configuración del sistema, presione F2 inmediatamente después de iniciar o reiniciar el sistema.
2. En la pantalla **System Setup Main Menu (Menú principal de la configuración del sistema)**, haga clic en **System BIOS (BIOS del sistema)** > **System Security (Seguridad del sistema)**.
3. En la pantalla **System Security (Seguridad del sistema)**, compruebe que la opción **Password Status (Estado de la contraseña)** está en **Unlocked (Desbloqueado)**.
4. En el campo **System Password (Contraseña del sistema)**, escriba la contraseña del sistema y presione Entrar o Tab.
   Utilice las siguientes reglas para asignar la contraseña del sistema:
   - Una contraseña puede tener hasta 32 caracteres.

   Aparecerá un mensaje para que introduzca de nuevo la contraseña del sistema.
5. Vuelva a introducir la contraseña del sistema y, a continuación, haga clic en **Aceptar**.
6. En el campo **System Password (Contraseña del sistema)**, escriba la contraseña del sistema y, a continuación, pulse la tecla Intro o el tabulador.
   Aparecerá un mensaje para que introduzca de nuevo la contraseña de configuración.
7. Vuelva a introducir la contraseña de configuración y, a continuación, haga clic en **OK (Aceptar)**.
8. Presione Esc para volver a la pantalla BIOS del Sistema. Presione Esc nuevamente.
   Un mensaje le indicará que guarde los cambios.
   NOTA: La protección por contraseña no se aplicará hasta que reinicie el sistema.

Uso de la contraseña del sistema para proteger el sistema

Sobre esta tarea

Si ha asignado una contraseña de configuración, el sistema la acepta como contraseña del sistema alternativa.

Pasos

1. Encienda o reinicie el sistema.
2. Escriba la contraseña del sistema y presione Intro.

Siguientes pasos

Cuando **Password Status** (Estado de la contraseña) está establecida en **Locked** (Bloqueado), escriba la contraseña del sistema y presione Intro cuando se le solicite al reiniciar.

NOTA: Si escribe una contraseña del sistema incorrecta, el sistema muestra un mensaje y le solicita que vuelva a ingresarla. Dispone de tres intentos para escribir la contraseña correcta. Tras el tercer intento erróneo, el sistema muestra un mensaje de error indicando que ha sistema dejado de funcionar y se debe apagar. Este error aparecerá aunque apague y reinicie el sistema, y lo hará hasta que se introduzca la contraseña correcta.

Eliminación o cambio de la contraseña del sistema o de configuración

Requisitos previos

NOTA: No se puede eliminar ni cambiar una contraseña del sistema o de configuración existente si **Estado de la contraseña** está establecido en **Bloqueado**.

Pasos

1. Para ingresar a Configuración del sistema, presione F2 inmediatamente después de encender o reiniciar el sistema.
2. En la pantalla **Menú principal de la configuración del sistema**, haga clic en **BIOS del sistema** > **Seguridad del sistema**.
3. En la pantalla **System Security (Seguridad del sistema)**, asegúrese de que el **Password Status (Estado de la contraseña)** está establecido en **Unlocked (Desbloqueado)**.

4. En el campo **Contraseña del sistema**, cambie o elimine la contraseña del sistema existente y, a continuación, presione Entrar o Tab.
5. En el campo System **Password (Contraseña del sistema)**, modifique, altere o elimine la contraseña de configuración existente, y, a continuación, pulse Enter (Intro) o Tab (Tabulador).

   Si modifica el sistema y la contraseña de configuración, aparecerá un mensaje que le solicitará que vuelva a introducir la contraseña nueva. Si elimina el sistema y la contraseña de configuración, aparecerá un mensaje que le solicitará que confirme la eliminación.
6. Presione Esc para volver a la pantalla **BIOS del sistema**. Presione Esc de nuevo y un mensaje le indicará que guarde los cambios.
7. Seleccione **Setup Password (Contraseña de configuración)**, modifique o elimine la contraseña de configuración existente, y presione Entrar o Tab.

   NOTA: Si modifica la contraseña del sistema o la contraseña de configuración, aparecerá un mensaje que le solicitará que vuelva a introducir la nueva contraseña. Si elimina la contraseña del sistema o la contraseña de configuración, aparecerá un mensaje que le solicitará que confirme la eliminación.

Funcionamiento con la contraseña de configuración habilitada

Si la opción **Setup Password** (Configurar contraseña) está establecida en **Enabled** (Habilitada), introduzca la contraseña de configuración correcta antes de modificar las opciones de configuración del sistema.

Dispone de tres intentos para introducir la contraseña correcta. Si no lo hace, el sistema mostrará este mensaje:

```
Invalid Password! Number of unsuccessful password attempts: <x> System Halted! Must power
down.
```

```
Password Invalid. Number of unsuccessful password attempts: <x> Maximum number of password
attempts exceeded.System halted.
```

El mensaje de error aparecerá aunque apague y reinicie el sistema hasta que introduzca la contraseña correcta. Las siguientes opciones son excepciones:

- Si la **System Password** (Contraseña del sistema) no está **Enabled** (Habilitada) y no está bloqueada con la opción **Password Status** (Estado de la contraseña), puede asignar una contraseña del sistema. Para obtener más información, consulte la sección de la pantalla de configuración de seguridad del Sistema.
- No puede deshabilitar ni cambiar una contraseña del sistema existente.

NOTA: Puede utilizar la opción de estado de la contraseña y la opción de contraseña de configuración para proteger la contraseña del sistema de cambios no autorizados.

Control de SO redundante

Para ver la pantalla **Control de sistema operativo redundante**, encienda el sistema, presione F2 y haga clic en **Menú principal de configuración del sistema** > **BIOS del sistema** > **Control de sistema operativo redundante**.

Tabla 25. Detalles de Control de sistema operativo redundante

Opción	Descripción
Ubicación de SO redundante	Permite seleccionar un disco de copia de seguridad a partir de los siguientes dispositivos: • **Ninguno** • **IDSDM** • **Puertos SATA en modo de AHCI** • **Tarjetas PCIe BOSS (unidades M.2 internas)** • • **USB interno** **NOTA:** Las configuraciones de RAID y tarjetas NVMe no se incluyen, ya que el BIOS no tiene la capacidad de distinguir las unidades individuales en este tipo de configuraciones.
Estado de SO redundante	**NOTA:** Esta opción está deshabilitada si **Redundant OS Location (Ubicación del sistema operativo redundante)** se configura como **None (Ninguno)**. Si se configura como **Visible**, la lista de arranque y el SO pueden visualizar el disco de respaldo. Si se configura como **Oculta**, la lista de arranque y el SO no pueden visualizar el disco de

Tabla 25. Detalles de Control de sistema operativo redundante (continuación)

Opción	Descripción
	respaldo, ya que se deshabilita. De manera predeterminada, esta opción está configurada como **Visible**. **NOTA:** El BIOS deshabilita el dispositivo en el hardware, para que el sistema operativo no pueda acceder a él.
Inicio de SO redundante	**NOTA:** Esta opción está deshabilitada si **Redundant OS Location (Ubicación del sistema operativo redundante)** se configura como **None (Ninguno)** o si **Redundant OS State (Estado de sistema operativo redundante)** se configura como **Hidden (Oculto)**. Si se establece en **Enabled** (Habilitado), el BIOS se inicia al dispositivo especificado en **Redundant OS Location** (Ubicación del sistema operativo redundante). Si se configura como **Deshabilitado**, el BIOS conserva la configuración de la lista de arranque actual. Esta opción está establecida en **Habilitada** de manera predeterminada.

Otros ajustes

Para ver la pantalla **Otros ajustes**, encienda el sistema, presione F2 y haga clic en **Menú principal de la configuración del sistema** > **BIOS del sistema** > **Otros ajustes**.

Tabla 26. Detalles de Otros ajustes

Opción	Descripción
Hora del sistema	Permite fijar la hora del sistema.
System Date (Fecha del sistema)	Permite fijar la fecha del sistema.
Etiqueta de activo	Muestra la etiqueta de activo y permite modificarla por motivos de seguridad y seguimiento.
Keyboard NumLock (Bloqueo numérico del teclado)	Permite establecer si el sistema se inicia con la opción Bloq Núm del teclado habilitada o deshabilitada. De manera predeterminada, esta opción está establecida en **Encendido**. **NOTA:** Esta opción no es aplicable a los teclados de 84 teclas.
Aviso de F1/F2 en caso de error	Habilita o deshabilita el indicador de F1/F2 en caso de error. Esta opción está establecida en **Habilitada** de manera predeterminada. El indicador de F1/F2 también incluye los errores del teclado.
Load Legacy Video Option ROM (Cargar ROM de opción de video anterior)	Habilita o deshabilita la opción de Carga de ROM de opción de video heredado. Esta opción está establecida en **Deshabilitada** de manera predeterminada.
Acceso al BIOS de Dell Wyse P25/P45	Habilita o deshabilita el acceso al BIOS de Dell Wyse P25/P45. Esta opción está establecida en **Habilitada** de manera predeterminada.
Solicitud de ciclo de encendido	Habilita o deshabilita la solicitud de ciclo de encendido. De manera predeterminada, esta opción está establecida en **Ninguno**.

Utilidad iDRAC Settings (Configuración de iDRAC)

La utilidad de configuración de la iDRAC es una interfaz que se puede utilizar para establecer y configurar los parámetros de la iDRAC utilizando UEFI. Puede habilitar o deshabilitar diversos parámetros de la iDRAC mediante la utilidad de configuración de la iDRAC.

NOTA: Para acceder a algunas funciones de la utilidad iDRAC Settings (Configuración de iDRAC) se requiere la actualización de la licencia de iDRAC Enterprise.

Para obtener más información sobre el uso de iDRAC, consulte la *Guía del usuario de Integrated Dell Remote Access Controller* en https://www.dell.com/idracmanuals.

Device Settings (Configuración del dispositivo)

La **Configuración del dispositivo** le permite configurar los parámetros del dispositivo, como las controladoras de almacenamiento o las tarjetas de red.

Dell Lifecycle Controller

Dell Lifecycle Controller (LC) proporciona capacidades avanzadas de administración de sistemas integrados, lo que incluye implementación, configuración, actualización, mantenimiento y diagnóstico de los sistemas. LC se distribuye como parte de la solución fuera de banda de la iDRAC y las aplicaciones integradas Unified Extensible Firmware Interface (UEFI) del sistema Dell.

Administración de sistema integrada

Lifecycle Controller de Dell proporciona administración de sistema integrada avanzada durante el ciclo de vida del sistema. Dell Lifecycle Controller se puede iniciar durante la secuencia de arranque y funciona independientemente del sistema operativo.

NOTA: Puede que determinadas configuraciones de plataforma no admitan el conjunto completo de funciones que ofrece Dell Lifecycle Controller.

Para obtener más información acerca de la configuración de Lifecycle Controller de Dell, la configuración de hardware y firmware, y la implementación del sistema operativo, consulte la documentación de Lifecycle Controller de Dell en https://www.dell.com/idracmanuals.

Boot Manager (Administrador de inicio)

La pantalla **Administrador de arranque** permite seleccionar las opciones de arranque y las utilidades de diagnóstico.

Para ingresar al **Administrador de arranque**, encienda el sistema y presione F11.

Tabla 27. Detalles del Administrador de arranque

Opción	Descripción
Continue Normal Boot (Continuar inicio normal)	El sistema intenta iniciar los dispositivos empezando por el primer elemento en el orden de inicio. Si el intento de inicio falla, el sistema lo intenta con el siguiente elemento y así sucesivamente hasta iniciar uno o acabar con las opciones existentes.
Menú de inicio de BIOS único	Lo lleva al menú de inicio, donde puede seleccionar un dispositivo de inicio de una vez desde el que iniciar.
Launch System Setup (Iniciar Configuración del sistema)	Permite acceder a System Setup (Configuración del sistema).
Launch Lifecycle Controller (Ejecutar Lifecycle Controller)	Sale del administrador de arranque e inicia el programa de Dell Lifecycle Controller.
System Utilities (Utilidades del sistema)	Permite iniciar el menú de utilidades del sistema, como el inicio de diagnósticos, el explorador de archivos de actualización del BIOS y el reinicio del sistema.

Inicio PXE

Puede utilizar la opción de ambiente de ejecución previo al arranque (PXE) para iniciar y configurar los sistemas en red de manera remota.

Para acceder a la opción **Arranque de PXE**, inicie el sistema y presione F12 durante la POST en lugar de utilizar la secuencia de arranque estándar de la configuración del BIOS. No aparecerá ningún menú ni le permitirá administrar los dispositivos de red.