Actualización de información de PowerEdge R550: hoja técnica

Noviembre de 2022
Rev. 1

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.

Tabla de contenido

1

Visión general

La información de este documento reemplaza la información en las secciones pertinentes del Manual de instalación y servicio, la Guía de referencia de BIOS y UEFI, y las Especificaciones técnicas.

Para obtener la información completa, consulte los documentos disponibles en https://www.dell.com/poweredgemanuals.

Temas:

Historial de revisiones

En esta sección, se proporciona una descripción de los cambios del documento.

Tabla 1. Historial de revisiones del documento

Revisión del documento	Fecha	Descripción de cambios
1	Noviembre de 2022	1. Nota agregada para la nueva PIB 2. Configuración mínima para la POST actualizada 3. BIOS y seguridad del sistema actualizadas 4. PSU actualizadas

2

Actualización de información

Temas:

Extracción de la tarjeta mediadora de alimentación

Requisitos previos

1. Siga las reglas de seguridad que se enumeran en Instrucciones de seguridad.
2. Siga el procedimiento que se describe en Antes de trabajar en el interior del sistema.
3. Quite la cubierta para flujo de aire.
4. Quite la PSU.
5. Desconecte los cables que están conectados a la placa intercaladora de alimentación (PIB) y observe la colocación de los cables.

NOTA: Los sistemas enviados desde noviembre del 2022 pueden tener una placa de distribución de alimentación y conectores diferentes.

Pasos

1. Con un destornillador Phillips n.º 2, quite los tornillos que fijan la placa intercaladora de alimentación (PIB) al sistema.
2. Levante la PIB para quitarla del sistema.

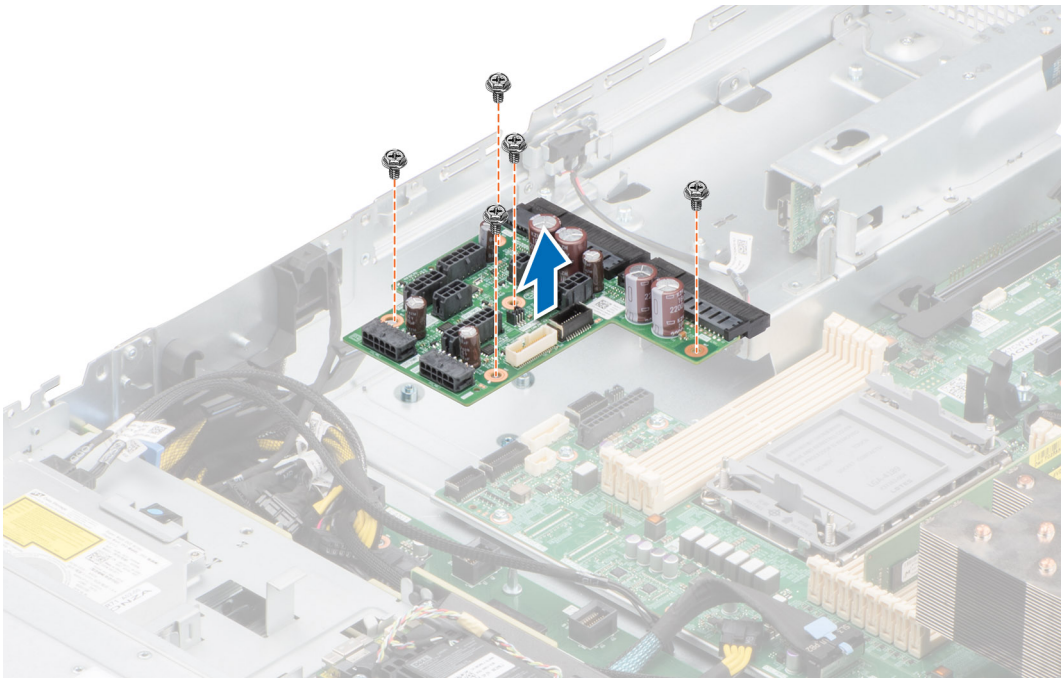

Ilustración 1. Extracción de la tarjeta mediadora de alimentación

Siguientes pasos

Reemplace la placa intercaladora de alimentación.

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 2. Detalles de Seguridad del sistema

Opción	Descripción
AES-NI de la CPU	Mejora la velocidad de las aplicaciones mediante el cifrado y descifrado con el conjunto de instrucciones de estándar de cifrado avanzado (AES-NI). 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 manera 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 la contraseña	Bloquea la contraseña del sistema. Esta opción está establecida en **Desbloqueada** de manera predeterminada.
Información de TPM	Indica el tipo de Módulo de plataforma segura, si hay una presente.

Tabla 3. Información de seguridad de TPM 1.2

Opción		Descripción
Información de TPM		
Seguridad de 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 de TPM** está establecida en **Desactivada**. 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 inicio** o **Encendido sin medidas previas al inicio**. Si el TPM 1.2 está instalado, la opción **Seguridad de TPM** está establecida en **Apagada**, **Encendida con medidas previas al arranque** o **Encendida sin medidas previas al arranque**.
Información de TPM		Muestra el estado operativo del TPM.
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. Esta opción está establecida en **Ninguna** de manera predeterminada.
Configuración avanzada de TPM	**Aprovisionamiento de omisión de PPI de TPM**	Si se establece en **Habilitada**, permite que el sistema operativo omita las peticiones de la interfaz de presencia física (PPI) al emitir las operaciones de aprovisionamiento de interfaz de potencia y configuración avanzada de PPI (ACPI).
	Borrado de omisión de PPI de TPM	Si se establece en **Habilitada**, permite que el sistema operativo omita las peticiones de la interfaz de presencia física (PPI) al emitir las operaciones claras de interfaz de potencia y configuración avanzada de PPI (ACPI).

Tabla 4. Información de seguridad de TPM 2.0

Opción	Descripción	
Información de TPM		
Seguridad de 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 de TPM** está establecida en **Desactivada**. Si el TPM 2.0 está instalado, la opción **Seguridad de TPM** se establece en **Activada** o **Desactivada**. De manera predeterminada, esta opción está establecida en **Desactivada**.	
Información de TPM	Muestra el estado operativo del TPM.	
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	**Aprovisionamiento de omisión de PPI de TPM**	Si se establece en **Habilitada**, permite que el sistema operativo omita las peticiones de la interfaz de presencia física (PPI) al emitir las operaciones de aprovisionamiento de interfaz de potencia y configuración avanzada de PPI (ACPI).
	Borrado de omisión de PPI de TPM	Si se establece en **Habilitada**, permite que el sistema operativo omita las peticiones de la interfaz de presencia física (PPI) al emitir las operaciones claras de interfaz de potencia y configuración avanzada de PPI (ACPI).
	Selección de algoritmo TPM2	Permite al usuario cambiar los algoritmos criptográficos en el Módulo de plataforma segura (TPM). Las opciones disponibles dependen del firmware del TPM. Para activar la Selección de algoritmo de TPM2, la tecnología Intel(R) TXT debe estar desactivada. La opción Selección de algoritmos de TPM2 es compatible con SHA1, SHA128, SHA256, SHA512 y SM3 mediante la detección del módulo TPM. Esta opción está establecida en **SHA1** de manera predeterminada.

Tabla 5. Detalles de Seguridad del sistema (continuación)

Opción	Descripción
Intel(R) TXT	Permite establecer la opción Tecnología de ejecución de confianza (TXT) de Intel. Para habilitar la opción **Intel TXT**, la tecnología de virtualización y la seguridad del TPM deben estar activadas con medidas previas al arranque para TPM 1.2 o configuradas en **Activado** con algoritmo SHA256 para TPM 2.0. De manera predeterminada, esta opción está establecida en **Desactivada**. Se estableció en **On (Activado)** para la compatibilidad con el inicio seguro (protección de firmware) en Windows 2022.
Cifrado de memoria	Habilita o inhabilita Intel Total Memory Encryption (TME) y Multi-Tenant (Intel® TME-MT). Cuando la opción está establecida en **Deshabilitada**, el BIOS desactiva las tecnologías TME y MK-TME. Cuando la opción está establecida en **Single Key (Clave única)**, el BIOS activa la tecnología TME. Cuando la opción está establecida en **Varias claves**, el BIOS habilita la tecnología TME-MT, la opción Límite de dirección física de la CPU debe estar deshabilitada para seleccionar la opción Varias claves. De manera predeterminada, esta opción está establecida en **Deshabilitada**.
Intel(R) SGX	Permite establecer la opción de Intel Software Guard Extension (SGX). Para habilitar la opción **Intel SGX**, el procesador debe ser compatible con SGX, la ocupación de la memoria debe

Tabla 5. Detalles de Seguridad del sistema (continuación)

Opción	Descripción
	ser compatible (8 módulos idénticos de DIMM1 a DIMM8 por conector de CPU como mínimo, no admitida en la configuración de la memoria persistente), el modo de funcionamiento de la memoria debe estar configurado en Modo optimizador, el cifrado de la memoria debe estar habilitado y el intercalado de nodos debe estar inhabilitado. Esta opción está establecida en **Apagada** de manera predeterminada. Cuando esta opción está **Desactivada**, el BIOS desactiva la tecnología SGX. Cuando esta opción está **Activada**, el BIOS activa la tecnología SGX.
Acceso dentro de banda de información de paquete de SGX	Le permite acceder a la opción dentro de banda de información del paquete de Intel Software Guard Extension (SGX). Esta opción está establecida en **Apagada** de manera predeterminada.
Tamaño de PPMRR	Establece el tamaño de PPMRR.
QoS de SGX	Activa o desactiva la calidad de servicio de SGX.
Seleccionar el tipo de entrada de EPOCH del propietario	Le permite seleccionar **Cambiar a EPOCH de nuevo propietario aleatorio** o **EPOCH de propietario definido por el usuario manual**. Cada EPOCH tiene 64 bits. Una vez que se genera un nuevo EPOCH mediante la selección de **Cambiar a EPOCH de nuevo propietario aleatorio**, la opción regresa a **EPOCH de propietario definido por el usuario manual**.
	Epoch n de Software Guard Extensions: establece los valores de Epoch de Software Guard Extensions.
Activar escritura en SGXLEPUBKEYHASH[3:0] desde SO/SW	Activa o desactiva las operaciones de escritura en SGXLEPUBKEYHASH[3:0] desde SO/SW.
	Hash0 de clave pública LE de SGX: establece los bytes de 0-7 para iniciar el hash de clave pública de enclave de lanzamiento en SGX.
	Hash1 de clave pública LE de SGX: establece los bytes de 8-15 para iniciar el hash de clave pública de enclave de lanzamiento en SGX.
	Hash2 de clave pública LE de SGX: establece los bytes de 16-23 para iniciar el hash de clave pública de enclave de lanzamiento en SGX.
	Hash3 de clave pública LE de SGX: establece los bytes de 24-31 para iniciar el hash de clave pública de enclave de lanzamiento en SGX.
Activar/desactivar el agente de registro de MP automático para SGX	Permite desactivar el registro de MP automático para SGX. El agente de registro de MP está encargado de registrar la plataforma.
Restablecimiento de fábrica de SGX	Le permite restablecer la opción de SGX a la configuración de fábrica. Esta opción está establecida en **Apagada** de manera predeterminada.
Botón de encendido	Permite activar y desactivar el botón de encendido de la parte frontal del sistema. Esta opción está establecida en **Activada** de manera predeterminada.
AC Power Recovery	Permite establecer la reacción del sistema después de que se restablece la alimentación de CA. De manera predeterminada, esta opción está establecida en **Último**. **NOTA:** El sistema host no se encenderá hasta que se complete la raíz de confianza (RoT) de iDRAC. El encendido del host se demorará durante 90 segundos como mínimo después de que se aplique la CA.
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. Esta opción está establecida en **Inmediata** de manera predeterminada. Si esta opción se establece en **Inmediata**, no hay demoras en el encendido. Si se establece en **Aleatoria**, el sistema creará una demora aleatoria para el encendido. Cuando esta opción se establece en **Definida por el usuario**, el tiempo de demora del sistema para encenderse es el manual.
Demora definida por el usuario (60 s a 600 s)	Establece la opción **Demora definida por el usuario** cuando está seleccionada la opción **Definido por el usuario** para **Demora de recuperación de alimentación de CA**. El tiempo de recuperación real de CA debe agregar el tiempo de confianza de raíz de iDRAC (alrededor de 50 segundos).
Acceso a variables de UEFI	Proporciona diversos grados de variables UEFI de garantía. Cuando se establece en **Estándar** (valor predeterminado), las variables de UEFI son accesibles en el sistema operativo por la

Tabla 5. Detalles de Seguridad del sistema (continuación)

<table>
<tr><th>Opción</th><th>Descripción</th></tr>
<tr><td></td><td>especificación UEFI. Cuando se establece en Controlado, las variables de UEFI seleccionadas están protegidas en el entorno y las nuevas entradas de arranque de UEFI se ven obligadas a estar en el extremo de la orden de arranque actual.</td></tr>
<tr><td>Interfaz de facilidad de administración dentro de banda</td><td>Si se establece en Desactivado, el ajuste oculta los dispositivos HECI del motor de administración (ME) y los dispositivos de IPMI del sistema operativo. Esto evita que el sistema operativo a la de cambiar el límite de alimentación ME configuración, y bloquea el acceso a todos los dentro de banda las herramientas de administración. Toda la administración debe ser administrada a través de fuera de banda. Esta opción está establecida en Habilitada de manera predeterminada.
NOTA: Actualización del BIOS requiere dispositivos HECI en funcionamiento y las actualizaciones de DUP requieren una interfaz de IPMI en funcionamiento. Este valor se debe establecer en Activado para evitar errores de actualización.</td></tr>
<tr><td>Migración de seguridad de SMM</td><td>Activa o desactiva las protecciones de migración de seguridad de SMM para UEFI. Está habilitada para la compatibilidad con Windows 2022.</td></tr>
<tr><td>Arranque seguro</td><td>Habilita Arranque seguro, donde el BIOS autentica cada imagen de arranque previo usando los certificados de la política de arranque seguro. El arranque seguro está establecido en Estándar de manera predeterminada.</td></tr>
<tr><td>Política de arranque seguro</td><td>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 arranque seguro está establecida en Personalizada, el BIOS utiliza las claves y los certificados definidos por el usuario. La política de arranque seguro está establecida en Estándar de manera predeterminada.</td></tr>
<tr><td>Modo de arranque seguro</td><td>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 aplicado, las opciones disponibles son Modo de usuario y Modo aplicado. Si el modo actual se establece en modo de usuario, las opciones disponibles son Modo de usuario, modalidad de auditoría y modo aplicado.
Tabla 6. Modo de arranque seguro
<table>
<tr><th>Opciones</th><th>Descripciones</th></tr>
<tr><td>Modo de uso</td><td>En Modo de usuario, la PK debe estar instalada y el BIOS realiza una verificación de firma en intentos programáticos de actualizar los objetos de política.
El BIOS permite transiciones programadas no autenticadas entre los modos.</td></tr>
<tr><td>Modo de auditoría</td><td>En Modo de auditoría, la PK no está presente. El BIOS no autentica actualizaciones programáticas a los objetos de política y transiciones entre 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.</td></tr>
<tr><td>Modo aplicado</td><td>El Modo aplicado es el modo más seguro. En Modo aplicado, la PK debe estar instalada y el BIOS realiza una verificación de firma en intentos programáticos de actualizar los objetos de política.
Impide que el modo aplicado mediante programación transiciones de modo.</td></tr>
</table></td></tr>
<tr><td>Resumen de política de arranque seguro</td><td>Muestra la lista de certificados y hashes que el inicio seguro utiliza para autenticar las imágenes.</td></tr>
<tr><td>Configuración de la política personalizada de inicio seguro</td><td>Configura la Política personalizada de inicio seguro. Para habilitar esta opción, establezca la política de arranque seguro en la opción Personalizada. En la siguiente lista, se proporcionan</td></tr>
</table>

Tabla 5. Detalles de Seguridad del sistema (continuación)

Opción	Descripción
	las descripciones de las diferentes configuraciones de política personalizada de arranque seguro disponibles: • **Clave de plataforma (PK):** importe, exporte, elimine o restaure la clave de la plataforma (PK) • **Base de datos de clave de intercambio de claves (KEK):** importe, exporte, elimine o restaure entradas en la base de datos de clave de intercambio de claves (KEK) • **Base de datos de firma autorizada (db):** importe, exporte, elimine o restaure las entradas en la base de datos de firma autorizada (db) • **Base de datos de firma prohibida (dbx):** importe, exporte, elimine o restaure las entradas en la base de datos de firma prohibida (dbx) • **Eliminar todas las entradas de políticas (PK, KEK, db, y dbx):** restaure las entradas predeterminadas del fabricante del sistema para la base de datos PK, KEK, db y dbx. Se eliminarán todas las entradas importadas. • **Exportar valores hash de firmware**: exporte valores para imágenes de firmware de otros fabricantes, como el firmware de la controladora de red y el firmware de la controladora de almacenamiento ○ **Seleccionar imagen de firmware**: esta es una lista de imágenes de firmware de otros fabricantes que el sistema intentó cargar en este arranque. Elija una imagen y, a continuación, seleccione "Exportar" para escribir el valor de hash SHA-256 de la imagen en un archivo ○ **Exportar entrada seleccionada**: escriba la entrada de la base de datos seleccionada en un archivo

Configuración mínima para POST

Los componentes que se enumeran a continuación son la configuración mínima para POST:

- Una sola unidad de fuente de alimentación
- Tarjeta madre
- Un procesador en el conector de procesador 1
- Placa intercaladora de alimentación (PIB) y cables
- Un módulo de memoria (DIMM) instalado en el conector A1

Especificaciones de PSU

El sistema PowerEdge R550 es compatible con hasta dos unidades de fuente de alimentación (PSU) de CA o CC.

Tabla 7. Especificaciones de PSU

PSU	Clase	Disipación de calor (máxima)	Frecuencia	Voltaje	CA		CC	Corriente
					Línea alta de 200 a 240 V	Línea baja de 100 a 120 V		
1100 W de CC	NA	4265 BTU/h	NA	-48 a (-60) V	NA	NA	1100 W	27 A
1100 W con modo mixto	Titanium	4125 BTU/h	50/60 Hz	100-240 V CA	1100 W	1050 W	NA	12 A- 6,3 A
	NA	4125 BTU/h	NA	240 V CC	NA	NA	1100 W	5,2 A
800 W con modo mixto	Platinum	3000 BTU/h	50/60 Hz	100 a 240 V de CA, autoajustable	800 W	800 W	NA	9,2 - 4,7 A
	NA	3000 BTU/h	NA	240 V de CC, autoajustable	NA	NA	800 W	3,8 A

Tabla 7. Especificaciones de PSU (continuación)

PSU	Clase	Disipación de calor (máxima)	Frecuencia	Voltaje	CA		CC	Corriente
					Línea alta de 200 a 240 V	Línea baja de 100 a 120 V		
700 W con modo mixto	Titanium	2625 BTU/h	50/60 Hz	200-240 V CA	700 W	NA	NA	4,1 A
	NA	2625 BTU/h	NA	240 V CC	NA	NA	700 W	3,4 A
600 W con modo mixto	Platinum	2250 BTU/h	50/60 Hz	100 a 240 V de CA, autoajustable	600 W	600 W	NA	7,1 a 3,6 A
	NA	2250 BTU/h	NA	240 V de CC, autoajustable	NA	NA	600 W	2,9 A

NOTA: Este sistema también ha sido diseñado para la conexión a sistemas de alimentación de TI con un voltaje entre fases no superior a 240 V.

NOTA: La disipación de calor se calcula mediante la potencia en vatios del sistema de alimentación.

NOTA: Cuando seleccione o actualice la configuración del sistema, para garantizar una utilización de energía óptima, verifique el consumo de energía del sistema con Dell Energy Smart Solution Advisor, disponible en **Dell.com/ESSA**.