DELL Technologies

Documentación técnica

Documentación técnica: Seguridad de resiliencia cibernética en servidores Dell EMC PowerEdge

Diciembre de 2020

Revisiones

Fecha	Descripción
Enero de 2018	Versión inicial
Noviembre de 2020	Versión revisada:

Tabla de contenido

Tabla de contenido

Resumen ejecutivo

El enfoque de Dell Technologies hacia la seguridad es intrínseco: las características de seguridad se incorporan de fábrica, no se agregan posteriormente y forman parte de cada etapa del ciclo de vida de desarrollo seguro de Dell. Nos esforzamos por garantizar la evolución continua de los controles, las características y las soluciones de seguridad de PowerEdge para cumplir con los requisitos de un panorama de amenazas en constante crecimiento y seguimos afianzando la seguridad con Silicon Root of Trust. En este documento, se detallan las características de seguridad incorporadas en la plataforma de resiliencia cibernética de PowerEdge, habilitadas, en su mayoría, por Dell Remote Access Controller (iDRAC9). Se agregaron varias características nuevas desde la documentación técnica anterior de seguridad de PowerEdge, que abarcan desde control de acceso hasta cifrado de datos y garantía de la cadena de suministro. Entre ellas se encuentran: Análisis en vivo del BIOS, personalización del arranque seguro de la UEFI, MFA de RSA SecurID, administración segura de claves empresariales (SEKM), Secured Component Verification (SCV), borrado mejorado del sistema, inscripción y renovación automáticas de certificados, selección de cifrado y compatibilidad con CNSA. Todas las características emplean inteligencia y automatización generalizadamente para ayudarlo a adelantarse a la curva de amenazas, y permitir la capacidad de expansión que exigen los modelos de uso en constante crecimiento.

1. Introducción

A medida que evoluciona el panorama de amenazas, los profesionales de TI y de seguridad se esfuerzan por controlar los riesgos que presenta para sus datos y recursos. Los datos se utilizan en muchos dispositivos, en las instalaciones y en la nube, y las vulneraciones de datos de alto impacto continúan aumentando. Históricamente, la atención se ha centrado en la seguridad del SO, las aplicaciones, los firewalls y los sistemas IPS e IDS. Estas áreas siguen siendo relevantes. Sin embargo, dados que los sucesos de los últimos años han amenazado la seguridad del hardware, consideramos que es crítico proteger la infraestructura basada en hardware, como el firmware, el BIOS, el BMC y otro tipo de protección de hardware, como la garantía de la cadena de suministro.

En el índice de transformación digital de Dell Technologies de 2020, se informó que la privacidad de datos y las preocupaciones de ciberseguridad son el principal obstáculo para la transformación digital.[1] El 63 % de las empresas experimentó una pérdida en la integridad de sus datos debido a la explotación de una vulnerabilidad.[2]. Los daños globales relacionados con los ciberdelitos llegarán a los US$6 billones en 2021[3].

Debido al aumento en la relevancia de los servidores en una arquitectura de centro de datos definida por software, la seguridad de los servidores se ha convertido en un elemento fundamental de la seguridad empresarial general. La seguridad de los servidores debe centrarse en el nivel de hardware y de firmware mediante la utilización de una raíz de confianza fija que se puede implementar para comprobar las operaciones posteriores dentro del servidor. De esta manera, se establece una cadena de confianza que se extiende a lo largo del ciclo de vida útil del servidor, desde la implementación hasta el mantenimiento y el retiro.

La 14.ª y la 15.ª generación de servidores Dell EMC PowerEdge con iDRAC9 ofrecen esta cadena de confianza y la combinan con controles de seguridad y herramientas de administración integrales a fin de proporcionar capas sólidas de seguridad en el hardware y el firmware. El resultado es una arquitectura de resiliencia cibernética en todo el servidor, que incluye el firmware integrado del servidor, los datos almacenados en el sistema, el sistema operativo y los dispositivos periféricos, además de las operaciones de administración relacionadas. Las organizaciones pueden desarrollar un proceso para proteger su valiosa infraestructura de servidores y los datos en ella, detectar cualquier anomalía, vulneración u operación no autorizada, y recuperarse tras eventos no intencionados o maliciosos.

[1] Índice de transformación digital de Dell Technologies de 2020

[2] Se compararon las amenazas de seguridad actuales con el control a nivel del BIOS. Un informe acerca del liderazgo intelectual realizado por Forrester Consulting y encargado por Dell, 2019

[3] Ransomware Attacks Predicted to Occur... The National Law Review, 2020

2. La ruta hacia una infraestructura de servidor segura

La seguridad de los servidores Dell EMC PowerEdge ha sido sólida durante varias generaciones e incluye la innovación en el uso de la seguridad de datos basada en el silicio. Los servidores Dell EMC PowerEdge 14G extendieron la seguridad basada en el silicio para autenticar el BIOS y el firmware con una raíz de confianza criptográfica durante el proceso de arranque del servidor. El equipo de productos de Dell EMC consideró varios requisitos clave durante el diseño de la 14.ª y la 15.ª generación de servidores PowerEdge en respuesta a las amenazas de seguridad que enfrentan los entornos de TI modernos:

- **Protección:** proteja el servidor en todos los aspectos del ciclo de vida útil, incluidos el BIOS, el firmware, los datos y el hardware físico
- **Detección:** detecte ataques cibernéticos maliciosos y cambios no aprobados; involucre proactivamente a los administradores de TI
- **Recuperación:** recupere el BIOS, el firmware y el sistema operativo a un buen estado conocido; retire o reutilice los servidores de manera segura

Los servidores Dell EMC PowerEdge cumplen con los estándares clave de la industria en criptografía y seguridad, tal como se elabora en este documento, y realizan el seguimiento y la administración continua de vulnerabilidades nuevas.

Dell EMC ha implementado el proceso de ciclo de vida de desarrollo de seguridad, en el que la seguridad constituye un elemento clave de todos los aspectos de desarrollo, adquisición, fabricación, envío y soporte, lo que genera una arquitectura de resiliencia cibernética.

2.1 Ciclo de vida de desarrollo de seguridad

A fin de ofrecer una arquitectura de resiliencia cibernética, se requiere conocimiento de la seguridad y disciplina en cada etapa del desarrollo. Este proceso se denomina modelo del ciclo de vida de desarrollo de seguridad (SDL), en el que la seguridad no es una idea de último momento, sino que forma parte integral del proceso de diseño general de servidor. Este proceso de diseño incluye una perspectiva de las necesidades de seguridad en todo el ciclo de vida útil del servidor, como se indica en los siguientes puntos y se ilustra en la figura 1:

Figura 1: Ciclo de vida de desarrollo de seguridad de Dell EMC

- Las funciones se conciben, diseñan, analizan con prototipos, implementan, ponen en producción y mantienen con la seguridad como criterio clave
- El firmware de servidor está diseñado para obstruir, oponerse a y contrarrestar la inyección de código malicioso durante todas las fases del ciclo de vida de desarrollo de productos
  - » La cobertura del modelado de amenazas y la prueba de infiltración durante el proceso de diseño
  - » Se aplican prácticas de codificación seguras en cada etapa de desarrollo de firmware
- En el caso de las tecnologías críticas, las auditorías externas complementan el proceso interno de SDL para garantizar que el firmware se adhiera a las mejores prácticas de seguridad conocidas
- Pruebas y evaluaciones continuas de nuevas vulnerabilidades potenciales mediante las herramientas de evaluación de seguridad más recientes
- Respuesta rápida a las vulnerabilidades y exposiciones habituales (CVE) críticas, que incluye las medidas de corrección recomendadas, si corresponde.

2.2 Arquitectura de resiliencia cibernética

Los servidores Dell EMC PowerEdge de 14.ª y 15.ª generación cuentan con una arquitectura de resiliencia cibernética mejorada que proporciona un diseño de servidor endurecido para proteger, detectar y recuperarse de los ataques cibernéticos. Estos son algunos de los aspectos clave de esta arquitectura:

- **Protección eficaz contra ataques**
  - » Raíz de confianza en el silicio
  - » Inicio seguro
  - » Actualizaciones firmadas de firmware
  - » Bloqueo dinámico del sistema
  - » Cifrado de disco duro y administración de claves empresariales
- **Detección confiable de ataques**
  - » Configuración y detección de desviaciones de firmware
  - » Registro de eventos persistentes
  - » Registro de auditoría y alertas
  - » Detección de intrusiones en el chasis
- **Recuperación rápida con un nivel bajo a inexistente de interrupciones para la empresa**
  - » Recuperación de BIOS automatizada
  - » Recuperación rápida de SO
  - » Reversión de firmware
  - » Borrado ágil del sistema

2.3 Amenazas actuales

Existen varios vectores de amenazas en el panorama cambiante actual. La tabla 1 resume el enfoque de Dell EMC respecto a la administración de amenazas de back-end críticas.

Tabla 1: Cómo aborda Dell EMC los vectores de amenazas habituales

Capas de la plataforma de servidores		
Capa de seguridad	**Vector de amenazas**	**Solución de Dell EMC**
Servidor físico	Manipulación de servidores/componentes	Secured Component Verification (SCV), detección de intrusiones en el chasis
Firmware y software	Corrupción de firmware, inyección de malware	Raíz de confianza basada en silicio; Intel Boot Guard; Raíz de confianza segura de AMD; Personalización del arranque seguro de la UEFI Firmware firmado y validado criptográficamente;
	Software	Generación de informes de CVE; Parches según corresponda
Funciones de confianza mediante atestación	Suplantación de identidad de servidores	TPM, TXT, cadena de confianza
Administración del servidor	Configuraciones y actualizaciones falsas, ataques no autorizados de puerto abierto	iDRAC9. Atestación remota

Capas del entorno del servidor		
Capa de seguridad	**Vector de amenazas**	**Solución de Dell EMC**
Datos	Vulneración de datos	SED (unidades de autocifrado): FIPS u Opal/TCG Administración segura de claves empresariales para unidades que solo admiten ISE (borrado seguro instantáneo) Autenticación segura del usuario
Integridad de la cadena de suministro	Componentes falsificados Amenazas de malware	Certificación ISO9001 para todos los sitios de fabricación de servidores a nivel global; Secured Component Verification; prueba de posesión Medidas de seguridad implementadas como parte del proceso de ciclo de vida de desarrollo seguro (SDL)
Seguridad de la cadena de suministro	Seguridad física en sitios de fabricación Robo y manipulación durante el transporte	Requisitos de seguridad para las instalaciones de la Asociación para la protección de activos transportados (TAPA) Asociación de Aduanas-Comercio contra el Terrorismo (C-TPAT); SCV

3. Protección

La función de “protección” es un componente clave de la infraestructura de ciberseguridad de NIST y sirve para protegerse contra los ataques de ciberseguridad. Esta función consta de varias categorías, como el control de acceso, la seguridad de datos, el mantenimiento y la tecnología de protección. La filosofía subyacente clave es que los activos de infraestructura deben proporcionar una protección sólida contra el acceso no autorizado a los recursos y los datos como parte de un entorno integral de computación e instalación segura. Esto incluye la protección contra modificaciones no autorizadas de componentes críticos, como el BIOS y el firmware. La plataforma cumple con las recomendaciones actuales en NIST SP 800-193.

La arquitectura de resiliencia cibernética en los servidores PowerEdge ofrece un alto nivel de protección de la plataforma que incluye las siguientes funcionalidades:

- Arranque seguro con verificación criptográfica
- Seguridad de acceso del usuario
- Actualizaciones firmadas de firmware
- Almacenamiento de datos cifrados
- Seguridad física
- Integridad y seguridad de la cadena de suministro

3.1 Arranque seguro con verificación criptográfica

Uno de los aspectos más críticos de la seguridad de los servidores es garantizar que se pueda verificar la seguridad del proceso de arranque. Este proceso proporciona un ancla de confianza para todas las operaciones posteriores, como el arranque de un sistema operativo o la actualización de firmware. Los servidores PowerEdge han empleado seguridad basada en el silicio durante varias generaciones en funciones como el vault de credenciales de iDRAC, una memoria cifrada segura en iDRAC para el almacenamiento de información confidencial. El proceso de arranque se verifica con una raíz de confianza en el silicio para cumplir con las recomendaciones en NIST SP 800-147B (“Pautas de protección del BIOS para servidores”) y NIST SP 800-155 (“Pautas de medición de integridad del BIOS”).

3.1.1 Raíz de confianza en el silicio

Los servidores PowerEdge de 14.ª y 15.ª generación (basados en Intel o AMD) ahora utilizan una raíz de confianza fija y basada en el silicio para atestiguar de forma criptográfica la integridad del BIOS y el firmware de iDRAC. Esta raíz de confianza se basa en claves públicas programables únicas de solo lectura, que brindan protección contra la manipulación de malware. El proceso de arranque del BIOS emplea tecnología Intel Boot Guard o de raíz de confianza de AMD, que verifica que la firma digital del hash criptográfico de la imagen de arranque coincida con la firma que almacena Dell EMC en el silicio de fábrica. Si se produce una falla durante la comprobación, el servidor se apaga, se envía una notificación de usuario en el registro de Lifecycle Controller y el usuario puede iniciar el proceso de recuperación del BIOS. Si Boot Guard se valida correctamente, el resto de los módulos del BIOS se validan mediante un procedimiento de cadena de confianza hasta que se entregue el control al sistema operativo o al hipervisor.

Además del mecanismo de comprobación de Boot Guard, iDRAC9 4.10.10.10 o superior proporciona un mecanismo de raíz de confianza para comprobar la imagen del BIOS en el momento del arranque del host. El host solo puede arrancar después de que la imagen del BIOS se haya validado correctamente. iDRAC9 también proporciona un mecanismo para validar la imagen del BIOS en el momento de la ejecución, a pedido o en intervalos programados por el usuario.

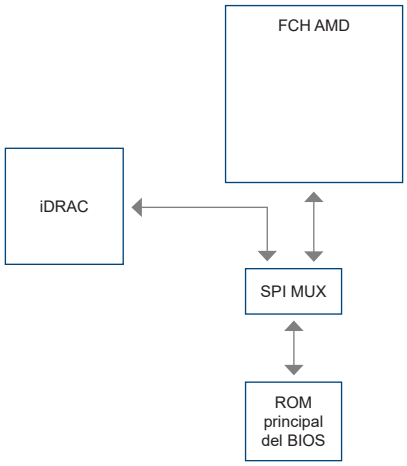
Analicemos en detalle la cadena de confianza. Cada módulo del BIOS contiene un hash del siguiente módulo en la cadena. Los módulos clave en el BIOS son IBB (Initial Boot Block), SEC (Security), PEI (Pre-EFI Initialization), MRC (Memory Reference Code), DXE (Driver Execution Environment) y BDS (Boot Device Selection). Si Intel Boot Guard autentica IBB (Initial Boot Block), IBB valida SEC+PEI antes de entregar el control. Luego, SEC+PEI valida PEI+MRC, que valida los módulos DXE+BDS. En este momento se entrega el control al arranque seguro de la UEFI, como se explica en la siguiente sección.

De manera similar, en el caso de los servidores Dell EMC PowerEdge basados en AMD EPYC, la tecnología segura de raíz de confianza de AMD garantiza que los servidores arranquen únicamente con imágenes de firmware de confianza. Además, la tecnología de ejecución segura de AMD se diseña para cifrar la memoria principal y mantenerla protegida contra intrusos maliciosos que tengan acceso al hardware. No es necesario modificar las aplicaciones para utilizar esta función y el procesador de seguridad nunca expone las claves de cifrado fuera del procesador.

iDRAC también asume la función de las tecnologías de seguridad basadas en hardware y accede a la ROM principal del BIOS a través del SPI, y el chipset Fusion Controller Hub (FCH) de AMD, y realiza el proceso de RoT.

Si se producen las siguientes condiciones, iDRAC9 recupera el BIOS.

1. Se produce un error en la comprobación de integridad del BIOS.
2. Se produce un error en la autocomprobación del BIOS.
3. Se usa el comando de RACADM: **racadm recover BIOS.Setup.1-1**



El proceso de arranque de iDRAC utiliza su propia raíz de confianza independiente basada en el silicio que verifica la imagen de firmware de iDRAC. La raíz de confianza de iDRAC también proporciona un ancla de confianza fundamental para la autenticación de las firmas de los paquetes de actualización de firmware de Dell EMC (DUP).

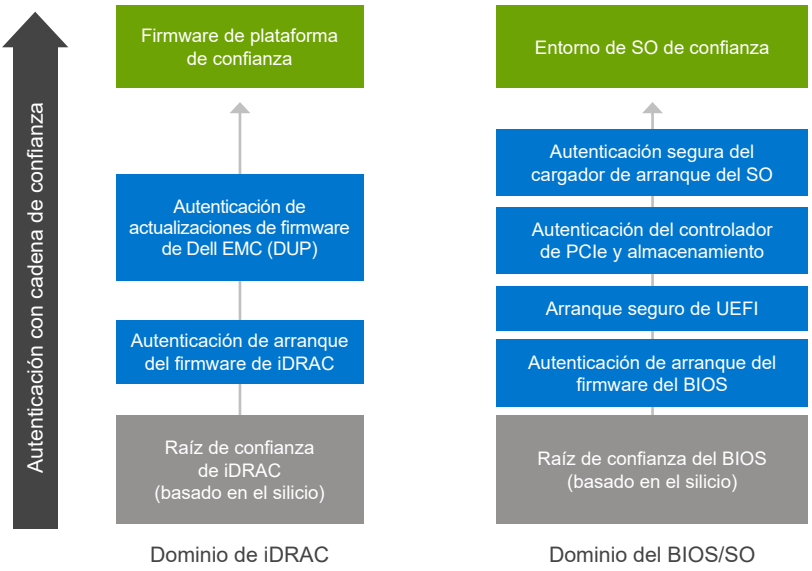


Figura 2: Dominios de raíz de confianza basada en el silicio en servidores PowerEdge

3.1.2 Escaneo activo del BIOS

Con el escaneo activo del BIOS, se verifica la integridad y autenticidad de la imagen del BIOS en la ROM principal cuando el host está encendido, pero no se encuentra en proceso de POST. Esta es una función única de AMD y está disponible solo con iDRAC9 4.10.10.10 o superior con licencia Datacenter. Para poder llevar a cabo esta operación, debe tener privilegios de administrador o privilegios de operador con la funcionalidad de depuración de “ejecución de comandos de depuración”. Es posible programar el escaneo a través de las interfaces de usuario de iDRAC, RACADM y Redfish

3.1.3 Personalización del arranque seguro de la UEFI

Los servidores PowerEdge también son compatibles con el arranque seguro de la UEFI (Interfaz de firmware extensible unificada) estándar de la industria, que comprueba las firmas criptográficas de los controladores de la UEFI y otros códigos que se cargan antes de que la ejecución del SO. El arranque seguro constituye un estándar en toda la industria para la seguridad en el entorno previo al arranque. Proveedores de sistemas informáticos, proveedores de tarjetas de expansión y proveedores de sistemas operativos colaboran en esta especificación para garantizar la interoperabilidad.

Si se habilita, el arranque seguro de la UEFI evita que se carguen controladores de dispositivos en la UEFI si no tienen firma (es decir, no son de confianza), muestra un mensaje de error y no permite que el dispositivo funcione. Debe deshabilitar el arranque seguro si desea cargar controladores de dispositivos sin firma.

Además, los servidores PowerEdge de 14.ª y 15.ª generación ofrecen a los clientes la flexibilidad única de emplear un certificado de gestor de arranque personalizado sin firma de Microsoft. Se trata principalmente de una función para administradores de entornos Linux que desean firmar sus propios gestores de arranque de SO. Los certificados personalizados se pueden cargar con la API de iDRAC preferida para autenticar el gestor de arranque del SO específico del cliente. La NSA recomienda este método de personalización de PowerEdge UEFI para reducir las vulnerabilidades de Grub2 en los servidores.

3.1.4 Compatibilidad con TPM

Los servidores PowerEdge admiten tres versiones de TPM:

- TPM 1.2 con certificación FIPS, TCG y criterios comunes (Nuvoton)
- TPM 2.0 con certificación FIPS, TCG y criterios comunes (Nuvoton)
- TPM 2.0 China (NationZ)

TPM se puede utilizar para llevar a cabo funciones criptográficas de claves públicas, funciones hash de procesamiento, generar, administrar y almacenar claves de manera segura, y realizar atestaciones. También se admite la funcionalidad de TXT (tecnología de ejecución confiable) de Intel y la función Platform Assurance de Microsoft en Windows Server 2016. TPM también se puede utilizar para habilitar la función de cifrado de disco duro de BitLocker™ en Windows Server 2012/2016.

Las soluciones de atestación y atestación remota pueden utilizar TPM para realizar mediciones en el momento del arranque del hardware, el hipervisor, el BIOS y el sistema operativo del servidor, y compararlas de forma criptográficamente segura con las mediciones de base almacenadas en el TPM. Si no coinciden, es posible que la identidad del servidor se encuentre comprometida, y los administradores de sistemas puedan deshabilitar y desconectar el servidor de forma local o remota.

Los servidores se pueden pedir con o sin TPM, pero en varios sistemas operativos y debido a otras medidas de seguridad, se está convirtiendo en un estándar. TPM se habilita con una opción del BIOS. Es una solución con módulo plug-in. La tecnología planar incluye un conector para este módulo plug-in.

3.1.5 Certificaciones de seguridad

Dell EMC ha recibido certificaciones de estándares como NIST FIPS 140-2 y Criterios comunes EAL-4. Estas certificaciones son relevantes para cumplir con los requisitos del DoD de los Estados Unidos y otros tipos de requisitos gubernamentales. Se han recibido las siguientes certificaciones para los servidores PowerEdge:

- Plataformas de servidor: Cuentan con certificación de Criterios comunes EAL4+ en RHEL y son compatibles con las certificaciones de CC del partner
- Cuentan con certificación FIPS 140-2 de nivel 1 para iDRAC y CMC
- OpenManage Enterprise: Modular cuenta con certificación EAL2+
- Con certificación FIPS 140-2 y de Criterios comunes para TPM 1.2 y 2.0

3.2 Seguridad de acceso del usuario

Garantizar la autenticación y la autorización adecuadas es un requisito clave de cualquier política moderna de control de acceso. Las interfaces principales de acceso de los servidores PowerEdge son las API, las CLI o la GUI de la iDRAC integrada. Las API y CLI preferidas para la automatización de la administración de servidores son las siguientes:

- API RESTful de la iDRAC con Redfish
- CLI RACADM
- SELinux

Cada una de estas proporciona seguridad sólida para las credenciales, como el nombre de usuario y la contraseña, mediante una conexión cifrada, como HTTPS, si se lo desea. SSH autentica a un usuario con un conjunto de claves criptográficas correspondientes (y, por lo tanto, elimina la necesidad de ingresar contraseñas menos seguras).
Se admiten protocolos más antiguos, como IPMI, pero no se recomiendan en implementaciones nuevas debido a los diversos problemas de seguridad detectados en los últimos años. Le recomendamos que, si actualmente utiliza IPMI, evalúe y realice la transición a la API RESTful de la iDRAC con Redfish.

Los **certificados TLS/SSL** se pueden cargar en la iDRAC para autenticar las sesiones del navegador web.
Existen tres opciones:

- **Certificado TLS/SSL de Dell EMC autofirmado:** la iDRAC genera automáticamente y autofirma el certificado.
  - » Ventaja: No es necesario mantener una autoridad de certificación independiente (consulte X.509/IETF PKIX std).
- **Certificado TLS/SSL firmado a la medida:** el certificado se genera y se firma automáticamente con una clave privada que ya se cargó en la iDRAC.
  - » Ventaja: CA única de confianza para todas las iDRAC. Es posible que su CA interna ya sea de confianza en sus estaciones de administración.
- **Certificado TLS/SSL firmado por una CA:** se genera una solicitud de firma de certificados (CSR) y se envía a su CA interna o a una CA externa, como VeriSign, Thawte y Go Daddy para que se aplique la firma.
  - » Ventajas: Puede emplear una autoridad de certificación comercial (consulte los estándares X.509/IETF PKIX). CA única de confianza para todas sus iDRAC. Si se utiliza una CA comercial, es muy probable que ya sea de confianza en sus estaciones de administración.

iDRAC9 permite la integración con **Active Directory** y **LDAP** dado que aprovecha los esquemas de autenticación y autorización existentes de los clientes que ya proporcionan acceso seguro a los servidores PowerEdge. También es compatible con el **control de acceso basado en funciones (RBAC)** que permite otorgar el nivel adecuado de acceso (Administrador, operador o de solo lectura) según la función de la persona que participa en las operaciones de servidor. Se recomienda encarecidamente utilizar RBAC de esta manera y no otorgar el nivel más elevado (es decir, administrador) a todos los usuarios.

iDRAC9 también proporciona maneras adicionales de protegerse contra el acceso no autorizado, como el **bloqueo y filtrado de IP**. El bloqueo de IP permite determinar de forma dinámica cuando se producen numerosos errores de inicio de sesión desde una dirección IP en particular y bloquear (o evitar) que se inicie sesión desde esa dirección en la iDRAC9 durante un período de tiempo seleccionado con anterioridad. El filtrado de IP limita el rango de direcciones IP de los clientes que acceden a la iDRAC. Se compara la dirección IP de un inicio de sesión entrante con el rango especificado y se permite el acceso a la iDRAC solo desde una estación de administración cuya dirección IP de origen se encuentre dentro del rango. Se rechaza el resto de las solicitudes de inicio de sesión.

La **autenticación de múltiples factores (MFA)** se utiliza más ampliamente en la actualidad debido a la creciente vulnerabilidad de los esquemas de autenticación de un solo factor basados en el nombre de usuario y la contraseña. iDRAC9 permite el uso de tarjetas inteligentes para el acceso remoto a la GUI y admitirá tokens de RSA. En ambos casos, los múltiples factores incluyen la presencia física del dispositivo o la tarjeta, y el PIN asociado.

3.2.1 MFA de RSA SecurID

Es posible emplear RSA SecurID como otro medio para autenticar a un usuario en un sistema. iDRAC9 comienza a admitir RSA SecurID con licencia Datacenter y firmware 4.40.00.00 como otro método de autenticación de dos factores.

3.2.2 2FA simplificada

Otro método de autenticación que se ofrece es Easy 2FA, en el que se envía un token generado aleatoriamente al correo electrónico del usuario cuando inicia sesión en la iDRAC.

3.2.3 Infraestructura SELinux

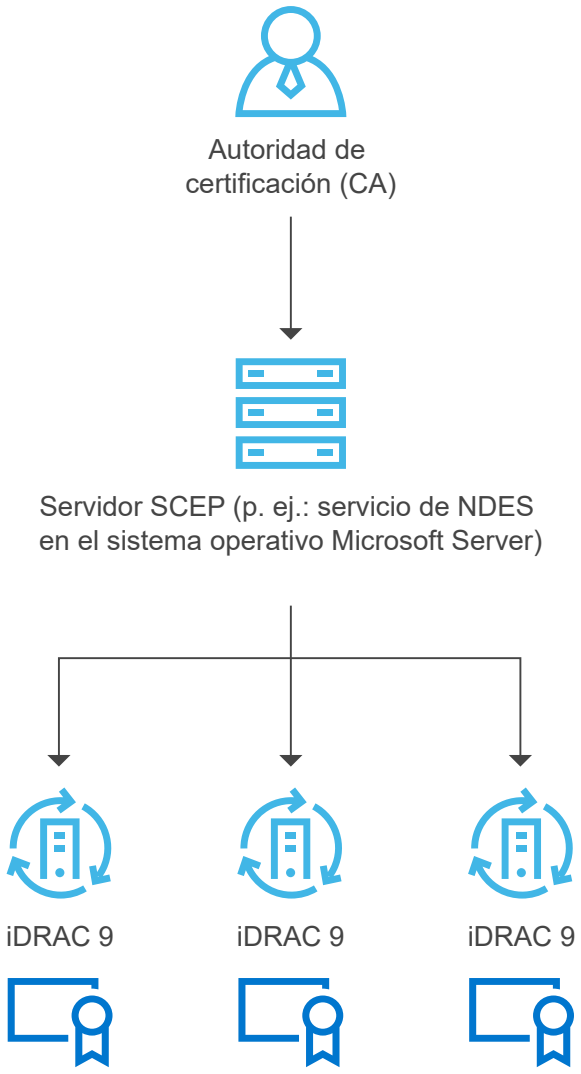
SELinux funciona en el nivel del núcleo de la iDRAC y no requiere que los usuarios configuren ni ingresen datos. SELinux registra los mensajes de seguridad cuando se detecta un ataque. Estos mensajes de registro indican cuándo y cómo un atacante intentó irrumpir en el sistema. En la actualidad, estos registros están disponibles a través de SupportAssist para los clientes que eligen esta nueva función. En versiones futuras de la iDRAC, estos registros estarán disponibles en los registros de Lifecycle Controller.

3.2.4 Privilegio mínimo

Todos los procesos internos de la iDRAC se ejecutan con los privilegios mínimos; un concepto básico de seguridad de Unix. Esta protección garantiza que el proceso de un sistema que pueda ser atacado no pueda acceder a los archivos o al hardware fuera del alcance de ese proceso. Por ejemplo, el proceso que proporciona KVM virtual no debe ser capaz de cambiar las velocidades del ventilador. La ejecución de estos dos procesos como funciones discretas permite proteger el sistema al evitar que los ataques se propaguen de un proceso a otro.

3.2.5 Inscripción y renovación automáticas de certificados

iDRAC9 v4.0 ha agregado un cliente para admitir el Protocolo de inscripción simple de certificados (SCEP) y requiere la licencia Datacenter. SCEP es un protocolo estándar que se utiliza para administrar certificados de una gran cantidad de dispositivos de red con un proceso de inscripción automático. La iDRAC se puede integrar con servidores compatibles con SCEP, como el servicio NDES de Microsoft Server, para mantener los certificados SSL/TLS de forma automática. Esta función se puede utilizar para inscribir y actualizar un certificado de servidor web cuyo vencimiento se acerca. Es posible realizarlo de manera individual en la GUI de la iDRAC, establecerlo en el perfil de configuración del servidor y desarrollar scripts con herramientas como RACADM.



3.2.6 Contraseña predeterminada generada de fábrica

De manera predeterminada, todos los servidores PowerEdge 14G se envían con una contraseña de iDRAC única y generada de fábrica a fin de proporcionar seguridad adicional. Esta contraseña se genera en la fábrica y se encuentra en la etiqueta de información extraíble ubicada en la parte frontal del chasis, adyacente a la etiqueta de activo del servidor. Los usuarios que seleccionen esta opción predeterminada deben tener en cuenta esta contraseña y usarla para iniciar sesión en la iDRAC por primera vez, en lugar de usar una contraseña predeterminada universal. Por motivos de seguridad, Dell EMC recomienda encarecidamente cambiar la contraseña predeterminada.

3.2.7 Bloqueo dinámico del sistema

iDRAC9 ofrece una nueva función que “bloquea” la configuración de hardware y firmware de un servidor o servidores, y requiere una licencia Enterprise o Datacenter. Este modo se puede habilitar con la GUI, CLI como RACADM, o como parte del perfil de configuración del servidor. Los usuarios con privilegios de administrador pueden establecer el modo de bloqueo del sistema, lo que impide que usuarios con privilegios menores realicen cambios en el servidor. El administrador de TI puede habilitar o deshabilitar esta función. Todos los cambios que se realizan cuando se deshabilita el bloqueo del sistema se agregan al registro de Lifecycle Controller. Si se habilita el modo de bloqueo, es posible evitar la desviación de la configuración en el centro de datos cuando se utilizan herramientas y agentes de Dell EMC, y protegerse contra ataques maliciosos en el firmware integrado cuando se utilizan paquetes de actualización de Dell EMC. El modo de bloqueo se puede habilitar de forma dinámica, sin necesidad de reiniciar el sistema. iDRAC9 v4.40 presenta mejoras dado que, además del bloqueo del sistema actual, que solo controla las actualizaciones con Dell Update Package (DUP), esta funcionalidad también se encuentra en determinadas NIC. (NOTA: el bloqueo mejorado para NIC solo incluye el bloqueo de firmware a fin de evitar las actualizaciones de firmware.) No se admite el bloqueo de configuración (x-UEFI). Cuando el cliente establece el modo de bloqueo en el sistema mediante la activación/configuración de un atributo en cualquiera de las interfaces compatibles, iDRAC tomará las acciones adicionales según la configuración del sistema. Estas acciones dependen de los dispositivos de otros fabricantes que se detectan como parte del proceso de detección de la iDRAC.

3.2.8 Aislamiento de dominio

Los servidores PowerEdge de 14.ª y 15.ª generación proporcionan seguridad adicional mediante el **aislamiento de dominio**, una función importante en entornos de hosting con varios grupos de usuarios. Con el fin de proteger la configuración del hardware del servidor, es posible que los proveedores de hosting deseen bloquear la capacidad de los grupos de usuarios de cambiar la configuración. El aislamiento de dominio es una opción de configuración que garantiza que las aplicaciones de administración en el sistema operativo host no tengan acceso a la iDRAC fuera de banda o las funciones del chipset de Intel, como el motor de administración (ME) o el motor de innovación (IE).

3.3 Actualizaciones firmadas de firmware

Los servidores PowerEdge han empleado firmas digitales en las actualizaciones de firmware por varias generaciones a fin de garantizar que solo se ejecute firmware auténtico en la plataforma de servidor. Firmamos de forma digital todos nuestros paquetes de firmware mediante hash SHA-256 con cifrado RSA de 2048 bits para la firma de todos los componentes clave del servidor, incluido el firmware para iDRAC, BIOS, PERC, adaptadores de I/O y LOM, fuentes de alimentación, unidades de almacenamiento, CPLD y controladoras de backplane. iDRAC analizará las actualizaciones de firmware y comparará sus firmas con la información prevista empleando la raíz de confianza basada en el silicio; los paquetes de firmware que no aprueban la validación se cancelan y se registra un mensaje de error en el registro de ciclo de vida útil (LCL) para alertar a los administradores de TI.

La autenticación de firmware mejorada está integrada en muchos dispositivos de terceros que proporcionan validación de firmas mediante sus propios mecanismos de raíz de confianza. Esto evita que se use una herramienta de actualización de otros fabricantes vulnerable para cargar el firmware malicioso en, por ejemplo, una NIC o una unidad de almacenamiento (y omitir el uso de paquetes de actualizaciones de Dell EMC firmados). Muchos de los dispositivos PCIe y de almacenamiento de otros fabricantes que se envían con servidores PowerEdge utilizan una raíz de confianza de hardware para validar sus respectivas actualizaciones de firmware.

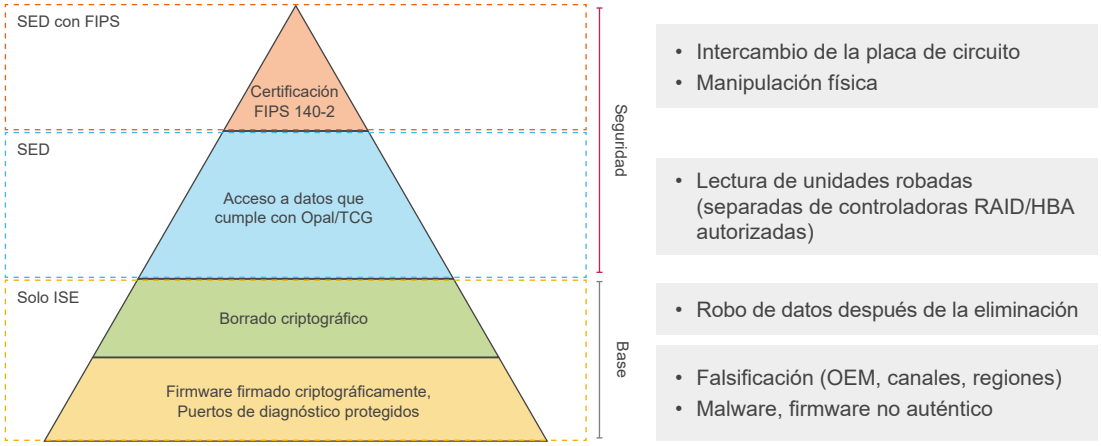
Si se sospecha que el firmware de un dispositivo ha sufrido una manipulación maliciosa, los administradores de TI pueden revertir muchas de las imágenes de firmware de la plataforma a una versión anterior de confianza almacenada en la iDRAC. Conservamos 2 versiones de firmware del dispositivo en el servidor: la versión de producción existente (“N”) y una versión de confianza anterior (“N-1”).

3.4 Almacenamiento de datos cifrados

Los servidores PowerEdge de 14.ª y 15.ª generación ofrecen varias opciones de unidades de almacenamiento para proteger los datos. Como se muestra a continuación, las opciones comienzan con unidades que admiten el borrado seguro instantáneo (ISE), una nueva tecnología que permite borrar de forma instantánea y segura los datos de usuario. Los servidores de 14.ª y 15.ª generación ofrecen unidades con ISE de manera predeterminada. El ISE se analiza en detalle más adelante en este documento como parte de la descripción de la función de borrado del sistema.

La siguiente opción de seguridad más elevado son las unidades de autocifrado (SED) que ofrecen protección de bloqueo que vincula la unidad de almacenamiento con el servidor y la tarjeta RAID utilizados. De esta manera, se protege contra el robo “exprés” de unidades y la pérdida posterior de la información confidencial de los usuarios. Cuando un ladrón intente utilizar la unidad, no conocerá la frase de contraseña de bloqueo necesaria y, por lo tanto, no podrá acceder a los datos de la unidad cifrada. Los clientes pueden protegerse contra el robo de todo el servidor con Secure Enterprise Key Manager (SEKM), que se analiza más adelante en este documento.

El nivel más elevado de protección se ofrece mediante SED con certificación NIST FIPS 140-2. Las unidades que cumplen con este estándar han recibido la acreditación de los laboratorios de prueba y cuentan con etiquetas adhesivas resistentes a la manipulación. Las unidades SED de Dell EMC cuentan con certificación FIPS 140-2 de manera predeterminada.



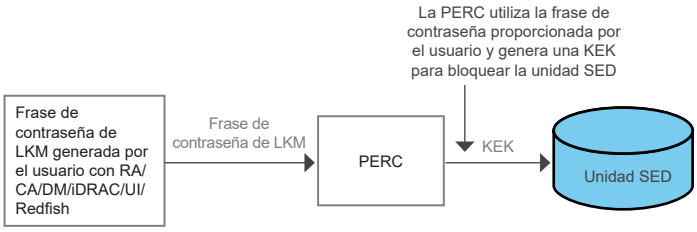
3.4.1 Vault de credenciales de iDRAC

El procesador de servicio de la iDRAC proporciona una memoria de almacenamiento segura que protege diversa información confidencial, como la información de identificación de usuario y las claves privadas de la iDRAC en certificados SSL autofirmados. Esta memoria constituye otro ejemplo de seguridad basada en el silicio dado que la memoria se cifra con una clave de raíz única fija que se programa en cada chip de la iDRAC en el momento de la fabricación. De este modo, se garantiza la protección contra ataques físicos en los que el atacante extrae el chip para intentar obtener acceso a los datos.

3.4.2 Administración de claves local (LKM)

Los servidores PowerEdge actuales proporcionan a los usuarios la capacidad de proteger las unidades SED conectadas a una controladora PERC mediante la administración de claves local.

A fin de garantizar la protección de los datos de usuario cuando se roba una unidad, la SED debe bloquearse con una clave independiente, de modo que no sea posible descifrar los datos de usuario a menos que se proporcione esa clave, que se denomina clave de cifrado de claves (KEK). Con este objetivo, un usuario establece una ID de clave/frase de contraseña en la controladora PERC a la que está conectada la SED, y la controladora PERC genera una KEK con la frase de contraseña y la utiliza para bloquear la SED. Cuando la unidad se encienda, será una SED bloqueada y cifrará/descifrará los datos del usuario solo cuando se proporcione la KEK para desbloquearla. La PERC proporciona la KEK a la unidad para desbloquearla, de modo que si se produce el robo de la unidad, esta enciende “bloqueada” y si el atacante no puede proporcionar la KEK, los datos de usuario permanecen protegidos. Es una clave local, ya que la frase de contraseña y la KEK se almacenan de manera local en la PERC. En el siguiente diagrama, se muestra la solución de LKM.

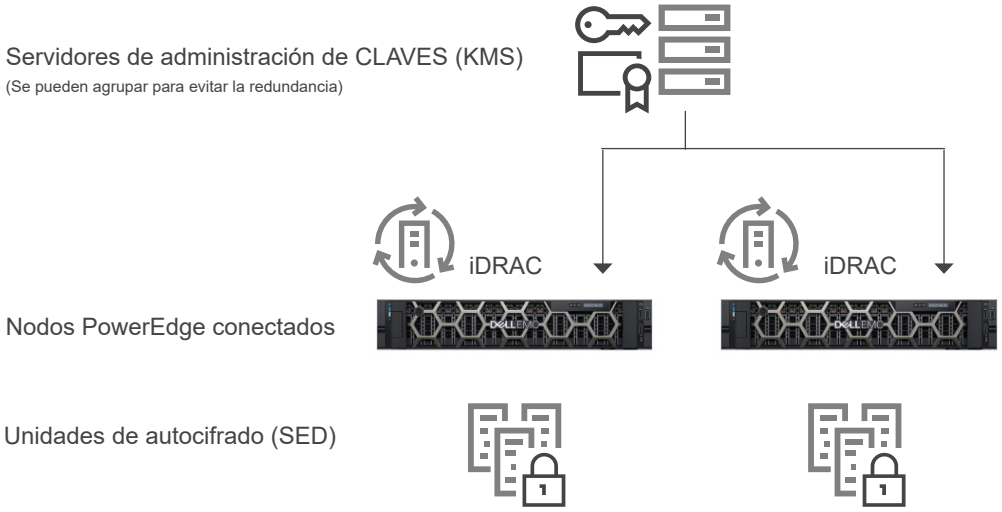


3.4.3 Administrador de claves empresariales seguras (SEKM)

OpenManage SEKM ofrece una solución de administración central de claves para administrar los datos en reposo en toda la organización. Permite que el cliente utilice un servidor de administración de claves (KMS) externo para administrar las claves que pueden emplear la iDRAC para bloquear y desbloquear dispositivos de almacenamiento en un servidor Dell EMC PowerEdge. Con un código integrado que se activa con una licencia especial, iDRAC solicita que el KMS cree una clave para cada controladora de almacenamiento, que obtiene y proporciona a la controladora de almacenamiento en el momento del arranque del host, de modo que la controladora de almacenamiento pueda desbloquear las unidades de autocifrado (SED).

Las ventajas de utilizar el SEKM en lugar de la administración de claves local (LKM) son las siguientes:

- Protección contra el “robo de un servidor”, ya que las claves no se almacenan en el servidor, se almacenan de forma externa y se recuperan mediante nodos conectados del servidor PowerEdge (a través de la iDRAC)
- Administración de claves centralizada y escalable para dispositivos cifrados con alta disponibilidad
- Compatibilidad con el protocolo KMIP estándar de la industria, lo que permite el uso de otros dispositivos compatibles con KMIP
- Protección de los datos en reposo cuando las unidades o todo el servidor se encuentran vulnerables
- El rendimiento del cifrado en la unidad se amplía a medida que aumenta la cantidad de unidades



3.5 Seguridad de hardware

La seguridad del hardware es una parte importante de cualquier solución de seguridad integral. Algunos clientes desean limitar el acceso a los puertos de entrada, como USB. Por lo general, no es necesario abrir el chasis de un servidor tras la puesta en marcha. En todos los casos, a los clientes les gustaría, como mínimo, realizar un seguimiento y registrar cualquier actividad de este tipo. El objetivo general es desalentar y limitar las intrusiones físicas.

3.5.1 Alerta de intrusión en el chasis

Los servidores PowerEdge proporcionan registro y detección de intrusiones de hardware, con una detección que funciona incluso cuando no hay alimentación de CA disponible. Los sensores en el chasis detectan cuando alguien abre o manipula el chasis, incluso durante el tránsito. Los servidores que se hayan abierto durante el tránsito generan una entrada en el registro del ciclo de vida útil de iDRAC una vez que se aplica la alimentación.

3.5.2 Administración dinámica de puertos USB

Para obtener más seguridad, puede deshabilitar completamente los puertos USB. También puede deshabilitar únicamente los puertos USB frontales. Por ejemplo, los puertos USB pueden deshabilitarse durante la producción y, luego, habilitarse temporalmente para otorgar acceso a un carrito de emergencia con el fin de realizar tareas de depuración.

3.5.3 iDRAC Direct

iDRAC Direct es un puerto USB especial que está conectado al procesador de mantenimiento de la iDRAC para tareas de depuración y administración en el servidor desde la parte frontal del servidor (pasillo frío). Le permite al usuario conectar un cable USB Micro-AB estándar a este puerto y el otro extremo (Type A) a una laptop. A continuación, un navegador web estándar puede acceder a la GUI de la iDRAC para realizar tareas exhaustivas de depuración y administración del servidor. Si se instala la licencia de iDRAC Enterprise, el usuario incluso puede acceder al escritorio del sistema operativo a través de la función de consola virtual de la iDRAC.

Dado que las credenciales habituales de la iDRAC se utilizan para iniciar sesión, iDRAC Direct funciona como un carrito de emergencia seguro con la ventaja adicional de que brinda administración de hardware y diagnósticos de mantenimiento exhaustivos. Se trata de una opción interesante para proteger el acceso físico al servidor en ubicaciones remotas (en este caso, se pueden deshabilitar los puertos USB y las salidas VGA del host).

3.5.4 iDRAC Connection View con ubicación geográfica

Connection View proporciona la capacidad de que la iDRAC brinde informes sobre los switches y los puertos externos conectados al módulo de I/O del servidor. Esta función se encuentra en determinados dispositivos de redes y requiere que se habilite el protocolo LLDP (protocolo de detección de nivel de enlace) en los switches conectados.

Estos son algunos de los beneficios de Connection View:

- Compruebe de forma remota y rápida si los módulos de I/O del servidor (LOM, NDC y tarjetas PCIe adicionales) están conectados a los switches y puertos correctos
- Evite el costoso envío remoto de técnicos a otras ubicaciones para solucionar los errores de cableado.
- Evite el seguimiento de los cables en los pasillos calientes de la sala de servidores
- Se puede realizar a través de la GUI, o los comandos RACADM pueden proporcionar información sobre todas las conexiones 14G

Además de los ahorros evidentes de tiempo y dinero, existe una ventaja adicional de Connection View: proporciona la ubicación geográfica en tiempo real de un servidor físico o máquina virtual. Con iDRAC Connection View, los administradores pueden identificar un servidor para ver exactamente a qué switch y puerto está conectado el servidor, lo que permite evitar que los servidores se conecten a redes y dispositivos que no cumplan con las pautas de seguridad o las mejores prácticas corporativas.

Connection View valida la ubicación del servidor de forma indirecta identificando las identidades de los switches a los que está conectado. La identidad del switch permite determinar la ubicación geográfica y garantizar que el servidor no sea un servidor falso en un sitio no autorizado, lo que proporciona una capa de seguridad física adicional. Además, permite afirmar que una aplicación o máquina virtual no ha “cruzado” las fronteras del país y que se ejecuta en un entorno seguro y aprobado.

3.6 Integridad y seguridad de la cadena de suministro

La integridad de la cadena de suministro se centra en dos desafíos clave:

1. Mantenimiento de la integridad del hardware: garantizar que no se manipule el producto si se agreguen componentes falsificados antes de enviar el producto a los clientes
2. Mantenimiento de la integridad del software: garantizar que no se agregue malware en el firmware o los controladores de dispositivos antes de enviar el producto a los clientes, además de evitar las vulnerabilidades de codificación

Dell EMC define la seguridad de la cadena de suministro como la práctica y la aplicación de medidas preventivas y de control de detección que protegen los activos físicos, el inventario, la información, la propiedad intelectual y las personas. Estas medidas de seguridad también permiten garantizar la cadena de suministro y su integridad reduciendo las oportunidades de incorporación maliciosa o negligente de malware o componentes falsificados en la cadena de suministro.

3.6.1 Integridad de hardware y software

Dell EMC se centra en garantizar que se implementen los procesos de control de calidad para minimizar las oportunidades de que los componentes falsificados se infiltren en nuestra cadena de suministro. Los controles que implementa Dell EMC incluyen la selección de proveedores, el aprovisionamiento, los procesos de producción y la gestión a través de auditorías y pruebas. Luego de la selección de un proveedor, el nuevo proceso de incorporación de productos permite verificar que todos los materiales utilizados durante todas las etapas de fabricación provengan de la lista de proveedores aprobados y coincidan con la lista de materiales según corresponda. Las inspecciones de materiales durante la producción ayudan a identificar los componentes que están mal marcados, se desvían de los parámetros de rendimiento habituales o contienen un identificador electrónico incorrecto.

Las piezas se reciben directamente del fabricante de diseño original (ODM) o del fabricante de componentes original (OCM) cuando sea posible. La inspección de materiales que se produce durante el nuevo proceso de incorporación de productos proporciona varias oportunidades de identificar componentes falsificados o corruptos que puedan haberse agregado a la cadena de suministro.

Además, Dell EMC conserva la certificación ISO 9001 en todos los sitios de fabricación a nivel global. El cumplimiento estricto de estos procesos y controles permite minimizar el riesgo de que los componentes falsificados se incluyan en productos Dell EMC, o que el malware se agregue en el firmware o los controladores de dispositivos. Estas medidas se implementan como parte del proceso de ciclo de vida de desarrollo de software (SDL).

3.6.2 Seguridad física

Dell EMC cuenta con varias prácticas clave duraderas que establecen y garantizan la seguridad en las instalaciones de fabricación y en las redes de logística. Por ejemplo, requerimos que ciertas fábricas en las que se fabrican productos Dell EMC cumplan con los requisitos de seguridad para instalaciones de la Asociación de protección de activos transportados (TAPA), que incluyen el uso de cámaras de circuito cerrado monitoreadas en áreas clave, controles de acceso, y entradas y salidas continuamente protegidas. También se han implementado medidas de protección para proteger los productos contra robos y manipulaciones durante el transporte como parte de un programa de logística líder en la industria. Este programa garantiza un centro de comando con personal permanente para monitorear los envíos entrantes y salientes en todo el mundo a fin de asegurar que los envíos se realicen de un destino a otro sin interrupciones.

Dell EMC también participa activamente en varios programas e iniciativas voluntarias de seguridad de la cadena de suministro. Una de estas iniciativas es la Asociación de Aduanas-Comercio contra el Terrorismo (C-TPAT), creada por el gobierno de los Estados Unidos tras el 9/11, con el fin de reducir el terrorismo a través de medidas de seguridad consolidadas en la frontera y la cadena de suministro. Como parte de esta iniciativa, la Oficina de aduanas y protección fronteriza de los Estados Unidos solicita a los miembros participantes que garanticen la integridad de sus prácticas de seguridad y comuniquen sus pautas de seguridad a sus partners dentro de la cadena de suministro. Dell EMC ha sido un participante activo desde 2002 y conserva el estado más elevado de membresía.

3.6.3 Dell Technologies Secured Component Verification (SCV) para PowerEdge

Dell Technologies Secured Component Verification (SCV) para PowerEdge es una oferta de garantía de la cadena de suministro que les permite a los clientes de Dell EMC verificar que el servidor PowerEdge que reciben los clientes coincide con las especificaciones de fábrica. Para validar los componentes de forma criptográfica con seguridad, durante el proceso de fabricación, se genera un certificado en la fábrica que contiene los ID únicos de los componentes de un servidor específico. Este certificado recibe la firma de la fábrica de Dell Technologies y se almacena en la iDRAC y, luego, el cliente lo utiliza en la aplicación SCV. El cliente utiliza la aplicación SCV para reunir el inventario actual del sistema, que incluye los ID únicos de los componentes, y lo compara con el inventario en el certificado de SCV a fin de validarlo.

El informe generado por la aplicación SCV permite verificar qué componentes coinciden y qué componentes no coinciden con el registro de instalación de la fábrica. También es posible verificar el certificado y la cadena de confianza junto con la prueba de posesión de la clave privada de SCV para la iDRAC. La implementación actual es compatible con los clientes de envío directo y no incluye VAR o escenarios de reemplazo de piezas.

4. Detección

Es fundamental tener una funcionalidad de detección que proporcione visibilidad completa de la configuración, el estado y los eventos de cambios dentro del sistema de servidor. Esta visibilidad también debe permitir visualizar los cambios maliciosos o de otro tipo en el BIOS, el firmware y las ROM opcionales durante el arranque y el proceso de tiempo de ejecución del sistema operativo. El sondeo proactivo debe combinarse con la capacidad de enviar alertas de todos y cada uno de los eventos en el sistema. Los registros deben proporcionar información completa sobre el acceso y los cambios en el servidor. Sobre todo, el servidor debe garantizar estas funcionalidades en todos los componentes.

4.1 Monitoreo completo a través de iDRAC

En lugar de depender de los agentes del sistema operativo para comunicarse con los recursos administrados en un servidor, la iDRAC emplea una ruta de banda lateral directa para cada dispositivo. Dell EMC ha empleado los protocolos estándar de la industria, como MCTP, NC-SI y NVMe-MI para comunicarse con dispositivos periféricos, como controladoras PERC RAID, NIC Ethernet, HBA Fibre Channel, HBA SAS y unidades NVMe. Esta arquitectura es el resultado de asociaciones de varios años con proveedores líderes de la industria con el fin de proporcionar administración de dispositivos sin agentes en nuestros servidores PowerEdge. Las operaciones de configuración y actualización de firmware también emplean las funciones potentes de la UEFI y la HII que respaldan Dell EMC y nuestros partners.

Gracias a esta funcionalidad, la iDRAC puede monitorear los eventos de configuración, los eventos de intrusiones (como la detección de intrusiones en el chasis mencionada previamente en este documento) y los cambios de estado del sistema. Los eventos de configuración se vinculan directamente a la identidad del usuario que inició el cambio, ya sea que se trate de un usuario de GUI, un usuario de API o un usuario de consola.

4.1.1 Registro de ciclo de vida útil

El registro de ciclo de vida útil es una recopilación de eventos que se producen en un servidor durante un período de tiempo. El registro de ciclo de vida útil proporciona una descripción de los eventos con marcas de hora, gravedad, ID de usuario u origen, acciones recomendadas y otra información técnica que podría resultar muy útil para el seguimiento o las alertas.

A continuación, se enumeran los distintos tipos de información en el registro de ciclo de vida útil (LCL):

- Cambios en la configuración de los componentes de hardware del sistema
- Cambios en la configuración de iDRAC, BIOS, NIC y RAID
- Registros de todas las operaciones remotas
- Historial de actualización de firmware basado en el dispositivo, la versión y la fecha
- Información sobre las piezas reemplazadas
- Información sobre las piezas con fallas
- ID de mensaje de eventos y mensajes
- Eventos relacionados con la alimentación del host
- Errores de POST
- Eventos de inicio de sesión de usuario
- Eventos de cambio del estado del sensor

4.1.2 Alertas

La iDRAC brinda la capacidad de configurar diferentes alertas de eventos, así como las acciones que se deberán llevar a cabo cuando se produzca un evento concreto en los registros de ciclo de vida útil. Cuando se genera un evento, este se reenvía a los destinos configurados a través de los mecanismos de tipo de alerta seleccionados. Puede habilitar o deshabilitar alertas a través de la interfaz web de la iDRAC, RACADM, o con la utilidad de ajustes de la iDRAC.

iDRAC admite diferentes tipos de alertas:

- Correo electrónico o alerta de IPMI
- SNMP trap
- Registros del sistema operativo y del sistema remoto
- Evento de Redfish

Las alertas también se pueden clasificar por gravedad: crítica, advertencia o informativa.

Se pueden aplicar los siguientes filtros a las alertas:

- Estado del sistema: por ejemplo, la temperatura, el voltaje o los errores del dispositivo
- Estado de almacenamiento: por ejemplo, errores de la controladora, errores de disco físico o virtual
- Cambios en la configuración: por ejemplo, cambio en la configuración de RAID, extracción de tarjetas PCIe
- Registros de auditoría: por ejemplo, errores en la autenticación de la contraseña
- Firmware/controlador: por ejemplo, actualizaciones a una versión anterior o más reciente

Por último, el administrador de TI puede establecer diferentes acciones para las alertas: Reiniciar, Ejecutar ciclo de apagado y encendido, Apagar o Sin acciones.

4.2 Detección de desviaciones

Mediante la implementación de configuraciones estandarizadas y la adopción de una política de “tolerancia cero” para cualquier cambio, las organizaciones pueden reducir la probabilidad de abuso. La consola de Dell EMC OpenManage Enterprise permite que el cliente defina su propia base de configuración de severidad y monitoree la desviación de sus servidores de producción a partir de esas bases. La base se puede crear según diversos criterios para adaptarse a diferentes exigencias de la producción, como la seguridad y el rendimiento. OpenManage Essentials puede informar cualquier desviación de la base y, de manera opcional, reparar la desviación con un flujo de trabajo simple para realizar los cambios en la iDRAC fuera de banda. Luego, se pueden realizar cambios en las próximas ventanas de mantenimiento mientras los servidores se reinician para que el entorno de producción vuelva a ser apto. Este proceso en etapas permite que el cliente implemente cambios en la configuración durante la producción sin tiempo de inactividad durante las horas de no mantenimiento. Aumenta la disponibilidad del servidor sin comprometer la facilidad de reparación o la seguridad.

5. Recuperación

Las soluciones de servidores deben admitir la recuperación a un estado conocido y coherente en respuesta a una variedad de eventos:

- Vulnerabilidades recientemente detectadas
- Ataques maliciosos y manipulación de datos
- Corrupción de firmware debido a fallas de memoria o procedimientos de actualización incorrectos
- Reemplazo de los componentes del servidor
- Retiro o replanificación de un servidor

A continuación, analizaremos en detalle cómo respondemos a las vulnerabilidades y los problemas de corrupción nuevos, y cómo recuperar el servidor a su estado original, de ser necesario.

5.1 Respuesta rápida a vulnerabilidades nuevas

Las vulnerabilidades y las exposiciones habituales (CVE) son vectores de ataque recientemente detectados que comprometen la integridad de los productos de software y hardware. Las respuestas oportunas a las CVE son críticas para la mayoría de las empresas, dado que permiten evaluar la exposición y tomar las medidas adecuadas con rapidez.

Las CVE se pueden generar en respuesta a vulnerabilidades nuevas identificadas en muchos elementos, que incluyen:

- Código abierto, como OpenSSL
- Navegadores web y otro software de acceso a Internet
- Hardware y firmware de los productos del proveedor
- Sistemas operativos e hipervisores

Dell EMC trabaja de manera agresiva para responder rápidamente a las nuevas CVE en nuestros servidores PowerEdge y proporcionar a los clientes información oportuna, como la siguiente:

- ¿Qué productos se ven afectados?
- ¿Qué pasos de corrección se pueden llevar a cabo?
- De ser necesario, ¿cuándo estarán disponibles las actualizaciones para abordar las CVE?

5.2 Recuperación del BIOS y el SO

Los servidores Dell EMC PowerEdge de 14.ª y 15.ª generación incluyen dos tipos de recuperación: Recuperación del BIOS y recuperación rápida del sistema operativo (SO). Estas funciones permiten una rápida recuperación desde el BIOS dañado o las imágenes del sistema operativo. En ambos casos, se oculta un área de almacenamiento especial del software de tiempo de ejecución (BIOS, SO, firmware del dispositivo, etc.). Estas áreas de almacenamiento contienen imágenes prístinas que se pueden utilizar como alternativas al software principal comprometido.

La recuperación rápida del sistema operativo permite una recuperación rápida desde una imagen de sistema operativo dañada (o una imagen del sistema operativo sospechosa de manipulación maliciosa). Los medios de recuperación pueden ser tarjetas SD internas, puertos SATA, unidades M.2 o USB internos. El dispositivo seleccionado puede estar expuesto a la lista de arranque y el sistema operativo durante la instalación de la imagen de recuperación. A continuación, se puede deshabilitar y ocultar desde la lista de arranque y el sistema operativo. En el estado oculto, el BIOS deshabilita el dispositivo de modo que el sistema operativo no pueda acceder a él. En el caso de una imagen de sistema operativo dañada, la ubicación de recuperación se puede habilitar durante el arranque. Se puede acceder a estos ajustes a través del BIOS o de la interfaz de la iDRAC.

En casos extremos, si el BIOS está dañado (ya sea debido a un ataque malicioso, una pérdida de energía durante el proceso de actualización o cualquier otro evento imprevisto), es importante proporcionar una manera de recuperar el BIOS a su estado original. Una imagen de respaldo del BIOS se almacena en la iDRAC, de modo que se pueda utilizar para recuperar la imagen del BIOS, de ser necesario. La iDRAC coordina todo el proceso de recuperación.

- El BIOS inicia su propia recuperación automática.
- Los usuarios pueden iniciar la recuperación del BIOS a petición con el comando de la CLI RACADM.

5.3 Reversión de firmware

Se recomienda mantener actualizado el firmware para asegurarse de contar con las funciones y las actualizaciones de seguridad más recientes. Sin embargo, es posible que deba revertir una actualización o instalar una versión anterior si se producen problemas después de una actualización. Si desea volver a la versión anterior, también se verifica con su firma.

Actualmente, la reversión de firmware de la versión de producción existente “N” a una versión anterior “N-1” es compatible con las siguientes imágenes de firmware:

- BIOS
- iDRAC con Lifecycle Controller
- Tarjeta de interfaz de red (NIC)
- Controladora RAID PowerEdge (PERC)
- Fuente de alimentación (PSU)
- Backplane

Puede revertir el firmware a la versión instalada anteriormente (“N-1”) con cualquiera de los siguientes métodos:

- Interfaz Web de la iDRAC
- Interfaz Web de la CMC
- CLI RACADM: iDRAC y CMC
- GUI de Lifecycle Controller
- Lifecycle Controller: servicios remotos

Puede revertir el firmware de la iDRAC o de cualquier dispositivo que admita Lifecycle Controller, incluso si la actualización se realizó anteriormente con otra interfaz. Por ejemplo, si el firmware se actualizó con la GUI de Lifecycle Controller, puede revertir el firmware con la interfaz web de la iDRAC. Puede realizar la reversión de firmware en varios dispositivos con un reinicio del sistema.

En los servidores PowerEdge de 14.ª y 15.ª generación que cuentan con un único firmware de iDRAC y Lifecycle Controller, si se revierte el firmware de la iDRAC, también se revierte el firmware de Lifecycle Controller.

5.4 Restauración de la configuración del servidor tras el mantenimiento de hardware

La corrección de los eventos de mantenimiento constituye una parte fundamental de cualquier operación de TI. La capacidad de cumplir con los objetivos de tiempo de recuperación y los objetivos de punto de recuperación tiene implicaciones directas en la seguridad de la solución. La restauración de la configuración del servidor y el firmware garantiza el cumplimiento automático de las políticas de seguridad para el funcionamiento del servidor.

Los servidores PowerEdge proporcionan una funcionalidad que restaura con rapidez la configuración del servidor en las siguientes situaciones:

- Reemplazo de piezas individuales
- Reemplazo de la placa base (respaldo y restauración del perfil de todo el servidor)
- Reemplazo de la placa base (Easy Restore)

5.4.1 Reemplazo de piezas

La iDRAC guarda automáticamente la imagen del firmware y los ajustes de configuración de tarjetas NIC, controladoras RAID y fuentes de alimentación (PSU). En caso de se produzca un reemplazo de campo de estas piezas, la iDRAC detecta automáticamente la nueva tarjeta y restaura el firmware y la configuración de la tarjeta reemplazada. Esta funcionalidad ahorra tiempo crítico, y garantiza una configuración coherente y que se cumpla la política de seguridad. La actualización se produce automáticamente durante el reinicio del sistema después de reemplazar la pieza compatible.

5.4.2 Easy Restore (para el reemplazo de placas base)

Los reemplazos de la placa base pueden consumir mucho tiempo y afectar la productividad. iDRAC ofrece la capacidad de respaldar y restaurar la configuración y el firmware del servidor PowerEdge a fin de minimizar el esfuerzo necesario para reemplazar una placa base fallida.

Existen dos formas en las que el servidor PowerEdge puede llevar a cabo un respaldo y una restauración:

1. Los servidores PowerEdge respaldan automáticamente los ajustes de configuración del sistema (BIOS, iDRAC, NIC), la etiqueta de servicio, la aplicación de diagnósticos de la UEFI y otros datos con licencia en la memoria flash.

   Después de reemplazar la placa base de su servidor, Easy Restore le indica que restaure de forma automática los datos.
2. Para obtener un respaldo más completo, el usuario puede respaldar la configuración del sistema, como las imágenes de firmware instaladas en varios componentes, como BIOS, RAID, NIC, iDRAC, Lifecycle Controller y tarjetas de red secundarias (NDC), y los ajustes de configuración de esos componentes. La operación de respaldo también incluye los datos de configuración del disco duro, la placa base y las piezas reemplazadas. Durante el respaldo, se crea un solo archivo que puede guardarse en una tarjeta SD vFlash o un recurso compartido de red (CIFS, NFS, HTTP o HTTPS).

   El usuario puede restaurar este respaldo de perfil en cualquier momento. Dell EMC recomienda que realice un respaldo de cada perfil del sistema que considere que podría desear restaurar en algún momento.

5.5 Borrado del sistema

Al final del ciclo de vida útil de un sistema, este debe retirarse o reutilizarse. El objetivo del borrado del sistema es borrar información confidencial y los ajustes de los dispositivos de almacenamiento del servidor y los almacenes no volátiles del servidor, como la memoria caché y los registros, de modo que no se posible que la información confidencial se filtre involuntariamente. Es una utilidad de Lifecycle Controller que está diseñada para borrar los registros, los datos de configuración, los datos de almacenamiento, la memoria caché y las aplicaciones integradas.

Los dispositivos, los ajustes de configuración y las aplicaciones siguientes se pueden borrar mediante la función de borrado del sistema:

- iDRAC se restablece a la opción predeterminada
- Datos de Lifecycle Controller (LC)
- BIOS
- Paquetes de controladores de SO y diagnósticos integrados
- iSM
- Informes de recopilación de SupportAssist

Además, también se pueden borrar los siguientes componentes:

- Caché de hardware (eliminar NVCache de la PERC)
- Tarjeta SD vFlash (inicializar la tarjeta) (Nota: vFlash no disponible en servidores 15G o posteriores).

Los datos de los siguientes componentes se desechan de forma criptográfica mediante el proceso de borrado del sistema, como se describe a continuación:

- SED (unidades de autocifrado)
- Unidades de solo admiten ISE (unidades con borrado seguro instantáneo)
- Dispositivos NVM (Apache Pass, NVDIMM)

Además, los discos duros SATA que no admiten ISE se pueden borrar mediante la sobrescritura de los datos.

Tenga en cuenta que el borrado seguro instantáneo (ISE) destruye la clave de cifrado interno que se emplea en unidades de 14.ª y la 15.ª generación, por lo que los datos de usuario no se pueden recuperar. ISE es un método reconocido de borrado de datos en las unidades de almacenamiento a las que se hace referencia en la publicación especial de NIST 800-88 “Guidelines for Media Sanitization”.

Estas son las ventajas de la nueva función de ISE con el borrado del sistema:

- **Velocidad:** mucho más rápido que las técnicas de sobrescritura de datos como DoD 5220.22-M (segundos en lugar de horas)
- **Eficacia:** ISE representa todos los datos de la unidad, incluidos los bloques reservados, completamente ilegibles
- **Mejor TCO:** los dispositivos de almacenamiento se pueden volver a utilizar en lugar de que se aplasten o destruyan físicamente de otra manera.

El borrado del sistema se puede realizar mediante los siguientes métodos:

- Lifecycle Controller GUI (F10)
- CLI RACADM
- Redfish

5.6 Selección de cifrado de iDRAC9

Se puede implementar la selección del conjunto de cifrado a fin de limitar los cifrados que el navegador web puede emplear para comunicarse con la iDRAC. También es posible determinar la seguridad de la conexión. Estos ajustes se pueden configurar con la interfaz web de la iDRAC, RACADM y Redfish. Esta funcionalidad está disponible en varias versiones de la iDRAC: iDRAC7, iDRAC8 (2.60.60.60 y superior) y la versión actual iDRAC9 (3.30.30.30 y superior).

5.7 Compatibilidad con CNSA

Los cifrados compatibles disponibles en la iDRAC9 con TLS de 1,2 bits y cifrado de 256 bits se muestran en la imagen de captura de pantalla a continuación. Los cifrados disponibles incluyen cifrados del conjunto aprobado por la CNSA.

5.8 Ciclo de apagado y encendido completo

En un ciclo de apagado y encendido completo, el servidor, así como todos sus componentes, se reinician. Se retira la alimentación principal y auxiliar del servidor y todos los componentes. También se borran todos los datos en la memoria volátil.

Para llevar a cabo un ciclo físico de apagado y encendido completo, se debe desconectar el cable de alimentación de CA, esperar 30 segundos y luego volver a colocar el cable. Esto representa un desafío cuando se trabaja con un sistema remoto. Una nueva función en los servidores 14G y 15G le permite realizar un ciclo de apagado y encendido completo eficaz desde iSM, GUI de IDRAC, BIOS o un script. El ciclo de apagado y encendido completo se efectúa durante el siguiente ciclo de apagado y encendido.

La función de ciclo de apagado y encendido completo elimina la necesidad de que haya una persona físicamente presente en el centro de datos y, por lo tanto, reduce el tiempo necesario para solucionar problemas. Permite eliminar, por ejemplo, cualquier malware que permanezca en la memoria.

6. Resumen

La seguridad del centro de datos es primordial para el éxito empresarial y la seguridad de la infraestructura de servidores subyacente es fundamental. Los ataques cibernéticos tienen el potencial de generar tiempo de inactividad en el sistema y la empresa, pérdida de ingresos y clientes, daños legales y el deterioro de la reputación corporativa durante un período prolongado. Para garantizar la protección, detección y recuperación de los ataques cibernéticos orientados al hardware, la seguridad debe incorporarse en el diseño del hardware del servidor, no después del hecho.

Dell EMC ha sido un líder en el empleo de seguridad basada en el silicio con el fin de proteger el firmware y la información confidencial de los usuarios en servidores PowerEdge durante las últimas dos generaciones. Las líneas de productos PowerEdge de 14.ª y 15.ª generación cuentan con una arquitectura de resiliencia cibernética mejorada, que incorpora la raíz de confianza basada en el silicio para endurecer aún más la seguridad del servidor e incluye las siguientes funciones:

- El **Arranque de confianza con verificación criptográfica** afianza la seguridad integral del servidor y la seguridad general del centro de datos. Incluye funciones como la raíz de confianza basada en el silicio, el firmware con firma digital y la recuperación automática del BIOS.
- El **Arranque seguro** comprueba las firmas criptográficas de los controladores de la UEFI y otros códigos cargados antes de que se ejecute el sistema operativo.
- El **Vault de credenciales de la iDRAC** es un espacio de almacenamiento seguro para credenciales, certificados y otra información confidencial que se cifran con una llave basada en el silicio única para cada servidor
- El **Bloqueo dinámico del sistema** es una funcionalidad exclusiva de PowerEdge, que permite proteger la configuración del sistema y el firmware de cambios maliciosos o no intencionados, y alerta a los usuarios sobre cualquier intento de modificación del sistema.
- La **Administración de claves empresariales** ofrece una solución de administración central de claves que permite administrar los datos en reposo en toda la organización.
- El **Borrado del sistema** permite a los usuarios retirar o replanificar con facilidad sus servidores PowerEdge de 14.ª y 15.ª generación mediante el borrado seguro y rápido de los datos de las unidades de almacenamiento y de otras memorias no volátiles integradas
- La **Seguridad de la cadena de suministro** proporciona garantía de la cadena de suministro dado que garantizar que no haya manipulación de los productos ni se falsifiquen los componentes antes de enviar los productos a los clientes.

En conclusión, los servidores PowerEdge de 14.ª y 15.ª generación, con seguridad líder en la industria, forman una base confiable para la transformación de la TI con la que los clientes podrán ejecutar de forma segura sus cargas de trabajo y operaciones de TI.

A. Apéndice: Lectura adicional

Documentación técnica y material de marketing sobre seguridad

- (Directo del equipo de desarrollo) SYSTEM ERASE ON POWEREDGE SERVERS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444242
- SECURING 14TH GENERATION DELL EMC POWEREDGE SERVERS WITH SYSTEM ERASE
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444269
- (Directo del equipo de desarrollo) SECURITY IN SERVER DESIGN
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444243
- (Directo del equipo de desarrollo) CYBER-RESILIENCY STARTS AT THE CHIPSET AND BIOS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444061
- CONTRASEÑA PREDETERMINADA GENERADA DE FÁBRICA DE IDRAC9
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444368
- DELL EMC IDRAC RESPONSE TO CVE-2017-1000251 “BLUEBORNE”
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444605
- (Video) SECURE BOOT CONFIGURATION AND CERTIFICATE MANAGEMENT USING RACADM
  https://youtu.be/mrIIN4X380c
- SECURE BOOT MANAGEMENT ON DELL EMC POWEREDGE SERVERS
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444259/download
- Signing UEFI images for Secure Boot feature in the 14th and 15th generation and later Dell EMC PowerEdge servers
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444255
- RAPID OPERATING SYSTEM RECOVERY
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444249
- Managing iDRAC9 Event Alerts on 14th generation (14G) Dell EMC PowerEdge Servers
  http://en.community.dell.com/techcenter/extras/m/white_papers/20444266
- Personalización del arranque seguro de la UEFI
  https://media.defense.gov/2020/Sep/15/2002497594/-1/-1/0/CTR-UEFI-Secure-Boot-Customization-UOO168873-20.PDF

Documentación técnica de PowerEdge

- Visión general de la iDRAC
  http://www.DellTechCenter.com/iDRAC
- Visión general de la consola de OpenManage
  http://www.DellTechCenter.com/OME
- Visión general de OpenManage Mobile
  http://www.DellTechCenter.com/OMM
- Reemplazo de piezas con Lifecycle Controller
  http://en.community.dell.com/techcenter/extras/m/white_papers/20276457
- Reemplazo de la placa base
  http://en.community.dell.com/techcenter/extras/m/white_papers/20168832
- Inscripción automática de certificados de iDRAC
  https://www.dellemc.com/resources/es-mx/asset/white-papers/products/software/direct-from-development-idrac-automatic-certificate-enrollment.pdf
- Funciones de seguridad de servidor mejoradas en iDRAC9 con SELinux
  https://downloads.dell.com/manuals/all-products/esuprt_solutions_int/esuprt_solutions_int_solutions_resources/dell-management-solution-resources_white-papers20_en-us.pdf
- Selección de cifrado de iDRAC9: seguridad mejorada para servidores Dell EMC PowerEdge
  https://downloads.dell.com/manuals/all-products/esuprt_software_int/esuprt_software_ent_systems_mgmt/idrac9-lifecycle-controller-v33-series_white-papers11_en-us.pdf

Obtenga más información acerca de los servidores PowerEdge

Obtenga más información acerca de los servidores PowerEdge

Obtenga más información acerca de nuestras soluciones de administración de sistemas

Busque contenido en nuestra biblioteca de recursos

Siga a los servidores PowerEdge en Twitter

Comuníquese con un experto de Dell Technologies para obtener asistencia de ventas o soporte

DELL Technologies