# Seguridad de datos simple, integral y flexible para toda la organización.

## Dell Encryption

Hoy en día, las organizaciones necesitan proteger los endpoints y los datos que contienen, a la vez que brindan apoyo a la movilidad del equipo de trabajo. Las soluciones de cifrado tradicionales son limitadas y restrictivas en términos de implementación, alcance de la cobertura del endpoint y rendimiento del usuario. Si bien las soluciones de cifrado tradicionales intentan abordar estas necesidades, muchas de ellas son difíciles de implementar y administrar, carecen de cobertura para todos los endpoints y disminuyen el rendimiento para los usuarios.

Dell Encryption Enterprise ofrece opciones con su tecnología de cifrado flexible, como el enfoque basado en políticas centradas en datos, así como un enfoque Full Disk Encryption para proteger los datos. La solución está diseñada para lo siguiente:

– Facilidad de implementación

– Transparencia del usuario final

– Cumplimiento sin inconvenientes

– Facilidad de administración con una sola consola

Dell Encryption es un conjunto flexible de soluciones de seguridad mejoradas que incluyen cifrado basado en archivos, Full Disk Encryption, administración centralizada mejorada de cifrado nativo (Microsoft BitLocker y Mac FireVault) y protección de datos en medios externos, unidades de cifrado automático y dispositivos móviles.

## Dell Encryption Enterprise

Dell Encryption Enterprise permite que TI aplique fácilmente las políticas de cifrado, ya sea que los datos residan en la unidad del sistema o en los medios externos, y no requiere la intervención del usuario final.

Encryption Enterprise, una solución perfecta para entornos de proveedores mixtos, permite lo siguiente:

- Implementación y aprovisionamiento automáticos cuando se instala en fábrica en dispositivos comerciales de Dell
- Implementación en menos de 30 minutos en entornos VMware con instalación basada en asistente y administración de claves y base de datos totalmente integradas
- No necesita desfragmentación antes del cifrado
- Cifrado de medios externos y de discos del sistema en una sola solución
- Puede elegir entre el software Full Disk Encryption o el cifrado basado en archivos
- Fácil administración y auditoría del cumplimiento con plantillas de políticas de cumplimiento de un solo paso, administración remota y rápida recuperación del sistema
- Integración con los procesos actuales de autenticación, aplicación de parches y más
- Ventas y soporte para las soluciones de hardware y seguridad desde una sola fuente
- Cifrado de todos los datos, a excepción de los archivos esenciales para el arranque del sistema operativo o el cifrado del disco completo, según sus preferencias
- Sistema mejorado de control de puertos para prevenir el filtrado de datos
- Capacidad para cifrar en función de los perfiles, datos y grupos de usuarios finales de la organización
- Administración centralizada de todas las políticas de cifrado, incluidos las unidades de autocifrado, el cifrado de disco completo y el cifrado de Microsoft BitLocker
- Autenticación mejorada para los dispositivos OPAL estándares, incluido el inicio de sesión único en el SO a través de la Autenticación con arranque previo (PBA) mediante tarjetas y contraseñas inteligentes

## La ventaja de Dell Encryption

**Protección integral, mayor nivel de seguridad**

- Protege los datos en cualquier dispositivo y medio externo
- Los registros y las claves de arranque maestro nunca se exponen

**Productividad y simplicidad para TI y los usuarios finales**

- Elija Security Management Server Virtual para lograr una implementación simplificada o Security Management Server para llegar a miles de usuarios
- Integración sin inconvenientes con procesos de autenticación y administración de sistemas existentes
- El cifrado es transparente para los usuarios finales y los ayuda a mantener la productividad

**Cifrado flexible**

- Basado en el perfil del usuario final, en la confidencialidad de los datos, en el rendimiento o en las necesidades de cumplimiento
- Cifra los datos de medios externos o desactiva todos los puertos, y permite que los dispositivos no relacionados con el almacenamiento funcionen
- Administra e inspecciona las unidades con Microsoft BitLocker y de cifrado automático para ayudarlo a alcanzar el cumplimiento

## Dell Security Management Server Virtual

Al utilizar un servidor de administración virtual con diseño específico y una aplicación de consola para VMware que permite una implementación simplificada, Dell ha elevado el nivel de facilidad y rapidez en nuestra solución de cifrado de endpoints. Dell Encryption puede establecerse y ponerse en marcha en la mayoría de los entornos de medianas empresas con hasta 3500 endpoints.

Dell Security Management Server Virtual hace de Dell Encryption la opción ideal para SME que ya tienen las soluciones VMware y buscan una plataforma de administración simple y de rápida implementación para las políticas de cifrado y autenticación. Contiene las mismas características y los mismos beneficios del servidor estándar, incluido el soporte completo para el amplio rango de cobertura de cifrado disponible para laptops, computadoras de escritorio y medios externos.

## Administración de las unidades de cifrado automático con Dell Encryption Enterprise

Las organizaciones que utilizan unidades con autocifrado (SED) también necesitan una administración cuidadosa si deben ser efectivas al reducir el riesgo de pérdida de datos y al cumplir con los objetivos de la auditoría y el cumplimiento.

Dell Encryption Enterprise ofrece una administración centralizada y segura para las unidades con autocifrado en toda la organización, tanto local como remota. Todas las políticas, la autenticación, las tareas de administración, el almacenamiento y la recuperación de claves de cifrado están disponibles en una sola consola, lo que reduce el trabajo de proteger los datos críticos y reduce el riesgo de que los sistemas queden desprotegidos en caso de pérdidas o acceso no autorizado. Más aún, la administración de dispositivos con el estándar OPAL está completamente integrada en la misma plataforma de protección de datos que el cifrado basado en archivos, Microsoft BitLocker y el cifrado de medios extraíbles.

**Las capacidades de administración remota incluyen la capacidad de hacer lo siguiente:**

- Deshabilitar los inicios de sesión y eliminar la memoria caché por usuario para proteger los datos y asegurar que solo un administrador autorizado pueda volver a habilitar el acceso a los datos protegidos
- Deshabilitar el dispositivo para prevenir que cualquier usuario inicie sesión en el sistema hasta que se envíe un comando de desbloqueo
- Habilitar el dispositivo de forma que los usuarios puedan iniciar sesión para utilizar el SED
- Realizar un desbloqueo remoto y automático en el disco para permitir que los administradores realicen tareas básicas, tales como aplicar parches sin tener que dejar el dispositivo desbloqueado toda la noche
- Proporcionar autenticación completa previa al arranque, que incluye autenticación con Active Directory
- Establecer políticas para las respuestas automáticas a los ataques (incluidos los ataques de fuerza bruta)

## Administración del cifrado de disco completo con Dell Encryption Enterprise

Las organizaciones que utilizan Full Disk Encryption pueden proteger los datos confidenciales que residen en el equipo y en otros endpoints las 24 horas del día, los 7 días de la semana. La última funcionalidad de Dell Enterprise Encryption, Full Disk Encryption, ayuda a cumplir de manera eficaz con las exigentes necesidades de protección de datos. Full Disk Encryption ofrece lo siguiente:

- Complementa nuestra oferta de cifrado actual y hace de nuestra solución de cifrado una de las mejores de la industria
- Ofrece autenticación previa al arranque de clase empresarial para su implementación en empresas
- Usa TPM para proteger las claves que impiden que cualquier atacante elimine la unidad de disco duro de la plataforma y realice un ataque sin conexión de claves ofuscadas almacenadas en la unidad
- Cifra todos los discos duros locales dentro de una implementación simplificada y un marco de trabajo de administración remoto

- El cifrado de disco completo también ofrece una manera sencilla de administrar la tecnología de cifrado, que se puede habilitar y mantener con un mínimo de personal
- Una experiencia transparente y de alto rendimiento para los usuarios
- Con la autenticación empresarial previa al arranque, el cifrado de disco completo proporciona lo siguiente:
  - o Single Sign On en el SO y la red
  - o Soporte de un único cliente para varios usuarios
  - o Recuperación simple y guiada por el administrador de claves de cifrado y acceso a los datos

Nota: En la actualidad, el cifrado de disco completo de Dell es compatible con las PC comerciales de Dell (X7 y posteriores) en el modo de arranque UEFI con el factor de autenticación de contraseña. Las PC que no son Dell y el modo de arranque heredado con autenticación de tarjeta inteligente serán compatibles con versiones posteriores.

## Características y beneficios de Dell Encryption

### Implementación y administración simplificadas

Dado que usted necesita una solución que sea fácil de implementar y administrar sin que interfiera en los procesos de TI existentes, Dell Encryption lo ayuda a realizar lo siguiente:

- Implementar y aprovisionar automáticamente los usuarios cuando Dell Encryption se instala de fábrica en determinados dispositivos comerciales de Dell
- Implementar la solución en menos de treinta minutos[1] en entornos VMware con una base de datos totalmente integrada y administración de claves frente a soluciones competitivas conocidas que requieren de varios servidores, una base de datos independiente y varias licencias
- Implementar el procesamiento de desfragmentación de disco completo, con implementación completa que lleva mucho tiempo
- Eliminar la preocupación por los procesos de TI preexistentes, con una solución que funciona de inmediato y que no requiere nuevas configuraciones
- Integrar la solución con los procesos de autenticación existentes, que incluyen contraseña de Windows, RSA, huella digital y tarjeta inteligente
- Corregir, proteger y regular: rápidamente detectar dispositivos, aplicar cifrado y auditarlos
- Cifrar los archivos o datos confidenciales de los usuarios cuando el equipo de TI necesite acceder al terminal
- Administrar los dispositivos con la norma OPAL se encuentra completamente integrado en una consola única para todos los terminales
- Proteger los terminales en entornos heterogéneos, independientemente del usuario, el dispositivo o la ubicación

## Más fácil de cumplir

Dell Encryption incluye plantillas de políticas predefinidas para ayudar a los clientes interesados en abordar las normativas de cumplimiento como
las siguientes:

- Normativas del sector: PCI DSS, Sarbanes Oxley (SOX)
- Normativas federales y estatales de los EE. UU.: HIPAA y la Ley de HITECH, Ley Gramm Leach Bliley: California — SB1386, Massachusetts—201 CMR 17, Nevada—NRS 603A (que requiere PCI DSS) y más de 45 otras leyes estatales y jurisdiccionales de los EE. UU.
- Normativas internacionales: Safe Harbor entre EE. UU. y Europa, Directiva de Protección de Datos de la UE 95/46/EC, Ley de Protección de Datos del Reino Unido, BDSG (Bundes-daten-schutz-gesetz) de Alemania y legislaciones similares para todos los países miembros de la UE, Canadá: PIPEDA

## Especificaciones técnicas

Dell Encryption Enterprise está disponible para entornos de proveedores combinados que cumplan con las especificaciones que se indican a continuación.

**Sistemas operativos de cliente compatibles:**

- Microsoft Windows 7 Ultimate, Enterprise y Professional Editions
- Microsoft Windows 8 y 8.1 Enterprise y Professional Editions
- Microsoft Windows 10 Education, Enterprise y Pro Editions
- macOS X El Capitan, Sierra

**Dell Security Management Server se ha validado en los siguientes entornos operativos:**

- Windows Server 2008 R2 SP0-SP1 de 64 bits Standard y Enterprise Editions
- Windows Server 2012 R2 Standard y Datacenter Edition
- Windows Server 2016 Standard y Datacenter Edition
- VMware ESXi 5.5, 6.0 y 6.5
- VMware Workstation 11 y 12.5

**Se admite el acceso a la consola de administración remota y a Compliance Reporter a través de los siguientes navegadores de Internet:**

- Internet Explorer 11.x o posterior
- Mozilla Firefox 41.x o posterior
- Google Chrome 46.x o posterior

### Productividad del usuario final

Entendemos la importancia de funcionar a máxima capacidad, sin interrupción ni retraso. Por eso implementamos nuestra solución de forma transparente, ayudando a eliminar las interrupciones durante el cifrado de dispositivos. De hecho, como es tan discreta, es posible que las personas no noten que sus dispositivos fueron cifrados.

## Servicios de implementación

Permítanos implementar su solución. Le ofrecemos una gama integral de servicios para implementar soluciones de seguridad en el entorno. Primero, nuestro equipo de expertos en ciberseguridad evaluará su entorno para identificar áreas de mejora de la seguridad de los datos en los endpoints, servidores, datos en la nube y dispositivos móviles. Luego, implementamos, optimizamos y administramos la solución.

## Amplia protección con cifrado

Confíe en Dell Encryption para que lo ayude a proteger los datos valiosos en cualquier dispositivo o medio externo y en el almacenamiento de nube pública, y mantener la productividad. Es solo otra manera de darle el poder para hacer más. Para obtener más información sobre Dell Data Security, visite Dell.com/DataSecurity.

**Obtenga más información en Dell.com/DataSecurity**