Guía de seguridad de Oracle® Server X6-2L

Referencia: E73724-01
Abril de 2016

Referencia: E73724-01

Accesibilidad a la documentación

Para obtener información acerca del compromiso de Oracle con la accesibilidad, visite el sitio web del Programa de Accesibilidad de Oracle en `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc`.

Acceso a Oracle Support

Los clientes de Oracle que hayan adquirido servicios de soporte disponen de acceso a soporte electrónico a través de My Oracle Support. Para obtener información, visite `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info` o `http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs` si tiene problemas de audición.

Contenido

Seguridad básica

En este documento, se proporcionan directrices de seguridad generales para ayudarlo a proteger el servidor Oracle, las interfaces de red del servidor y los conmutadores de red conectados.

Póngase en contacto con el responsable de la seguridad de TI para conocer los requisitos de seguridad adicionales relacionados con el sistema y el entorno específico.

Existen principios de seguridad básicos que debe cumplir al utilizar todo el hardware y software. En esta sección, se describen los cuatro principios de seguridad básicos:

Acceso

El acceso se refiere al acceso físico al hardware, o al acceso físico o virtual al software.

- Utilice los controles físicos y de software para proteger el hardware y los datos contra posibles intrusiones.
- Cambie todas las contraseñas predeterminadas cuando instale un sistema nuevo. La mayoría de los tipos de equipos utilizan contraseñas predeterminadas, como `changeme`, que son ampliamente conocidas y, por lo tanto, es posible que permitan el acceso no autorizado al hardware o software.
- Consulte la documentación incluida con el software para activar las funciones de seguridad disponibles para el software.
- Instale servidores y equipos relacionados en una habitación cerrada con llave y de acceso restringido.
- Si el equipo se instala en un bastidor con una puerta con llave, mantenga la puerta cerrada, a menos que sea necesario reparar algún componente del bastidor.
- Restrinja el acceso a consolas y puertos USB. Los dispositivos, como los controladores del sistema, las unidades de distribución de energía (PDU) y los conmutadores de red, tienen conexiones USB que pueden proporcionar acceso directo al sistema. El acceso físico es un método más seguro para acceder a componentes, ya que elimina la posibilidad de ataques basados en red.

- Restrinja la capacidad para reiniciar el sistema mediante la red.
- Restrinja el acceso especialmente a los dispositivos de conexión en caliente o intercambio en caliente, porque se pueden eliminar fácilmente.
- Almacene las unidades sustituibles en campo (FRU) y las unidades sustituibles por el cliente (CRU) de repuesto en un armario cerrado. Restrinja el acceso al armario cerrado al personal autorizado.

Autenticación

La autenticación indica la manera en que se identifica un usuario, generalmente mediante información confidencial, como nombre de usuario y contraseña. La autenticación garantiza que los usuarios del hardware o software sean quienes dicen ser.

- Configure funciones de autenticación, por ejemplo, un sistema de contraseñas, en los sistemas operativos de la plataforma para asegurarse de que los usuarios sean quienes dicen ser.
- Asegúrese de que el personal utilice correctamente las identificaciones de empleado para ingresar a la sala de cómputo.
- Para las cuentas de usuario: use listas de control de acceso cuando corresponda, establezca tiempos de espera para sesiones prolongadas y establezca niveles de privilegios para los usuarios.

Autorización

La autorización permite que los administradores controlen las tareas que puede realizar un usuario o los privilegios que puede utilizar. El personal únicamente puede realizar las tareas y usar los privilegios que le han sido asignados. La autorización se refiere a las restricciones que se aplican al personal para trabajar con hardware o software.

- Permita al personal trabajar únicamente con hardware y software que estén capacitados y cualificados para utilizar.
- Establezca un sistema de permisos de lectura, escritura y ejecución para controlar el acceso del usuario a los comandos, el espacio en el disco, los dispositivos y las aplicaciones.

Cuentas y auditoría

La función de cuentas y autoría implica mantener un registro de la actividad de un usuario en el sistema. Los servidores Oracle tienen funciones de software y hardware que permiten que los administradores supervisen la actividad de inicio de sesión y mantengan inventarios de hardware.

- Use los logs del sistema para supervisar el inicio de sesión de los usuarios. Supervise las cuentas de servicio y administrador del sistema particularmente, ya que esas cuentas permiten acceder a comandos que, si se ejecutan de forma incorrecta, pueden dañar el sistema u originar la pérdida de datos. El acceso y los comandos deben supervisarse cuidadosamente mediante los logs del sistema.
- Registre los números de serie de todo el hardware. Utilice los números de serie de los componentes para realizar un seguimiento de los activos del sistema. Los números de referencia de Oracle se registran electrónicamente en las tarjetas, módulos y placas base, y pueden utilizarse para efectos de inventario.
- Para detectar los componentes y realizar un seguimiento de ellos, realice una marca de seguridad en todos los elementos de hardware del equipo que sean importantes, como las unidades sustituibles en campo y las unidades sustituibles por el cliente. Utilice plumas ultravioleta o etiquetas en relieve especiales.
- Mantenga las licencias y las claves de activación de hardware en una ubicación segura y de fácil acceso para el administrador del sistema, especialmente, en caso de emergencias del sistema. Los documentos impresos podrían ser su única prueba para demostrar la propiedad.

Uso seguro de las herramientas de configuración y gestión del servidor

Siga las directrices de seguridad proporcionadas en estas secciones al utilizar herramientas de software y firmware para configurar y gestionar el servidor:

- "Seguridad de Oracle ILOM" [11]
- "Seguridad de Oracle Hardware Management Pack" [12]

Póngase en contacto con el responsable de la seguridad de TI para conocer los requisitos de seguridad adicionales relacionados con el sistema y el entorno específico.

Seguridad de Oracle ILOM

Puede proteger, gestionar y supervisar activamente los componentes del sistema mediante el firmware de gestión Oracle Integrated Lights Out Manager (Oracle ILOM), que está incrustado en los servidores x86 de Oracle y en los servidores SPARC de Oracle. Según el nivel de autorización otorgado a los administradores del sistema, estas funciones pueden incluir la capacidad de apagar el servidor, crear cuentas de usuario, montar dispositivos de almacenamiento remoto, etc.

- **Use una red interna segura de confianza.**

  Independientemente de que establezca una conexión de gestión física con Oracle ILOM mediante el puerto serie local, el puerto de gestión de red dedicado, el puerto de gestión de banda lateral o el puerto de red de datos estándar, es fundamental que este puerto físico del servidor siempre esté conectado a una red interna de confianza o a una red privada o de gestión segura dedicada.

  Nunca conecte el procesador de servicio (SP) de Oracle ILOM a una red pública, como Internet. Debe mantener el tráfico de gestión del SP de Oracle ILOM en una red de gestión separada y otorgar acceso solo a los administradores del sistema.
- **Limite el uso de la cuenta de administrador por defecto.**

  Limite el uso de la cuenta de administrador por defecto (`root`) a la conexión inicial a Oracle ILOM. Esta cuenta de administrador por defecto se proporciona únicamente para brindar ayuda con la instalación inicial del servidor. Por lo tanto, para garantizar el entorno más seguro, debe cambiar la contraseña de administrador por defecto (`changeme`)

en la configuración inicial del sistema. Si un usuario obtiene acceso a la cuenta de administrador por defecto, podrá acceder libremente a todas las funciones de Oracle ILOM. Además, establezca nuevas cuentas de usuario con contraseñas únicas y asigne niveles de autorización (roles de usuario) para cada usuario nuevo de Oracle ILOM.

- **Considere cuidadosamente los riesgos al conectar el puerto serie a un servidor de terminales**.

  Los dispositivos de terminal no siempre proporcionan los niveles adecuados de autorización o autenticación de usuarios requeridos para proteger la red contra intrusiones maliciosas. Para proteger el sistema contra intrusiones de red no deseadas, no establezca una conexión serie (puerto serie) a Oracle ILOM mediante cualquier tipo de dispositivo de redirección de red, como un servidor de terminales, a menos que el servidor tenga controles de acceso suficientes.

  Además, determinadas funciones de Oracle ILOM, como el restablecimiento de contraseñas y el menú Preboot (Preinicio), únicamente están disponibles mediante el puerto serie físico. La conexión de un puerto serie a una red mediante un servidor de terminales no autenticado elimina la necesidad de acceso físico y disminuye la seguridad asociada con estas funciones.

- **El acceso al menú Preboot (Preinicio) requiere acceso físico al servidor.**

  El menú Preboot (Preinicio) de Oracle ILOM es una utilidad eficaz que ofrece una manera de restablecer Oracle ILOM a los valores por defecto y de actualizar el firmware si Oracle ILOM deja de responder. Una vez que se restablece Oracle ILOM, el usuario debe pulsar un botón en el servidor (por defecto) o escribir una contraseña. La propiedad de presencia física de Oracle ILOM controla esta comportamiento (`check_physical_presence= true`). Para contar con máxima seguridad al acceder al menú Preboot (Preinicio), no cambie la configuración por defecto (`true`), de modo que el acceso al menú Preboot (Preinicio) siempre requiera acceso físico al servidor.

- **Consulte la documentación de Oracle ILOM.**

  Consulte la documentación de Oracle ILOM para obtener más información sobre la configuración de contraseñas, la gestión de usuarios y la aplicación de funciones relacionadas con la seguridad, incluidas la autenticación de RADIUS, Secure Socket Layer (SSL) y Secure Shell (SSH). Para obtener directrices de seguridad específicas de Oracle ILOM, consulte la *Guía de seguridad de Oracle ILOM*, que forma parte de la biblioteca de documentación de Oracle ILOM. Puede encontrar la documentación de Oracle ILOM en:

  `http://www.oracle.com/goto/ilom/docs`

Seguridad de Oracle Hardware Management Pack

Oracle Hardware Management Pack está disponible para su servidor, para muchos otros servidores x86 de Oracle y para algunos servidores SPARC de Oracle. Oracle Hardware Management Pack cuenta con dos componentes: un agente de supervisión SNMP y una familia de herramientas de interfaz de línea de comandos (herramientas de CLI) compatibles con distintos sistemas operativos para gestionar el servidor. Puede usar las herramientas de la CLI del servidor Oracle para configurar servidores Oracle. Las herramientas de la CLI funcionan

con los sistemas operativos Oracle Solaris, Oracle Linux, Oracle VM, otras variantes de Linux y Microsoft Windows.

- **Use los plugins de SNMP de Hardware Management Agent.**

  SNMP es un protocolo estándar utilizado para supervisar o gestionar un sistema. Con los plugins de SNMP de Hardware Management Agent, puede usar SNMP para supervisar los servidores Oracle en el centro de datos, sin necesidad de conectarse a dos puntos de gestión (el host y Oracle ILOM). Esta funcionalidad le permite usar una dirección IP única (la dirección IP del host) para supervisar varios servidores.

  Los plugins de SNMP se ejecutan en el sistema operativo host de los servidores Oracle. El plugin de SNMP extiende el agente SNMP nativo en el sistema operativo host a fin de proporcionar capacidades adicionales de MIB de Oracle. Oracle Hardware Management Pack no incluye un agente SNMP. Para Linux, se agrega un módulo al agente net-snmp. Para Oracle Solaris, se agrega un módulo a Oracle Solaris Management Agent. Para Microsoft Windows, el plugin extiende el servicio SNMP nativo. La configuración de seguridad relacionada con SNMP para Oracle Hardware Management Pack es determinada por la configuración de un servicio o agente SNMP nativo, no por el plugin.

  Tenga en cuenta que SNMPv1 y SNMPv2c no proporcionan cifrado y utilizan cadenas comunitarias como forma de autenticación. SNMPv3 es más seguro y es la versión recomendada, ya que utiliza el cifrado para proporcionar un canal seguro, además de nombres de usuario y contraseñas individuales.

- **Consulte la documentación de Oracle Hardware Management Pack.**

  Para obtener más información sobre estas funciones, consulte la documentación de Oracle Hardware Management Pack. Si desea obtener directrices de seguridad específicas de Oracle Hardware Management Pack, consulte la *Guía de seguridad de Oracle Hardware Management Pack (HMP)*, que forma parte de la biblioteca de documentación de Oracle Hardware Management Pack. Puede encontrar la documentación de Oracle Hardware Management Pack en:

  `http://www.oracle.com/goto/ohmp/docs`

Planificación de un entorno seguro

Antes de la llegada del sistema, debe haber implementadas directrices de seguridad. Después de la llegada del sistema, las directrices de seguridad deben revisarse y ajustarse periódicamente para adaptarse a los requisitos de seguridad de la organización.

Utilice la información de estas secciones antes de la instalación y la configuración de un servidor y los equipos relacionados, y durante estas tareas.

Póngase en contacto con el responsable de la seguridad de TI para conocer los requisitos de seguridad adicionales relacionados con el sistema y el entorno específico.

Protección mediante contraseña

Las contraseñas son un aspecto importante de la seguridad, ya que una contraseña mal elegida puede originar el acceso no autorizado a los recursos de la empresa. La implementación de mejores prácticas de gestión de contraseñas garantiza que los usuarios cumplan con un juego de directrices para crear y proteger sus contraseñas. Los componentes típicos de una política de contraseñas deben definir:

- Longitud y seguridad de la contraseña
- Duración de la contraseña
- Práctica común de la contraseña

Aplique las siguientes prácticas estándar para la creación de contraseñas complejas y seguras:

- No cree una contraseña que contenga el nombre de usuario, el nombre del empleado o apellidos.
- No elija contraseñas que se adivinen fácilmente.
- No cree contraseñas que contengan una cadena consecutiva de números, como 12345.

- No cree contraseñas que contengan una palabra o cadena que se pueda descubrir fácilmente mediante una simple búsqueda en Internet.
- No permita que los usuarios vuelvan a utilizar la misma contraseña en varios sistemas.
- No permita que los usuarios vuelvan a utilizar contraseñas anteriores.

Cambie las contraseñas periódicamente. Esto ayuda a evitar actividades maliciosas y garantiza que las contraseñas cumplan con las políticas de contraseñas actuales.

Directrices de seguridad del sistema operativo

Consulte los documentos del sistema operativo Oracle para obtener información sobre lo siguiente:

- Cómo utilizar las funciones de seguridad al configurar los sistemas.
- Cómo trabajar de forma segura al agregar aplicaciones y usuarios a un sistema.
- Cómo proteger las aplicaciones basadas en red.

Los documentos de la guía de seguridad para los sistemas operativos Oracle admitidos forman parte de la biblioteca de documentación del sistema operativo. Para encontrar el documento de la guía de seguridad de un sistema operativo Oracle, vaya a la biblioteca de documentación del sistema operativo Oracle:

Sistema operativo	Enlace
Sistema operativo Oracle Solaris	http://www.oracle.com/technetwork/documentation/solaris-11-192991.html
Sistema operativo Oracle Linux	http://www.oracle.com/technetwork/documentation/ol-1-1861776.html
Oracle VM	http://www.oracle.com/technetwork/documentation/vm-096300.html

Para obtener información sobre los sistemas operativos de otros proveedores, como Red Hat Enterprise Linux, SUSE Linux Enterprise Server, Microsoft Windows y VMware ESXi, consulte la documentación de los proveedores.

Puertos y conmutadores de red

Los conmutadores de red ofrecen diferentes niveles de funciones de seguridad para puertos. Consulte la documentación del conmutador para aprender a realizar lo siguiente:

- Utilizar las funciones de autenticación, autorización y cuentas para el acceso local y remoto al conmutador.

- Cambiar todas las contraseñas de los conmutadores de red que puedan tener varias cuentas de usuario y contraseñas de forma predeterminada.
- Gestionar conmutadores fuera de banda (separados del tráfico de datos). Asignar un número de red de área local virtual (VLAN) separado para la gestión en banda, si la gestión fuera de banda no es posible.
- Utilizar la capacidad de duplicación de puertos del conmutador de la red para el acceso del sistema de detección de intrusos (IDS).
- Mantenga un archivo de configuración del switch fuera de línea y limite el acceso solamente a administradores autorizados. El archivo de configuración debe contener comentarios descriptivos para cada opción.
- Implemente la seguridad de los puertos para limitar el acceso basándose en las direcciones MAC. Desactive la función de enlace troncal automático en todos los puertos.
- Utilice estas funciones de seguridad para puertos si están disponibles en el switch:
  - **Bloqueo de MAC**: consiste en asociar una dirección de control de acceso a medios (MAC, Media Access Control) de uno o más dispositivos conectados a un puerto físico en un switch. Si bloquea un puerto del switch a una dirección MAC en particular, los superusuarios no pueden crear las puertas traseras en su red con peligrosos puntos de acceso.
  - **Cierre de MAC**: desactiva la conexión de una dirección MAC especificada a un switch.
  - **Aprendizaje de MAC**: utiliza el conocimiento sobre las conexiones directas de cada puerto del switch de manera que el switch de red pueda definir la seguridad en función de las conexiones actuales.

Seguridad de una VLAN

Si configura una red de área local virtual (VLAN), recuerde que las VLAN comparten el ancho de banda de la red y requieren medidas de seguridad adicionales. Si desea tomar medidas de seguridad adicionales, siga estas directrices:

- Al usar VLAN, separe los clusters sensibles de sistemas del resto de la red. De esta manera, se reduce la probabilidad de que los usuarios tengan acceso a la información almacenada en esos clientes y servidores.
- Asigne un número de VLAN nativo único a los puertos de enlace troncal.
- Limite las VLAN que se pueden transportar sobre un enlace troncal a las que sean estrictamente necesarias.
- Desactive el protocolo de enlace troncal de VLAN (VTP), si es posible. De lo contrario, configure lo siguiente para el VTP: dominio de gestión, contraseña y eliminación. A continuación, defina VTP en modo transparente.
- Utilice configuraciones de VLAN estáticas, cuando sea posible.
- Desactive los puertos de switch no utilizados y asígneles un número de VLAN que no esté en uso.

Seguridad de InfiniBand

Para aumentar la seguridad cuando se usa InfiniBand, siga estas directrices:

- Mantenga los hosts InfiniBand protegidos. Un tejido InfiniBand solamente es tan seguro como su host InfiniBand menos seguro.
- Tenga en cuenta que realizar una partición no protege un tejido InfiniBand. La partición solo ofrece aislamiento del tráfico InfiniBand entre máquinas virtuales de un host.

Mantenimiento de un entorno seguro

Después de la instalación y la configuración iniciales, use las funciones de seguridad del hardware y el software de Oracle para continuar controlando el hardware y realizando un seguimiento de los activos del sistema.

Utilice la información que se proporciona en estas secciones para mantener un entorno seguro:

Póngase en contacto con el responsable de la seguridad de TI para conocer los requisitos de seguridad adicionales relacionados con el sistema y el entorno específico.

Control de energía

Puede usar software para encender y apagar algunos sistemas de Oracle. Las unidades de distribución de energía (PDU) de algunos armarios de sistemas pueden activarse y desactivarse de manera remota. La autorización para estos comandos se suele definir durante la configuración del sistema y normalmente está limitada a los administradores del sistema y al personal de mantenimiento.

Consulte la documentación del sistema o del armario para obtener más información.

Seguimiento de Activos

Utilice los números de serie para hacer un seguimiento del inventario. Oracle incrusta los números de serie del firmware en tarjetas opcionales y placas base del sistema. Puede leer estos números de serie mediante conexiones de red de área local (LAN).

También puede utilizar lectores inalámbricos de identificación por radiofrecuencia (RFID) para simplificar aún más el seguimiento de los activos. Las notas del producto de Oracle *Cómo*

realizar un seguimiento de los activos del sistema Oracle Sun mediante RFID, están disponibles en:

http://www.oracle.com/technetwork/articles/systems-hardware-architecture/o11-001-rfid-oracle-214567.pdf

Actualizaciones para software y firmware

Las mejoras de seguridad están incluidas en los parches y las nuevas versiones de software. La gestión de parches preventiva y eficaz es una parte fundamental de la seguridad del sistema. Para mejores prácticas de seguridad, actualice el sistema con la versión de software más reciente y todos los parches de seguridad necesarios.

- Busque periódicamente actualizaciones de software o firmware, y parches de seguridad.
- Instale siempre la versión publicada más reciente del software o el firmware en su equipo.
- Instale los parches de seguridad necesarios para el software.
- Recuerde que los dispositivos como los switches de red también incluyen firmware y pueden requerir parches y actualizaciones de firmware.

Puede encontrar actualizaciones de software y parches de seguridad en el sitio web My Oracle Support, en:

https://support.oracle.com

Seguridad de red

Una vez que las redes se configuraron según los principios de seguridad, es necesario realizar una revisión y un mantenimiento periódicos.

Para proteger el acceso local y remoto a los sistemas, siga estas directrices:

- Limite la configuración remota a direcciones IP específicas mediante SSH en lugar de Telnet. Telnet acepta nombres de usuario y contraseñas en texto no cifrado y, como consecuencia, puede permitir que todos los miembros del segmento de red de área local (LAN) vean las credenciales de inicio de sesión. Defina una contraseña segura para SSH.
- Utilice la versión 3 del protocolo simple de gestión de redes (SNMP) para proporcionar transmisiones seguras. Las primeras versiones de SNMP no son seguras y transmiten datos de autenticación en texto no cifrado. SNMPv3 utiliza el cifrado para proporcionar un canal seguro, además de contraseñas y nombres de usuario individuales.
- Cambie la cadena de comunidad SNMP por defecto por una cadena de comunidad segura, si es necesario utilizar SNMPv1 o SNMPv2. Algunos productos tienen el valor PUBLIC

establecido como cadena de comunidad SNMP por defecto. Los atacantes pueden pedir a una comunidad que realice un mapa de red muy completo y, posiblemente, que modifiquen los valores de la base de información de gestión (MIB).

- Siempre cierre la sesión después de usar el controlador del sistema si este controlador utiliza una interfaz de explorador.
- Active los servicios de red necesarios y configure estos servicios de manera segura. Desactive los servicios de red innecesarios, por ejemplo, el protocolo de control de transmisión (TCP) o el protocolo de transferencia de hipertexto (HTTP).
- Use las medidas de seguridad de LDAP al utilizar LDAP para acceder al sistema.
- Cree un mensaje de banner que aparezca durante el inicio de sesión para indicar que el acceso no autorizado está prohibido. Puede informar a los usuarios sobre reglas o políticas importantes. El banner se puede utilizar para advertir a los usuarios sobre restricciones de acceso especiales para un sistema determinado o para recordar a los usuarios las políticas de contraseñas y el uso apropiado.
- Utilice listas de control de acceso para aplicar restricciones, cuando corresponda.
- Establezca el timeout para sesiones prolongadas y establezca niveles de privilegio.
- Utilice las funciones de autenticación, autorización y cuentas para el acceso local y remoto a un switch.
- Utilice estos servicios de red en entornos muy seguros, ya que están protegidos por certificados y otras formas de cifrado de alta seguridad para proteger el canal:
  - Directorio Activo.
  - LDAP/SSL (Lightweight Directory Access Protocol/Secure Socket Layer).
- Utilice estos servicios de red en redes seguras privadas donde no existan sospechas de usuarios maliciosos:
  - RADIUS (Remote Authentication Dial In User Service).
  - TACACS+ (Terminal Access Controller Access-Control System).
- Utilice la capacidad de reflejo de puertos del switch para el acceso del sistema de detección de intrusos (IDS).
- Implemente la seguridad de los puertos para limitar el acceso en función de una dirección MAC. Desactive la función de enlace troncal automático en todos los puertos.

Para obtener más información sobre la seguridad de red, consulte la *Guía de seguridad de Oracle ILOM*, que forma parte de la biblioteca de documentación de Oracle ILOM. Puede encontrar la documentación de Oracle ILOM en:

http://www.oracle.com/goto/ilom/docs

Protección de datos y seguridad

Siga estas directrices para maximizar la seguridad y la protección de los datos.

- Realice una copia de seguridad de datos importantes mediante dispositivos como discos duros externos o dispositivos de almacenamiento USB. Almacene la copia de seguridad de los datos en una segunda ubicación segura fuera del sitio.
- Utilice software de cifrado de datos para guardar de manera segura la información confidencial en unidades de disco duro.
- Al desechar una unidad de disco duro antigua, destruya físicamente la unidad o borre por completo todos los datos almacenados en ella. Después suprimir los archivos o de volver a formatear una unidad, aún se puede recuperar la información de la unidad. La supresión de los archivos o el formateo de la unidad elimina únicamente las tablas de direcciones de la unidad. Utilice software de borrado del disco para borrar por completo todos los datos de una unidad.
- Por lo general, las unidades de disco duro se usan para almacenar información confidencial. Para proteger esta información de la divulgación no autorizada, las unidades de disco duro deberían sanearse antes de ser reutilizadas, retiradas o desechadas.
  - Utilice herramientas de borrado de disco, como el comando `format(1M)` de Oracle Solaris, para borrar por completo todos los datos del disco duro. De manera alternativa, puede utilizar, si corresponde y están disponibles, herramientas de desmagnetización física.
  - En algunos casos, la información almacenada en los discos duros posee tal nivel de confidencialidad que el único método de saneamiento apropiado es la destrucción física del disco duro por medio de la pulverización o la incineración.
  - Se recomienda a las organizaciones que consulten sus respectivas políticas de protección de datos para determinar el método más apropiado para sanear los discos duros.

Atención - Debido a la manera en que se gestiona el acceso a los datos, quizá no sea posible suprimir algunos de los datos en discos duros modernos (especialmente los SSD) con software de borrado de disco duro.

Mantenimiento de logs

Inspeccione y mantenga los archivos log de manera periódica. Use estos métodos para proteger los archivos log:

- Active la creación de logs y envíe los logs del sistema a un host de log dedicado seguro.
- Configure el registro para incluir información de tiempo precisa mediante el protocolo de tiempo de red (NTP) y registros de hora.
- Realice análisis periódicos planificados de logs de dispositivos de red para detectar accesos o actividad de red inusuales.
- Revise los logs para detectar posibles incidentes y archívelos de acuerdo con una política de seguridad.

- Retire con regularidad los archivos log cuando excedan un tamaño razonable. Mantenga copias de los archivos retirados para utilizarlos en el futuro para referencia o análisis estadístico.