centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 442

IMPLEMENTACIÓN DE SEGURIDAD SOBRE VMWARE VSPHERE 8.x

JULIO 2025

Edita:

centro criptológico nacional

centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL,
2.5.4.97=VATES-S2800155J, ou=CENTRO
CRIPTOLOGICO NACIONAL, o=CENTRO
CRIPTOLOGICO NACIONAL, c=ES
2025.07.21 12:37:54 +02'00'

Fecha de Edición: julio de 2025

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE VMWARE VSPHERE 8.x EN EL ENS 6
ANEXO A.1. DESCRIPCIÓN DE LAS MEDIDAS DE SEGURIDAD EN EL ENS 6
1. APLICACIÓN DE MEDIDAS EN WMWARE VSPHERE 8.x 6
1.1. MARCO OPERACIONAL 7
1.1.1. CONTROL D E ACCESO 7
1.1.1.1. OP. ACC. 2. REQUISITOS DE ACCESO 7
1.1.1.2. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS 8
1.1.1.3. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO 8
1.1.1.4. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN (usuarios externos) 9
1.1.1.5. OP. ACC. 6. MECANISMO DE AUTENTICACIÓN (usuarios de la organización) 10
1.1.2. EXPLOTACIÓN 10
1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD 11
1.1.2.2. OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD 11
1.1.2.3. OP. EXP. 8. REGISTRO DE LA ACTIVIDAD 12
1.2. MEDIDAS DE PROTECCIÓN 12
1.2.1. PROTECCIÓN DE LAS COMUNICACIONES 13
1.2.1.1. MP. COM. 3. PROTECCIÓN DE LA INTEGRIDAD Y DE LA AUTENTICIDAD 13
1.2.1.2. MP. COM. 4. SEPARACIÓN DE FLUJOS DE INFORMACIÓN EN LA RED 13
1.2.2. PROTECCIÓN DE LA INFORMACIÓN 14
1.2.2.1. SEGURIDAD EN MÁQUINAS VIRTUALES 14
1.2.2.1.1. MP. INFO. 3. FIRMA ELECTRÓNICA 15
1.2.2.2. MP. INFO. 6. COPIAS DE SEGURIDAD 15
2. RESUMEN Y APLICACIÓN DE MEDIDAS EN VMWARE VSPHERE 8.X 16
ANEXO A.2. CATEGORÍA BÁSICA 18
ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD EN VMWARE VSPHERE 8.x SOBRE SERVIDORES QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS 18
3. CONFIGURACIÓN DE SEGURIDAD EN VCENTER 24
3.1. CONFIGURACIÓN EN CONMUTADORES VIRTUALES DISTRIBUIDOS 29
3.1.1. CONFIGURACIÓN EN GRUPOS DE PUERTOS 31
3.2. CONFIGURACIÓN DE SEGURIDAD EN SERVIDORES ESXI 32
3.2.1. CONFIGURACIÓN EN CONMUTADORES VIRTUALES ESTÁNDAR 45
3.2.2. CONFIGURACIÓN DE MÁQUINAS VIRTUALES 47
3.2.3. CONFIGURACIÓN DE ESX SHELL Y SSH 50

ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA VSPHERE 8.x 55
1. SERVIDORES VCENTER 55
1.1. CONMUTADORES VIRTUALES DISTRIBUIDOS 58
1.2. GRUPOS DE PUERTOS 59
2. SERVIDORES ESXI 60
2.1. CONMUTADORES VIRTUALES ESTÁNDAR 62
2.2. MÁQUINAS VIRTUALES 63
2.3. COMPROBACIONES Y PASOS FINALES EN SERVIDOR ESXI 65
ANEXO A.3. CATEGORÍA MEDIA 72
ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD EN VMWARE VSPHERE 8.x SOBRE SERVIDORES QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS 72
1. PREPARACIÓN DEL SERVIDOR ESXI 72
2. CONFIGURACIÓN DE SEGURIDAD EN VCENTER 80
2.1. CONFIGURACIÓN EN CONMUTADORES VIRTUALES DISTRIBUIDOS 96
2.1.1. CONFIGURACIÓN EN GRUPOS DE PUERTOS 98
2.2. CONFIGURACIÓN DE SEGURIDAD EN SERVIDORES ESXI 99
2.2.1. CONFIGURACIÓN EN CONMUTADORES VIRTUALES ESTÁNDAR 116
2.2.2. CONFIGURACIÓN DE MÁQUINAS VIRTUALES 117
2.2.3. CONFIGURACIÓN DE ESX SHELL Y SSH 120
ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA VSPHERE 8.x 125
1. SERVIDORES VCENTER 125
1.1. CONMUTADORES VIRTUALES DISTRIBUIDOS 130
1.2. GRUPOS DE PUERTOS 131
2. SERVIDORES ESXI 132
2.1. CONMUTADORES VIRTUALES ESTÁNDAR 135
2.2. MÁQUINAS VIRTUALES 135
2.3. COMPROBACIONES Y PASOS FINALES EN SERVIDOR ESXI 138
ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA 145
ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD EN VMWARE VSPHERE 8.x SOBRE SERVIDORES QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA 145
1. PREPARACIÓN DEL SERVIDOR ESXI 145
2. CONFIGURACIÓN DE SEGURIDAD EN VCENTER 153
2.1. CONFIGURACIÓN DE SERVIDOR KMS 169
2.2. CONFIGURACIÓN EN CONMUTADORES VIRTUALES DISTRIBUIDOS 173

2.2.1. CONFIGURACIÓN EN GRUPO DE PUERTOS 175
2.3. CONFIGURACIÓN DE SEGURIDAD EN SERVIDORES ESXI 176
2.3.1. ACTIVAR USO DE CIFRADO EN HOST ESXI 194
2.3.2. CONFIGURACIÓN EN CONMUTADORES VIRTUALES ESTÁNDAR 194
2.3.3. CONFIGURACIÓN EN MÁQUINAS VIRTUALES 196
2.3.3.1. CIFRADO DE DISCOS EN MÁQUINAS VIRTUALES 199
2.3.4. CONFIGURACIÓN DE ESX SHELL Y SSH 200
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS PARA VSPHERE 8.x 205
1. SERVIDORES VCENTER 205
1.1. CONMUTADORES VIRTUALES DISTRIBUIDOS 211
1.2. GRUPOS DE PUERTOS 212
2. SERVIDORES ESXI 213
2.1. CONMUTADORES VIRTUALES ESTÁNDAR 216
2.2. MÁQUINAS VIRTUALES 216
2.2.1. CIFRADO DE MÁQUINAS VIRTUALES 219
2.3. COMPROBACIONES Y PASOS FINALES EN SERVIDOR ESXI 219

ANEXO A. CONFIGURACIÓN SEGURA DE VMWARE VSPHERE 8.X EN EL ENS

ANEXO A.1. DESCRIPCIÓN DE LAS MEDIDAS DE SEGURIDAD EN EL ENS

1. APLICACIÓN DE MEDIDAS EN WMWARE VSPHERE 8.x

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde se implemente la solución VMware vSphere 8.x bajo el ámbito de aplicación del Esquema Nacional de Seguridad (ENS), esta guía establece las condiciones necesarias para garantizar un entorno seguro. Estas medidas se materializarán mediante la aplicación de plantillas de seguridad, configuraciones específicas y procedimientos técnicos destinados a proteger la infraestructura.

Nota: En redes clasificadas categorizadas como Difusión Limitada, deberá aplicarse lo dispuesto en el "ANEXO A.4 CATEGORÍA ALTA / DIFUSIÓN LIMITADA" como referencia para el refuerzo adicional de seguridad.

Este documento detalla las características y configuraciones específicas aplicables a VMware vSphere 8.x, incluyendo sus componentes clave: ESXi y vCenter Server Appliance (VCSA). La solución se implementará preferentemente en entornos gestionados mediante dominio Active Directory, y donde convivan sistemas Linux compatibles con las funciones de infraestructura.

A partir de vSphere 7.0, vCenter Server ya no puede desplegarse sobre sistemas Windows. El único método de implementación soportado por el fabricante es mediante el vCenter Server Appliance (VCSA), una máquina virtual basada en Photon OS. Por tanto, todas las configuraciones de seguridad deberán tener en cuenta esta arquitectura.

No es objeto de esta guía detallar los métodos de instalación ni la arquitectura física sobre la que se despliegue la solución. Este documento está orientado a definir las configuraciones de seguridad necesarias que aseguren el cumplimiento con el ENS, de acuerdo con el nivel de seguridad asignado a la red o sistema.

Tampoco es propósito de esta guía abordar la creación o administración de objetos como centros de datos, máquinas o redes virtuales, sino establecer los controles de seguridad sobre los elementos existentes de la infraestructura vSphere 8.x, tales como:

Redes y conmutadores virtuales

Máquinas virtuales

Adaptadores de almacenamiento

Hosts ESXi

Servidores vCenter

El hipervisor ESXi incluye un sistema operativo embebido y ligero (VMkernel), sobre el cual se aplicarán medidas de seguridad específicas que se describen en este anexo.

Esta guía incorpora todos los ficheros de configuración y scripts necesarios para aplicar las medidas, además de incluir instrucciones para realizar ajustes manuales tanto desde la consola del host ESXi como a través de vSphere Web Client o PowerCLI.

En entornos con dominio Active Directory o donde se requiera la resolución de nombres (DNS), deberá asegurarse la correcta configuración de los registros host A y sus correspondientes PTR para resolución inversa, garantizando que los hosts puedan validar identidades y realizar comunicaciones seguras.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso cubre todo el conjunto de acciones que, bien preparatorias o ejecutivas, están orientadas a determinar qué o quién puede o no acceder a un recurso del sistema mediante una determinada acción. Con el cumplimiento de todas las medidas se garantizará que nadie accederá a recursos, ya sean las propias máquinas virtuales o el propio servidor que administra dichas máquinas virtuales, sin la debida autorización.

Adicionalmente, se establece la necesidad de que el uso del sistema quede registrado para detectar y reaccionar ante una incidencia de seguridad o fallo del sistema.

Toda medida de control de acceso busca el equilibrio entre la usabilidad y la protección del sistema de tal forma que la seguridad se irá incrementando en base a la categoría exigida. Por lo tanto, se requiere una menor exigencia de seguridad para la categoría básica mientras que en la categoría media y alta se requiere una mayor exigencia.

1.1.1.1. OP. ACC. 2. REQUISITOS DE ACCESO

Los requisitos de acceso se aplican desde la categoría básica y atenderán a la necesidad de proteger los recursos del sistema (ficheros, directorios y recursos compartidos) con algún mecanismo que impida su utilización, salvo a usuarios o perfiles de usuario que disfruten de los derechos de acceso suficientes.

Estos derechos se controlarán y asignarán atendiendo a la política y normativa de seguridad de la organización, a través de la persona responsable de dicha determinación y haciendo uso de las tecnologías necesarias.

Así mismo, dicha persona responsable será la encargada de determinar aquellos recursos que serán compartidos y cuáles serán accesibles para los usuarios.

Desde el punto de vista tecnológico, esta medida abarca un gran número de actividades de tal forma que los puntos de control para restringir o conceder un acceso son abundantes. Realizar la administración del Directorio Activo, acceder a un fichero o una carpeta o imprimir en un recurso, son acciones que pueden ser controladas y determinar para ello los permisos asignados.

Así mismo, es importante la creación de grupos con el objetivo de establecer los permisos a través de dichos grupos, permitiendo una gestión global y sencilla sobre el acceso a los recursos que ofrece VMware vSphere 8.x. De este modo se evita modificar los permisos individuales de cada usuario para conceder o no permisos sobre un mismo recurso.

Se deberá evitar el uso de usuarios genéricos como, por ejemplo, el usuario “root” que deberá ser inhabilitado para el acceso a los servidores de ESXi.

Se deberá establecer, adicionalmente, un control de pertenencia al grupo de excepción en modo de bloqueo.

En el caso de que se realicen implementaciones de configuraciones de hosts a través de los perfiles de host (cuyo uso está recomendado tanto por reducción de costes administrativos como

por seguridad), se recomienda el uso de un servicio de vSphere Authentication Proxy para evitar el almacenamiento de credenciales en el perfil y la transmisión de éstas a través de la red. No es objeto de esta guía la configuración de este servicio adicional, pero se recomienda su uso en caso de que el entorno lo permita o requiera.

Para reforzar la seguridad de vCenter Server, VMware ha reemplazado el uso de la cuenta de servicio local por una serie de cuentas de servicio virtuales. Definiendo una cuenta de servicio individual para cada uno de los servicios que ejecuta. Este hecho limita la vulnerabilidad de la solución ya que en caso de que una cuenta se vea comprometida, esta no permite operar sobre el resto de los servicios.

En caso de estar haciendo uso de un sistema de dominio de Directorio Activo, se deberá otorgar el privilegio de iniciar sesión como servicio tanto a la cuenta de servicio definida durante la instalación de vCenter como al grupo “NT SERVICES\ALL SERVICES”.

Así mismo, la cuenta de servicio definida como principal durante la instalación de la solución deberá tener privilegios de administración sobre el equipo servidor sobre el que se haya implementado vCenter Server.

1.1.1.2. OP. ACC. 3. SEGREGACIÓN DE FUNCIONES Y TAREAS

Aplicable a partir de la categoría media. Se considera un requerimiento importante para una organización la segregación de funciones en base a la actividad. De esta forma se establecen cadenas de autorización y control enfocadas a evitar la existencia de una única persona autorizada y que ésta pueda abusar de sus derechos para cometer alguna acción ilícita.

Desde el punto de vista formal la segregación de funciones deberá realizarse al menos para las siguientes tareas.

a) Desarrollo de operación.

b) Configuración y mantenimiento del sistema de operación.

c) Auditoría o supervisión de otra función.

Así mismo, a partir de la categoría media, se deberá tomar en cuenta la trazabilidad en mayor medida. Por tanto, se deberá hacer uso de usuarios únicos, lo que conlleva establecer usuarios individuales con aquellos permisos específicos que les otorguen solo los privilegios que necesita.

A partir de la categoría media, los diferentes roles y privilegios deberán ser tratados de forma personalizada estableciendo específicamente aquello a lo que se tiene permiso y, por tanto, se deberá evitar hacer uso de grupos o roles administrativos predefinidos.

Independientemente del sistema sobre el que se ha implementado la solución, se deberá utilizar una cuenta de servicio específica para iniciar y hacer uso de los servicios específicos de la solución.

1.1.1.3. OP. ACC. 4. PROCESO DE GESTIÓN DE DERECHOS DE ACCESO

Este proceso requiere consolidación de los derechos de acceso, de tal forma que:

a) Exista la aplicación del mínimo privilegio. Los privilegios de cada recurso se reducirán al mínimo estrictamente necesario para poder cumplir las obligaciones.

b) Necesidad de conocer. Los privilegios se limitarán de forma que los usuarios sólo accederán al conocimiento de aquella información requerida para cumplir sus obligaciones.

c) Capacidad de autorizar. Sólo y exclusivamente el personal con competencia para ello podrá conceder, alterar o anular la autorización de acceso a los recursos conforme a los criterios establecidos por su propietario.

En la navegación a Internet, acceso a recursos o tratamientos ofimáticos por citar algunos ejemplos frecuentes, un usuario no requiere del privilegio de administrador para poder utilizarlos. Así, y sin darse cuenta, podría estar poniendo en grave riesgo la seguridad del sistema al tratar ficheros, ejecutables, componentes y otros, descargados de Internet u otras fuentes de dudosa confianza, con máximos privilegios.

Se deberán establecer, así mismo, niveles de control de acceso para impedir que un usuario no autorizado pueda visualizar contenido que no es requerido para las funciones que desempeña. Se establece, por lo tanto, a nivel de los recursos, el aplicar mecanismos para permitir la visualización de contenido o edición de éste a los usuarios que los requieran exclusivamente.

De esta forma, el principio de mínima exposición y menor privilegio se puede materializar de forma extensiva a los propios administradores de los servidores y servicios que gestiona la organización.

Se deberá tener en consideración, debido a dicha norma, que los permisos otorgados a los usuarios serán los mínimos requeridos, no siendo necesario que estos posean permisos adicionales a la tarea que van a realizar. Por ejemplo, si un usuario tiene permiso para alterar el contenido de una carpeta no por ello implica que sea necesario que posea permisos para alterar los accesos y permisos para otros usuarios o para sí mismo. Con la concesión de estos permisos se le estarían otorgando privilegios más allá de las necesidades que requiere.

1.1.1.4. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN (usuarios externos)

Para el acceso de usuarios externos a sistemas clasificados según el Esquema Nacional de Seguridad (ENS), se deberán implementar mecanismos de autenticación robustos, priorizando el uso de autenticación multifactor (MFA). Esta medida es especialmente crítica en sistemas de categoría media y alta.

Requisitos mínimos:

- Obligatorio el uso de RSA SecurID, tarjetas inteligentes u otros dispositivos criptográficos certificados por el Centro Criptológico Nacional (CCN).
- En sistemas clasificados como categoría media o alta, se prohíbe el uso exclusivo de contraseñas.
- Se exigirá un segundo factor de autenticación basado en:
    - Certificados digitales emitidos por una entidad certificadora reconocida.
    - Dispositivos físicos (tokens) o biometría.
- Los algoritmos y dispositivos utilizados deberán cumplir con las guías técnicas del CCN, como la CCN-STIC-808.

Medidas de refuerzo recomendadas:

Gestión centralizada de identidades externas mediante soluciones de federación (ej. SAML, OpenID Connect) que permitan validar identidades de forma segura y trazable.

Registro y auditoría de accesos externos, incluyendo:

- Hora, IP de origen, método de autenticación y resultado.
- Integración con sistemas SIEM para correlación de eventos.

Bloqueo automático de cuentas tras múltiples intentos fallidos de autenticación (configurable, por ejemplo, tras 5 intentos).

Caducidad y renovación periódica de certificados digitales utilizados por usuarios externos.

Restricción geográfica o por IP para accesos externos, limitando el acceso solo desde ubicaciones autorizadas.

Notificación automática al usuario y al administrador ante accesos desde ubicaciones no habituales o dispositivos nuevos.

Revisión periódica de cuentas externas activas, eliminando accesos innecesarios o caducados.

Pruebas de robustez de los mecanismos MFA mediante simulaciones de ataques (ej. phishing controlado, ingeniería social).

1.1.1.5. OP. ACC. 6. MECANISMO DE AUTENTICACIÓN (usuarios de la organización)

Para usuarios internos, se aplicarán políticas de autenticación basadas en contraseñas seguras, complementadas con MFA en función de la criticidad del sistema:

- Longitud mínima de contraseña:
  - 10 caracteres para categoría básica.
  - 12 caracteres para categoría media.
  - 14 caracteres para categoría alta.
- Complejidad: al menos una letra mayúscula, una minúscula, un número y un carácter especial.
- Caducidad:
  - 90 días (básica), 60 días (media), 60 días (alta).
- Historial: mínimo de 24 contraseñas recordadas.
- Bloqueo de cuenta tras 8 intentos fallidos, con tiempos de bloqueo progresivos según la categoría.
- Autenticación multifactor obligatoria en categoría alta.

1.1.2. EXPLOTACIÓN

Se incluyen, en este apartado, todas aquellas medidas designadas como parte de la explotación de los servicios. El ENS define a través de ellas una serie de procesos tanto para el control, como para la gestión que deberán llevarse a cabo por parte de las entidades.

Las medidas atienden a diferentes tareas que deberán ser llevadas a la práctica por el departamento de informática.

1.1.2.1. OP. EXP. 2. CONFIGURACIÓN DE SEGURIDAD

Los equipos, antes de su entrada en producción, deberán configurarse de tal forma que:

a) Se retiren cuentas y contraseñas estándar.

b) Se aplique la regla de mínima funcionalidad.

Se considera indispensable que el sistema no proporcione funcionalidades gratuitas, solamente las estrictamente necesarias. Esto permitirá adaptarse al principio de mínima exposición. Para ello, se eliminarán o desactivarán mediante el control de la configuración, aquellas funciones que no sean de interés no sean necesarias e incluso aquellas que sean inadecuadas para el fin que se persigue.

Adicionalmente, se deshabilitarán, como parte de los mecanismos de mínima funcionalidad y mínima exposición de la información manejada, todos aquellos procesos que pudieran implicar el envío de información al fabricante o todos aquellos servicios automatizados susceptibles de reportar datos o funcionalidad de los servidores.

1.1.2.2. OP. EXP. 3. GESTIÓN DE LA CONFIGURACIÓN DE SEGURIDAD

La configuración de los componentes del sistema deberá gestionarse de forma que se garantice la seguridad por defecto y la funcionalidad mínima necesaria, conforme a los principios del ENS. Para ello, se deberán cumplir los siguientes requisitos:

Se deberá aplicar el principio de funcionalidad mínima, deshabilitando servicios, puertos y funcionalidades no necesarios, y asegurando una configuración segura por defecto en todos los componentes del sistema.

Toda modificación en la configuración deberá estar previamente autorizada, documentada y probada en un entorno de preproducción antes de su despliegue en producción, garantizando así la estabilidad y seguridad del sistema.

El sistema deberá contar con procedimientos para reaccionar ante vulnerabilidades e incidentes de seguridad, incluyendo:

- Aplicación de parches de seguridad en plazos definidos según la criticidad.
- Revisión periódica de configuraciones frente a guías de endurecimiento (hardening).
- Monitorización de cambios no autorizados.

Se deberán establecer mecanismos de control de uso de recursos (CPU, memoria, red, almacenamiento) para evitar situaciones de denegación de servicio (DoS), especialmente en entornos virtualizados como VMware vSphere 8.x.

Se deberán definir y aplicar configuraciones estandarizadas para las máquinas virtuales, incluyendo:

- Plantillas de despliegue (templates).
- Configuración de red (vSwitches, VLANs).
- Políticas de almacenamiento y snapshots.
- Parámetros de seguridad (por ejemplo, deshabilitar dispositivos innecesarios).

Toda configuración deberá estar documentada, versionada y auditada, permitiendo su trazabilidad y recuperación ante fallos o incidentes.

1.1.2.3. OP. EXP. 8. REGISTRO DE LA ACTIVIDAD

Aplicable a sistemas clasificados en categorías media y alta, se deberán implementar mecanismos que garanticen la trazabilidad completa de las acciones de los usuarios sobre los sistemas de información. Para ello, se deberán cumplir los siguientes requisitos:

Se deberá registrar quién realiza la actividad, cuándo la realiza, desde dónde y sobre qué recurso o servicio.

Los registros deben incluir tanto la actividad de los usuarios generales como, de forma especial, la de operadores y administradores, dado que estos últimos tienen capacidades para modificar configuraciones críticas y realizar tareas de mantenimiento.

Se deberán registrar tanto las acciones exitosas como los intentos fallidos de acceso o modificación, incluyendo accesos denegados, errores de autenticación y cambios en la configuración.

El nivel de detalle de los registros deberá definirse en función del análisis de riesgos del sistema, asegurando que se recoja la información necesaria para detectar, investigar y responder a incidentes de seguridad.

Para sistemas de categoría alta, será obligatorio disponer de un sistema automatizado de recolección, consolidación, correlación y análisis de registros, que permita la detección temprana de anomalías y facilite la respuesta ante incidentes.

En entornos VMware ESXi y vCenter, se deberán habilitar los mecanismos de auditoría de acceso a objetos. Dado que por defecto los registros se almacenan localmente, se deberá configurar un sistema de registro remoto para garantizar la persistencia y disponibilidad de los logs.

Se deberá establecer una auditoría específica del uso de puertos y servicios en los servidores ESXi, con el fin de detectar accesos no autorizados o comportamientos anómalos.

Se deberá configurar un almacén centralizado y seguro para los ficheros de auditoría, con capacidad suficiente para evitar sobrescrituras, y con políticas que aseguren la retención, integridad y disponibilidad de los registros durante el tiempo definido por la normativa vigente.

1.2. MEDIDAS DE PROTECCIÓN

Este conjunto de medidas cubre el espectro de aplicación de mecanismos más amplios en cuanto a dimensión. No obstante, debe tenerse en consideración que incluye una gran variedad de éstas y que son aplicables desde las más puramente procedimentales a las puramente físicas o a las de aplicación técnicas.

Solo éstas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado es de aplicación sobre las funcionalidades del propio sistema operativo servidor. La mayor parte de ellas se aplican en la red o cuando un sistema tipo portátil sale de la organización, cuestión que no se considera de aplicación a un servidor que se considera ubicado en un entorno estable dentro del centro de procesamiento de datos (CPD) que tuviera la organización.

Se considera, en este sentido, que la organización ha dispuesto todos aquellos mecanismos de control físico necesarios, con objeto de evitar el acceso a los servidores existentes por parte de personal no autorizado.

1.2.1. PROTECCIÓN DE LAS COMUNICACIONES

El conjunto de medidas orientadas a la protección de las comunicaciones tiene como objetivo proteger la información en tránsito, así como dotar a los mecanismos para la detección y bloqueo de intrusos en una red.

Aunque fundamentalmente tienen un alcance mayor en cuanto a la implementación de sistemas de electrónica de red y control perimetral, determinadas medidas pueden ser aplicables y gestionadas desde el propio servidor.

1.2.1.1. MP. COM. 3. PROTECCIÓN DE LA INTEGRIDAD Y DE LA AUTENTICIDAD

Se deberán establecer mecanismos que garanticen la autenticidad del origen y la integridad de los datos en todas las comunicaciones entre sistemas, especialmente cuando estas se realicen a través de redes no seguras o fuera del dominio de control de la organización. Para ello, se deberán cumplir los siguientes requisitos:

Antes de iniciar cualquier intercambio de datos, se deberá verificar la identidad del otro extremo del canal de comunicación mediante mecanismos criptográficos robustos, como certificados digitales emitidos por una entidad de certificación reconocida.

Se deberán implementar medidas para prevenir ataques activos (como suplantación, manipulación o repetición de mensajes). En caso de que no puedan evitarse, deberán al menos ser detectables, activando los procedimientos definidos en el plan de respuesta a incidentes.

En sistemas clasificados como de categoría media, además de los mecanismos anteriores, será obligatorio el uso de redes privadas virtuales (VPN) cuando las comunicaciones se realicen a través de redes externas a la organización. Estas VPN deberán utilizar algoritmos criptográficos acreditados por el Centro Criptológico Nacional (CCN), conforme a las guías CCN-STIC correspondientes.

En sistemas de categoría alta, se recomienda el uso de dispositivos de hardware específicos (como HSM o firewalls con capacidades VPN integradas) para el establecimiento de canales seguros, en lugar de soluciones puramente software. Se deberán emplear productos certificados y acreditados por el CCN.

Todos los mecanismos de protección deberán ser documentados, auditables y revisados periódicamente, garantizando su adecuación frente a nuevas amenazas y vulnerabilidades.

1.2.1.2. MP. COM. 4. SEPARACIÓN DE FLUJOS DE INFORMACIÓN EN LA RED

Para garantizar la seguridad de las comunicaciones y limitar la propagación de incidentes, se deberán establecer mecanismos de segregación de redes y separación de flujos de información, especialmente en entornos clasificados como categoría media y alta. Los requisitos mínimos son los siguientes:

Se deberá separar físicamente o lógicamente el tráfico de red según su naturaleza y criticidad. En particular:

- El tráfico de gestión y administración (por ejemplo, entre servidores ESXi y vCenter) deberá estar aislado del tráfico de servicio (entre máquinas virtuales).
- Se recomienda el uso de VLANs para garantizar el aislamiento lógico del tráfico.

En sistemas de categoría alta, la segregación de redes es obligatoria, permitiendo:

- Control de entrada: autenticación y autorización de usuarios que acceden a cada segmento.
- Control de salida: restricciones sobre la información que puede abandonar cada segmento.
- Supervisión reforzada en los puntos de interconexión, que deberán estar asegurados, mantenidos y monitorizados.

En entornos VMware vSphere 8.x, se deberá utilizar la infraestructura de red disponible (vSwitches estándar y distribuidos, conmutadores físicos) para implementar la segregación de redes. Se recomienda:

- Asignar interfaces de red físicas independientes para cada tipo de red (gestión, almacenamiento, servicio, etc.).
- Asociar las interfaces virtuales de las máquinas y del host ESXi a los vSwitches correspondientes, garantizando el aislamiento.

Se deberán establecer conexiones seguras hacia los sistemas de almacenamiento virtualizado, utilizando protocolos cifrados y autenticación robusta.

Se recomienda desplegar dispositivos de filtrado de tráfico (como firewalls virtuales o físicos) para proteger:

- Los interfaces de gestión del entorno VMware.
- El tráfico de servicio entre máquinas virtuales y hacia los servidores ESXi.

Las políticas de filtrado deberán permitir únicamente el tráfico mínimo necesario, en función de las funcionalidades habilitadas en el entorno, aplicando el principio de mínimo privilegio.

1.2.2. PROTECCIÓN DE LA INFORMACIÓN

1.2.2.1. SEGURIDAD EN MÁQUINAS VIRTUALES

Tal y como se había expuesto en el documento principal de la presente guía, en las máquinas virtuales que se gestionen desde la infraestructura de VMware vSphere 8.x deben haber sido aplicadas las guías acordes al sistema operativo y tipo de rol que desempeñan. Por tanto y en este caso, le corresponderá la guía adecuada a un entorno de redes clasificadas. Por ejemplo, en caso de instalar una máquina virtual con sistema operativo Windows Server 2022, le sería de aplicación la guía CCN-STIC-570A23.

La aplicación de seguridad llevaría implícito el principio de mínima funcionalidad y exposición, deshabilitando, por tanto, aquellos elementos de los cuales no se va a hacer uso según el propósito de la máquina virtual.

En un entorno de redes clasificadas se debe hacer uso de UEFI secure boot siempre y cuando sea posible su implementación. UEFI secure boot es un estándar de seguridad que ayuda a

controlar que las máquinas virtuales solamente arranquen con software confiable, en el caso de máquinas físicas por el fabricante. En el caso de las máquinas virtuales es posible hacer uso de UEFI secure boot como si de una máquina física se tratara.

En un sistema operativo que lo soporta, cada parte del arranque está firmada, esto incluye la secuencia inicial de arranque, el kernel y los drivers del sistema operativo. Esto se realiza a través de certificados emitidos por Microsoft y VMware.

El resultado de habilitar el uso de UEFI secure boot es que cuando la máquina arranca solo se ejecutarán los componentes que posean una firma válida. El arranque se detendría con error en caso de que alguno de los componentes no mostrara firma o ésta no fuera válida.

1.2.2.1.1. MP. INFO. 3. FIRMA ELECTRÓNICA

En sistemas clasificados como de categoría alta, el ENS establece la obligatoriedad del cifrado de la información durante su almacenamiento, así como la garantía de la autenticidad e integridad de los datos mediante mecanismos como la firma electrónica.

Los requisitos mínimos son los siguientes:

Se deberá garantizar la confidencialidad, integridad y autenticidad de la información almacenada mediante el uso de algoritmos criptográficos acreditados por el Centro Criptológico Nacional (CCN), conforme a las guías técnicas CCN-STIC.

En entornos VMware vSphere 8.x, se deberán habilitar las funcionalidades de cifrado de discos virtuales para las máquinas virtuales que gestionen información sensible. Este cifrado:

- Se configura desde el cliente vSphere.
- Permite seleccionar qué discos serán cifrados.
- Requiere que la máquina virtual esté previamente preparada para soportar cifrado.

Se deberá tener en cuenta que el uso de cifrado incrementa los requisitos de almacenamiento, por lo que se recomienda aprovisionar el doble de capacidad para garantizar el rendimiento y la disponibilidad.

Los archivos de configuración de las máquinas virtuales, como los ".VMDK" y ".VMX", no deben ser modificados manualmente una vez habilitado el cifrado, ya que contienen metadatos críticos. Cualquier alteración podría dejar la máquina virtual inoperativa.

En los casos en que se requiera firma electrónica, esta deberá realizarse mediante certificados digitales emitidos por una entidad de certificación reconocida, y utilizando dispositivos seguros de creación de firma (por ejemplo, tarjetas criptográficas o HSM).

Todos los mecanismos de cifrado y firma deberán estar documentados, auditados y revisados periódicamente, y su uso deberá integrarse en los procedimientos de gestión de claves y recuperación ante desastres.

1.2.2.2. MP. INFO. 6. COPIAS DE SEGURIDAD

A partir de la categoría básica del ENS, se establece la obligatoriedad de realizar copias de seguridad que permitan la recuperación de datos ante pérdidas accidentales o intencionadas. Estas copias deberán cumplir con los siguientes requisitos:

Las copias de seguridad deberán garantizar el mismo nivel de seguridad que los datos originales en cuanto a:

- Confidencialidad: mediante el uso de cifrado con algoritmos acreditados por el Centro Criptológico Nacional (CCN).
- Integridad: asegurando que los datos no han sido alterados.
- Autenticidad: mediante mecanismos de firma o control de acceso.
- Trazabilidad: registrando quién, cuándo y cómo se realiza cada copia.

Las copias deberán incluir:

- Información de trabajo de la organización.
- Aplicaciones en explotación, incluyendo sistemas operativos y configuraciones.
- Datos de configuración de servicios, aplicaciones y equipos.
- Claves criptográficas utilizadas para proteger la información.

Se deberá establecer una política de retención y rotación de copias, que defina:

- Frecuencia de las copias (diarias, semanales, mensuales).
- Tiempo de conservación.
- Procedimientos de restauración y pruebas periódicas de recuperación.

En entornos VMware vSphere, se deberán utilizar las funcionalidades nativas para realizar copias de seguridad de máquinas virtuales completas, incluyendo sus discos, configuraciones y estado operativo. Estas copias:

- Deberán almacenarse en repositorios seguros y separados del entorno de producción.
- Podrán integrarse con soluciones de backup externas compatibles con vSphere.

Se recomienda que las copias estén cifradas, especialmente en sistemas de categoría media y alta, y que se almacenen en ubicaciones geográficamente separadas para garantizar la resiliencia ante desastres.

Toda la gestión de copias deberá estar documentada, auditada y revisada periódicamente, como parte del plan de continuidad de la actividad.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN VMWARE VSPHERE 8.X

A continuación, se establece un cuadro resumen con las diferentes medidas a aplicar, así como los mecanismos que se implementarán para su aplicación. Dichas implementaciones podrán provenir de la revisión de otras guías de seguridad de la serie CCN-STIC-500, de la serie CCN-STIC-800 o bien la aplicación de políticas de seguridad a nivel de dominio o bien localmente.

Control	Medida	Mecanismo de aplicación
OP. ACC. 2	Requisitos de acceso	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización.
OP. ACC. 3	Segregación de funciones y tareas	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
OP. ACC. 4	Proceso de gestión de derechos de acceso	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización.
OP. ACC. 5	Mecanismo de autenticación (usuarios externos)	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización.
OP. ACC. 6	Mecanismo de autenticación (usuarios de la organización)	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización.
OP. EXP. 2	Configuración de seguridad	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización.
OP. EXP. 3	Gestión de la configuración de seguridad	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización.
OP. EXP. 8	Registro de la actividad	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización.
MP. COM. 3	Protección de la integridad y de la autenticidad	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización
MP. COM. 4	Separación de flujos de información en la red	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización
MP. INFO. 3	Firma electrónica	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización
MP. INFO. 6	Copias de seguridad	Revisión e implementación de guía CCN-STIC-442, adaptándolos a la organización

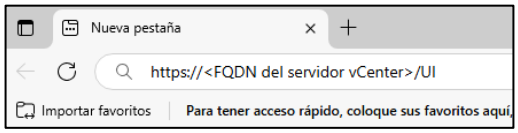
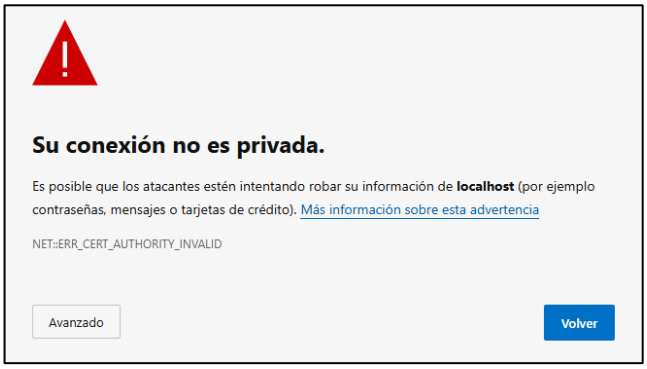
ANEXO A.2. CATEGORÍA BÁSICA

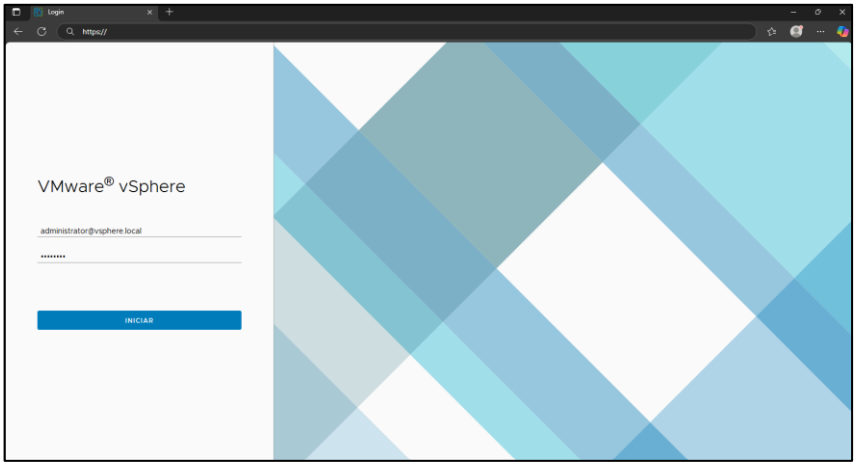
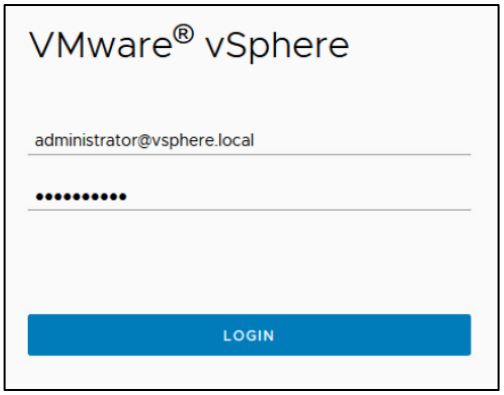
ANEXO A.2.1. IMPLEMENTACIÓN DE SEGURIDAD EN VMWARE VSPHERE 8.X SOBRE SERVIDORES QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

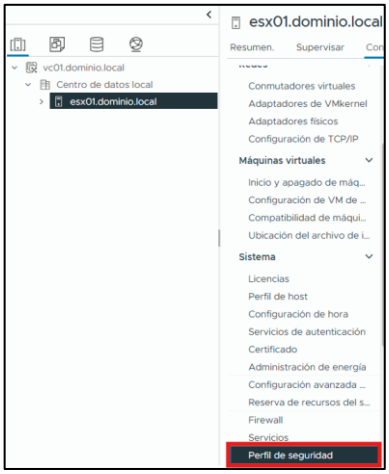
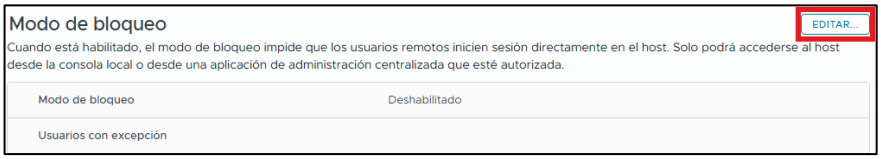
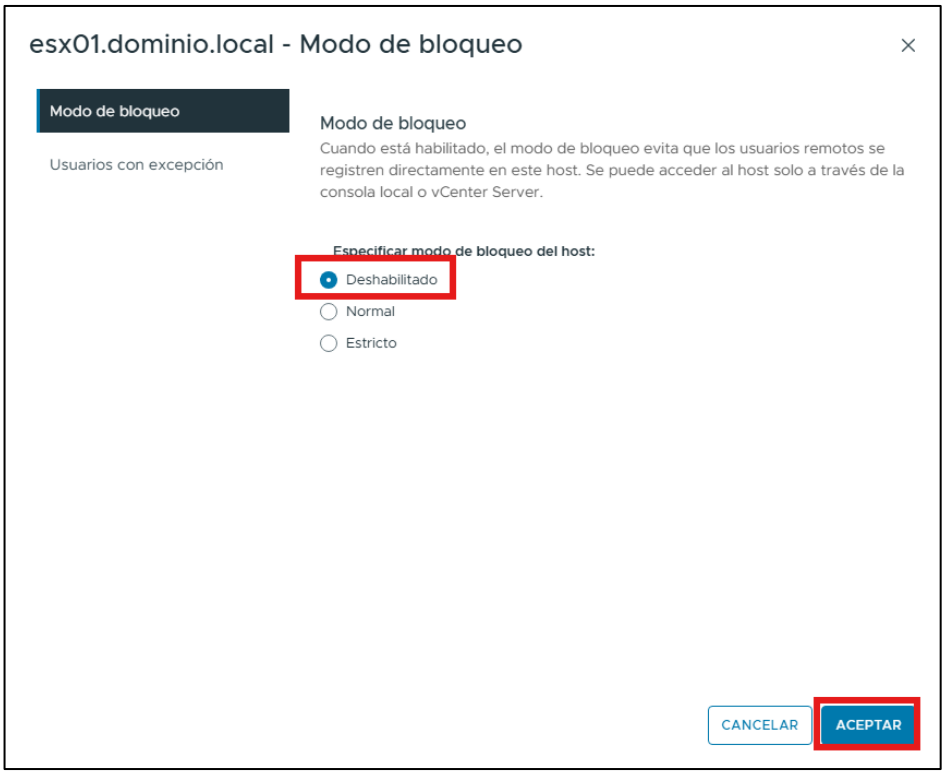
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se emplee la solución VMware vSphere 8.x con una categorización de seguridad básica según los criterios del Esquema Nacional de Seguridad.

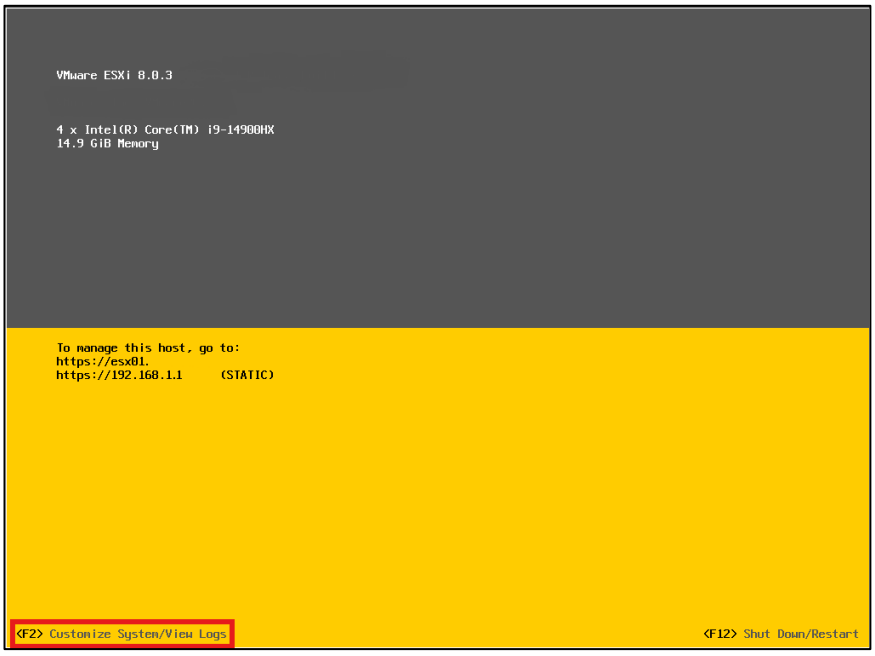
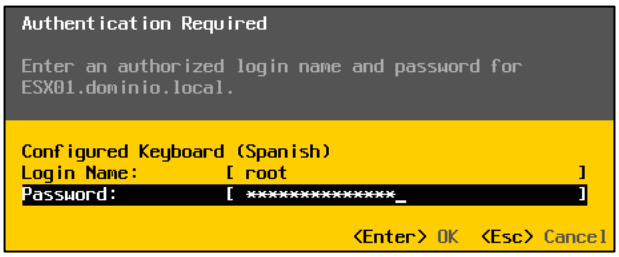
Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo II del RD 311/2022. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, deberá realizar las implementaciones según se referencian en el presente anexo.

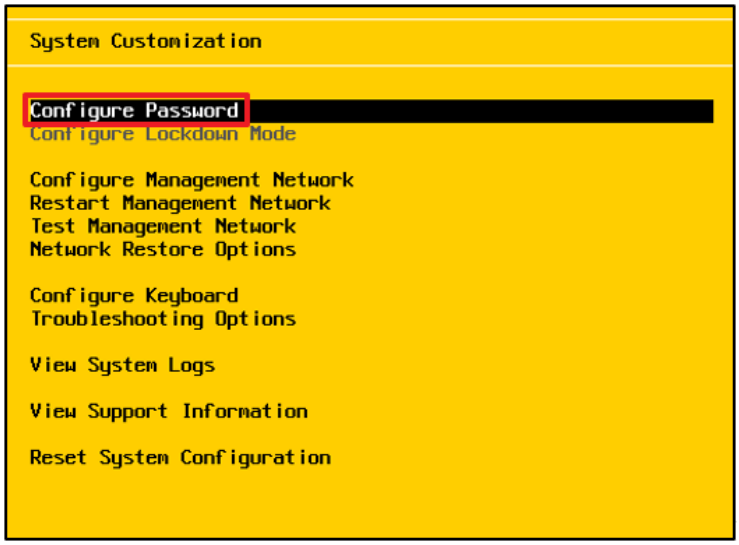
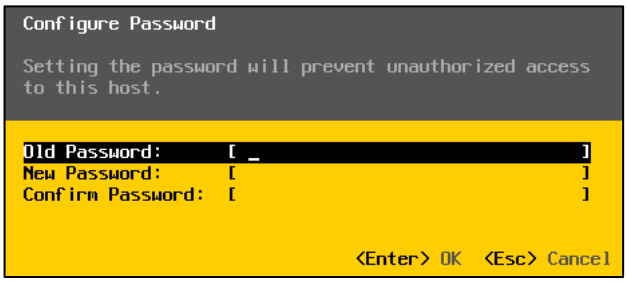
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

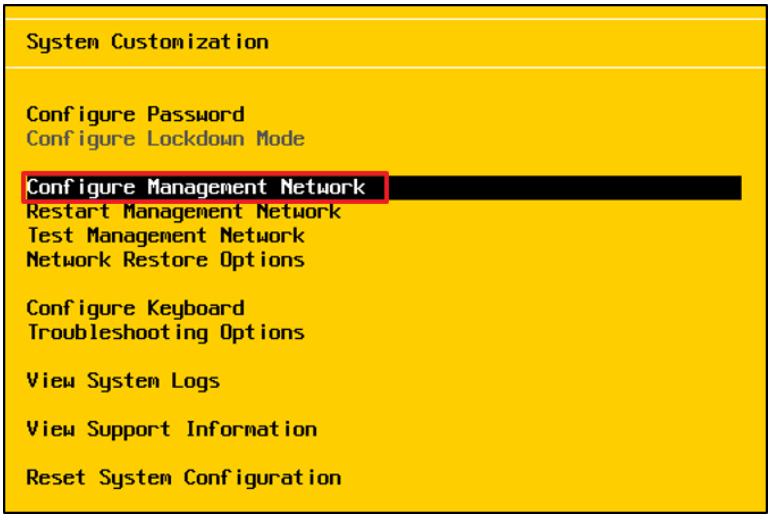
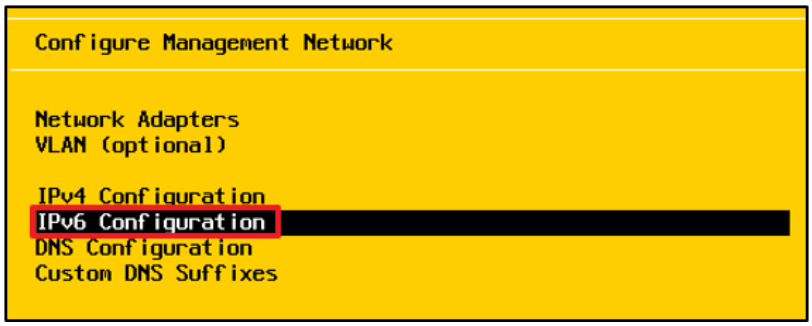
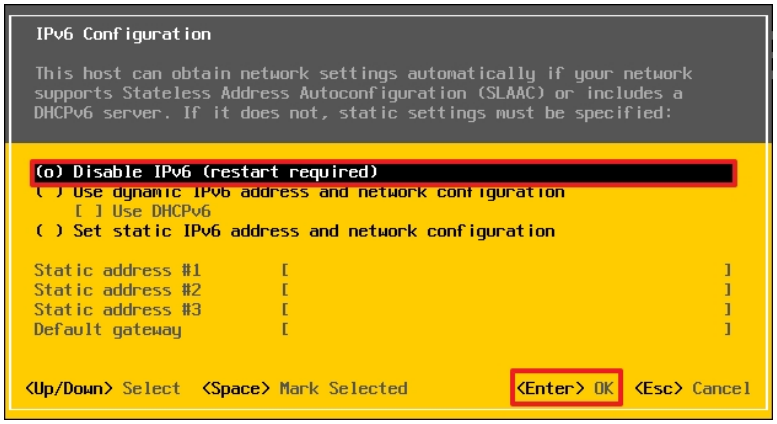
Paso	Descripción
1.	Inicie sesión directamente en el host ESXi utilizando el ESXi Host Client a través de su navegador web. Para ello, introduzca la siguiente URL: " https://<IP-o-FQDN-del-host-ESXi>/UI". 
2.	En caso de que aparezca una advertencia en el navegador que indica que el sitio no es seguro ignórela. Esto es debido a que se está empleando un certificado auto firmado. Pulse sobre la opción de Avanzado, Continuar a localhost (no seguro) ir al sitio web.  **Nota:** La captura y la opción a escoger podrían ser diferentes según el navegador que se esté empleando. En el ejemplo se ha utilizado Microsoft Edge.

Paso	Descripción
3.	En vSphere 8, el acceso al entorno se realiza exclusivamente a través del vSphere Client (HTML5), ya que el cliente basado en Flash ha sido descontinuado. 
4.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”.  **Nota:** Según los métodos de autenticación empleados, la pantalla podría diferir de la captura mostrada.
5.	En el menú de la izquierda, pulse sobre el icono que corresponde a “Host y clústeres”. 

Paso	Descripción
6.	Sitúese sobre el objeto “<FQDN del servidor ESXi>” sobre el que quiere aplicar la seguridad y en la pestaña “Configurar”, seleccione “Perfil de seguridad”. 
7.	En “Modo de Bloqueo” seleccione “Editar”. 
8.	En la ventana emergente, seleccione el modo “Deshabilitado” y pulse “ACEPTAR” para continuar.  **Nota:** En caso de que el modo de bloqueo figure como “Deshabilitado” puede obviar este paso.

Paso	Descripción
9.	Los siguientes pasos descritos a continuación se realizarán en el servidor ESXi para terminar de configurar el hipervisor de forma local. **Nota:** Los pasos que se detallan a continuación, se deberán realizar en cada host ESXi que se implemente en la infraestructura de VMware vSphere 8.x que se está implementando.
10.	Es recomendable establecer una contraseña para el BIOS del propio servidor de ESXi de modo que se eviten posibles ataques basados en el acceso al equipo, de forma física, ya que se puede manipular la secuencia de arranque y los elementos de configuración del propio BIOS del servidor. **Nota:** En esta guía no se explica cómo hacerlo ya que el modo de establecer una contraseña en el BIOS del servidor variará dependiendo del fabricante y modelo de este.
11.	Así mismo, sería conveniente establecer, a través del BIOS, la secuencia de arranque y la lista de dispositivos de arranque permitidos. En caso de no establecer dicha configuración, sería posible arrancar desde un medio extraíble no autorizado pudiendo acceder a la información del servidor.
12.	En el servidor de ESXi, pulse “F2” para realizar las tareas de configuración inicial. 
13.	El sistema solicitará credenciales. Introduzca la contraseña y pulse “Enter” para continuar. 

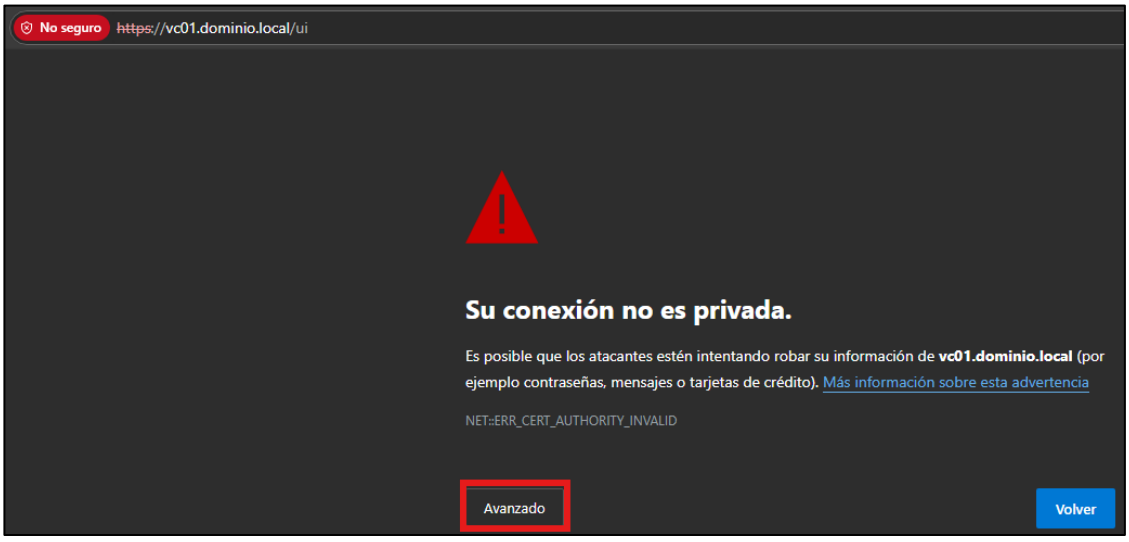
Paso	Descripción
14.	En caso de que la contraseña suministrada durante la instalación no cumpliera con los requisitos de complejidad necesarios, seleccione “Configure Password” situándose sobre él mediante las teclas de dirección y presione “Enter”. 
15.	Introduzca en el primer campo la contraseña suministrada durante la instalación y, a continuación, introduzca dos veces la contraseña deseada. Pulse “Enter” para validar la configuración y salir.  **Nota:** Recuerde que en esta categoría el nivel de complejidad y longitud de la contraseña deberá cumplir con los siguientes requisitos: - Mínimo 10 caracteres - Al menos 1 mayúscula - Al menos 1 minúscula - Al menos 1 carácter especial - Al menos 1 número

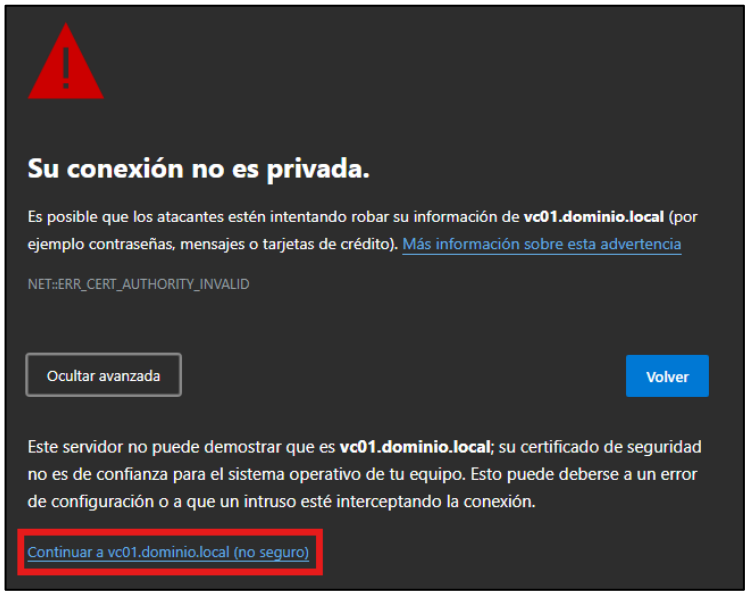
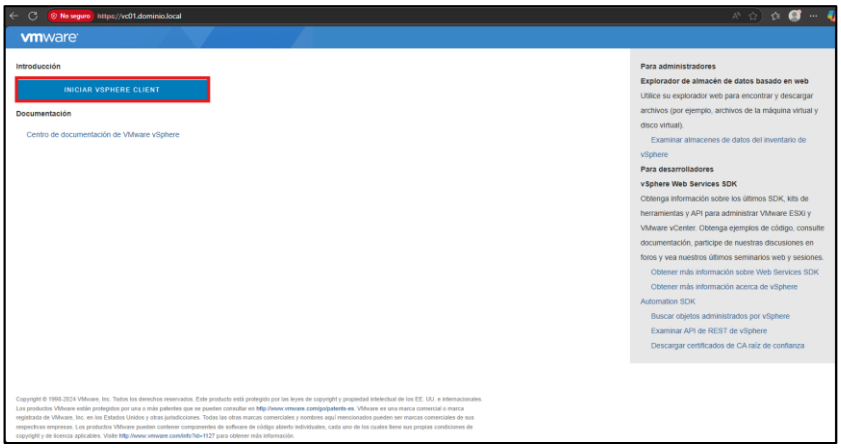
Paso	Descripción
16.	Seleccione “Configure Management Network” para deshabilitar TCP/IPv6. Para ello, sitúese sobre la opción mediante las teclas de dirección y pulse “Enter”.  **Nota:** Esta guía paso a paso asume que se está aplicando la seguridad sobre una infraestructura de VMware vSphere 8.x previamente operativa, por lo que no tendrán en cuenta parámetros de configuración e implementación y se ocupará de modificar las configuraciones relativas a la seguridad del sistema para alcanzar el nivel de seguridad deseado.
17.	Seleccione “IPv6 Configuration” situándose sobre la opción, mediante las teclas de dirección, y presione “Enter”. 
18.	Sitúese sobre “Disable IPv6 (restart required)” y utilice la barra espaciadora para seleccionarlo. Pulse “Enter” para guardar los cambios. 

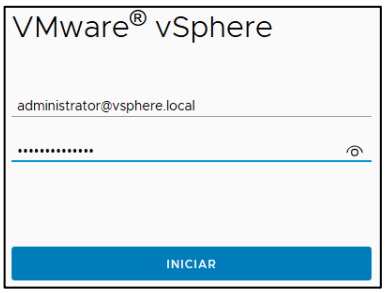
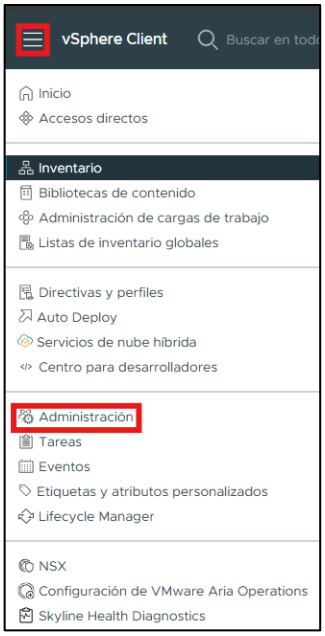
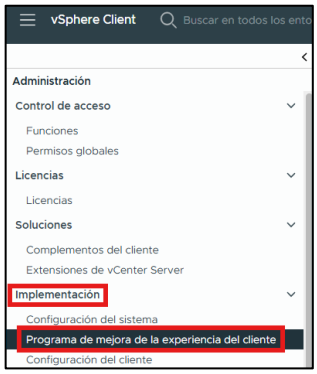
Paso	Descripción
19.	Pulse “Esc” para salir de la configuración de red.
20.	Ante la solicitud de aplicar los cambios y reiniciar el host seleccione "Yes" pulsando la tecla "Y". El servidor se reiniciará. 

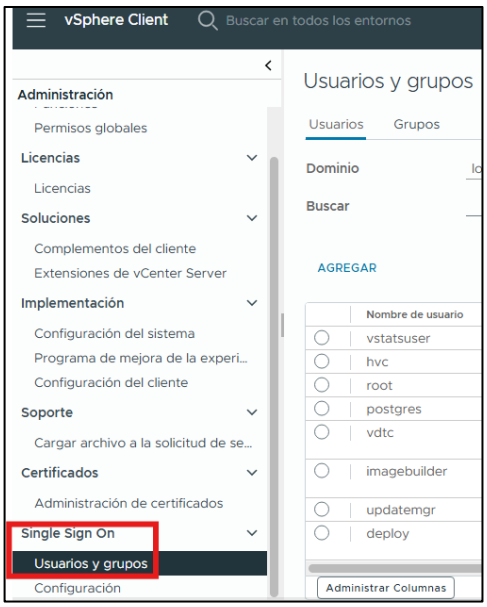
3. CONFIGURACIÓN DE SEGURIDAD EN VCENTER

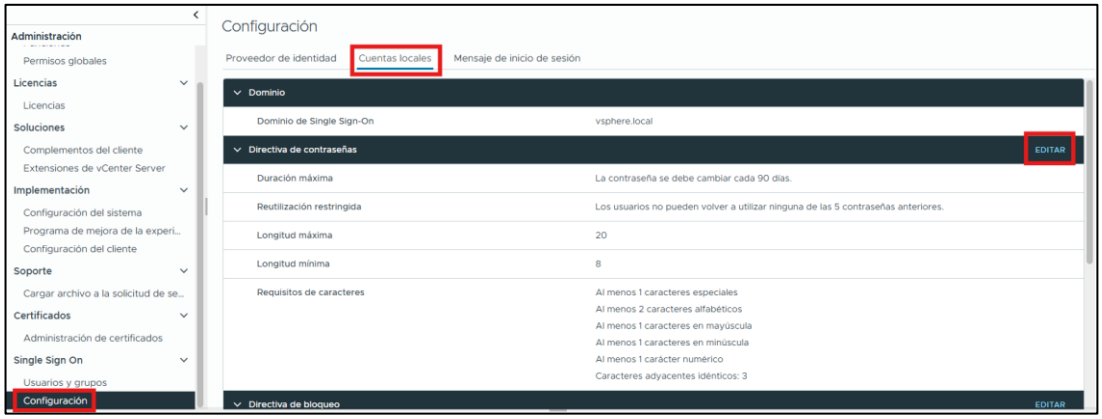
El resto de las configuraciones de seguridad que aplicarán al servidor de ESXi se realizarán a través del servidor de vCenter. Previamente se va a aplicar la configuración de seguridad de los propios servidores de vCenter. Deberá realizar los siguientes pasos en cada servidor de vCenter que pertenezca a la infraestructura.

Paso	Descripción
21.	Inicie sesión, a través del vSphere client mediante html5, en el servidor de vCenter. Para ello, en su navegador, introduzca la url “https://<FQDN del servidor vCenter>/UI”. Si el navegador muestra una advertencia indicando que el sitio no es seguro, puede ignorarla. Esto se debe a que se está utilizando un certificado autofirmado. Haga clic en la opción "Avanzado". 

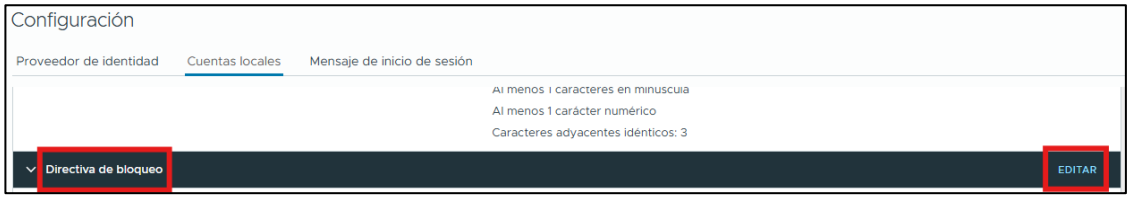
Paso	Descripción
22.	Haga clic en la opción “Continuar al sitio”  **Nota:** La apariencia de la advertencia de seguridad y las opciones disponibles pueden variar según el navegador utilizado. En este ejemplo se ha utilizado Microsoft Edge.
23.	El cliente basado en Flash (vSphere Web Client - Flex) ha sido retirado oficialmente y ya no es compatible en vSphere 8. Utilizaremos exclusivamente el vSphere Client (HTML5) para acceder y gestionar el entorno. 

Paso	Descripción
24.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”.  **Nota:** Según los métodos de autenticación empleados, la pantalla podría diferir de la captura mostrada.
25.	Pulse sobre el menú principal (☰) para acceder a la configuración del servidor de vCenter y seleccione “Administración” en el menú contextual que se ha desplegado. 
26.	Pulse sobre “Implementación → Programa de mejora de la experiencia del cliente”. 

Paso	Descripción
27.	El estado correcto debe ser “No Unido”. En caso de que el estado sea “Unido”, pulse sobre “Abandonar” en la zona inferior de la pantalla central. 
28.	Confirme pulsando sobre “Abandonar el programa”. 
29.	En el apartado “SingleSignOn” podrá añadir los “Usuarios y grupos que tendrán acceso al servicio de VMware vSphere 8.x y los privilegios que se les otorgarán.  **Nota:** Adapte los usuarios, grupos y permisos a las necesidades de la organización y rigiéndose por los criterios indicados en la presente guía.

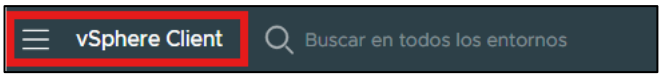
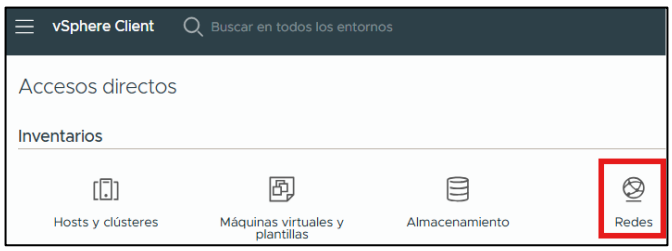
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>30.</td><td>Así mismo, en el apartado “SingleSignOn”, pulse sobre “Configuración” y en la pestaña “Cuentas locales”, pulse sobre “Directiva de contraseñas” y sobre “Editar”.
 
</td></tr>
<tr><td>31.</td><td>En la ventana emergente, establezca los siguientes parámetros y pulse “Guardar”.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Duración máxima</td><td>Hay que cambiar la contraseña cada “90” días</td></tr>
<tr><td>Reutilización restringida</td><td>Los usuarios no pueden reutilizar ninguna de las “24” contraseñas anteriores</td></tr>
<tr><td>Longitud mínima</td><td>“10”</td></tr>
<tr><td colspan="2">Al menos “1” caracteres especiales</td></tr>
<tr><td colspan="2">Al menos “1” caracteres en mayúsculas</td></tr>
<tr><td colspan="2">Al menos “1” caracteres en minúsculas</td></tr>
<tr><td colspan="2">Al menos “1” caracteres numéricos</td></tr>
</table>

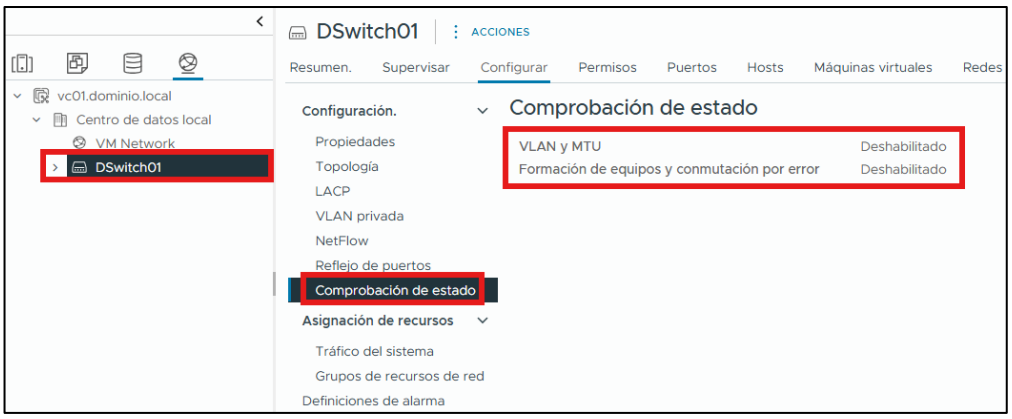

Nota: Estos parámetros corresponden a la complejidad mínima a establecer, el resto de las configuraciones refuerzan dicha complejidad. Mantenerlos con los valores indicados es una acción correcta de cara a mejorar la seguridad.</td></tr>
</table>

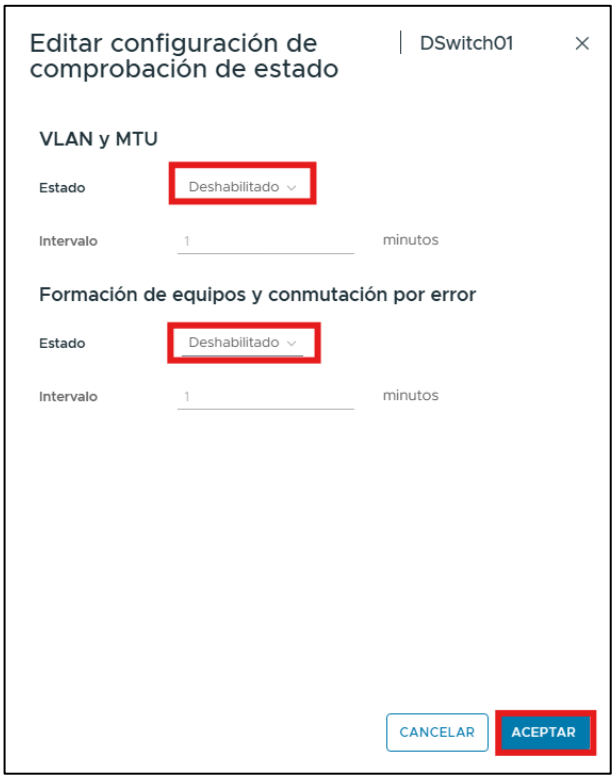
Paso	Descripción
32.	Sitúese sobre “Directiva de bloqueo” y pulse sobre “Editar”. 
33.	En la ventana emergente, establezca los siguientes parámetros y pulse “Guardar”. – Cantidad máxima de intentos fallidos de inicio de sesión: “8”. – Intervalo de tiempo entre errores: 1800 segundos. – Tiempo de desbloqueo: 1800 segundos. 

3.1. CONFIGURACIÓN EN CONMUTADORES VIRTUALES DISTRIBUIDOS

Las configuraciones descritas a continuación son a nivel de conmutadores virtuales distribuidos. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los conmutadores virtuales distribuidos existentes en el servicio de vCenter.

Paso	Descripción
34.	Haga clic sobre el icono “vSphere Client” para ir al menú principal. 
35.	Seleccione el icono correspondiente a “Redes”. 

Paso	Descripción
36.	Sitúese sobre cada conmutador distribuido y en la pestaña “Configurar” pulse sobre el elemento “Comprobación de estado”. A continuación, en caso de que esté habilitado alguno de estos dos elementos, deberá deshabilitarlos: – VLAN y MTU. – Formación de equipos y conmutación por error.  **Nota:** Estas opciones solamente deberían ser habilitadas en momentos de resolución de problemas y de forma temporal.
37.	Para ello, pulse sobre “Editar”. 

Paso	Descripción
38.	En la ventana emergente, modifique los campos de estado a “Deshabilitado” y pulse “Aceptar”. 

3.1.1. CONFIGURACIÓN EN GRUPOS DE PUERTOS

Las configuraciones descritas a continuación son a nivel de grupos de puertos. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los grupos de puertos existentes en los distintos conmutadores presentes en el servicio de vCenter.

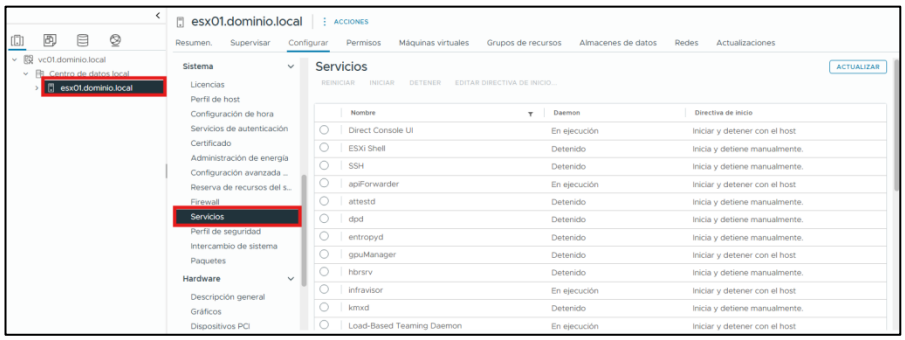
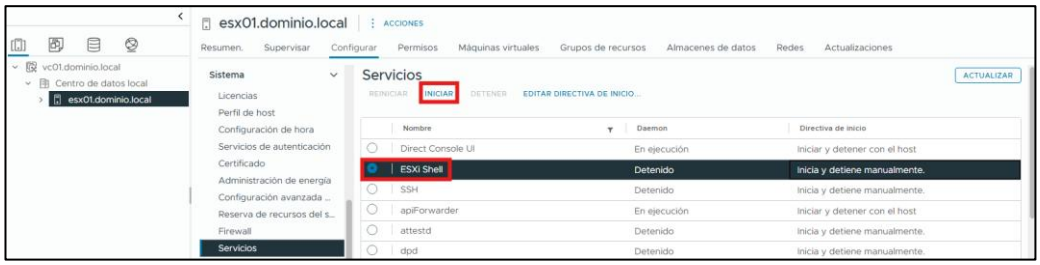
Paso	Descripción
39.	En el menú de la izquierda, seleccione el icono correspondiente a “Redes”. 

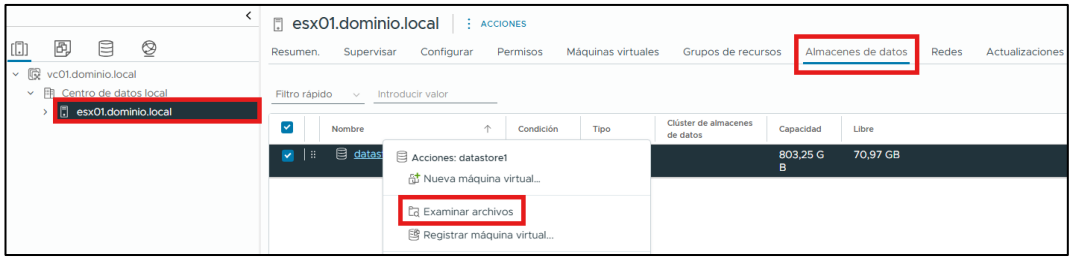
Paso	Descripción
40.	Sitúese sobre cada grupo de puertos (que se encontrarán dentro de la rama de cada conmutador virtual) y en la pestaña “Configurar”, seleccione “Directivas” y compruebe que las siguientes directivas de seguridad tienen el valor “Rechazar” y si no es así se deberá modificar el valor de las directivas: – Modo promiscuo – Cambios de dirección MAC – Transmisiones falsificadas 
41.	Para modificar las directivas pulse sobre “Editar”. 
42.	En la ventana emergente pulse sobre “Seguridad”, modifique las directivas deseadas y pulse “ACEPTAR” para validar la configuración. 

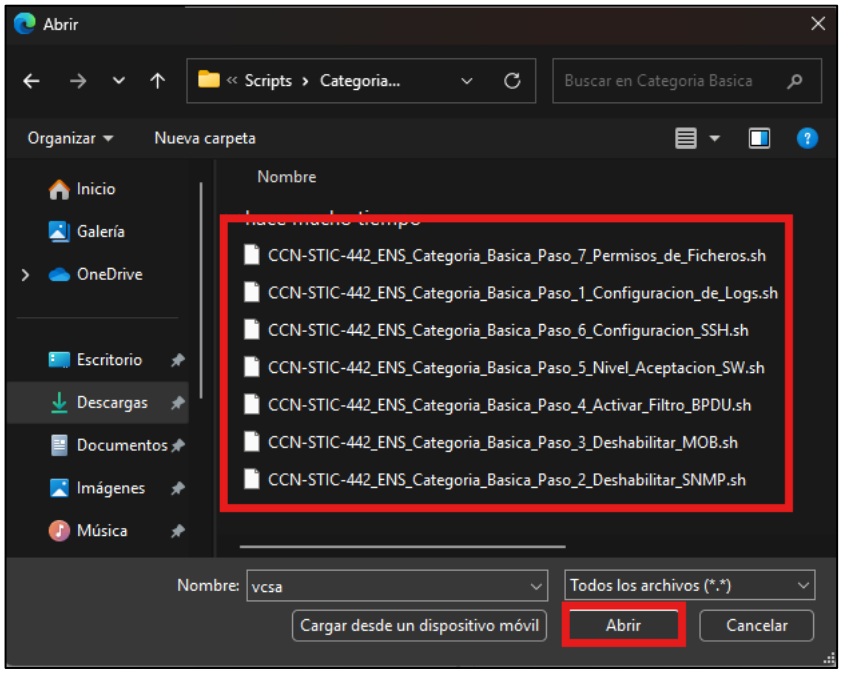
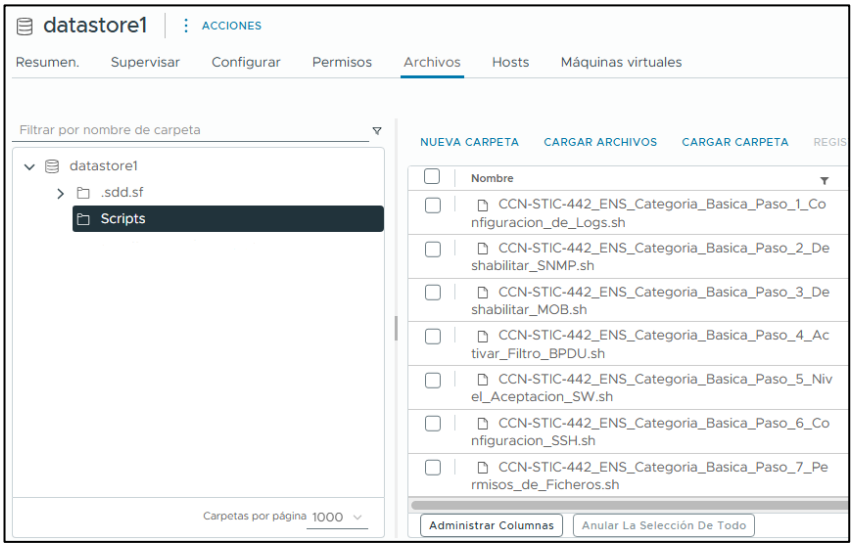
3.2. CONFIGURACIÓN DE SEGURIDAD EN SERVIDORES ESXI

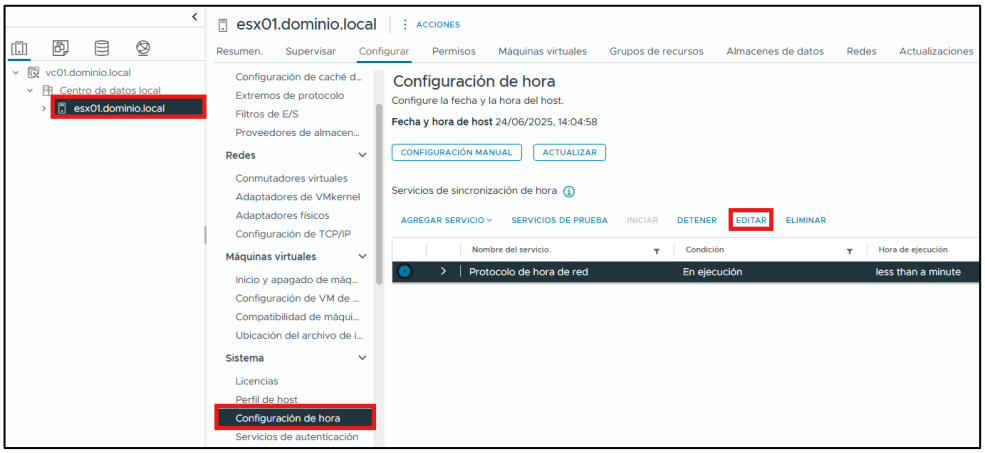
Los pasos descritos a continuación se realizan a nivel de servidor ESXi y deberán ser aplicados en cada uno de los host ESXi que se añadan al servidor de vCenter. Existe la posibilidad de establecer perfiles de host para definir las configuraciones, a modo de plantilla, de modo que se homogenice y automatice el proceso de implementación de los servidores de ESXi.

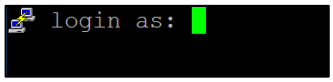
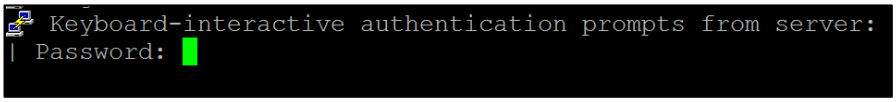
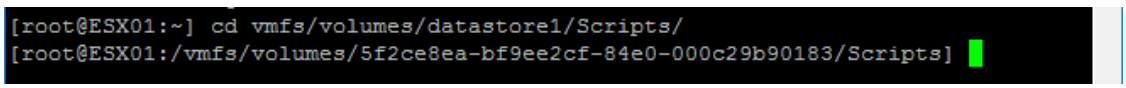
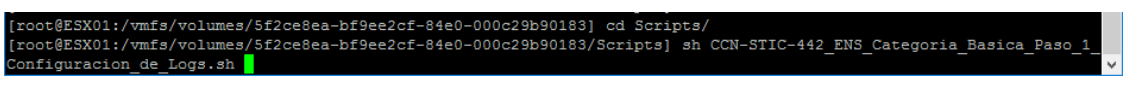
Muchos de los pasos se continúan realizando a través del cliente de vSphere pero la ejecución de scripts se realizará mediante una conexión directa por SSH a la consola ESXi Shell del host al que queremos aplicarle seguridad. Por tanto, será necesario activar los servicios de SSH y ESXi Shell en el host ESXi y, una vez completadas las configuraciones, se volverán a deshabilitar ambos servicios.

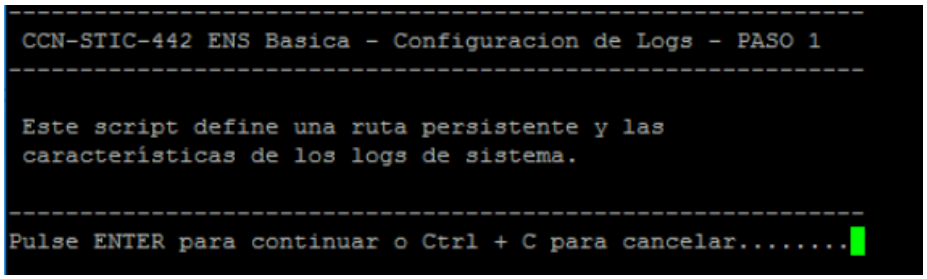
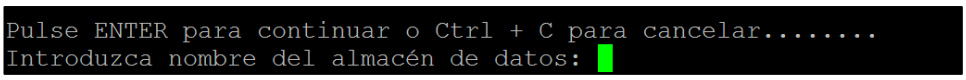
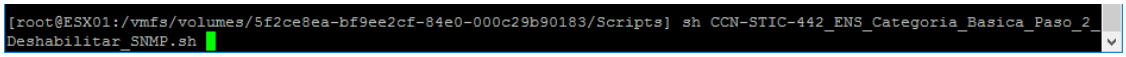
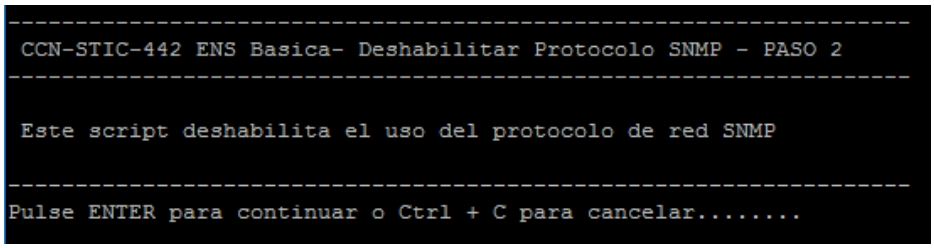
Paso	Descripción
43.	En el menú de la izquierda, pulse sobre el icono que corresponde a “Host y clústeres”. 
44.	Sitúese sobre el objeto “<FQDN del servidor ESXi>” sobre el que quiere aplicar la seguridad y en la pestaña “Configurar”, seleccione “Servicios”. 
45.	Sitúese sobre el servicio “ESX Shell” y pulse el botón “Iniciar”.  **Nota:** Si el servicio ya se encuentra activo no será necesario realizar ninguna acción.
46.	Realice la misma operación con el servicio “SSH”.  **Nota:** Si el servicio ya se encuentra activo no será necesario realizar ninguna acción.

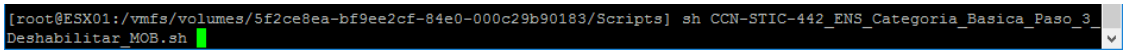
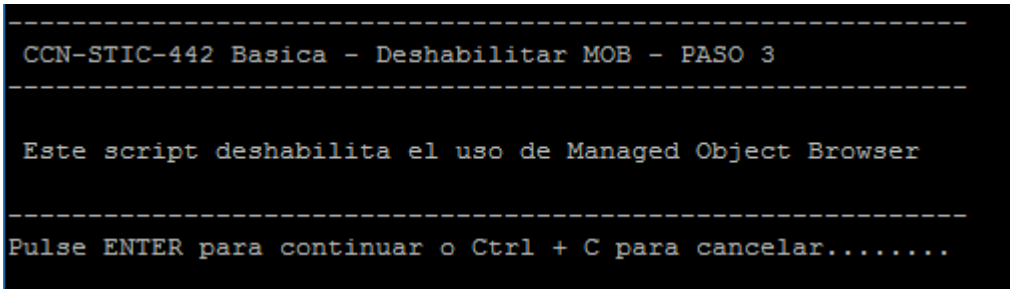
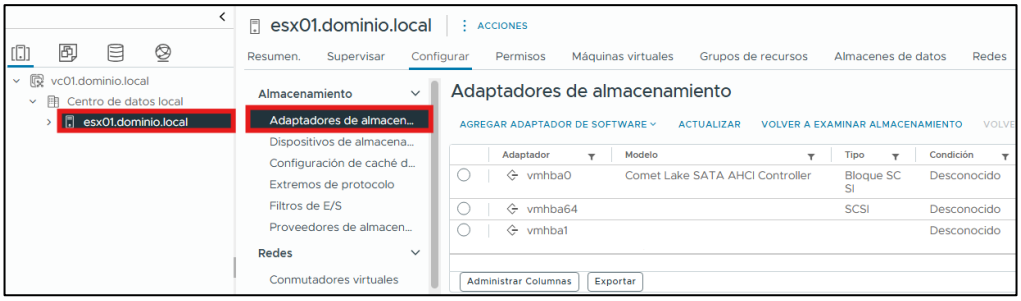
Paso	Descripción
47.	Sitúese, de nuevo, sobre el objeto <FQDN del Servidor ESXi> y en la pestaña “Almacenes de datos”, seleccione, con el botón derecho del ratón, el almacén donde alojará los Scripts de configuración de seguridad de la presente guía y pulse sobre “Examinar archivos”.  **Nota:** En el ejemplo se ha utilizado el almacén que se ha creado por defecto al añadir el host a vCenter. Adapte la configuración a las necesidades de su entorno.
48.	Seleccione “Nueva Carpeta” para crear la carpeta que contendrá los Scripts. 
49.	Establezca el nombre “Scripts” a la carpeta y pulse “Aceptar”. 
50.	Haga clic sobre la carpeta “Scripts” recién creada y seleccione “Cargar archivos”. 

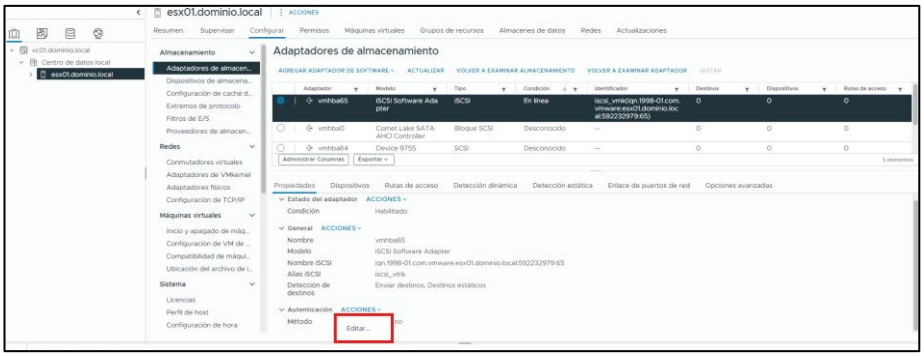
Paso	Descripción
51.	Localice los scripts que se aplican en este anexo, selecciónelos todos y pulse “Abrir”. 
52.	Los scripts quedarán almacenados en el almacén de datos. 
53.	El siguiente paso consiste en configurar el servidor para que sincronice la hora con la del servidor NTP. De nuevo, a través del navegador, pulse sobre el icono correspondiente a “Hosts y clústeres”. 

Paso	Descripción
54.	Sitúese sobre el objeto <FQDN del Servidor ESXi> y en la pestaña “Configurar”, seleccione “Configuración de hora”, “Protocolo de hora de red” y pulse “Editar”. 
55.	Introduzca la dirección o direcciones IP del servidor o servidores NTP que quiera utilizar para la sincronización. Pulse “Aceptar” para guardar la configuración.  **Nota:** Deberá adaptar las configuraciones a las necesidades del entorno y, en caso de utilizar el protocolo NTP, se deberán habilitar las configuraciones que lo permitan. No cierre el navegador y manténgalo en segundo plano mientras realiza los pasos siguientes.

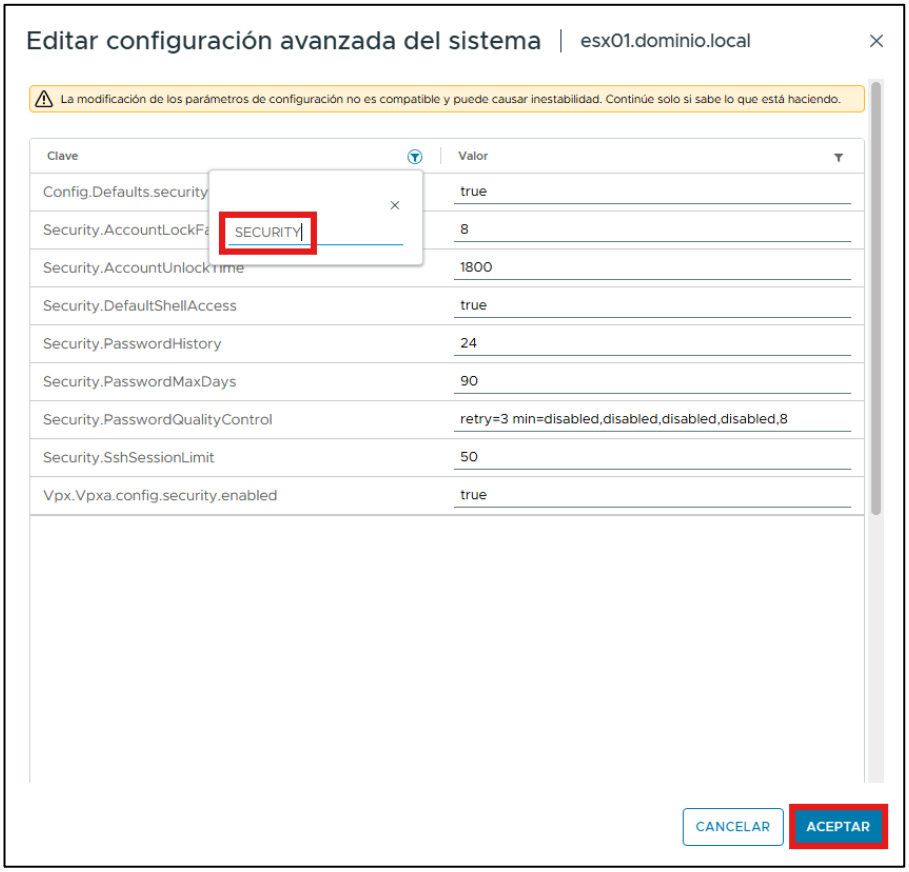
Paso	Descripción
56.	Para los siguientes pasos, deberá conectarse al host a través de un cliente SSH. Se le solicitarán credenciales de acceso. Introduzca un usuario con privilegios de administración sobre este host ESXi.  **Nota:** para establecer una conexión SSH hacia el servidor ESXi, se deberá permitir el tráfico correspondiente. El cliente utiliza, por defecto, el puerto 22 para realizar la conexión. Deberá adaptar estos pasos a las necesidades de su entorno. Al no estar utilizando certificados confiables, es posible que el cliente SSH muestre una advertencia. Puede continuar la conexión.
57.	Introduzca la contraseña definida para dicho usuario. 
58.	En este momento y si fuera posible, sería recomendable aplicar las actualizaciones sobre el servidor de ESXi. Para llevar a cabo esta acción y teniendo en cuenta que el entorno puede o no disponer de conectividad a internet, se puede hacer uso de un repositorio centralizado por medio de vSphere Update Manager, un plugin que puede ser añadido a la configuración de vCenter Server. **Nota:** Una vez las actualizaciones son accesibles, los comandos a utilizar, a través del CLI de ESXi, serían los siguientes: - **# esxcli software profile get** (para consultar el estado de las actualizaciones) - **# esxcli software vib get** (para consultar el estado de las actualizaciones) - **# esxcli software profile update** (para aplicar las actualizaciones) - **# esxcli software vib update** (para aplicar las actualizaciones)
59.	Acceda a la ruta del almacén de datos que ha configurado en los pasos anteriores a través de la siguiente línea de comandos: **# cd /vmfs/volumes/<almacén de datos>/Scripts**  **Nota:** La ruta seleccionada es la ruta en la que se almacenan por defecto los almacenes de datos. Deberá adaptar estos pasos a las necesidades de su entorno.
60.	A continuación, se modificarán los parámetros relativos a los registros de auditoría o ficheros log. Ejecute el script "CCN-STIC-442_ENS_Categoria_Basica _Paso_1_Configuracion_de_Logs.sh" mediante el siguiente comando y pulse "Enter". **# sh CCN-STIC-442_ENS_Categoria_Basica _Paso_1_Configuracion_de_Logs.sh** 

Paso	Descripción
61.	Pulse “Enter”, de nuevo, para continuar. 
62.	El sistema le solicitará el nombre del almacén de datos donde se encuentra la carpeta Scripts. Introduzca el nombre del almacén respetando mayúsculas, minúsculas, puntuación, espacios, etc. Pulse “Enter” para continuar.  **Nota:** En el ejemplo, el almacén de datos se llama “datastore1”.
63.	Es recomendable también el uso de un servidor de logs externo al que se exporten los logs del servidor. Para establecer dicha configuración, a través del vSphere Client, puede situarse en el servidor ESXi y seleccionar “Configuración → Configuración avanzada”. Los campos a modificar son los siguientes: – "Syslog.global.logHost" → “<Nombre del Host>”. – "Syslog.global.logDirUnique" → “True”.
64.	Ejecute el script “CCN-STIC-442_ENS_Categoria_Basica_Paso_2_Deshabilitar_SNMP.sh” mediante el siguiente comando y pulse “Enter” para continuar. **# sh CCN-STIC-442_ENS_Categoria_Basica_Paso_2_Deshabilitar_SNMP.sh**  **Nota:** En caso de que se haga uso del protocolo SNMP, no se debería ejecutar este paso. En su lugar, se debería ejecutar lo siguiente para establecer la seguridad adecuada en el uso del protocolo y evitar que elementos externos puedan extraer información de datos SNMP: - **# esxcli conn_options system snmp set --communities [COMMUNITY]** - **# esxcli conn_options system snmp set --targets [TARGET]@[PORT]/[COMMUNITY]** - **# esxcli conn_options system snmp set --enable true**
65.	Pulse “Enter”, de nuevo, para continuar. El Script indicará que ha finalizado. 

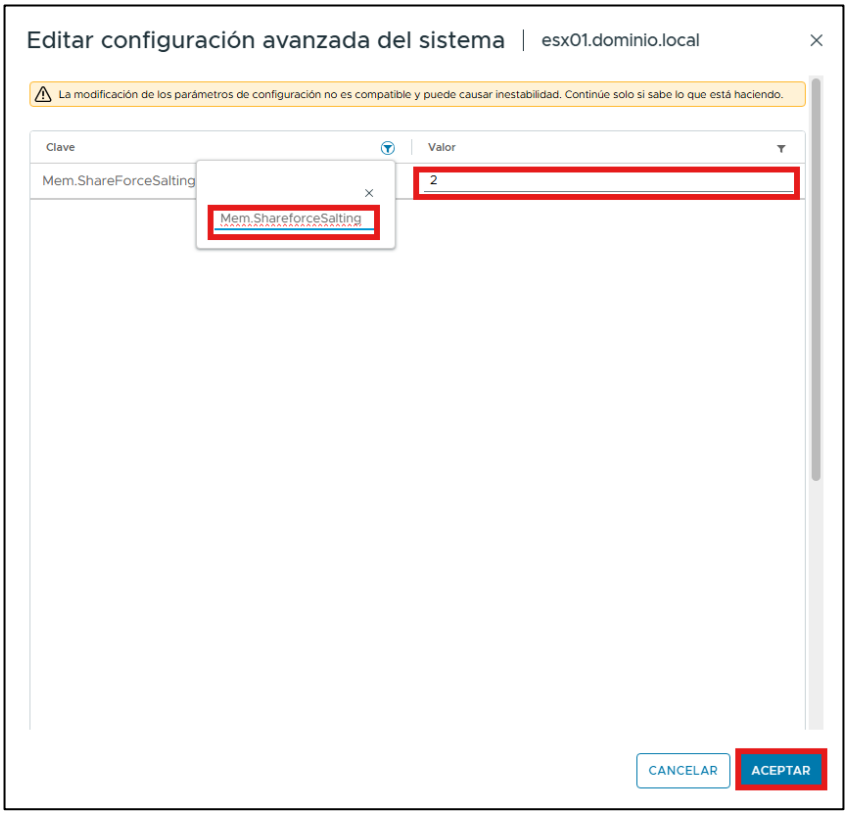
Paso	Descripción
66.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Basica_Paso_3_Deshabilitar_MOB.sh" mediante el siguiente comando y pulse "Enter" para continuar. **# sh CCN-STIC-442_ENS_Categoria_Basica_Paso_3_Deshabilitar_MOB.sh** 
67.	Pulse "Enter", de nuevo, para continuar. El Script indicará que ha finalizado.  **Nota:** No cierre la sesión SSH y manténgala en segundo plano mientras realiza los pasos siguientes.
68.	Todos los adaptadores y servidores de destino iSCSI deberán ser configurados con autenticación CHAP para asegurar la conexión. De nuevo, a través del navegador, pulse sobre el icono correspondiente a "Hosts y clústeres". 
69.	Pulse sobre el objeto del menú de la izquierda "<FQDN de servidor ESXi>" y en la pestaña "Configuración" seleccione "Adaptadores de almacenamiento". 

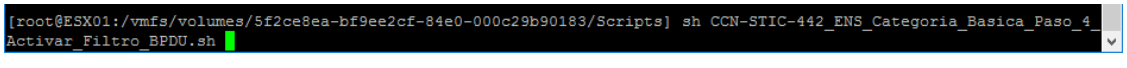
Paso	Descripción
70.	Pulse sobre el adaptador o adaptadores iSCSI mediante el cual se entrega el almacenamiento para el host ESXi. Diríjase ahora a la pestaña “Propiedades” y en el apartado “Autenticación” pulse sobre “Editar”. 
71.	Seleccione, en el menú contextual que se despliega al pulsar sobre el campo “Método de autenticación”, la opción “Usar CHAP bidireccional”. Establezca “Nombre” y “Secreto” para las credenciales CHAP salientes y entrantes. Una vez establecidos los parámetros pulse “Aceptar”.  **Nota:** Puede marcar “Usar nombre del iniciador” para establecer como nombre el iniciador iSCSI que se ha generado al crear el adaptador. Tenga en cuenta que el nombre no puede exceder los 255 caracteres y que el secreto no puede exceder los 100 caracteres (el secreto CHAP saliente no debe coincidir con el secreto CHAP entrante).

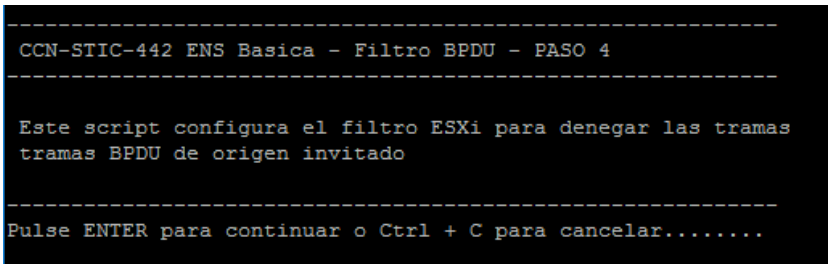
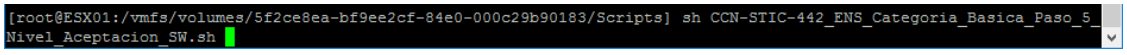
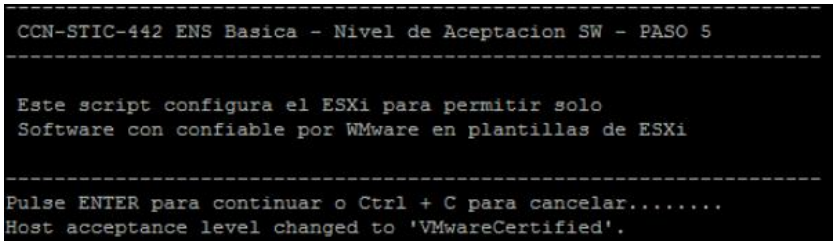
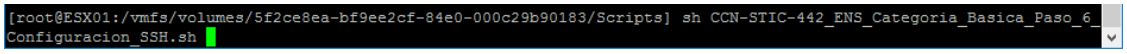
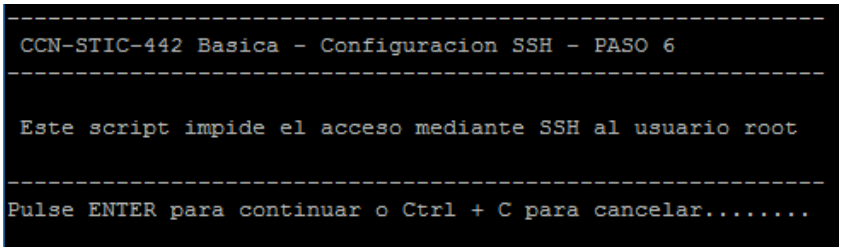
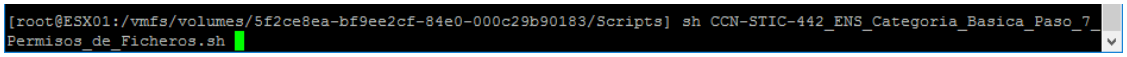
Paso	Descripción
72.	En este momento se definirán los criterios relativos a complejidad y comportamiento de contraseñas. Para configurar estos parámetros diríjase a "Configurar → Configuración avanzada" y pulse "Editar". 

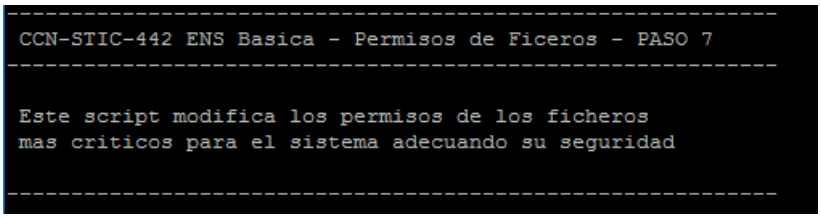
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>73.</td><td>
Introduzca en el filtro “Security” los objetos definidos a continuación y establezca los valores adecuados:
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Security.Account.LockFailures</td><td>8</td></tr>
<tr><td>Security.Account.UnlockTime</td><td>1800</td></tr>
<tr><td>Security.PasswordHistory</td><td>24</td></tr>
<tr><td>Security.PasswordMaxDays</td><td>90</td></tr>
<tr><td>Security.PasswordQualitycontrol</td><td>retry=3 min=disabled,disabled,disabled, disabled,10</td></tr>
</table>
Pulse “Aceptar” para continuar.


Nota: En caso de necesitar desbloquear, antes del tiempo definido, una cuenta que ha superado los intentos de introducción de contraseña, se puede hacer uso del comando siguiente a través de la consola ESXi Shell:
pam_tally –user <Usuario bloqueado> --reset
</td></tr>
</table>

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>74.</td><td>Pulse sobre “Editar” de nuevo.
 
</td></tr>
<tr><td>75.</td><td>Introduzca en el filtro “Mem.ShareforceSalting” y establezca el valor en “2”. Pulse “Aceptar” para continuar.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Mem.ShareforceSalting</td><td>2</td></tr>
</table>


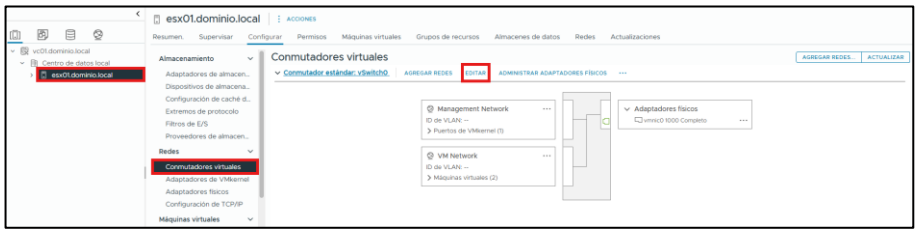
Nota: No cierre el navegador y manténgalo en segundo plano mientras realiza los siguientes pasos.</td></tr>
<tr><td>76.</td><td>Deberá utilizar de nuevo la sesión SSH que activó anteriormente para realizar los pasos que se indican a continuación. Ejecute el script “CCN-STIC-442_ENS_Categoria_Basica_Paso_4_Activar_Filtro_BPDU.sh” mediante el siguiente comando y pulse “Enter”.
<pre># sh CCN-STIC-442_ENS_Categoria_Basica_Paso_4_Activar_Filtro_BPDU.sh</pre>

</td></tr>
</table>

Paso	Descripción
77.	Pulse “Enter”, de nuevo, para continuar. El Script indicará que ha finalizado. 
78.	Ejecute el script “CCN-STIC-442_ENS_Categoria_Basica_Paso_5_Nivel_Aceptacion_SW.sh” mediante el siguiente comando y pulse “Enter”. **# sh CCN-STIC-442_ENS_Categoria_Basica_Paso_5_Nivel_Aceptacion_SW.sh** 
79.	Pulse “Enter”, de nuevo, para continuar. El Script indicará que ha finalizado. 
80.	Ejecute el script “CCN-STIC-442_ENS_Categoria_Basica_Paso_6_Configuracion_SSH.sh” mediante el siguiente comando y pulse “Enter”. **# sh CCN-STIC-442_ENS_Categoria_Basica_Paso_6_Configuracion_SSH.sh**  **Nota:** Antes de realizar este paso, es necesario disponer de una o varias cuentas con acceso a la consola ESXi Shell y que dispongan de los privilegios administrativos adecuados.
81.	Pulse, de nuevo, “Enter” para continuar. El sistema indicará que el Script ha finalizado. 
82.	Ejecute el script “CCN-STIC-442_ENS_Categoria_Basica_Paso_7_Permisos_de_Ficheros.sh” mediante el siguiente comando y pulse “Enter”. **# sh CCN-STIC-442_ENS_Categoria_Basica_Paso_7_Permisos_de_Ficheros.sh** 

Paso	Descripción
83.	Pulse “Enter” para continuar. El Script indicará que ha finalizado. 
84.	A continuación, cierre la sesión SSH abierta contra el servidor ESXi.

3.2.1. CONFIGURACIÓN EN CONMUTADORES VIRTUALES ESTÁNDAR

Las configuraciones descritas a continuación son a nivel de conmutadores estándar. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los conmutadores estándar de cada uno de los hosts ESXi existentes en el servicio de vCenter.

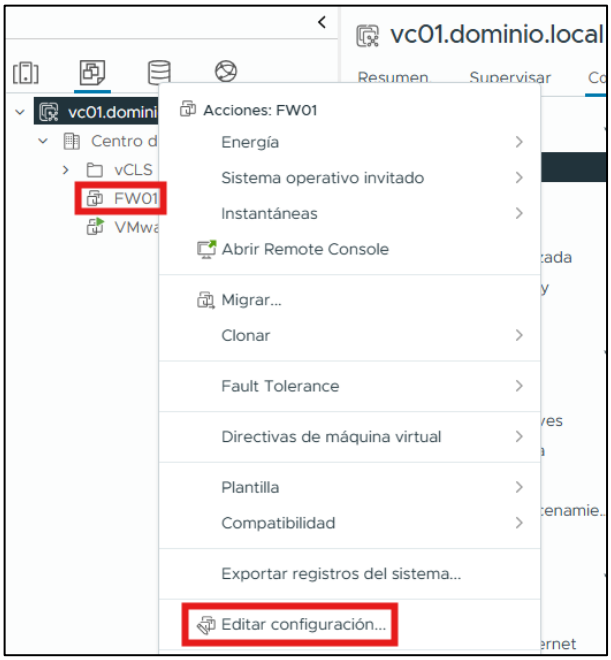
Paso	Descripción
85.	En el menú de la izquierda, seleccione el icono correspondiente a “Hosts y clústeres”. 
86.	En el menú de la izquierda, sitúese sobre el objeto “<FQDN del servidor ESXi>” y, en la pestaña “Configurar”, seleccione “Conmutadores virtuales”. Pulse “Editar” sobre cada conmutador virtual. 

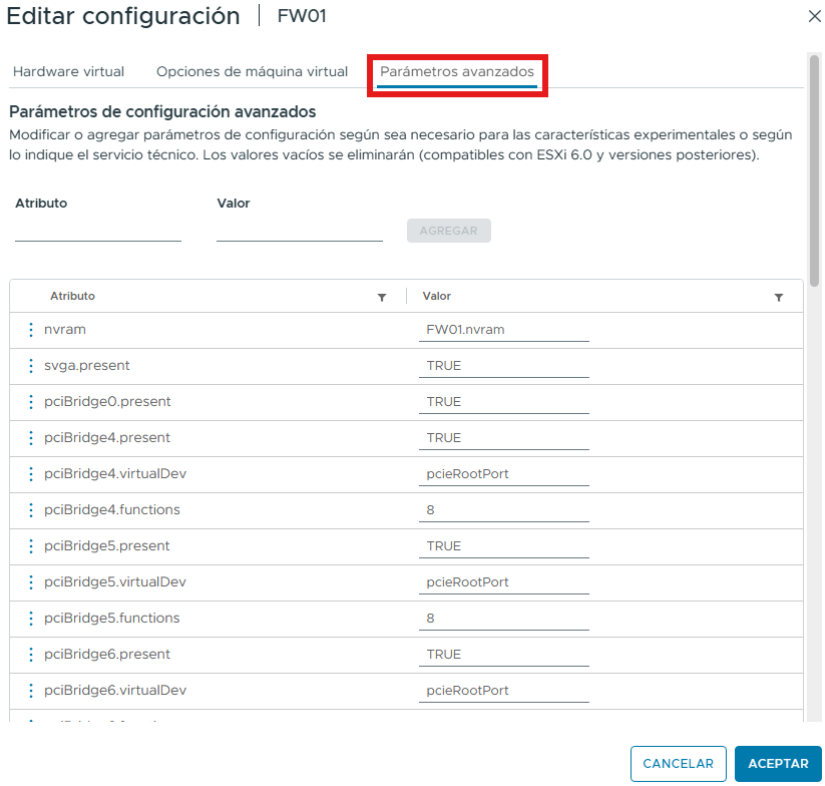
Paso	Descripción
87.	En la ventana emergente, pulse sobre “Seguridad” y compruebe el estado de los siguientes parámetros de seguridad (deberán tener el valor “Rechazar”): – Modo promiscuo – Cambios de dirección MAC – Transmisiones falsificadas 
88.	Modifique los parámetros al valor “Rechazar” y pulse “ACEPTAR” para validar la configuración. 

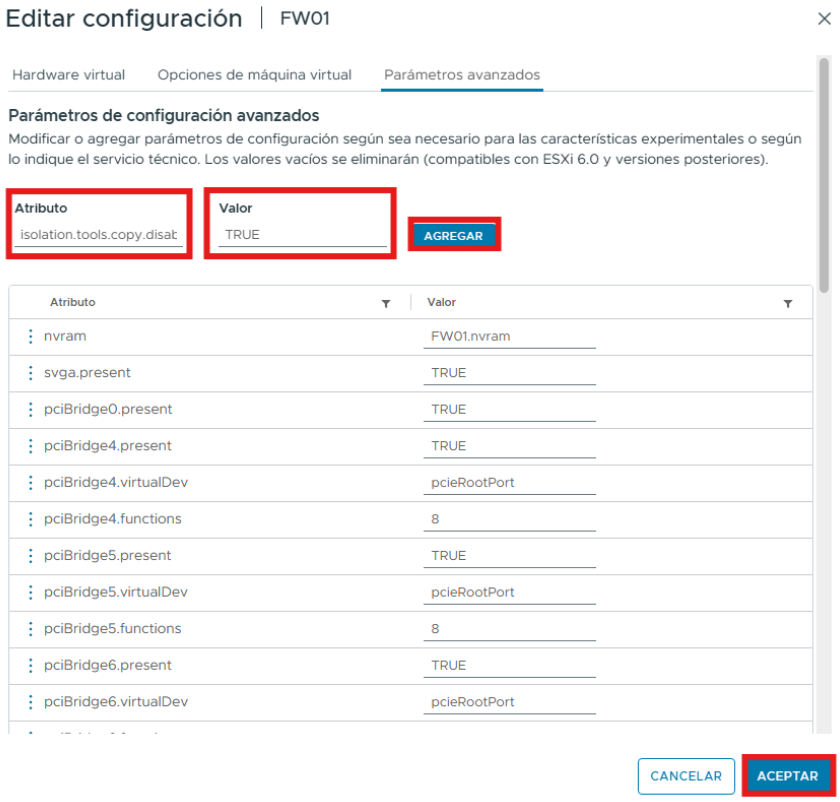
3.2.2. CONFIGURACIÓN DE MÁQUINAS VIRTUALES

Las configuraciones descritas a continuación son a nivel de máquina virtual. Por tanto, es necesario aplicar estas configuraciones de seguridad a todas las máquinas virtuales que se unan al host de ESXi que se está implementando.

Nota: Existe la posibilidad de convertir las máquinas virtuales configuradas en plantillas, de modo que se utilicen para generar nuevas máquinas, homogeneizando y simplificando las tareas administrativas.

Paso	Descripción
89.	En el menú de la izquierda, pulse el icono correspondiente a “Máquinas virtuales y plantillas”. 
90.	Asegúrese de que la máquina virtual esté apagada. Luego, sitúese sobre la máquina virtual sobre la que va a establecer las configuraciones de seguridad y pulse el botón derecho del ratón para seleccionar “Editar configuración…”. 

Paso	Descripción
91.	Diríjase a la pestaña “Parámetros avanzados”. 

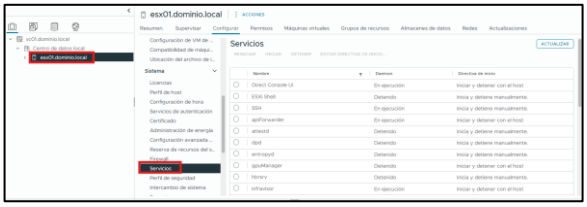
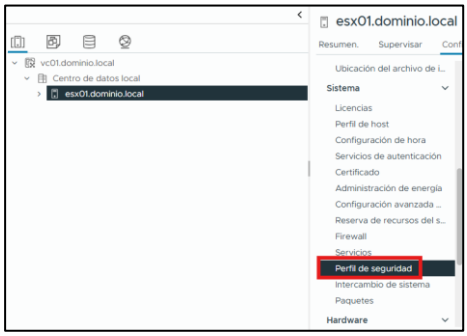
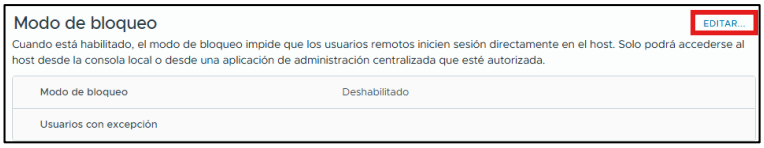
Paso	Descripción
92.	En el campo “Atributo” introduzca “isolation.tools.copy.disable” y en el campo “Valor” introduzca “True”. Pulse “Agregar” y “Aceptar” para guardar los cambios. 

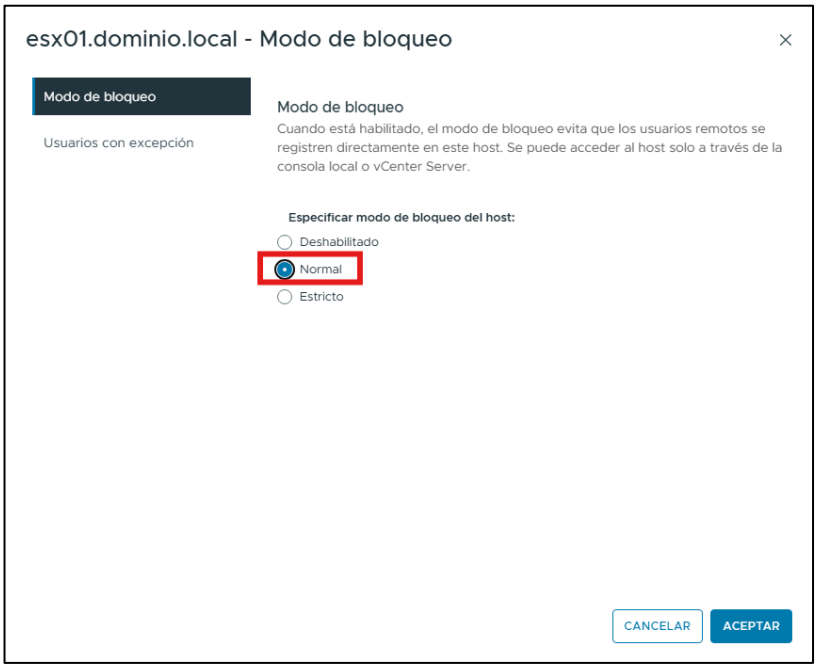
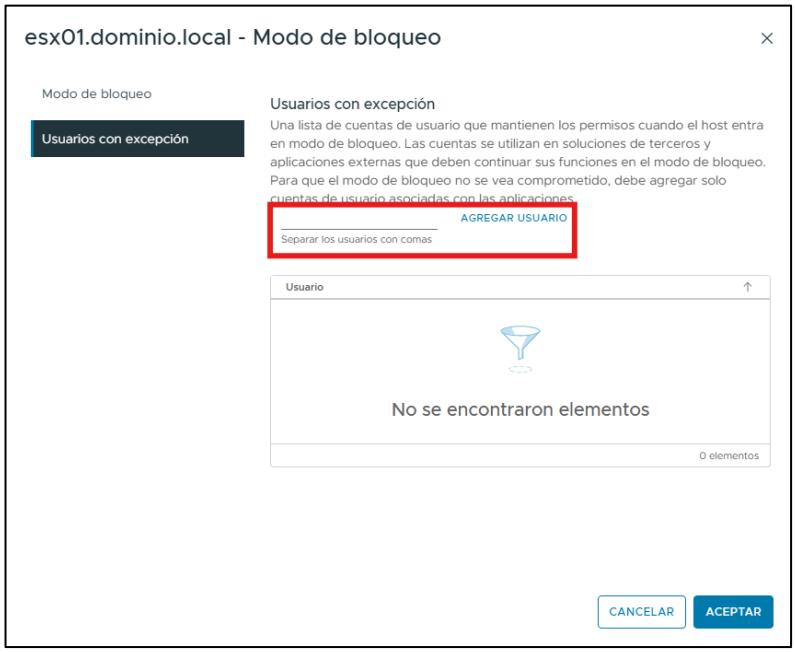
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>93.</td><td>Repita estos últimos pasos para añadir cada uno de los siguientes parámetros de configuración. Una vez haya introducido todos los parámetros, pulse “Aceptar” para continuar.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>isolation.tools.paste.disable</td><td>True</td></tr>
<tr><td>isolation.tools.setGUIOptions.enable</td><td>False</td></tr>
<tr><td>isolation.tools.diskShrink.disable</td><td>True</td></tr>
<tr><td>isolation.tools.diskWiper.disable</td><td>True</td></tr>
<tr><td>isolation.tools.connectable.disable</td><td>True</td></tr>
<tr><td>isolation.device.edit.disable</td><td>True</td></tr>
<tr><td>isolation.tools.setOption.disable</td><td>True</td></tr>
<tr><td>scsiX:Y.mode</td><td>Persistent</td></tr>
<tr><td>mks.enable3d</td><td>False</td></tr>
<tr><td>floppyX.present</td><td>False</td></tr>
<tr><td>parallelX.present</td><td>False</td></tr>
<tr><td>serialX.present</td><td>False</td></tr>
<tr><td>svga.vgaOnly</td><td>True</td></tr>
<tr><td>tools.setInfo.sizeLimit</td><td>1048576</td></tr>
<tr><td>RemoteDisplay.vnc.enabled</td><td>False</td></tr>
<tr><td>tools.guestlib.enableHostInfo</td><td>False</td></tr>
<tr><td>sched.mem.pshare.salt</td><td>Null</td></tr>
<tr><td>ethernetX.filterX. name = filtername</td><td>Null</td></tr>
<tr><td>pciPassthru*.present</td><td>False</td></tr>
<tr><td>Net.BlockGuestBPDU</td><td>1</td></tr>
</table>
Nota: Deberá adaptar la configuración a las necesidades del entorno.</td></tr>
</table>

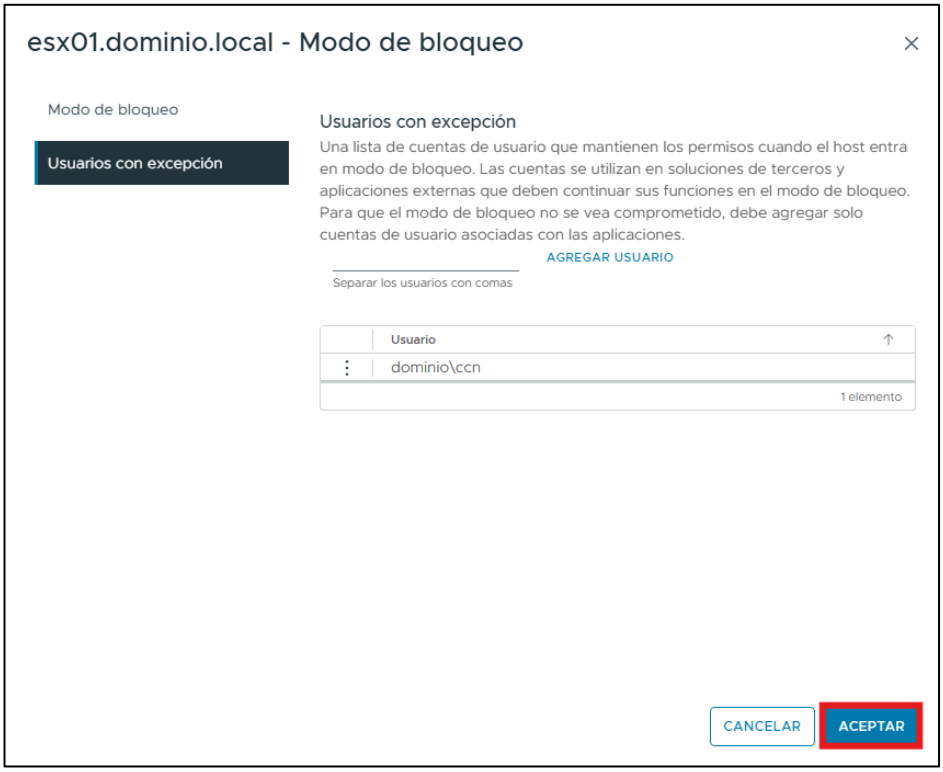
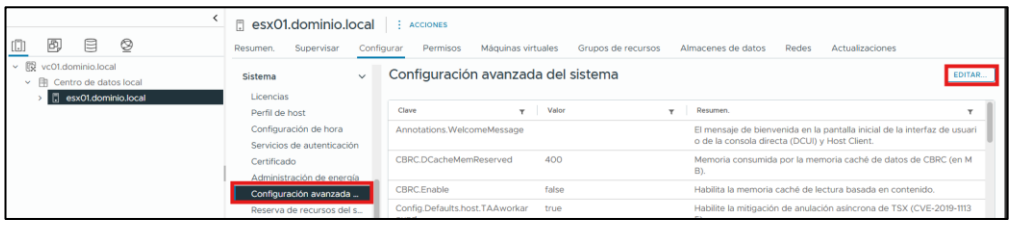
3.2.3. CONFIGURACIÓN DE ESX SHELL Y SSH

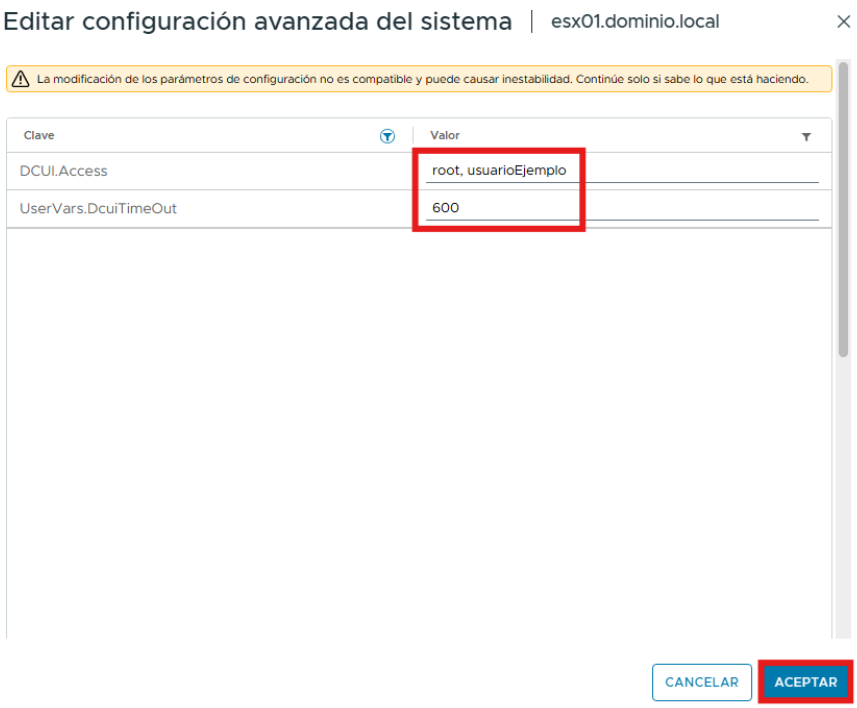
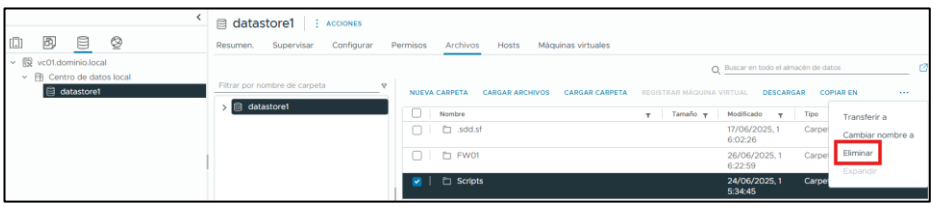
Por último, en el host ESXi, se deshabilitará SSH y la consola ESXi Shell. Así mismo, se activará el modo de bloqueo estricto. A partir de este momento, la administración del host solamente será a través del servidor de vCenter al que haya sido añadido. Se recomienda mantener la configuración de este modo salvo necesidad para resolución de problemas.

Paso	Descripción
94.	En el navegador, pulse sobre el icono que corresponde a “Hosts y clústeres”. 

Paso	Descripción
95.	En el menú de la izquierda, sitúese sobre el objeto “<FQDN del servidor ESXi>” y pulse sobre “Servicios”. 
96.	Seleccione el servicio “ESX Shell” y pulse “Detener”. 
97.	Realice la misma operación con el servicio “SSH”. 
98.	Defina el modo de bloqueo para el acceso a este host en modo “Normal” para que solo se pueda acceder al host de ESXi a través de servidores vCenter o localmente y no a través de clientes vSphere por conexión directa al host. Para ello, sitúese de nuevo sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar”, seleccione “Perfil de seguridad”.  **Nota:** El modo de bloqueo solamente se deberá desactivar, del mismo modo que solo se deberán activar la consola ESXi Shell y SSH, cuando se realicen tareas de resolución de problemas que no puedan ser solucionadas a través del servicio de vCenter o mediante el acceso local.
99.	En “Modo de Bloqueo” seleccione “Editar”. 

Paso	Descripción
100.	En la ventana emergente, seleccione el modo “Normal”. 
101.	En caso de que existan configuraciones y aplicativos que requieran conexión directa hacia el host, se deberán añadir sus usuarios al grupo de excepción para el modo estricto. Seleccione “Usuarios con excepción”, añada los usuarios que deberán tener acceso local al servidor ESXi, separados por “;” y pulse “AGREGAR USUARIO”.  **Nota:** a los usuarios que pertenecen a este grupo de excepción, se les permitirá traspasar el modo de bloqueo y acceder directamente al host. Estos usuarios no deben ser usuarios físicos, sino que deben ser usuarios automáticos que pertenezcan a procesos y aplicaciones. Así mismo, deberán ser auditados periódicamente pudiendo ser consultados mediante los pasos expuestos a continuación.

Paso	Descripción
102.	Los usuarios añadidos aparecerán en la lista. Pulse “ACEPTAR” para cerrar la ventana emergente.  **Nota:** En este paso se ha utilizado un usuario a modo ejemplo, adapte dicho paso a las necesidades de su organización. No se deben añadir a esta lista usuarios que no pertenezcan a aplicaciones o procesos automáticos que necesiten traspasar el modo de bloqueo.
103.	Así mismo, se deberán configurar también los usuarios físicos que podrán tener acceso a la infraestructura incluso cuando el modo de bloqueo está activado. Si esta configuración no contuviera ningún usuario, es posible que se pierda el control del ESXi completamente, no pudiendo volver a ser accesible. Para realizar la configuración, deberá acceder a “Configurar → Configuración avanzada” y pulsar sobre “Editar”. 

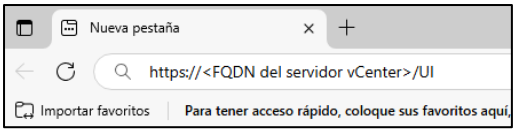
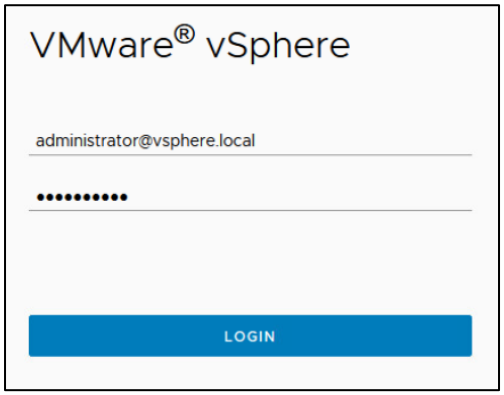
Paso	Descripción
104.	Añada, en el filtro, “DCUI” e introduzca los parámetros deseados añadiendo los usuarios (separados por coma) que podrán acceder por consola directa y el tiempo de bloqueo ante inactividad. Pulse “Aceptar” para continuar.  **Nota:** VMware desaconseja eliminar al usuario ROOT de esta lista.
105.	Pulse ahora sobre el icono correspondiente a “Almacenamiento”. 
106.	Sitúese sobre el almacén de datos donde alojó la carpeta “Scripts” y seleccione la pestaña “Archivos”. 
107.	Pulse sobre la carpeta “Scripts” y seleccione “Eliminar”. 

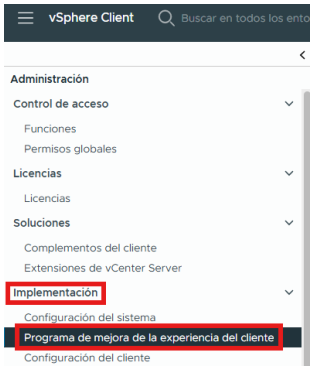
Paso	Descripción
108.	Pulse “Sí” para confirmar la eliminación. 

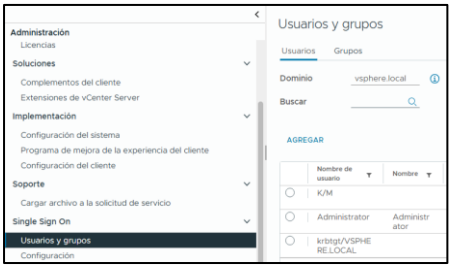
ANEXO A.2.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA BÁSICA DEL ENS PARA VSPHERE 8.x

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores que pertenecen a la infraestructura de VMware vSphere 8.x con implementación de seguridad de categoría básica del ENS.

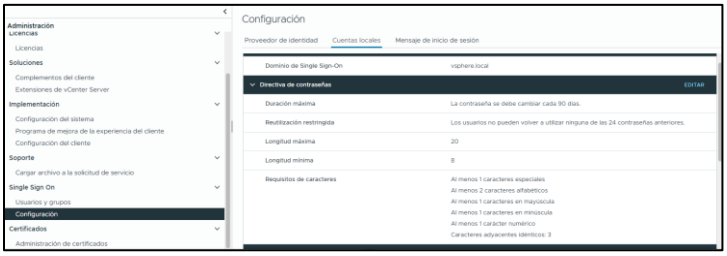
1. SERVIDORES VCENTER

Comprobación	OK/NOK	Como hacerlo
1. Acceso al servidor de vCenter.		Inicie sesión directamente en el host ESXi utilizando el ESXi Host Client a través de su navegador web. Para ello, introduzca la siguiente URL: “ https://<IP-o-FQDN-del-host-ESXi>/UI”.  Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter, pulse sobre “Iniciar”. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>2. Compruebe que el sistema no está unido al programa de mejora de VMware.</td><td></td><td>Pulse sobre “Implementación → Programa de mejora de la experiencia del cliente”.
 

El estado correcto debe ser “No unido”.
<table>
<tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Estado del programa</td><td>No unido</td><td></td></tr>
</table></td></tr>
<tr><td>3. Compruebe que los usuarios y grupos de administración son los correctos.</td><td></td><td>Compruebe que la lista de usuarios y grupos para hacer inicio de sesiones y labores administrativas es la adecuada. Pulse sobre “Usuarios y grupos” y revise la lista de usuarios mediante las pestañas.
 

<table>
<tr><th>Objetos</th><th>OK/NOK</th></tr>
<tr><td>Lista de usuarios</td><td></td></tr>
<tr><td>Lista de grupos</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>4. Compruebe la directiva de contraseñas para el servidor de vCenter.</td><td></td><td>Compruebe las directivas de contraseñas. Para ello, pulse sobre “Configuración” y sobre el botón “ Directiva de contraseñas ”.
 

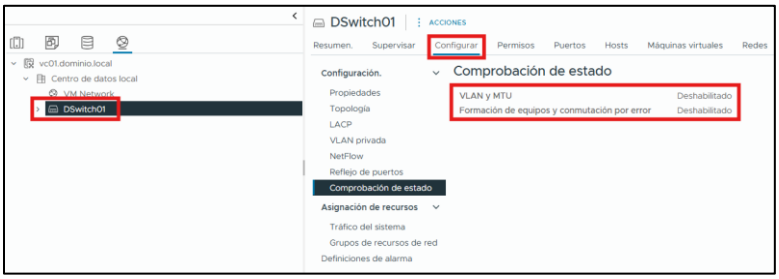
<table>
<tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Duración máxima</td><td>90</td><td></td></tr>
<tr><td>Reutilización restringida</td><td>24</td><td></td></tr>
<tr><td>Longitud mínima</td><td>10</td><td></td></tr>
<tr><td>Caracteres especiales</td><td>1</td><td></td></tr>
<tr><td>Caracteres en mayúscula</td><td>1</td><td></td></tr>
<tr><td>Caracteres en minúscula</td><td>1</td><td></td></tr>
<tr><td>Caracteres numéricos</td><td>1</td><td></td></tr>
</table></td></tr>
<tr><td>5. Compruebe la directiva de bloqueo para el servidor de vCenter.</td><td></td><td>Compruebe las directivas de contraseñas. Para ello, pulse sobre el botón “Directiva de bloqueo”.
<table>
<tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cantidad máxima de intentos fallidos de inicio de sesión</td><td>8</td><td></td></tr>
<tr><td>Intervalo de tiempo entre errores</td><td>1800</td><td></td></tr>
<tr><td>Tiempo de desbloqueo</td><td>1800</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>6. Compruebe que los servicios de vCenter son ejecutados por el usuario adecuado.</td><td></td><td>Revise los servicios principales del vCenter Server Appliance y asegúrese de que los siguientes se encuentren configurados con inicio automático y en estado activo:
<table>
<tr><th>Servicio</th><th>Inicio</th><th>OK/NOK</th></tr>
<tr><td>VMWareDirectoryService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareIdentityMgmtService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareCertificateService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareDNSService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareAfdService</td><td>Automático</td><td></td></tr>
<tr><td>VMwareSTS</td><td>Automático</td><td></td></tr>
<tr><td>vmon</td><td>Automático</td><td></td></tr>
<tr><td>Vmware-cis-config</td><td>Automático</td><td></td></tr>
</table>
Nota: La disponibilidad de algunos servicios puede variar en función de los componentes habilitados durante la instalación de vCenter. Todos los servicios son gestionados por el gestor de procesos vmon, y se ejecutan bajo el contexto del sistema root en el appliance VCSA basado en Photon OS.
Verificación del estado de los servicios
Para consultar el estado actual de los servicios en VCSA, utilice el siguiente comando desde una sesión SSH o desde la consola directa del appliance:
- service-control –status
En VCSA, los servicios corren bajo el usuario root y sus configuraciones se encuentran gestionadas desde /etc/init.d/, /usr/lib/vmware/ o mediante systemd.
Para revisar permisos de ejecución:
- ls -l /etc/init.d/
- ls -l /usr/lib/vmware/</td></tr>
</table>

1.1. CONMUTADORES VIRTUALES DISTRIBUIDOS

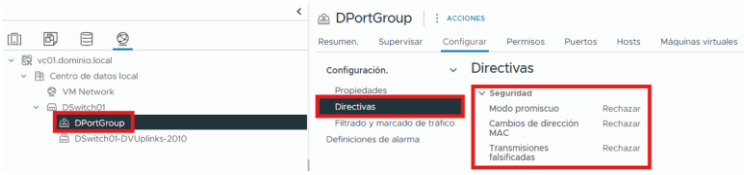
Las comprobaciones descritas a continuación son a nivel de conmutadores virtuales distribuidos. Por tanto, es necesario revisar la seguridad de todos los conmutadores virtuales distribuidos existentes en el servicio de vCenter.

Comprobación	OK/NOK	Como hacerlo
7. Compruebe que la “comprobación de estado” de los conmutadores virtuales		En el menú de la izquierda, seleccione el icono correspondiente a “Redes”.  Sitúese sobre cada conmutador distribuido y en la pestaña “Configurar” pulse sobre el elemento “Comprobación de

Comprobación	OK/NOK	Como hacerlo
distribuidos es correcta.		estado" y compruebe que los valores coinciden con los mostrados en la tabla.  **Parámetro** / **Estado** / **OK/NOK** VLAN y MTU — Deshabilitado — Formación de equipos y conmutación por error — Deshabilitado —

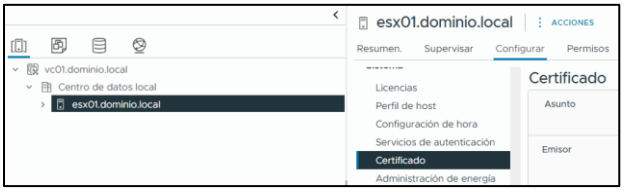
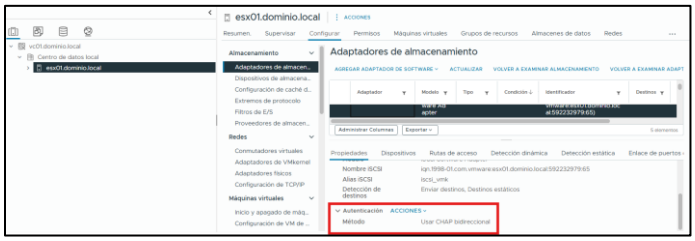
1.2. GRUPOS DE PUERTOS

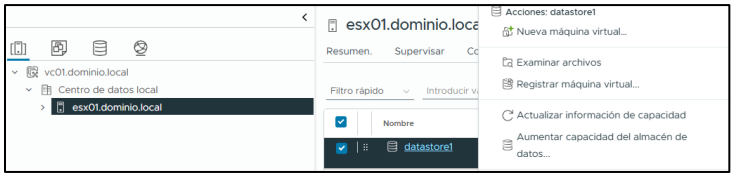
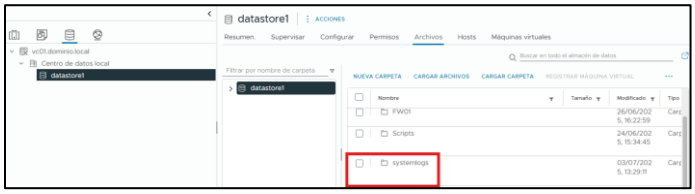
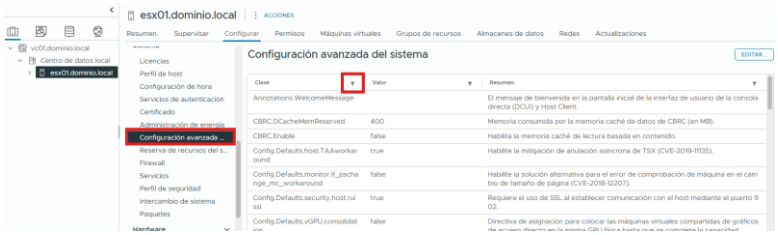
Las comprobaciones descritas a continuación son a nivel de grupos de puertos. Por tanto, es necesario revisar la seguridad de todos los grupos de puertos existentes en los distintos conmutadores presentes en el servicio de vCenter.

Comprobación	OK/NOK	Como hacerlo
8. Compruebe que la seguridad de los grupos de puertos es correcta.		En el menú de la izquierda, seleccione el icono correspondiente a "Redes".  Sitúese sobre cada grupo de puertos (que se encontrarán dentro de la rama de cada conmutador virtual) y, en la pestaña "Configurar", seleccione "Directivas" y compruebe que las siguientes directivas de seguridad tienen el valor "Rechazar"  **Directiva** / **Valor** / **OK/NOK** Modo Promiscuo — Rechazar — Cambios de dirección MAC — Rechazar — Transmisiones falsificadas — Rechazar —

2. SERVIDORES ESXI

Las comprobaciones descritas a continuación se realizan a nivel de servidor ESXi y deberán ser revisadas en cada uno de los host ESXi que se añadan a cada servidor de vCenter.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>9. Compruebe que el certificado del servidor ESXi es correcto.</td><td></td><td>Pulse sobre el icono que corresponde a “Host y clústeres”.
 
Sitúese sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar” seleccione “Certificado”. Compruebe que el certificado de servidor es el adecuado (emitido por una entidad certificadora autorizada)
  </td></tr>
<tr><td>10. Compruebe que está establecida la configuración NTP que se adecúa a las necesidades de la organización.</td><td></td><td>Seleccione “Configuración de hora” y compruebe que los valores son los deseados.
 
<table><tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Cliente NTP</td><td>Habilitado</td><td></td></tr><tr><td>Estado de servicio NTP</td><td>En ejecución</td><td></td></tr><tr><td>Servidores NTP</td><td>Configurado con un servidor de NTP válido</td><td></td></tr></table></td></tr>
<tr><td>11. Compruebe que el método de autenticación entre el servidor ESXi y el adaptador iSCSI es el adecuado.</td><td></td><td>Sitúese sobre “Adaptadores de almacenamiento” y pulse sobre cada adaptador iSCSI que quiera comprobar. En la pestaña “Propiedades” compruebe en “Autenticación” que el método CHAP está habilitado y la gestión de claves es bidireccional.
 
<table><tr><th>Propiedad</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Método</td><td>User CHAP bidireccional</td><td></td></tr></table></td></tr>
</table>

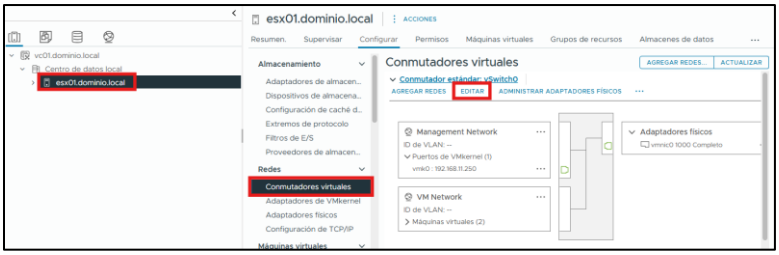
Comprobación	OK/NOK	Como hacerlo
12.Compruebe la configuración de logs.		Se deberá comprobar que los logs del sistema se encuentran en un almacén de datos persistente y accesible desde el servidor de vCenter. Pulse la pestaña “Almacén de datos” y pulse botón derecho sobre el almacén de datos que debería contener los logs. Seleccione “Examinar Archivos” en el menú contextual que se ha desplegado.  Deberá existir una carpeta denominada “systemlogs”.  Pulse doble clic sobre dicha carpeta para comprobar que contiene los ficheros de log y que estos se están llenando correctamente. 
13.Compruebe los parámetros de configuración avanzada en cada servidor de ESXi		Diríjase a “Configurar → Configuración avanzada” y compruebe los parámetros y valores especificados en la tabla.  **Nota:** Puede hacer uso de los filtros de columna para localizar las directivas.

Clave	Valor	OK/NOK
Security.Account.LockFailures	8	
Security.Account.UnlockTime	1800	
Security.PasswordHistory	24	

Comprobación	OK/NOK	Como hacerlo		
Security.PasswordMaxDays		90		
Security.PasswordQualitycontrol		retry=3 min=disabled,disabled,disabled, disabled,10		
Config.HostAgent.plugins.solo.enableMOB		false		
Mem.ShareforceShalting		2		
Net.BlockGuestBPDU		1		
Syslog.global.default.rotate		0		
Syslog.global.default.size		8192		
Syslog.global.logDir		“almacén de datos adecuado y persistente”		
		En este momento, aún no se han realizado todas las configuraciones específicas del servidor ESXi. Sin embargo, y dado que el resto de las configuraciones requieren de un acceso directo al host, se comprobarán el resto de los componentes tales como seguridad en las máquinas o conmutadores virtuales contenidos en el host para minimizar el tiempo de exposición del acceso directo o a través de SSH.		

2.1. CONMUTADORES VIRTUALES ESTÁNDAR

Las comprobaciones descritas a continuación son a nivel de conmutadores virtuales estándar. Por tanto, es necesario revisar la seguridad de todos los conmutadores virtuales estándar existentes en cada host ESXi contenido en cada servidor de vCenter.

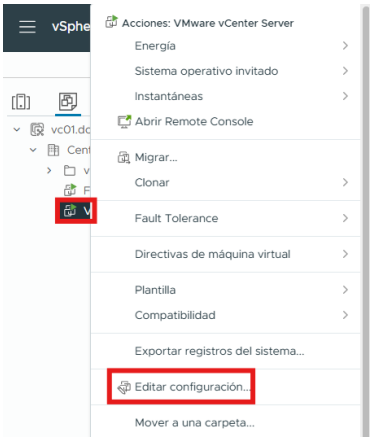
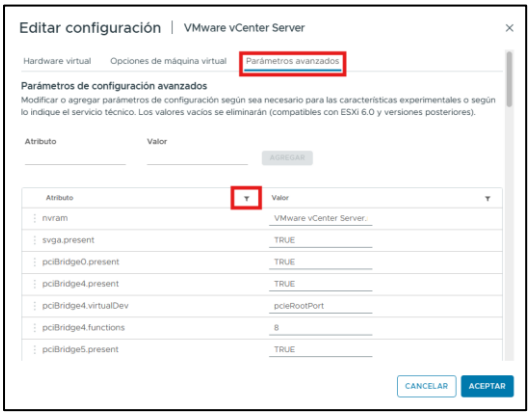
Comprobación	OK/NOK	Como hacerlo
14.Compruebe la seguridad en los conmutadores virtuales estándar de cada servidor ESXi.		Seleccione “Conmutadores virtuales”. Pulse “Editar” sobre cada conmutador virtual.  En la ventana emergente, pulse sobre “Seguridad” y compruebe el estado de los siguientes parámetros de seguridad (deberán tener el valor “Rechazar”).

Elemento	Valor	OK/NOK
Modo promiscuo	Rechazar	
Cambios de dirección MAC	Rechazar	
Transmisiones falsificadas	Rechazar	

2.2. MÁQUINAS VIRTUALES

Las comprobaciones descritas a continuación son a nivel de máquina virtual. Por tanto, es necesario aplicar estas configuraciones de seguridad a todas las máquinas virtuales que se unan al host de ESXi que se está implementando.

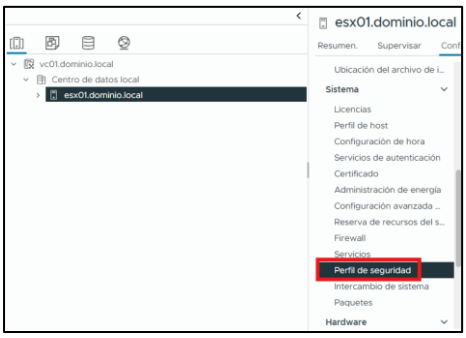
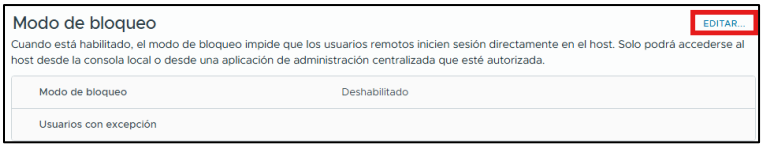
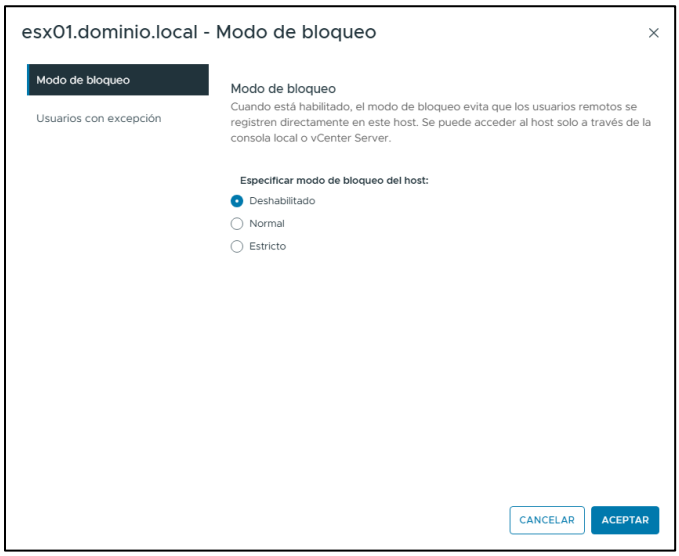
Nota: Adicionalmente, deberán ser comprobadas las medidas de seguridad aplicadas al sistema operativo invitado siguiendo las listas de comprobación de las guías STIC correspondientes.

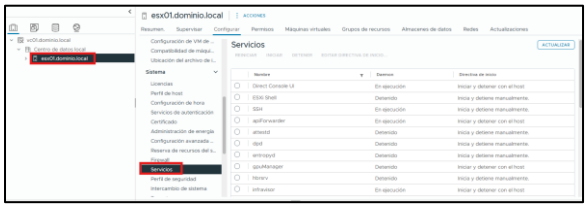
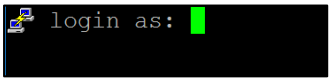
Comprobación	OK/NOK	Como hacerlo
15. Compruebe los parámetros de configuración avanzados para las máquinas virtuales.		Pulse el icono correspondiente a “Máquinas virtuales y plantillas”. 
		Sitúese sobre la máquina virtual sobre la que van a establecer las configuraciones de seguridad y pulse el botón derecho del ratón para seleccionar “Editar configuración…”.  Diríjase a la pestaña “Parámetros avanzados” y utilice la búsqueda por “Atributo”. 

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td></td><td></td><td>Localice los diferentes parámetros de configuración y compruebe que los valores coincides con los indicados en la tabla.
<table>
<tr><th>Elemento</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>isolation.tools.copy.disable</td><td>True</td><td></td></tr>
<tr><td>isolation.tools.paste.disable</td><td>True</td><td></td></tr>
<tr><td>isolation.tools.setGUIOptions.enable</td><td>False</td><td></td></tr>
<tr><td>isolation.tools.diskShrink.disable</td><td>True</td><td></td></tr>
<tr><td>isolation.tools.diskWiper.disable</td><td>True</td><td></td></tr>
<tr><td>isolation.tools.connectable.disable</td><td>True</td><td></td></tr>
<tr><td>isolation.device.edit.disable</td><td>True</td><td></td></tr>
<tr><td>isolation.tools.setOption.disable</td><td>True</td><td></td></tr>
<tr><td>scsiX:Y.mode</td><td>Persistent</td><td></td></tr>
<tr><td>mks.enable3d</td><td>False</td><td></td></tr>
<tr><td>floppyX.present</td><td>False</td><td></td></tr>
<tr><td>parallelX.present</td><td>False</td><td></td></tr>
<tr><td>serialX.present</td><td>False</td><td></td></tr>
<tr><td>svga.vgaOnly</td><td>True</td><td></td></tr>
<tr><td>tools.setInfo.sizeLimit</td><td>1048576</td><td></td></tr>
<tr><td>svga.vgaOnly</td><td>True</td><td></td></tr>
<tr><td>RemoteDisplay.vnc.enabled</td><td>False</td><td></td></tr>
<tr><td>tools.guestlib.enableHostInfo</td><td>False</td><td></td></tr>
<tr><td>sched.mem.pshare.salt</td><td>Null</td><td></td></tr>
<tr><td>ethernetX.filterX. name = filtername</td><td>Null</td><td></td></tr>
<tr><td>pciPassthru*.present</td><td>False</td><td></td></tr>
<tr><td>Net.BlockGuestBPDU</td><td>1</td><td></td></tr>
</table></td></tr>
</table>

2.3. COMPROBACIONES Y PASOS FINALES EN SERVIDOR ESXI

En este momento, se deberá deshabilitar el modo de bloqueo en cada servidor ESXi a comprobar ya que algunas de estas comprobaciones deberán ser realizadas a través de conexión directa al host. En los pasos finales se habilitará de nuevo para forzar el acceso único a través del servidor de vCenter.

Comprobación	OK/NOK	Como hacerlo
16. Deshabilite el modo de bloqueo		Pulse sobre el icono que corresponde a “Host y clústeres”.  Sitúese sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar”, seleccione “Perfil de seguridad”.  En “Modo de Bloqueo” seleccione “Editar”.  En la ventana emergente, seleccione el modo “Deshabilitado” y pulse “ACEPTAR” para continuar. 

Comprobación	OK/NOK	Como hacerlo
17. Habilite la consola ESXi y el acceso SSH		Pulse sobre “Servicios”.  Seleccione el servicio “ESX Shell” y pulse “Iniciar”.  Realice la misma operación con el servicio “SSH”.  **Nota:** No cierre aún el navegador web.
18. Realice la conexión al servidor de ESXi a través de SSH.		Utilice un cliente SSH para establecer una conexión al servidor e introduzca las credenciales de un usuario autorizado (no root) con privilegios administrativos para realizar las comprobaciones. 
19. Compruebe el estado los siguientes parámetros de seguridad.		Ejecute los comandos indicados en la tabla y compare los resultados.

Parámetro a comprobar	Valor devuelto	OK/NOK
# esxcli network ip get	IPv6Enable: false	
# esxcli system syslog config get	Local Log output: “Ruta al almacén de datos correcto y persistente”	
	Local Log Output Is Configured: true	
	Local Log Output Is Persistent: true	
	Local Login Default Rotation Size: 8192	
	Local Login Default Rotations: 0	
# esxcli system snmp get	Enable: false	
# esxcli software acceptance get	VMwareCertified	

Comprobación	OK/NOK	Como hacerlo
# grep PermitRootLogin /etc/ssh/sshd_config	PermitRootLogin no	
20.Compruebe los permisos sobre los siguientes ficheros de log		Diríjase a la ruta correspondiente al almacén de datos persistente donde se han alojado los ficheros log mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd "/vmfs/Volumes/<Nombre del almacén>/Syslogs** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l *.log** Compruebe que todos los ficheros con extensión .log tienen los mismos permisos como indica la tabla.

Ficheros	permisos	Propietario	OK/NOK
Todos los ficheros con extensión .log	-rw-------	root	

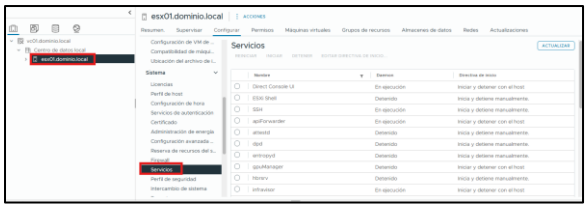
21.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe los permisos sobre la carpeta "/etc" y el propietario.

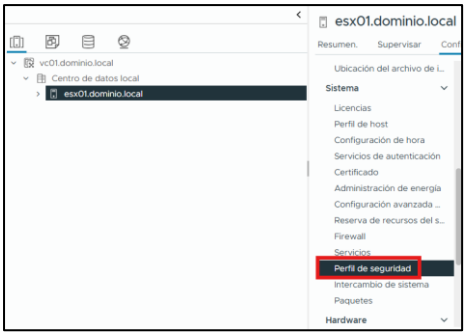
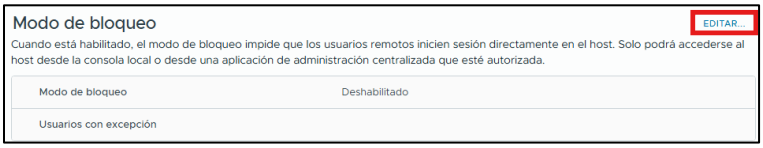
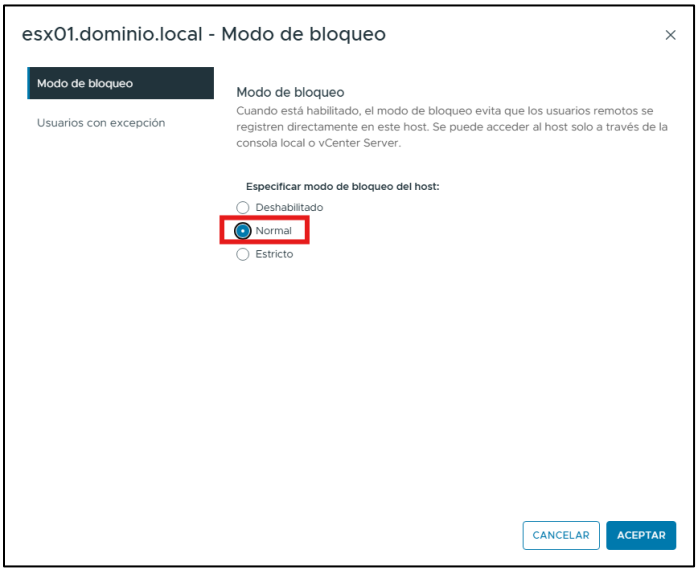
Ficheros	permisos	Propietario	OK/NOK
/etc	-rwxr-xr-x	root	

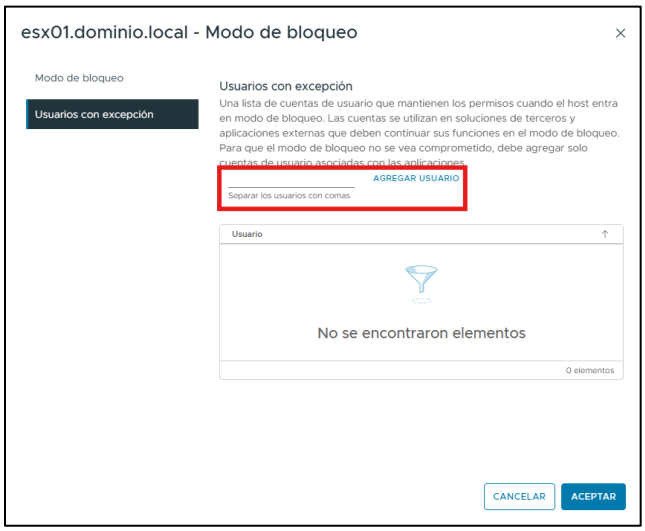
22.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.

Ficheros	permisos	Propietario	OK/NOK
/etc/profile	-rw-r--r--	root	
/etc/krb5.conf	-rw-r--r--	root	
/etc/krb5.realms	-rw-r--r--	root	
/etc/nscd.conf	-rw-r--r--	root	
/etc/resolv.conf	-rw-r--r--	root	
/etc/nsswitch.conf	-rw-r--r--	root	
/etc/ntp.conf	-rw-r--r--	root	
/etc/passwd	-rw-r--r--	root	

Comprobación	OK/NOK	Como hacerlo			
/etc/group			-rw-r--r--	root	
/etc/shadow			-r---------	root	
/etc/vmware/			-rwxr-xr-x	root	
23.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/ssh" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/ssh** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
/etc/ssh/sshd_config			-rw-------	root	
24.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/usr/sbin" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /usr/sbin** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l esxcfg*** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
Todos los ficheros que comienzan por esxcfg			-r-x------	root	
25.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/vmware" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/vmware** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
/etc/vmware/config			-rw-r--r--	root	
/etc/vmware/configrules			-rw-r--r--	root	
/etc/vmware/esx.conf			-rw-r--r--	root	
/etc/vmware/firewall			-rwxr-xr-x	root	
/etc/vmware/hostd			-rwxr-xr-x	root	
/etc/vmware/ima_plugin.conf			-rw-r--r--	root	
/etc/vmware/license.cfg			-rw-r--r--	root	

Comprobación	OK/NOK	Como hacerlo			
/etc/vmware/logfilters			-rw-r--r--	root	
/etc/vmware/pciid			-rwxr-xr-x	root	
/etc/vmware/pci.ids			-rw-r--r--	root	
/etc/vmware/service			-rwxr-xr-x	root	
/etc/vmware/snmp.xml			-rw-r--r--	root	
/etc/vmware/ssl			-rwxr-xr-x	root	
26.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/vmware/ssl" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/vmware/ssl** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
/etc/vmware/ssl/rui.crt			-rw-r—r--	root	
/etc/vmware/ssl/rui.key			-r--------		
27.Cierre la sesión SSH.		Cierre la sesión SSH.			
28.Una vez realizado, deshabilite SSH y la consola ESXi Shell (en caso de que no se hayan deshabilitado de forma automática).		En el navegador, pulse sobre el icono que corresponde a "Hosts y clústeres".  En el menú de la izquierda, sitúese sobre el objeto "<FQDN del servidor ESXi>" y pulse sobre "Servicios".  Seleccione el servicio "ESX Shell" y pulse "Detener".  Realice la misma operación con el servicio "SSH". 			

Comprobación	OK/NOK	Como hacerlo
29. Vuelva a habilitar el modo de bloqueo.		Defina el modo de bloqueo para el acceso a este host en modo “Normal” para que solo se pueda acceder al host de ESXi a través de servidores vCenter o localmente y no a través de clientes vSphere por conexión directa al. Para ello, sitúese de nuevo sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar”, seleccione “Perfil de seguridad”.  En “Modo de Bloqueo” seleccione “Editar”.  En la ventana emergente, seleccione el modo “Normal”. 
30. Compruebe la lista de usuarios autorizados para acceder directamente al host con		Compruebe la lista de usuarios autorizados pulsando sobre “Usuarios con excepción” y pulse “ACEPTAR” para finalizar.

Comprobación	OK/NOK	Como hacerlo
modo de bloqueo activo.		 **Nota:** Esta lista debería ser revisada periódicamente para evitar que haya usuarios no autorizados añadidos a ella.

ANEXO A.3. CATEGORÍA MEDIA

ANEXO A.3.1. IMPLEMENTACIÓN DE SEGURIDAD EN VMWARE VSPHERE 8.X SOBRE SERVIDORES QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

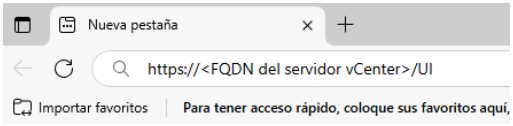
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores del entorno de virtualización VMware vSphere 8.x con una categorización de seguridad media según los criterios del Esquema Nacional de Seguridad.

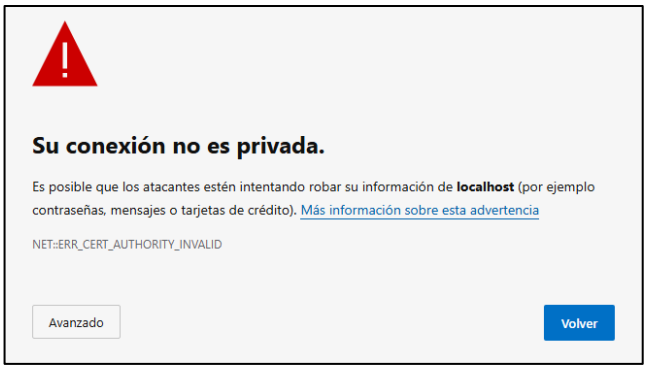
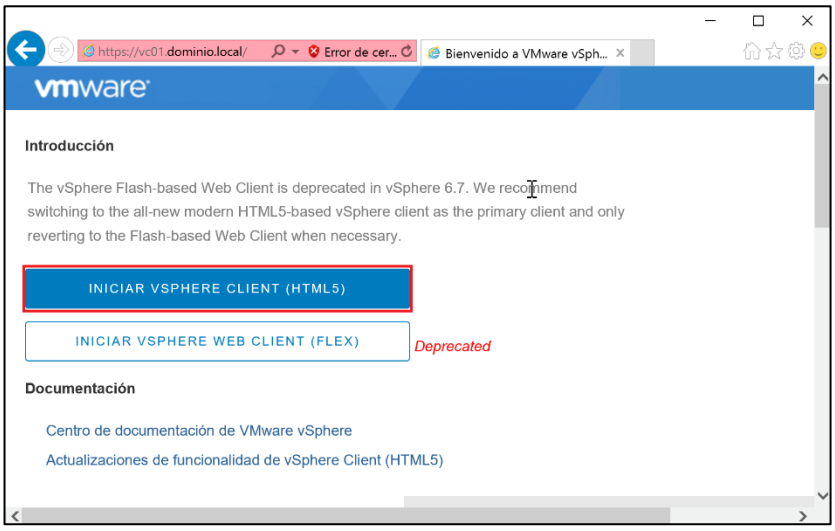
Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo II del RD 311/2022. Si algún elemento del conjunto resultante para todos los servicios e información manejada por la organización correspondiera a la categoría media y ninguno a la categoría alta - DL, deberá realizar las implementaciones según se referencian en el presente anexo.

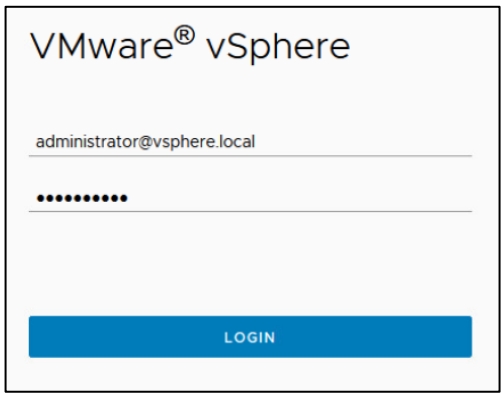
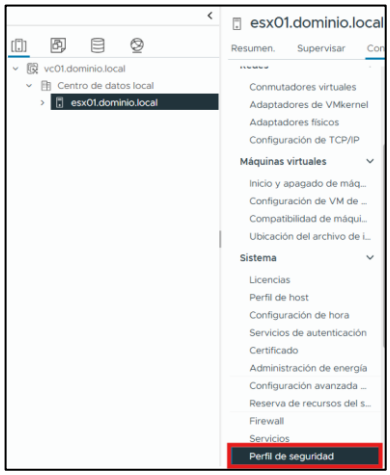
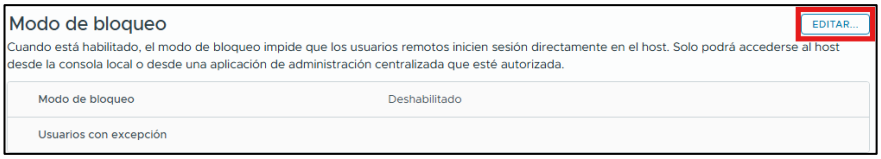
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

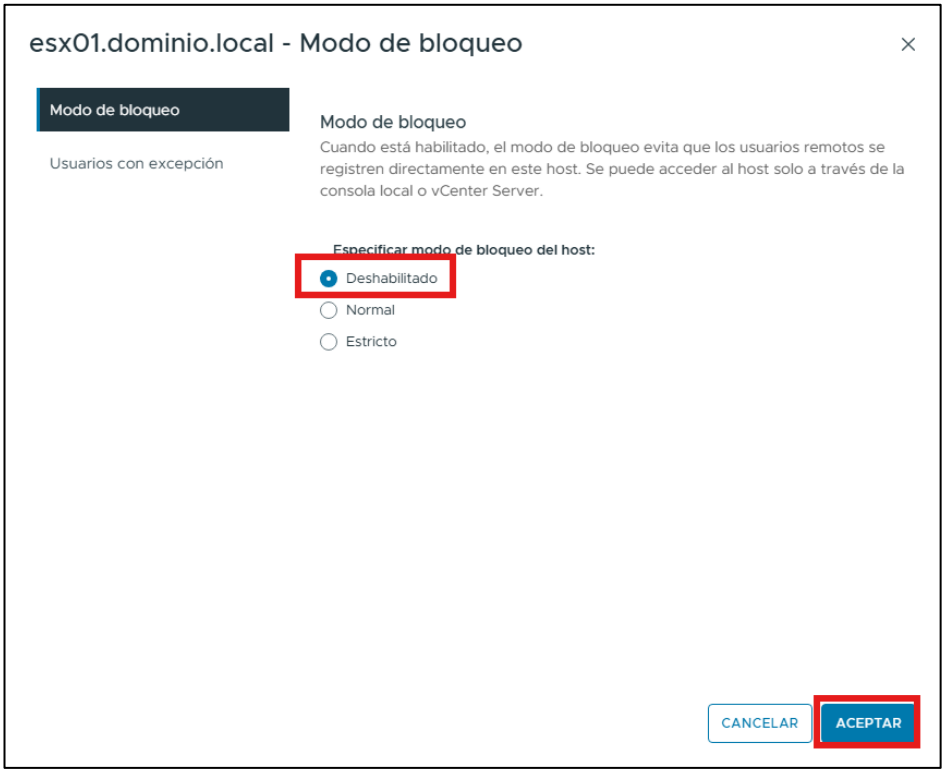
1. PREPARACIÓN DEL SERVIDOR ESXI

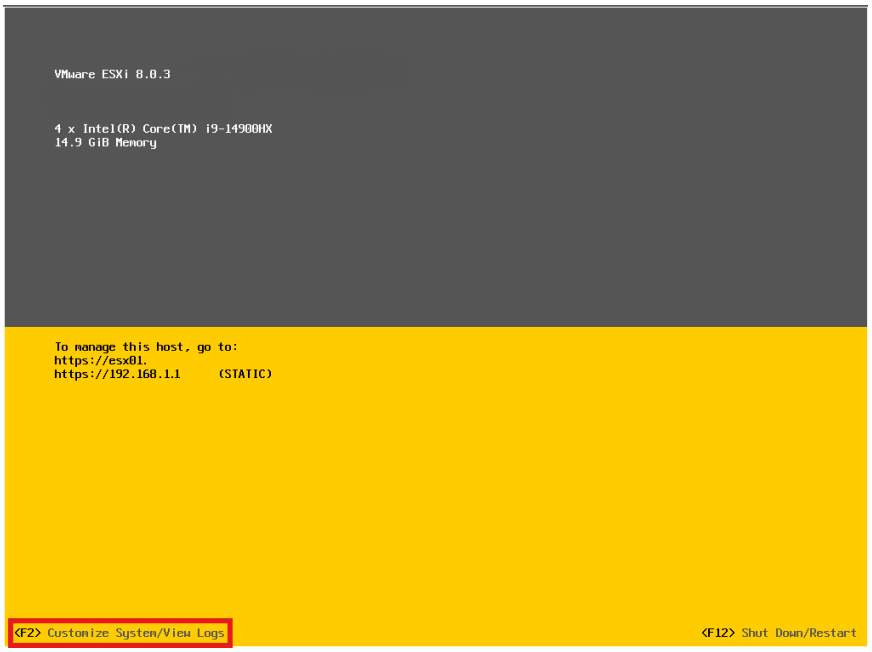
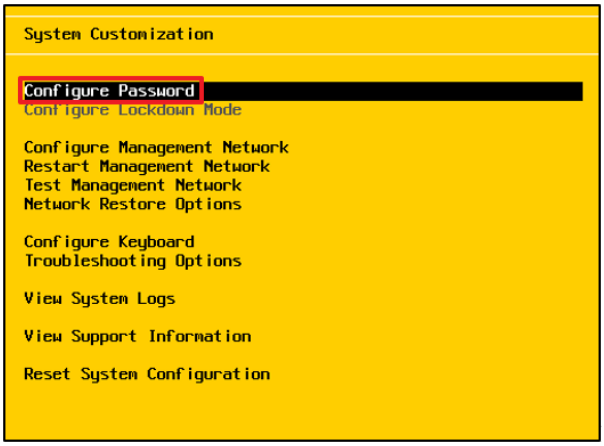
En caso de que esté habilitado, se deberá deshabilitar temporalmente el modo de bloqueo en cada servidor ESXi al que se le va a aplicar la seguridad ya que algunas de estas configuraciones deberán ser realizadas a través de conexión directa al host. En los pasos finales se habilitará de nuevo para forzar el acceso único a través del servidor de vCenter.

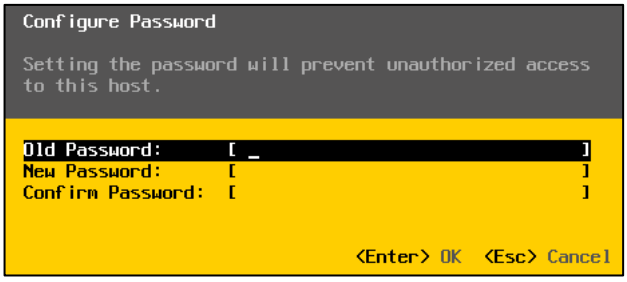
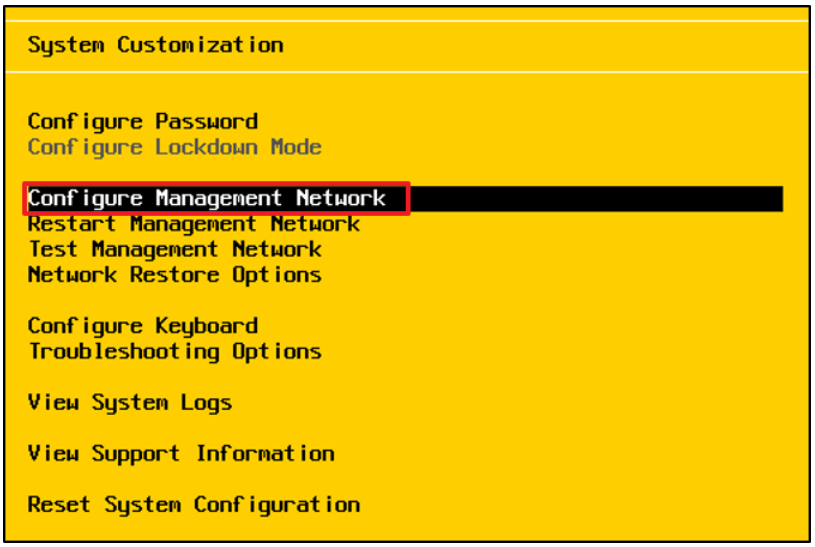
Paso	Descripción
1.	Inicie sesión directamente en el host ESXi utilizando el ESXi Host Client a través de su navegador web. Para ello, introduzca la siguiente URL: “ https://<IP-o-FQDN-del-host-ESXi>/UI”. 

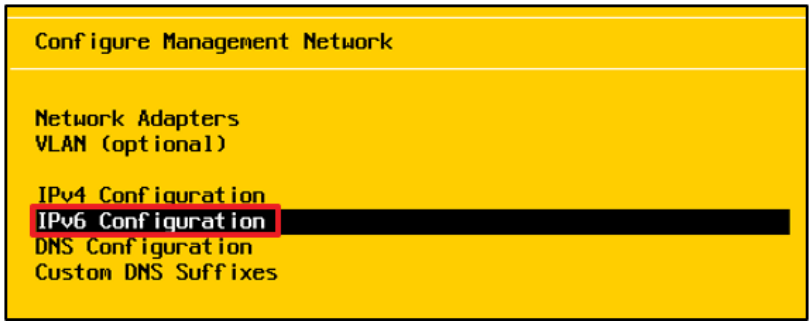
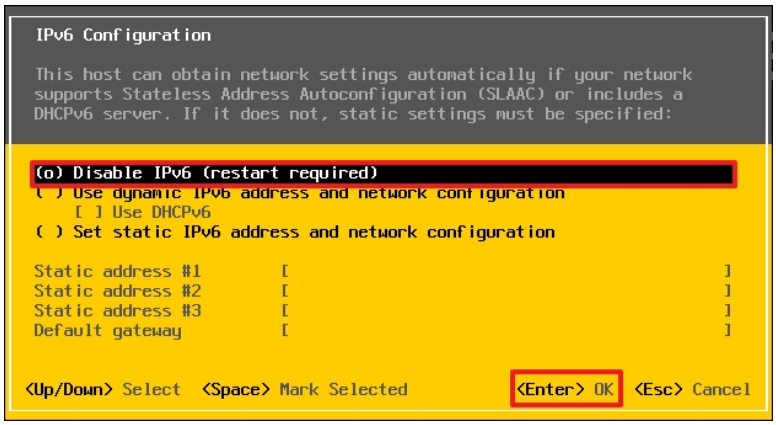
Paso	Descripción
2.	Inicie sesión, a través del vSphere client mediante html5, en el servidor de vCenter. Para ello, en su navegador, introduzca la url “https://<FQDN del servidor vCenter>/UI”. Si el navegador muestra una advertencia indicando que el sitio no es seguro, puede ignorarla. Esto se debe a que se está utilizando un certificado autofirmado. Haga clic en la opción "Avanzado".  **Nota:** La captura y la opción a escoger podrían ser diferentes según el navegador que se esté empleando. En el ejemplo se ha utilizado Microsoft Edge.
3.	En caso de que aparezca un mensaje permitiendo elegir entre “vSphere Client (HTML5)” y “vSphere Web Client”, deberá seleccionar la primera opción. 

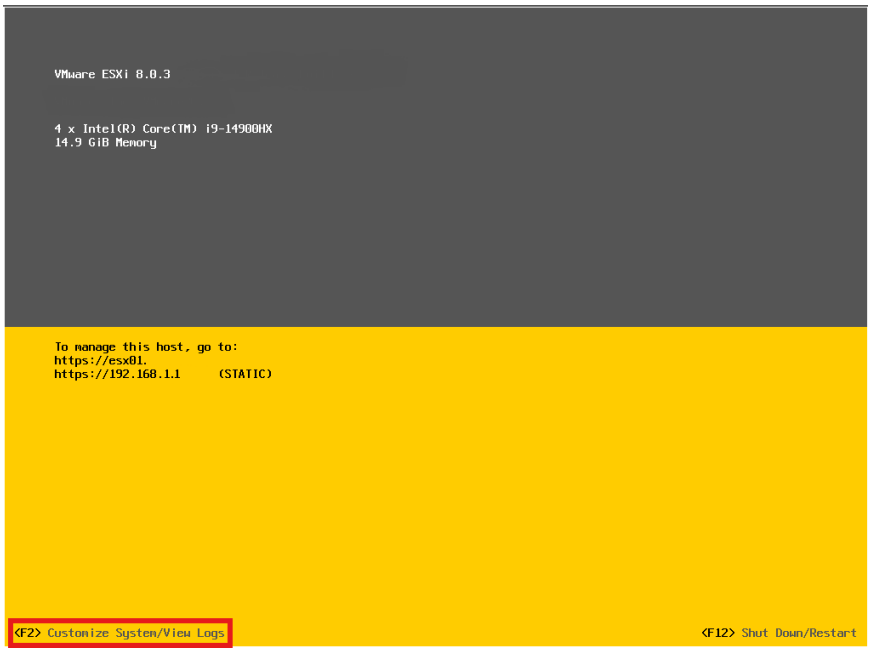
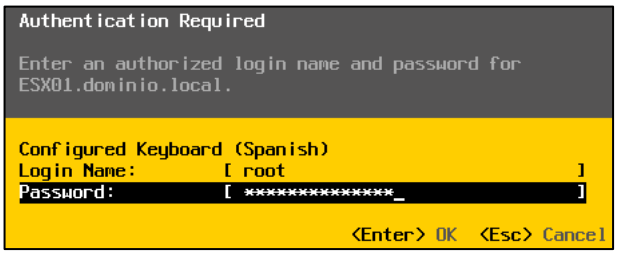
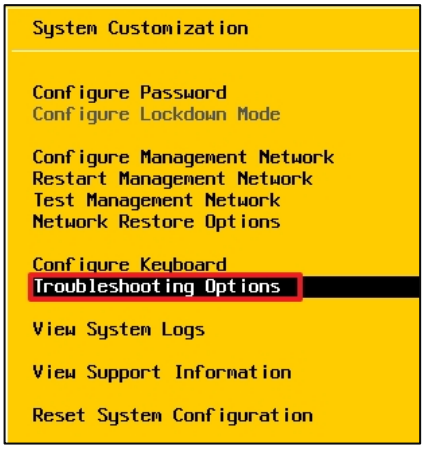
Paso	Descripción
4.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”.  **Nota:** Según los métodos de autenticación empleados, la pantalla podría diferir de la captura mostrada.
5.	En el menú de la izquierda, pulse sobre el icono que corresponde a “Host y clústeres”. 
6.	Sitúese sobre el objeto “<FQDN del servidor ESXi>” sobre el que quiere aplicar la seguridad y en la pestaña “Configurar”, seleccione “Perfil de seguridad”. 
7.	En “Modo de Bloqueo” seleccione “Editar”.  **Nota:** En caso de que el modo de bloqueo figure como “Deshabilitado” puede este paso.

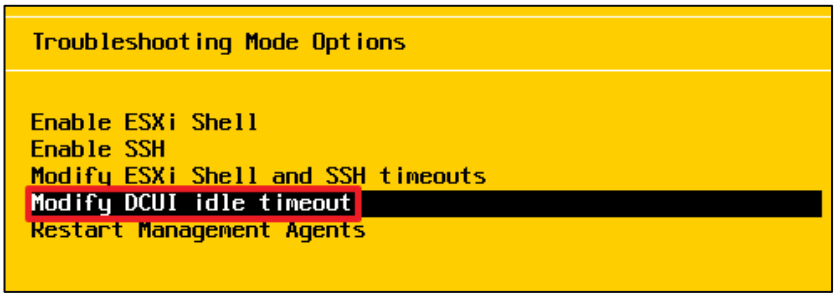
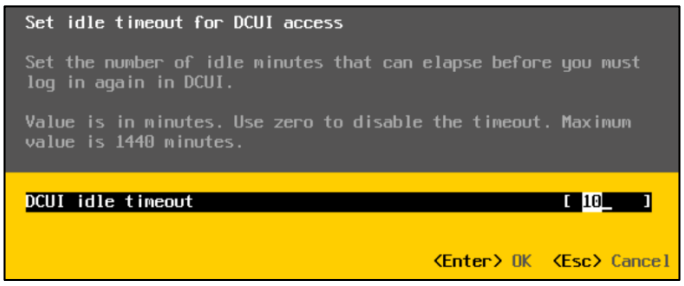
Paso	Descripción
8.	En la ventana emergente, seleccione el modo “Deshabilitado” y pulse “ACEPTAR” para continuar. 
9.	Los siguientes pasos descritos a continuación se realizarán en el servidor ESXi para terminar de configurar el hipervisor de forma local. **Nota:** Los pasos que se detallan a continuación, se deberán realizar en cada host ESXi que se implemente en la infraestructura de VMware vSphere 8.x que se está implementando.
10.	Es recomendable establecer una contraseña para el BIOS del propio servidor de ESXi de modo que se eviten posibles ataques basados en el acceso al equipo, de forma física, ya que se puede manipular la secuencia de arranque y los elementos de configuración del propio BIOS del servidor. **Nota:** En esta guía no se explica cómo hacerlo ya que el modo de establecer una contraseña en el BIOS del servidor variará dependiendo del fabricante y modelo de este.
11.	Así mismo, sería conveniente establecer, a través del BIOS, la secuencia de arranque y la lista de dispositivos de arranque permitidos. En caso de no establecer dicha configuración, sería posible arrancar desde un medio extraíble no autorizado pudiendo acceder a la información del servidor.

Paso	Descripción
12.	En el servidor de ESXi, pulse “F2” para realizar las tareas de configuración inicial. 
13.	El sistema solicitará credenciales. Introduzca la contraseña y pulse “Enter” para continuar. 
14.	En caso de que la contraseña suministrada durante la instalación no cumpliera con los requisitos de complejidad necesarios, seleccione “Configure Password” situándose sobre él mediante las teclas de dirección y presione “Enter”. 

Paso	Descripción
15.	Introduzca en el primer campo la contraseña suministrada durante la instalación y, a continuación, introduzca dos veces la contraseña deseada. Pulse “Enter” para validar la configuración y salir.  **Nota:** Recuerde que en esta categoría el nivel de complejidad y longitud de la contraseña deberá cumplir con los siguientes requisitos: - Mínimo 12 caracteres - Al menos 1 mayúscula - Al menos 1 minúscula - Al menos 1 carácter especial - Al menos 1 número
16.	Seleccione “Configure Management Network” para deshabilitar TCP/IPv6. Para ello, sitúese sobre la opción mediante las teclas de dirección y pulse “Enter”.  **Nota:** Esta guía paso a paso asume que se está aplicando la seguridad sobre una infraestructura de VMware vSphere 8.x previamente operativa, por lo que no tendrán en cuenta parámetros de configuración e implementación y se ocupará de modificar las configuraciones relativas a la seguridad del sistema para alcanzar el nivel de seguridad deseado.

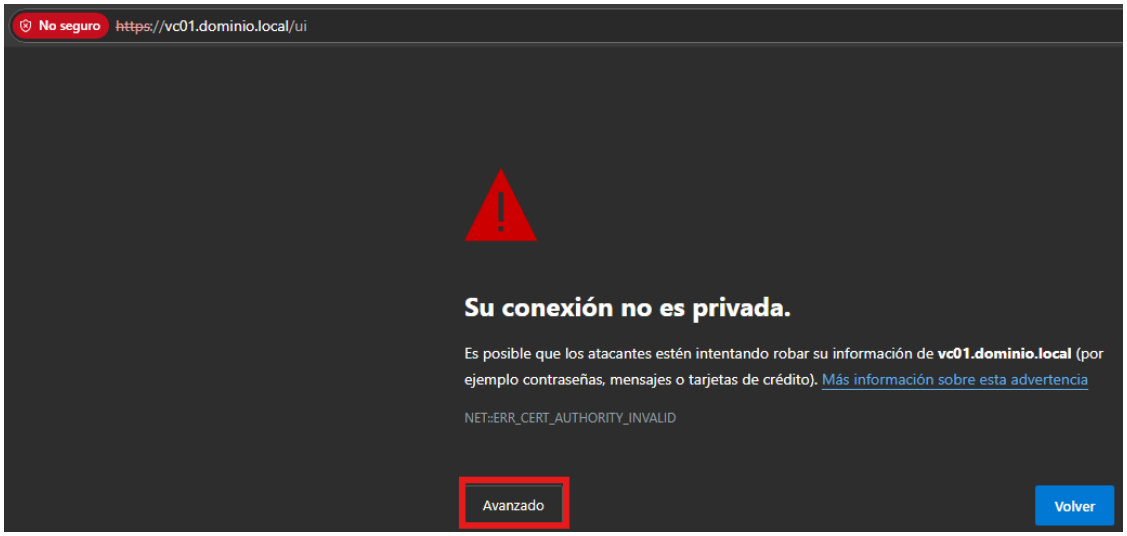
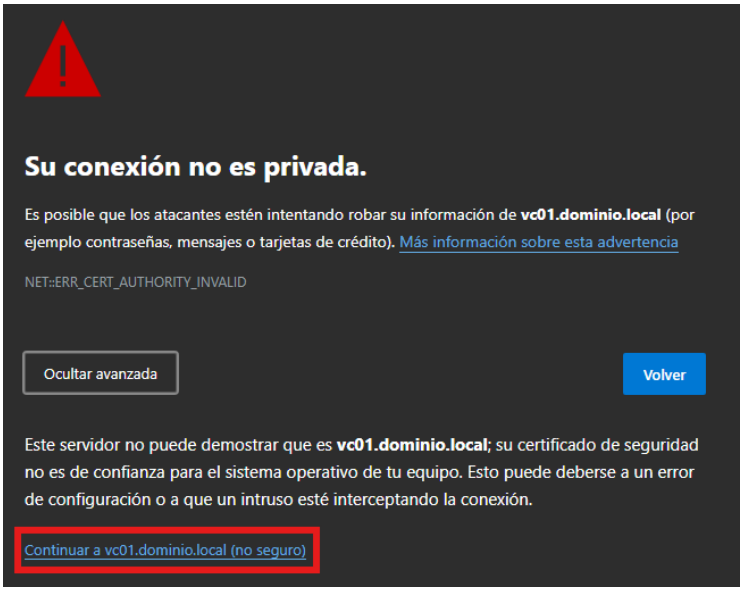
Paso	Descripción
17.	Seleccione “IPv6 Configuration” situándose sobre la opción, mediante las teclas de dirección, y presione “Enter”. 
18.	Sitúese sobre “Disable IPv6 (restart required)” y utilice la barra espaciadora para seleccionarlo. Pulse “Enter” para guardar los cambios. 
19.	Pulse “Esc” para salir de la configuración de red.
20.	Ante la solicitud de aplicar los cambios y reiniciar el host seleccione "Yes" pulsando la tecla "Y". El servidor se reiniciará. 

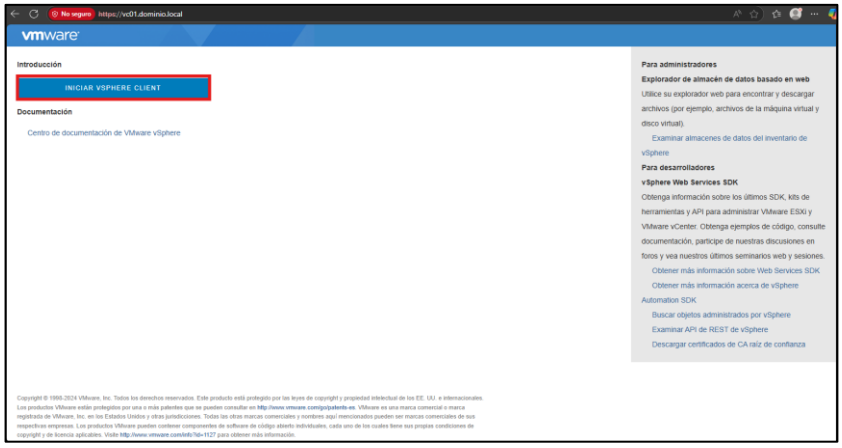
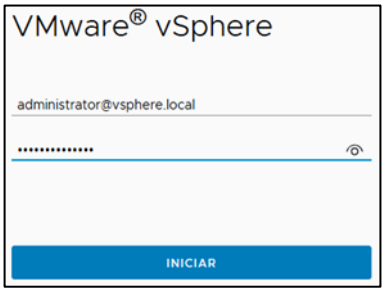
Paso	Descripción
21.	Una vez reiniciado el servidor, se procede a definir el tiempo de desconexión por inactividad. Pulse “F2” para abrir las herramientas de configuración del servidor ESXi. 
22.	El sistema solicitará credenciales. Introduzca la contraseña y pulse “Enter” para continuar. 
23.	Seleccione la opción “Troubleshooting options” y pulse “Enter” para continuar. 

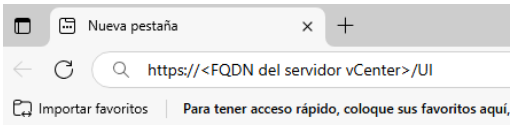
Paso	Descripción
24.	Pulse sobre “Modify DCUI idle timeouts” para establecer el tiempo de bloqueo de uso de la consola directa DCUI. 
25.	Introduzca el valor “10” y pulse “Enter” para registrarlo. Pulse “Esc” para salir al menú inicial. 
26.	Pulse “Esc” de nuevo para salir a la pantalla principal.

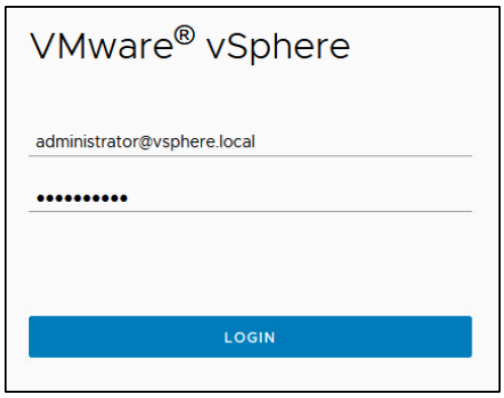
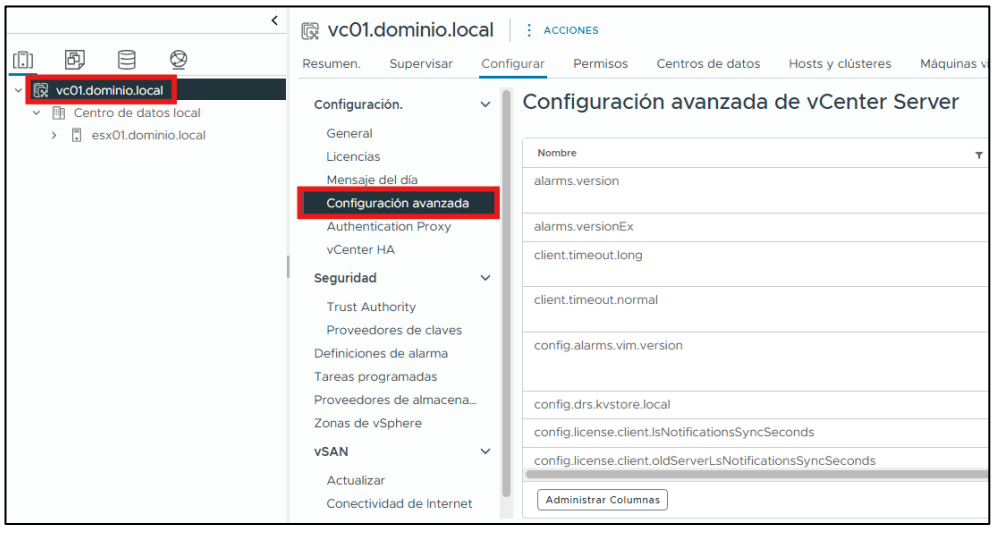
2. CONFIGURACIÓN DE SEGURIDAD EN VCENTER

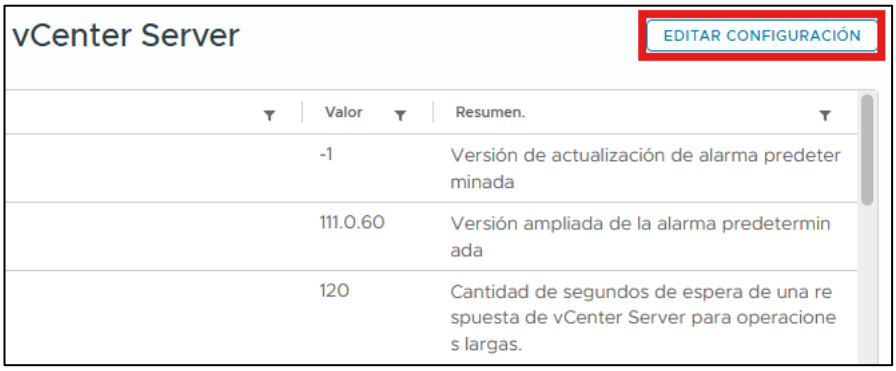
El resto de las configuraciones de seguridad que aplicarán al servidor de ESXi se realizarán a través del servidor de vCenter. Previamente se va a aplicar la configuración de seguridad de los propios servidores de vCenter. Deberá realizar los siguientes pasos en cada servidor de vCenter que pertenezca a la infraestructura.

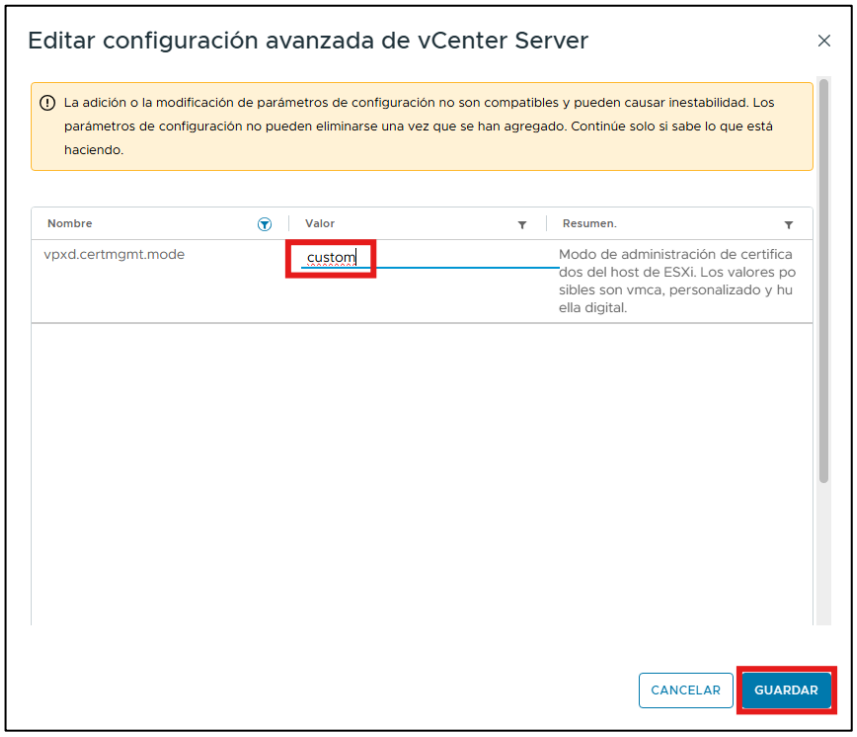
Paso	Descripción
27.	Inicie sesión, a través del vSphere client mediante html5, en el servidor de vCenter. Para ello, en su navegador, introduzca la url “https://<FQDN del servidor vCenter>/UI”. Si el navegador muestra una advertencia indicando que el sitio no es seguro, puede ignorarla. Esto se debe a que se está utilizando un certificado autofirmado. Haga clic en la opción "Avanzado". 
28.	Haga clic en la opción “Continuar al sitio”.  **Nota:** La apariencia de la advertencia de seguridad y las opciones disponibles pueden variar según el navegador utilizado. En este ejemplo se ha utilizado Microsoft Edge.

Paso	Descripción
29.	El cliente basado en Flash (vSphere Web Client - Flex) ha sido retirado oficialmente y ya no es compatible en vSphere 8. Utilizaremos exclusivamente el vSphere Client (HTML5) para acceder y gestionar el entorno. 
30.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”.  **Nota:** Según los métodos de autenticación empleados, la pantalla podría diferir de la captura mostrada.
31.	Se va a realizar una serie de pasos previos en el propio servidor de vCenter. Estas configuraciones deberán ser realizadas en los diferentes servidores de vCenter que pertenezcan a la organización. **Nota:** No es objeto de esta guía especificar los métodos de emisión de los certificados. Para más información sobre la generación y firma de certificados, consulte la guía CCN-STICEntidad de Certificación. Los pasos descritos a continuación, se realizan en el servidor de vCenter y tendrán que ser aplicados en cada servidor de vCenter implementado en la infraestructura.

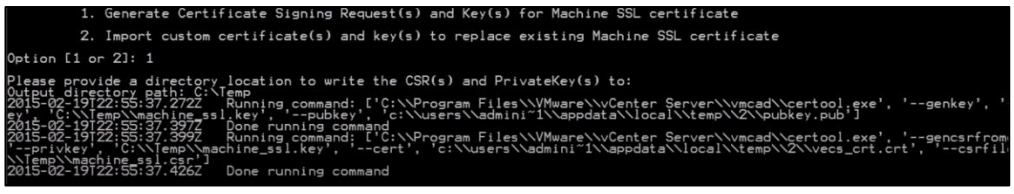
Paso	Descripción
32.	Los siguientes pasos consistirán en añadir y publicar en la infraestructura el certificado de la entidad de certificación raíz y el certificado de la subordinada. Una vez realizado esto, será posible añadir certificados de servidor a los servidores de ESXi. **Nota:** Antes de realizar este proceso, el servidor de vCenter no debe tener conectados los servidores de ESXi. En caso de haber añadido el servidor ESXi se deberá desconectar y se reconectará una vez realizados los pasos siguientes hasta el reinicio del servidor (Paso 56). Para desconectar el servidor ESXi, selecciónelo en el menú de la izquierda y con el botón derecho del ratón seleccione "Conexión → Desconectar" en el menú contextual que se ha desplegado. 
33.	El siguiente paso debe realizarse en el vCenter Server Appliance (VCSA), y consiste en publicar los certificados de la Entidad Certificadora (CA) raíz y, si aplica, de la Entidad Certificadora subordinada (SubCA) en el almacén de confianza del dominio de SSO (vsphere.local). Para ello, se utilizará el siguiente comando desde la consola del **appliance de vCenter (VCSA)**: **/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert <ruta_al_certificado_CA_base64>** **Nota:** Si el certificado fue firmado por una entidad certificadora subordinada, será necesario ejecutar, también, el siguiente comando: - **/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert <ruta_al_certificado_CA_subordinada_base64>** Asegúrese de que el certificado esté exportado en formato Base64 codificado (PEM).
34.	En caso de haber cerrado el navegador, inicie sesión, a través del vSphere client mediante html5, en el servidor de vCenter. Para ello, en su navegador, introduzca la url "https://<FQDN del servidor>/UI". 

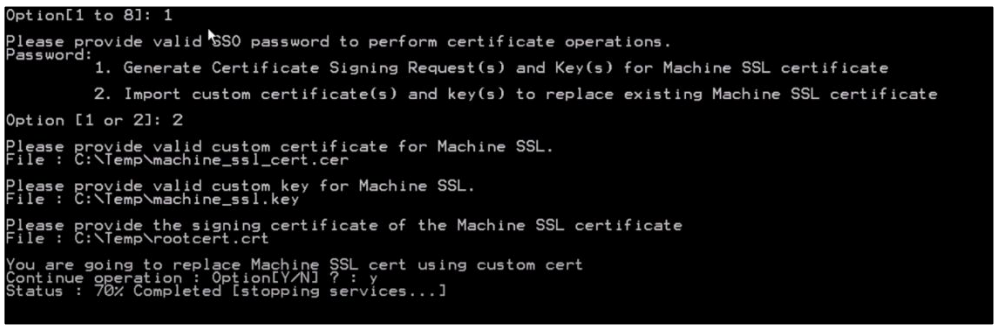
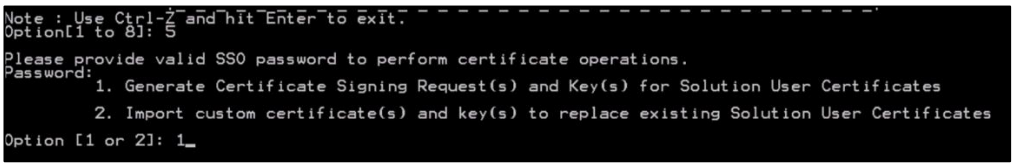
Paso	Descripción
35.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”. 
36.	A continuación, será necesario cambiar el modo de uso del certificado al modo personalizado. Para ello, a través de la consola de vSphere Client, pulse sobre el icono que corresponde a “Host y clústeres”. 
37.	En el menú de la izquierda, pulse sobre el objeto con el nombre del servidor de vCenter. 
38.	Vaya a la pestaña “Configurar” y seleccione “Configuración Avanzada”. 

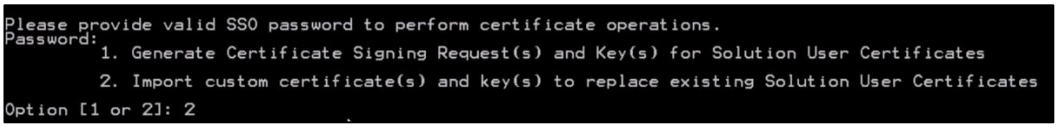
Paso	Descripción
39.	Pulse sobre “Editar configuración” en la zona superior derecha. 
40.	Pulse sobre la flecha a la derecha del título de la columna “Nombre”. 
41.	Teclee “vpxd.certmgmt.mode” y pulse la “X” de la zona superior para cerrar la ventana emergente. 

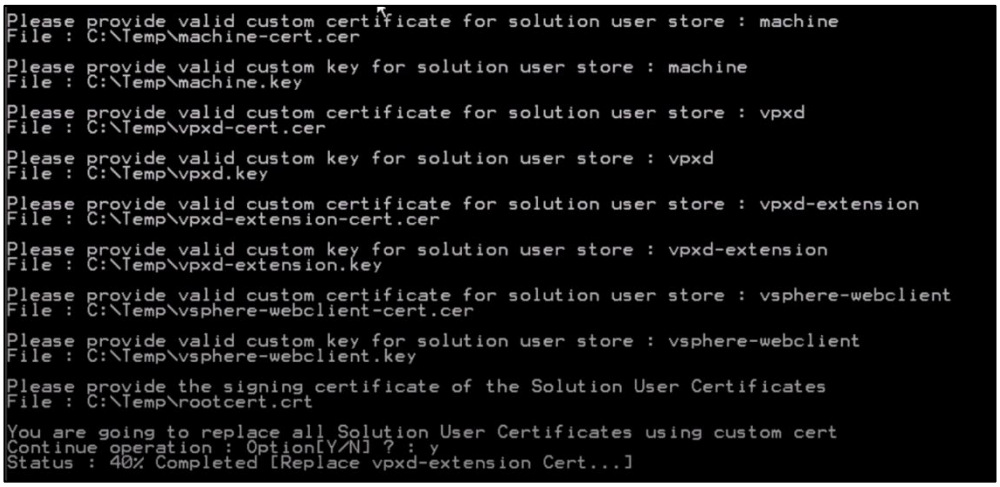
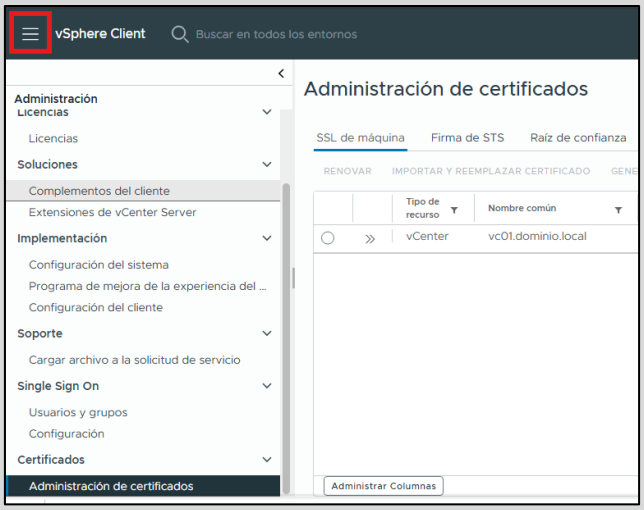
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>42.</td><td>Sustituya el valor “vmca” por “custom” y pulse “Guardar”
 
</td></tr>
<tr><td>43.</td><td>Se sustituirá, en este momento, el certificado de equipo existente por uno emitido por la entidad certificadora de terceros autorizada. El fichero de solicitud CSR que se deberá generar deberá responder a las siguientes características (es posible generar el fichero de solicitud CSR mediante una aplicación en el servidor de vCenter):
<table>
<tr><th>Elemento</th><th>Valor</th></tr>
<tr><td>Tamaño de clave</td><td>2048 bits o más</td></tr>
<tr><td>Formato</td><td>PEM / clave pública en formato CRT</td></tr>
<tr><td>SubjectAltName -> DNS Name</td><td>=<FQDN de la máquina></td></tr>
<tr><td>Usos permitidos</td><td>Firma digital, no repudio, cifrado de clave</td></tr>
<tr><td>Momento de validez</td><td>Un día antes del tiempo de solicitud</td></tr>
<tr><td>CN (y SubjectAltName)</td><td>Nombre del Host o dirección IP (debe coincidir con el nombre con el que se ha registrado el servidor de vCenter)</td></tr>
</table>
Así mismo, deberá emitir certificados para las aplicaciones web que vaya a utilizar (vpxd, vsphere-webclient, etc).

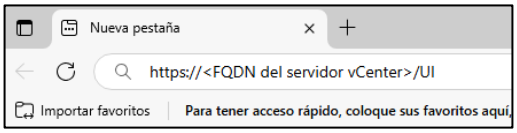
Nota: No es objeto de esta guía especificar los métodos de emisión de los certificados.</td></tr>
</table>

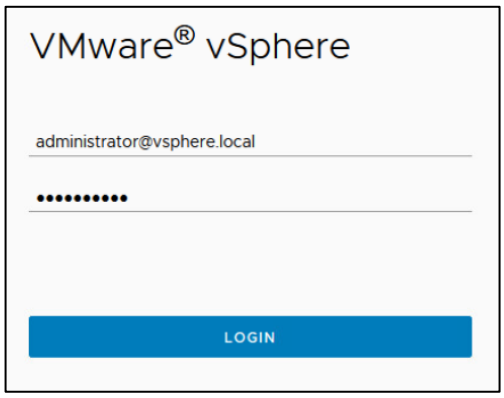
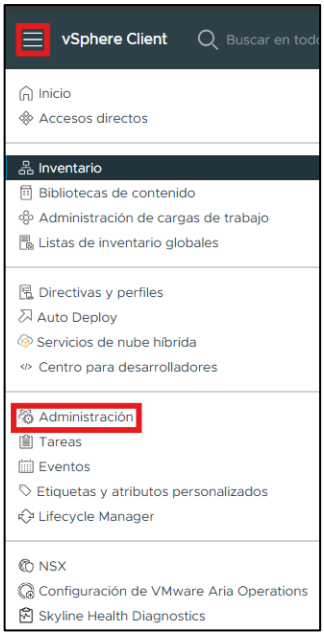
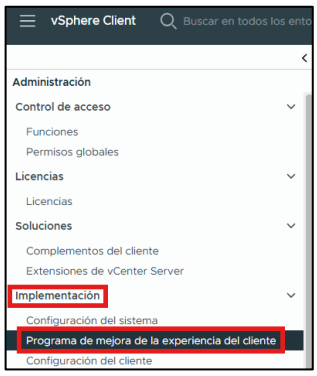
Paso	Descripción
44.	En el ejemplo se ha ejecutado la aplicación “certificate-manager” desde un servidor de vCenter sobre plataforma Windows. La ruta donde se encuentra dicha aplicación es “C:\Archivos de programa\VMware\vCenter Server\vmcad\certificate-manager.bat”. Pulse botón derecho sobre el ejecutable y seleccione “Ejecutar como administrador” en el menú contextual que se ha desplegado.  **Nota:** Si se desea instalar la aplicación desde un vCenter Appliance sobre Linux la ruta es **“/usr/lib/vmware-/vmca/bin/certificate-manager”**
45.	Seleccione la opción “1” en el menú principal de la aplicación, pulse “Enter” e introduzca un usuario con permisos para la gestión de certificados en el servidor. 
46.	Seleccione la opción “1” para generar el fichero de solicitud de certificado CSR (y el fichero de clave “.key”), pulse “Enter” y especifique la ruta donde almacenará el fichero de solicitud, pulse “Enter” de nuevo. 
47.	Envíe el fichero CSR generado a una entidad certificadora autorizada para que genere el certificado a partir de la solicitud. **Nota:** No es objeto de esta guía especificar los métodos de emisión de los certificados.

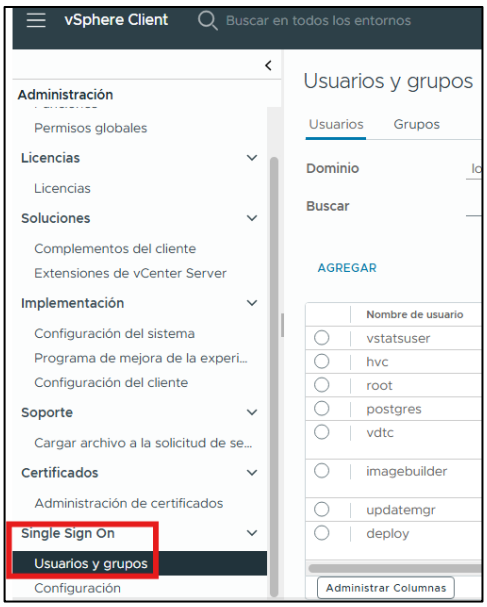
Paso	Descripción
48.	En caso de haber cerrado la sesión, vuelva a ejecutar la aplicación y seleccione la opción “1” en el menú principal (introduzca credenciales válidas), pulse “Enter” e introduzca un usuario con permisos para la gestión de certificados en el servidor. 
49.	Seleccione la opción “2” para importar el certificado generado, pulse “Enter” y especifique la ruta donde se encuentra el fichero generado por la entidad certificadora, la clave “.key” y el certificado de la entidad certificadora, pulse “Enter” de nuevo. Pulse “y” finalmente para confirmar la operación.  **Nota:** La ruta debe incluir también el fichero “.key” generado durante la fase de solicitud y el certificado de la entidad certificadora autorizada. De igual modo, la lista de certificados revocados (CRL) deberá ser accesible desde el servidor de vCenter para que este proceso pueda validar el certificado.
50.	Seleccione la opción “5”, “Enter” y “1” para generar los ficheros de solicitud de certificado CSR (y los ficheros de clave “.key”) de las diferentes soluciones web. Pulse “Enter” de nuevo. 
51.	Pulse “Enter” y especifique la ruta donde almacenarán los ficheros de solicitud, pulse “Enter” de nuevo.  **Nota:** Se generarán varios ficheros correspondientes a las claves y solicitudes de cada aplicación.

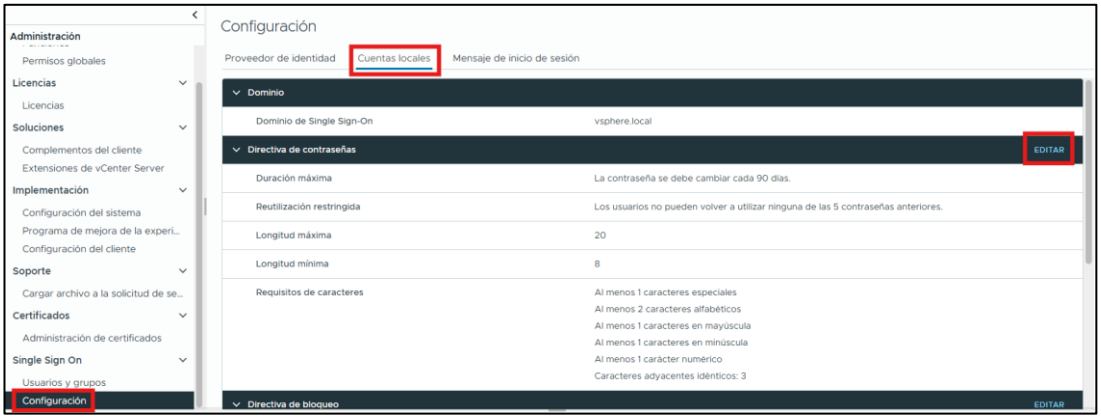
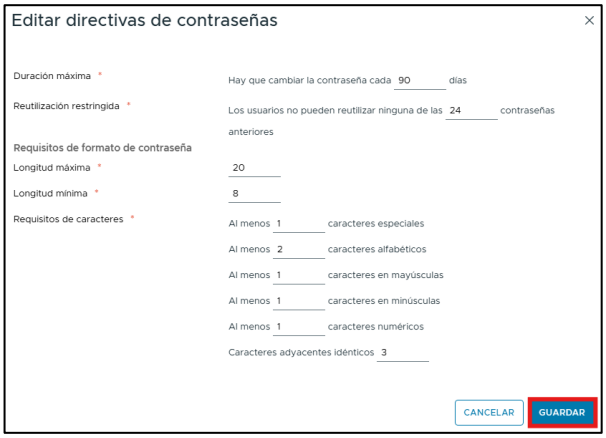
Paso	Descripción
52.	En caso de haber cerrado la sesión, vuelva a ejecutar la aplicación y seleccione la opción “5” en el menú principal (introduzca credenciales válidas), pulse “Enter” e introduzca un usuario con permisos para la gestión de certificados en el servidor. 
53.	Seleccione la opción “2” para importar los certificados generados y pulse “Enter.  **Nota:** La ruta debe incluir también los ficheros “.key” generados durante la fase de solicitud y el certificado de la entidad certificado.

Paso	Descripción
54.	Especifique las rutas donde se encuentran los ficheros generados por la entidad certificadora, las claves ".key" y el certificado de la entidad certificadora, pulse "Enter" de nuevo. Pulse "y" finalmente para confirmar la operación.  **Nota:** Es posible gestionar la importación de los certificados, también, a través de vSphere client mediante el **"Menú principal → Administración → Administración de certificados"**. 

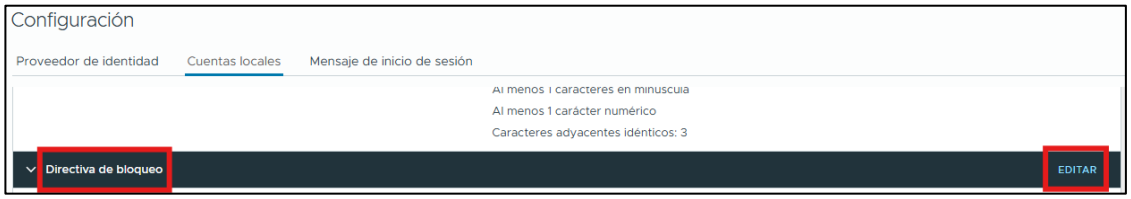
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>55.</td><td>Revise los servicios principales del vCenter Server Appliance y asegúrese de que los siguientes se encuentren configurados con inicio automático y en estado activo:
<table>
<tr><th>Servicio</th><th>Inicio</th><th>OK/NOK</th></tr>
<tr><td>VMWareDirectoryService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareIdentityMgmtService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareCertificateService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareDNSService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareAfdService</td><td>Automático</td><td></td></tr>
<tr><td>VMwareSTS</td><td>Automático</td><td></td></tr>
<tr><td>vmon</td><td>Automático</td><td></td></tr>
<tr><td>Vmware-cis-config</td><td>Automático</td><td></td></tr>
</table>
Nota: La disponibilidad de algunos servicios puede variar en función de los componentes habilitados durante la instalación de vCenter. Todos los servicios son gestionados por el gestor de procesos vmon, y se ejecutan bajo el contexto del sistema root en el appliance VCSA basado en Photon OS.
Verificación del estado de los servicios
Para consultar el estado actual de los servicios en VCSA, utilice el siguiente comando desde una sesión SSH o desde la consola directa del appliance:
- service-control –status
En VCSA, los servicios corren bajo el usuario root y sus configuraciones se encuentran gestionadas desde /etc/init.d/, /usr/lib/vmware/ o mediante systemd.
Para revisar permisos de ejecución:
- ls -l /etc/init.d/
- ls -l /usr/lib/vmware/</td></tr>
<tr><td>56.</td><td>Reinicie el servidor de vCenter server para aplicar los cambios.</td></tr>
<tr><td>57.</td><td>Una vez reiniciado el servicio, inicie sesión a través del vSphere client mediante html5, en el servidor de vCenter. Para ello, en su navegador, introduzca la url “https://<FQDN del servidor vCenter>/UI”.

</td></tr>
</table>

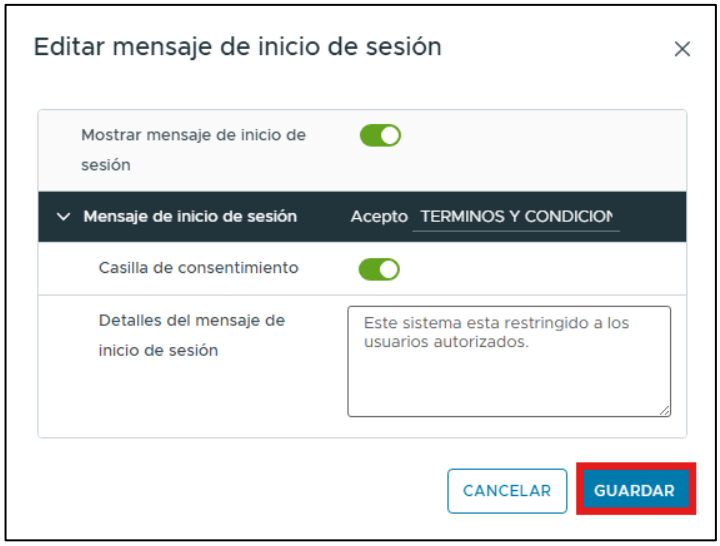
Paso	Descripción
58.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”.  **Nota:** Según los métodos de autenticación empleados, la pantalla podría diferir de la captura mostrada.
59.	Pulse sobre el menú principal (☰) para acceder a la configuración del servidor de vCenter y seleccione “Administración” en el menú contextual que se ha desplegado. 
60.	Pulse sobre “Implementación → Programa de mejora de la experiencia del cliente”. 

Paso	Descripción
61.	El estado correcto debe ser “No Unido”. En caso de que el estado sea “Unido”, pulse sobre “Abandonar” en la zona inferior de la pantalla central. 
62.	Confirme pulsando sobre “Abandonar el programa”. 
63.	En el apartado “SingleSignOn” podrá añadir los “Usuarios y grupos que tendrán acceso al servicio de VMware vSphere 8.x y los privilegios que se les otorgarán.  **Nota:** Adapte los usuarios, grupos y permisos a las necesidades de la organización y rigiéndose por los criterios indicados en la presente guía. A partir de esta categoría del ENS será necesario el uso de grupos personalizados con permisos administrativos específicos y usuarios únicos para responder a la necesidad de segregación de roles y trazabilidad de actuaciones.

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>64.</td><td>Así mismo, en el apartado “SingleSignOn”, pulse sobre “Configuración” y en la pestaña “Cuentas locales”, pulse sobre “Directiva de contraseñas” y sobre “Editar”.
 
</td></tr>
<tr><td>65.</td><td>En la ventana emergente, establezca los siguientes parámetros y pulse “Guardar”.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Duración máxima</td><td>Hay que cambiar la contraseña cada “60” días</td></tr>
<tr><td>Reutilización restringida</td><td>Los usuarios no pueden reutilizar ninguna de las “24” contraseñas anteriores</td></tr>
<tr><td>Longitud mínima</td><td>“12”</td></tr>
<tr><td colspan="2">Al menos “1” caracteres especiales</td></tr>
<tr><td colspan="2">Al menos “1” caracteres en mayúsculas</td></tr>
<tr><td colspan="2">Al menos “1” caracteres en minúsculas</td></tr>
<tr><td colspan="2">Al menos “1” caracteres numéricos</td></tr>
</table>


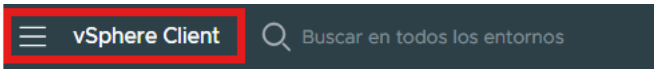
Nota: Estos parámetros corresponden a la complejidad mínima a establecer, el resto de las configuraciones refuerzan dicha complejidad. Mantenerlos con los valores indicados es una acción correcta de cara a mejorar la seguridad.</td></tr>
</table>

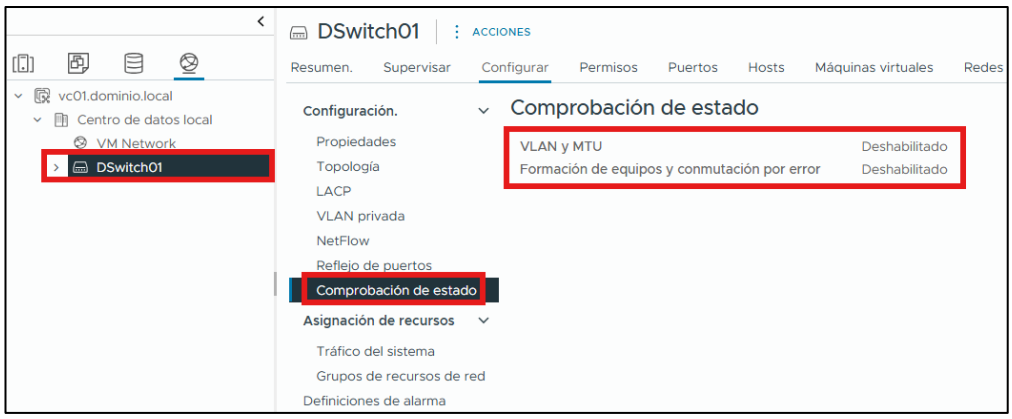
Paso	Descripción
66.	Sitúese sobre “Directiva de bloqueo” y pulse sobre “Editar”. 
67.	En la ventana emergente, establezca los siguientes parámetros y pulse “Guardar”. – Cantidad máxima de intentos fallidos de inicio de sesión: “8”. – Intervalo de tiempo entre errores: 1800 segundos. – Tiempo de desbloqueo: 3600 segundos. 
68.	Pulse sobre la pestaña “Mensaje de inicio de sesión” y sobre “Editar”. 

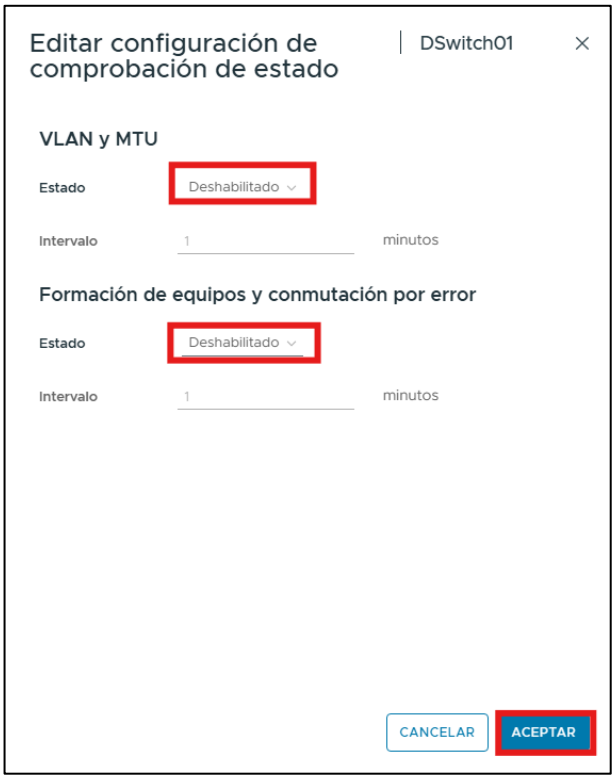
Paso	Descripción
69.	Pulse sobre los botones correspondientes a “Mostrar mensaje de inicio de sesión” y “Casilla de consentimiento” para habilitarlos y establezca un mensaje de seguridad. Pulse “Guardar” para continuar.  **Nota:** Adaptar el mensaje a las necesidades de su organización. A partir de este momento. El sistema, además de solicitar credenciales obliga a revisar las condiciones de acceso para marcar la aceptación de entrada a la aplicación. Podrán implementarse factores adicionales tales como autenticación por tarjeta inteligente o RSA secure ID. 

2.1. CONFIGURACIÓN EN CONMUTADORES VIRTUALES DISTRIBUIDOS

Las configuraciones descritas a continuación son a nivel de conmutadores virtuales distribuidos. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los conmutadores virtuales distribuidos existentes en el servicio de vCenter.

Paso	Descripción
70.	Haga clic sobre el icono “vSphere Client” para ir al menú principal. 
71.	Seleccione el icono correspondiente a “Redes”. 

Paso	Descripción
72.	Sitúese sobre cada conmutador distribuido y en la pestaña “Configurar” pulse sobre el elemento “Comprobación de estado”. A continuación, en caso de que esté habilitado alguno de estos dos elementos, deberá deshabilitarlos: – VLAN y MTU. – Formación de equipos y conmutación por error.  **Nota:** Estas opciones solamente deberían ser habilitadas en momentos de resolución de problemas y de forma temporal.
73.	Para ello, pulse sobre “Editar”. 

Paso	Descripción
74.	En la ventana emergente, modifique los campos de estado a “Deshabilitado” y pulse “Aceptar”. 

2.1.1. CONFIGURACIÓN EN GRUPOS DE PUERTOS

Las configuraciones descritas a continuación son a nivel de grupos de puertos. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los grupos de puertos existentes en los distintos conmutadores presentes en el servicio de vCenter.

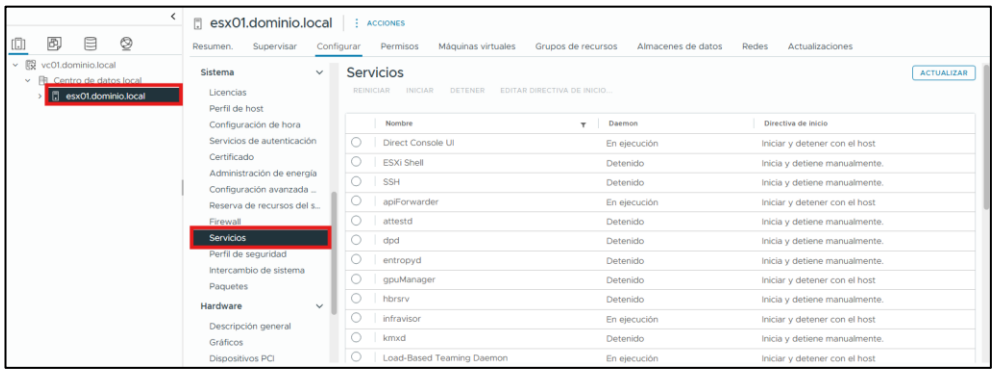
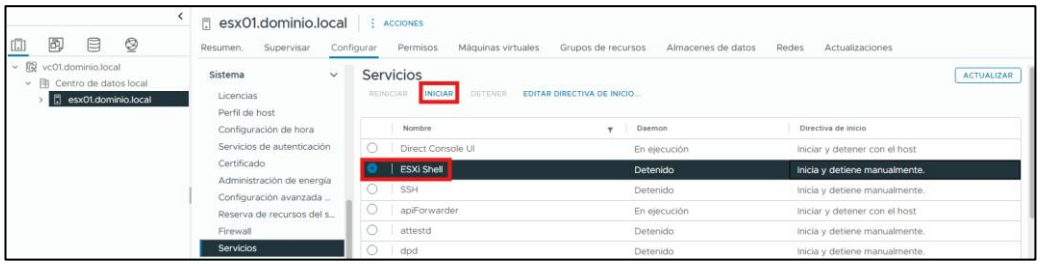
Paso	Descripción
75.	En el menú de la izquierda, seleccione el icono correspondiente a “Redes”. 

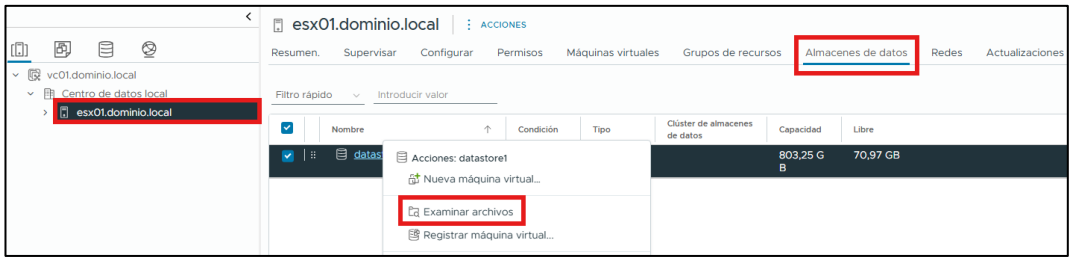
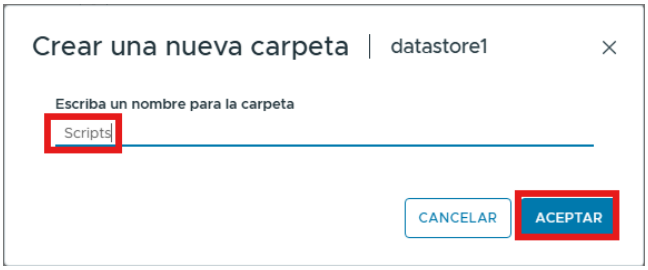
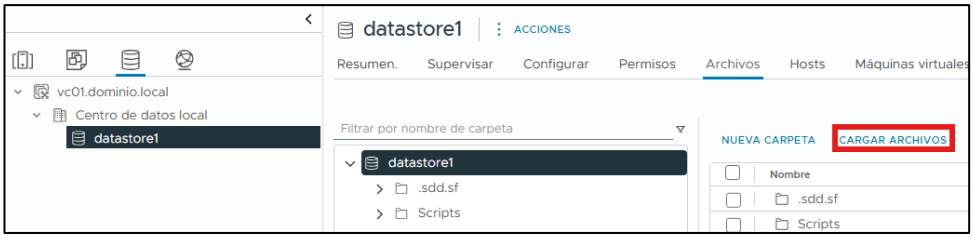
Paso	Descripción
76.	Sitúese sobre cada grupo de puertos (que se encontrarán dentro de la rama de cada conmutador virtual) y en la pestaña “Configurar”, seleccione “Directivas” y compruebe que las siguientes directivas de seguridad tienen el valor “Rechazar” y si no es así se deberá modificar el valor de las directivas: – Modo promiscuo – Cambios de dirección MAC – Transmisiones falsificadas 
77.	Para modificar las directivas pulse sobre “Editar”. 
78.	En la ventana emergente pulse sobre “Seguridad”, modifique las directivas deseadas y pulse “ACEPTAR” para validar la configuración. 

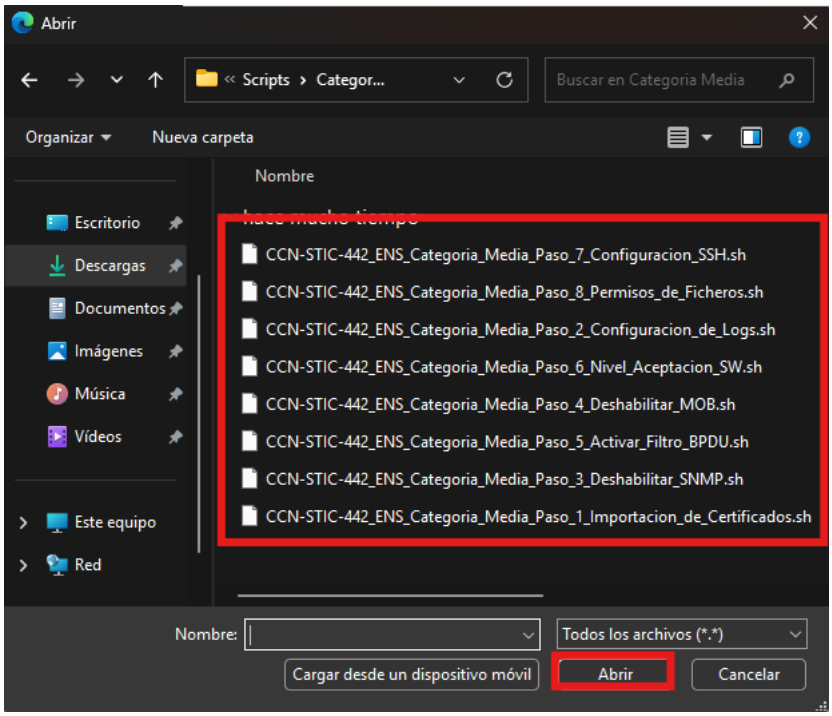
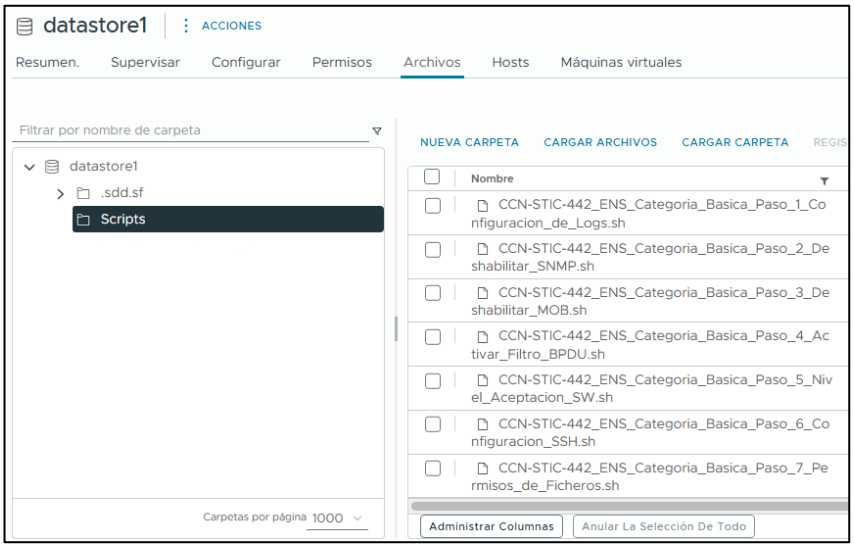
2.2. CONFIGURACIÓN DE SEGURIDAD EN SERVIDORES ESXI

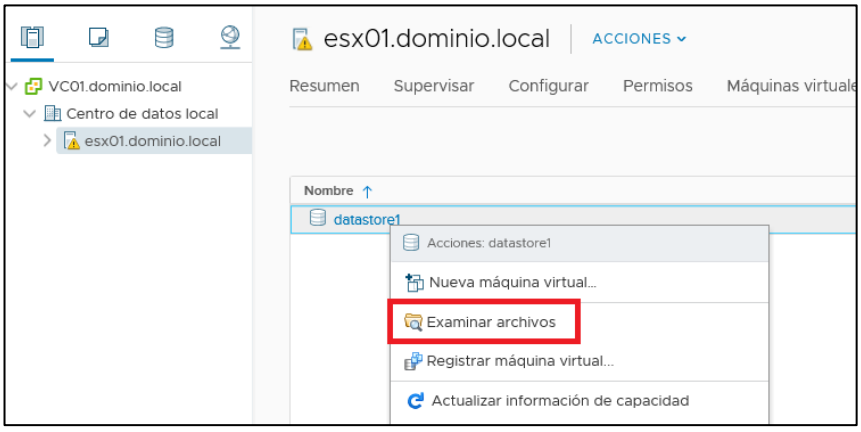
Los pasos descritos a continuación se realizan a nivel de servidor ESXi y deberán ser aplicados en cada uno de los host ESXi que se añadan al servidor de vCenter. Existe la posibilidad de establecer perfiles de host para definir las configuraciones, a modo de plantilla, de modo que se homogenice y automatice el proceso de implementación de los servidores de ESXi.

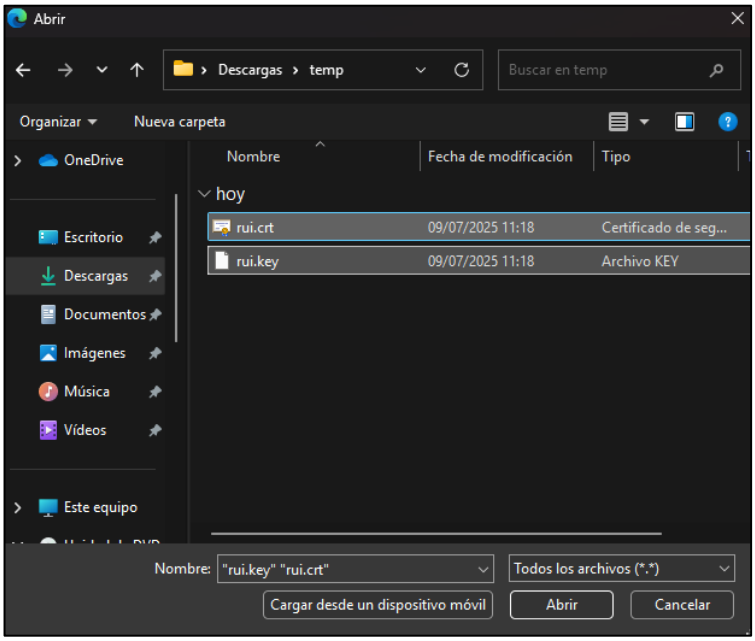
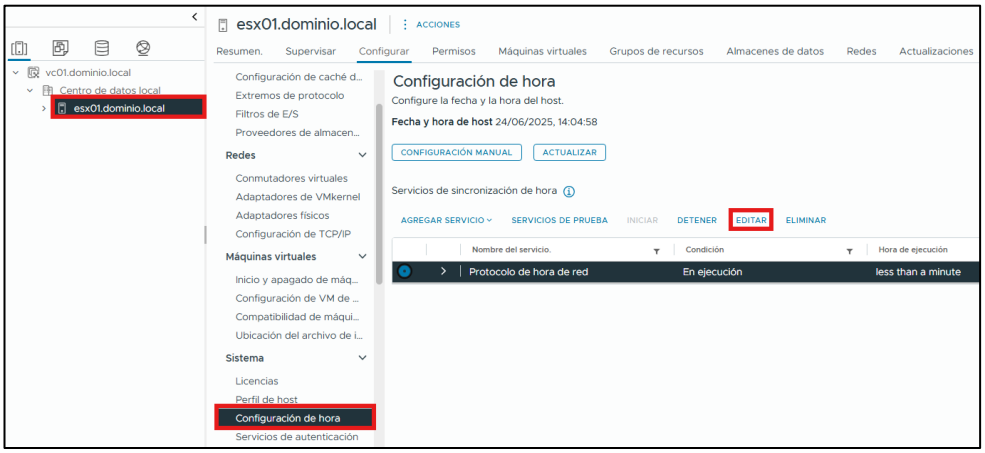
Muchos de los pasos se continúan realizando a través del cliente de vSphere pero la ejecución de scripts se realizará mediante una conexión directa por SSH a la consola ESXi Shell del host al que queremos aplicarle seguridad. Por tanto, será necesario activar los servicios de SSH y ESXi Shell en el host ESXi y, una vez completadas las configuraciones, se volverán a deshabilitar ambos servicios.

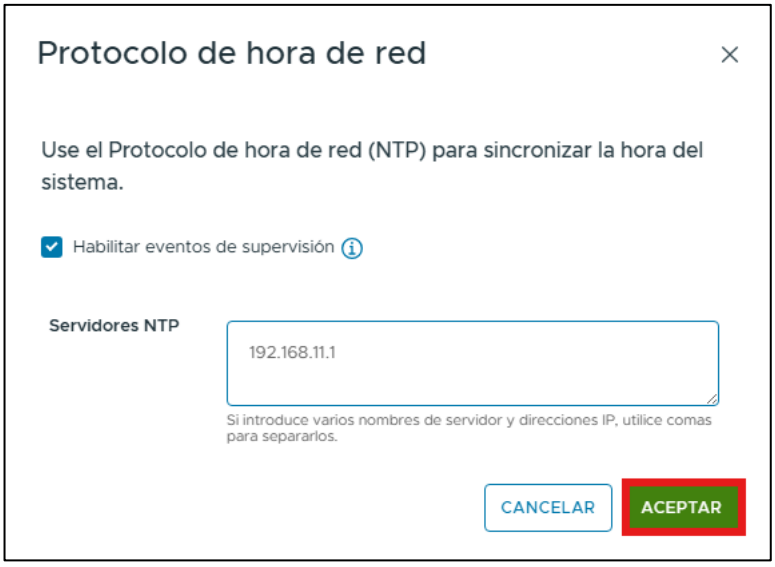
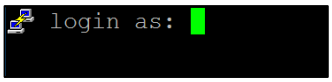
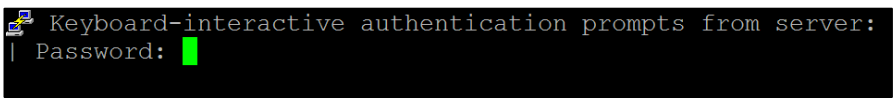
Paso	Descripción
79.	En el menú de la izquierda, pulse sobre el icono que corresponde a “Host y clústeres”. 
80.	Sitúese sobre el objeto “<FQDN del servidor ESXi>” sobre el que quiere aplicar la seguridad y en la pestaña “Configurar”, seleccione “Servicios”. 
81.	Sitúese sobre el servicio “ESX Shell” y pulse el botón “Iniciar”.  **Nota:** Si el servicio ya se encuentra activo no será necesario realizar ninguna acción.
82.	Realice la misma operación con el servicio “SSH”.  **Nota:** Si el servicio ya se encuentra activo no será necesario realizar ninguna acción.

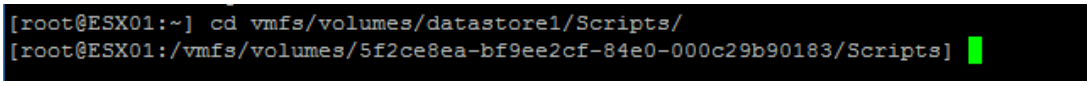
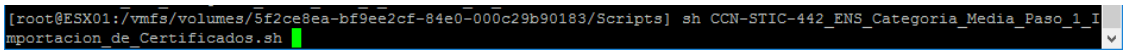
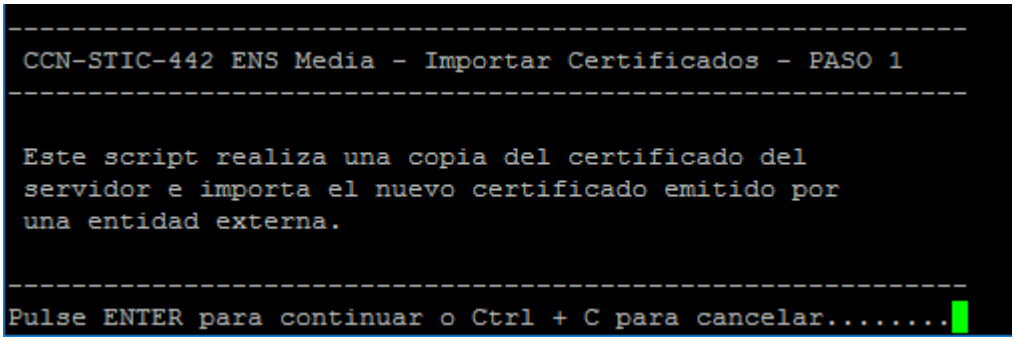
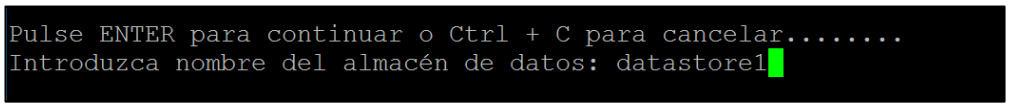
Paso	Descripción
83.	Sitúese sobre el objeto <FQDN del Servidor ESXi> y en la pestaña “Almacenes de datos”, seleccione, con el botón derecho del ratón, el almacén donde alojará los Scripts de configuración de seguridad de la presente guía y pulse sobre “Examinar archivos”.  **Nota:** En el ejemplo se ha utilizado el almacén que se ha creado por defecto al añadir el host a vCenter. Adapte la configuración a las necesidades de su entorno.
84.	Seleccione “Nueva Carpeta” para crear la carpeta que contendrá los Scripts. 
85.	Establezca el nombre “Scripts” a la carpeta y pulse “Aceptar”. 
86.	Haga clic sobre la carpeta “Scripts” recién creada y seleccione “Cargar archivos”. 

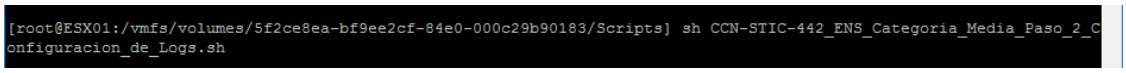
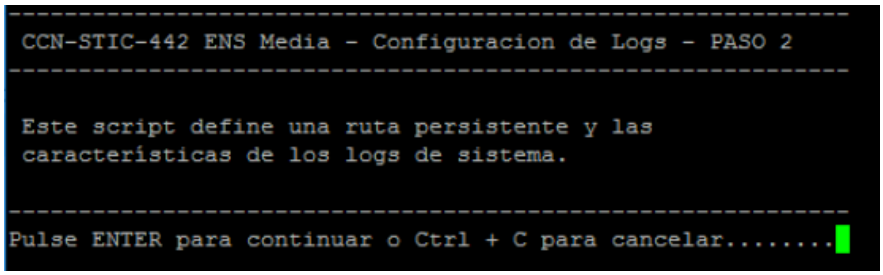
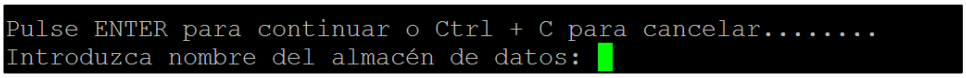
Paso	Descripción
87.	Localice los scripts que se aplican en este anexo, selecciónelos todos y pulse “Abrir”. 
88.	Los scripts quedarán almacenados en el almacén de datos. 

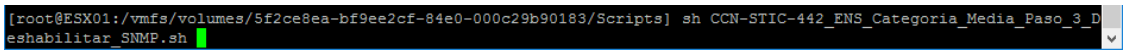
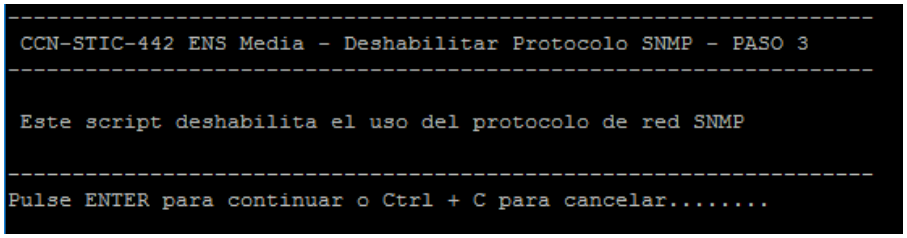
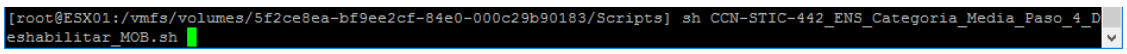
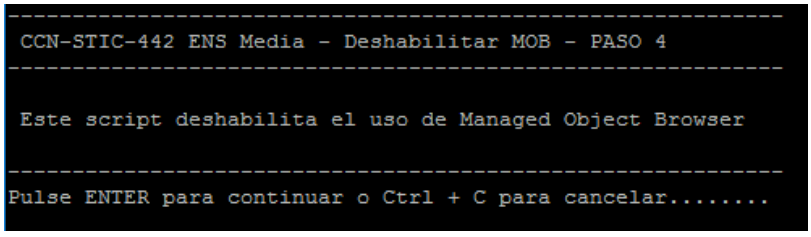
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>89.</td><td>Para establecer comunicaciones seguras entre el servidor de vCenter, y el servidor ESXi, se deberán generar y añadir certificados válidos emitidos y firmados por una entidad certificadora válida y confiable. El fichero CSR que se deberá generar deberá responder a las siguientes características:
<table>
<tr><th>Elemento</th><th>Valor</th></tr>
<tr><td>Tamaño de clave</td><td>2048 bits o más</td></tr>
<tr><td>Formato</td><td>PEM / clave pública en formato CRT</td></tr>
<tr><td>SubjectAltName -> DNS Name</td><td>=<FQDN de la máquina ESXi></td></tr>
<tr><td>Usos permitidos</td><td>Firma digital, no repudio, cifrado de clave</td></tr>
<tr><td>Momento de validez</td><td>Un día antes del tiempo de solicitud</td></tr>
<tr><td>CN (y SubjectAltName)</td><td>Nombre del Host o dirección IP (debe coincidir con el nombre con el que se ha registrado el servidor de ESXi)</td></tr>
</table>
Nota: No es objeto de esta guía especificar los métodos de emisión de los certificados.</td></tr>
<tr><td>90.</td><td>Una vez se disponga del fichero “.crt” firmado por la entidad certificadora autorizada y el fichero “.key” con la clave privada del certificado, se deberán renombrar a “rui.crt” y “rui.key” para posteriormente almacenarlos en la carpeta “Scripts” creada en pasos anteriores.</td></tr>
<tr><td>91.</td><td>Sitúese, de nuevo, sobre el objeto <FQDN del Servidor> y en la pestaña “Almacenes de datos”, seleccione, con el botón derecho del ratón, el almacén donde alojará los Scripts de configuración de seguridad de la presente guía y pulse sobre “Examinar archivos”.
 
</td></tr>
<tr><td>92.</td><td>Haga clic sobre la carpeta “Scripts” y seleccione “Cargar archivos”.
 
</td></tr>
</table>

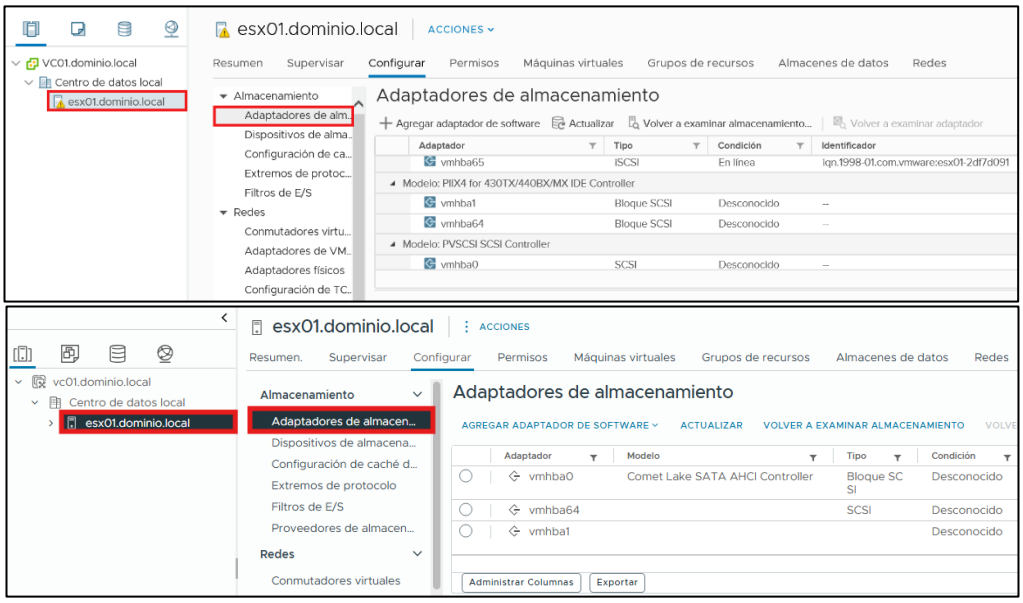
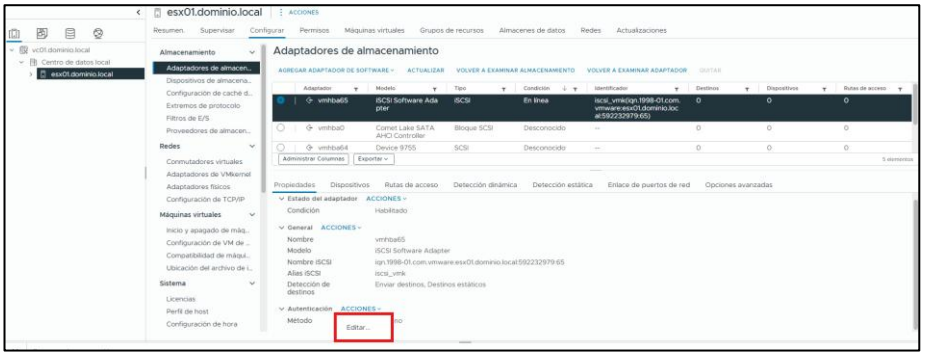
Paso	Descripción
93.	Localice los dos ficheros y cárguelos en el servidor seleccionándolos y pulsando “Abrir”.  **Nota:** No cierre el navegador y manténgalo en segundo plano mientras realiza los pasos siguientes.
94.	El siguiente paso consiste en configurar el servidor para que sincronice la hora con la del servidor NTP. De nuevo, a través del navegador, pulse sobre el icono correspondiente a “Hosts y clústeres”. 
95.	Sitúese sobre el objeto <FQDN del Servidor ESXi> y en la pestaña “Configurar”, seleccione “Configuración de hora”, “Protocolo de hora de red” y pulse “Editar”. 

Paso	Descripción
96.	Introduzca la dirección o direcciones IP del servidor o servidores NTP que quiera utilizar para la sincronización. Pulse “Aceptar” para guardar la configuración.  **Nota:** Deberá adaptar las configuraciones a las necesidades del entorno y, en caso de utilizar el protocolo NTP, se deberán habilitar las configuraciones que lo permitan. No cierre el navegador y manténgalo en segundo plano mientras realiza los pasos siguientes.
97.	Para los siguientes pasos, deberá conectarse al host a través de un cliente SSH. Se le solicitarán credenciales de acceso. Introduzca el usuario que configuró en el servidor de ESXi en los pasos iniciales del presente apartado.  **Nota:** para establecer una conexión SSH hacia el servidor ESXi, se deberá permitir el tráfico correspondiente. El cliente utiliza, por defecto, el puerto 22 para realizar la conexión. Deberá adaptar estos pasos a las necesidades de su entorno. Al no estar utilizando certificados confiables, es posible que el cliente SSH muestra una advertencia. Puede continuar la conexión.
98.	Introduzca la contraseña definida para dicho usuario. 

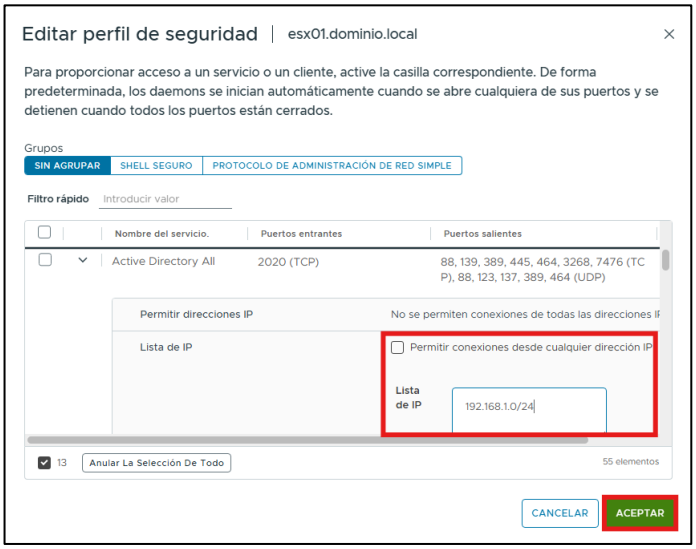
Paso	Descripción
99.	Acceda a la ruta del almacén de datos que ha configurado en los pasos anteriores a través de la siguiente línea de comandos: **# cd /vmfs/volumes/<almacén de datos>/Scripts**  **Nota:** La ruta seleccionada es la ruta en la que se almacenan por defecto los almacenes de datos. Deberá adaptar estos pasos a las necesidades de su entorno.
100.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Media_Paso_1_Importacion_de _Certificados.sh" mediante el siguiente comando y pulse "Enter" para continuar: **# sh CCN-STIC-442_ENS_Categoria_Media_Paso_1_Importacion_de_Certificados.sh** 
101.	Pulse "Enter", de nuevo, para continuar. 
102.	El sistema le solicitará el nombre del almacén de datos donde se encuentra la carpeta Scripts. Introduzca el nombre del almacén respetando mayúsculas, minúsculas, puntuación, espacios, etc. y pulse "Enter" para continuar.  **Nota:** En el ejemplo, el almacén de datos se llama "datastore1". Este script asume que la ruta donde se encuentran los ficheros de origen es "/vmfs/volumes/<nombre de almacén de datos>/Scripts" y los ficheros de destino en "/etc/vmware/ssl/". En caso de que las rutas sean distintas se deberá modificar en el script.

Paso	Descripción
103.	En este momento y si fuera posible, sería recomendable aplicar las actualizaciones sobre el servidor de ESXi. Para llevar a cabo esta acción y teniendo en cuenta que el entorno puede o no disponer de conectividad a internet, se puede hacer uso de un repositorio centralizado por medio de vSphere Update Manager, un plugin que puede ser añadido a la configuración de vCenter Server. **Nota:** Una vez las actualizaciones son accesibles, los comandos a utilizar, a través del CLI de ESXi, serían los siguientes: - **# esxcli software profile get** (para consultar el estado de las actualizaciones) - **# esxcli software vib get** (para consultar el estado de las actualizaciones) - **# esxcli software profile update** (para aplicar las actualizaciones) - **# esxcli software vib update** (para aplicar las actualizaciones) Recuerde que para poder ejecutar estos comandos deberá realizarlos desde la consola directa o activando el acceso SSH. En caso de haber aplicado las configuraciones de la guía, adicionalmente deberá pertenecer al grupo de excepciones en el modo de bloqueo o rebajar el nivel de bloqueo temporalmente siguiendo los pasos inversos a los descritos. **Nota:** No cierre la sesión SSH y manténgala en segundo plano mientras realiza los pasos siguientes.
104.	A continuación, se modificarán los parámetros relativos a los registros de auditoría o ficheros log. Para ello, deberá utilizar de nuevo la sesión SSH que activó para realizar los pasos anteriores. Ejecute el script "CCN-STIC-442_ENS_Categoria_Media _Paso_2_Configuracion_de_Logs.sh" mediante el siguiente comando y pulse "Enter". **# sh CCN-STIC-442_ENS_Categoria_Media_Paso_2_Configuracion_de_Logs.sh** 
105.	Pulse "Enter", de nuevo, para continuar. 
106.	El sistema le solicitará el nombre del almacén de datos donde se encuentra la carpeta Scripts. Introduzca el nombre del almacén respetando mayúsculas, minúsculas, puntuación, espacios, etc. Pulse "Enter" para continuar.  **Nota:** En el ejemplo, el almacén de datos se llama "datastore1".

Paso	Descripción
107.	Es recomendable también el uso de un servidor de logs externo al que se exporten los logs del servidor. Para establecer dicha configuración, a través del vSphere Client, puede situarse en el servidor ESXi y seleccionar "Configuración → Configuración avanzada". Los campos a modificar son los siguientes: – "Syslog.global.logHost" → "<Nombre del Host>". – "Syslog.global.logDirUnique" → "True".
108.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Media_Paso_3_Deshabilitar_SNMP.sh" mediante el siguiente comando y pulse "Enter" para continuar. **# sh CCN-STIC-442_ENS_Categoria_Media_Paso_3_Deshabilitar_SNMP.sh**  **Nota:** En caso de que se haga uso del protocolo SNMP, no se debería ejecutar este paso. En su lugar, se debería ejecutar lo siguiente para establecer la seguridad adecuada en el uso del protocolo y evitar que elementos externos puedan extraer información de datos SNMP: - **# esxcli conn_options system snmp set --communities [COMMUNITY]** - **# esxcli conn_options system snmp set --targets [TARGET]@[PORT]/[COMMUNITY]** - **# esxcli conn_options system snmp set --enable true**
109.	Pulse "Enter", de nuevo, para continuar. El Script indicará que ha finalizado. 
110.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Media_Paso_4_Deshabilitar_MOB.sh" mediante el siguiente comando y pulse "Enter" para continuar. **# sh CCN-STIC-442_ENS_Categoria_Media_Paso_4_Deshabilitar_MOB.sh** 
111.	Pulse "Enter", de nuevo, para continuar. El Script indicará que ha finalizado.  **Nota:** No cierre la sesión SSH y manténgala en segundo plano mientras realiza los pasos siguientes.

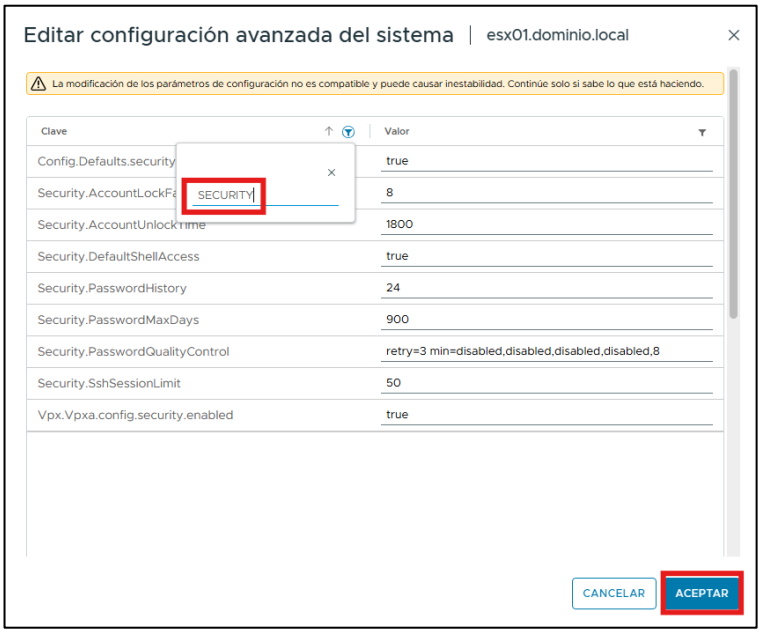
Paso	Descripción
112.	Todos los adaptadores y servidores de destino iSCSI deberán ser configurados con autenticación CHAP para asegurar la conexión. De nuevo, a través del navegador, pulse sobre el icono correspondiente a “Hosts y clústeres”. 
113.	Pulse sobre el objeto del menú de la izquierda “<FQDN de servidor ESXi>” y en la pestaña “Configuración” seleccione “Adaptadores de almacenamiento”. 
114.	Pulse sobre el adaptador o adaptadores iSCSI mediante el cual se entrega el almacenamiento para el host ESXi. Diríjase ahora a la pestaña “Propiedades” y en el apartado “Autenticación” pulse sobre “Editar”. 

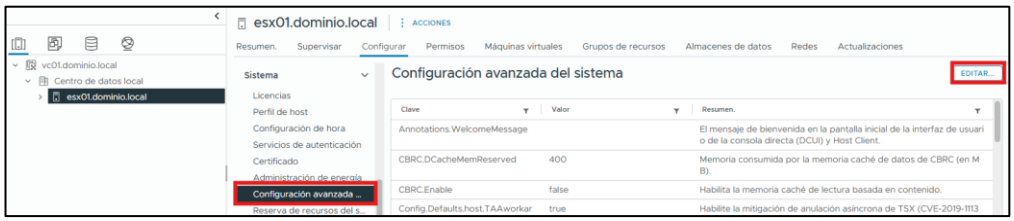
Paso	Descripción
115.	Seleccione, en el menú contextual que se despliega al pulsar sobre el campo “Método de autenticación”, la opción “Usar CHAP bidireccional”. Establezca Nombre y secreto para las credenciales CHAP salientes y entrantes. Una vez establecidos los parámetros pulse “Aceptar”.  **Nota:** Puede marcar “Usar nombre del iniciador” para establecer como nombre el iniciador iSCSI que se ha generado al crear el adaptador. Tenga en cuenta que el nombre no puede exceder los 255 caracteres y que el secreto no puede exceder los 100 caracteres (el secreto CHAP saliente no debe coincidir con el secreto CHAP entrante).
116.	A continuación, modifique el estado del cortafuegos del ESXi para que limite el tráfico a la red o redes específicas del entorno. Para ello, en la pestaña “Configurar”, seleccione “Firewall” y pulse sobre “Editar”. 

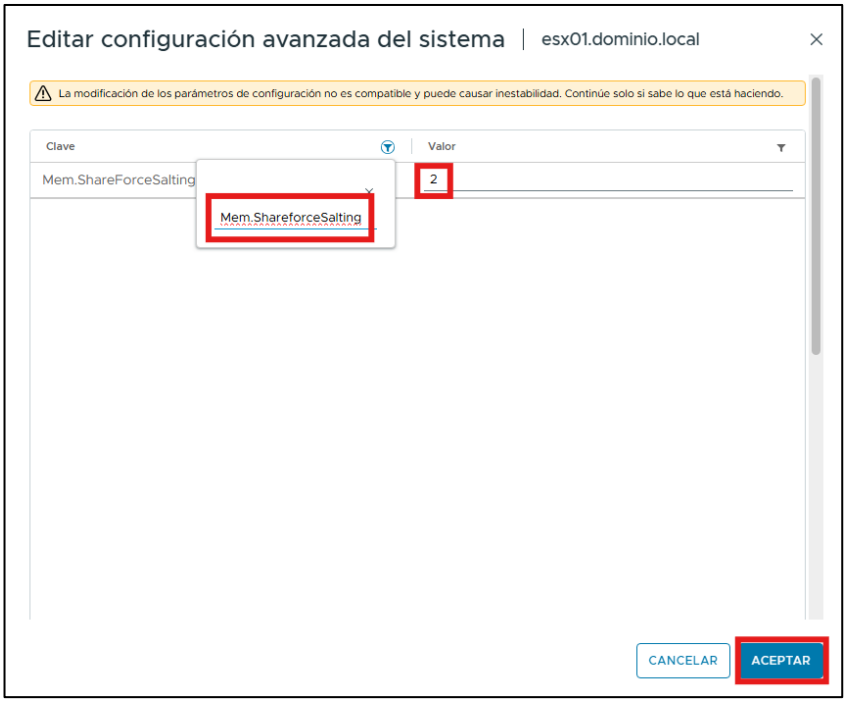
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>117.</td><td>Modifique cada uno de los parámetros siguientes y desmarque “Permitir conexiones desde cualquier dirección IP” para, a continuación, añadir la red o redes (separadas por comas) en las que se permitirá la comunicación. Pulse “Aceptar”.
<table>
<tr><th colspan="2">Protocolos</th></tr>
<tr><td>SSH server</td><td>Active Directory All</td></tr>
<tr><td>CIM SLP</td><td>DHCP client</td></tr>
<tr><td>DNS client</td><td>DVSsync</td></tr>
<tr><td>Fault tolerance</td><td>HBR</td></tr>
<tr><td>Iofiltervp</td><td>NFC</td></tr>
<tr><td>NTP client</td><td>Rabbitmqproxy</td></tr>
<tr><td>Software iSCSI client</td><td>vCenter Update Manager</td></tr>
<tr><td>vMotion</td><td>VMware vCenter agent</td></tr>
<tr><td>vSphere Web Access</td><td>vSphere Web client</td></tr>
</table>


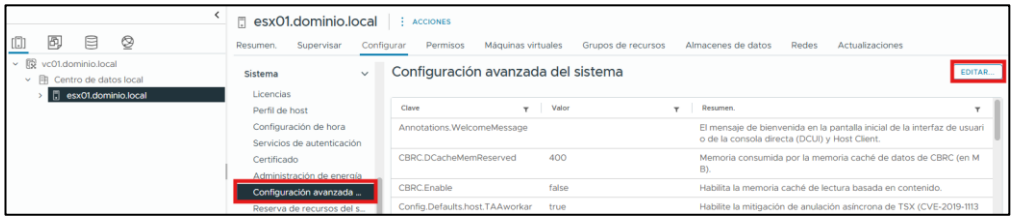
Nota: En caso de instalar y utilizar más servicios, del mismo modo, estos tendrán que ser modificados. Deberá adaptar esta configuración a las necesidades del entorno.</td></tr>
<tr><td>118.</td><td>En este momento se definirán los criterios relativos a complejidad y comportamiento de contraseñas. Para configurar estos parámetros diríjase a “Configurar → Configuración avanzada” y pulse “Editar”.

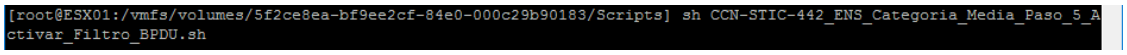
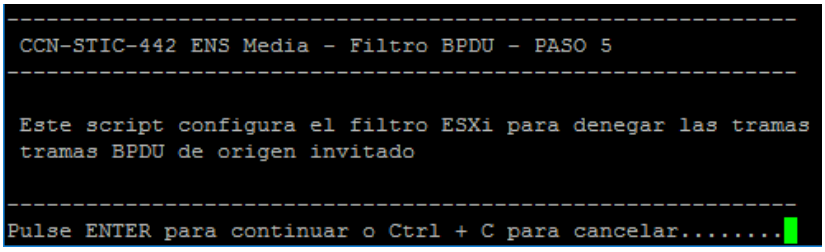
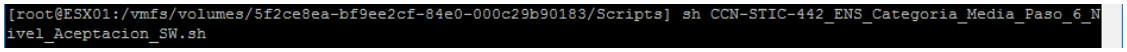
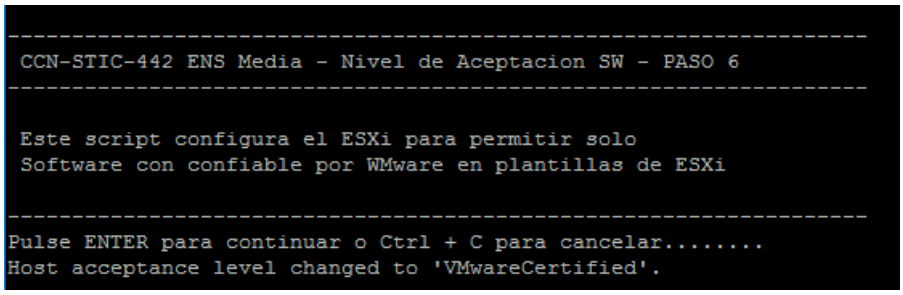
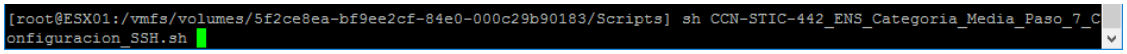
</td></tr>
</table>

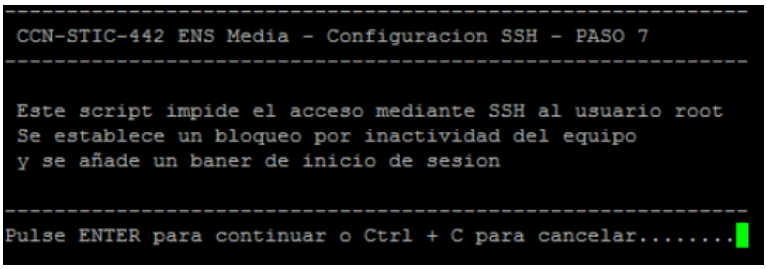
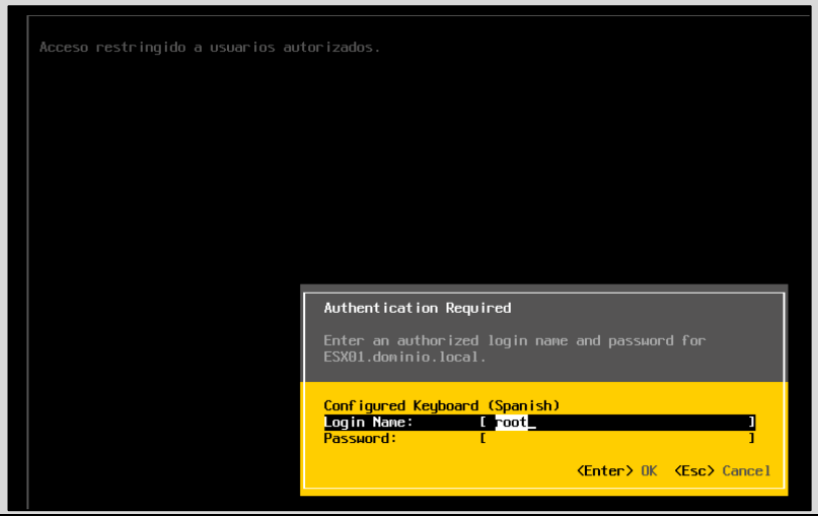
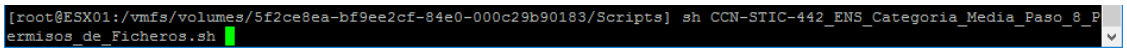
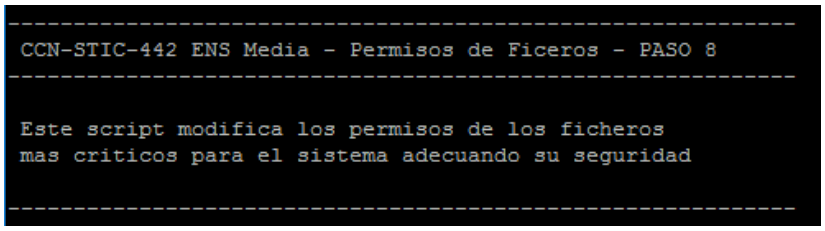
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>119.</td><td>Introduzca en el filtro “Security” y establezca los valores deseados:
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Security.Account.LockFailures</td><td>8</td></tr>
<tr><td>Security.Account.UnlockTime</td><td>3600</td></tr>
<tr><td>Security.PasswordHistory</td><td>24</td></tr>
<tr><td>Security.PasswordMaxDays</td><td>90</td></tr>
<tr><td>Security.PasswordQualitycontrol</td><td>retry=3 min=disabled,disabled,disabled, disabled,12</td></tr>
</table>
Pulse “Aceptar” para continuar.


Nota: En caso de necesitar desbloquear, antes del tiempo definido, una cuenta que ha superado los intentos de introducción de contraseña, se puede hacer uso del comando siguiente a través de la consola ESXi Shell:
- # pam_tally –user <Usuario bloqueado> --reset</td></tr>
<tr><td>120.</td><td>Pulse sobre “Editar” de nuevo.

</td></tr>
</table>

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>121.</td><td>Introduzca en el filtro “Mem.ShareforceShalting” y establezca el valor en “2”. Pulse “Aceptar” para continuar.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Mem.ShareforceShalting</td><td>2</td></tr>
</table>


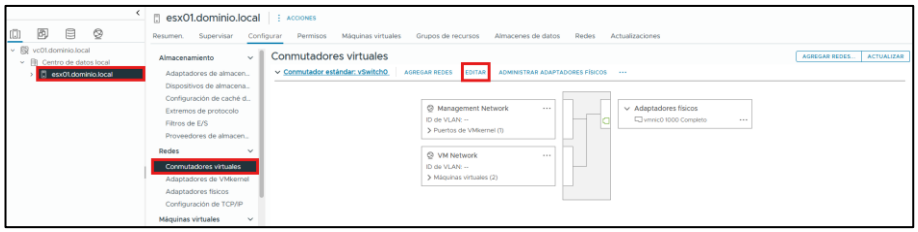
Nota: No cierre el navegador y manténgalo en segundo plano mientras realiza los pasos siguientes.</td></tr>
<tr><td>122.</td><td>Pulse sobre “Editar” de nuevo.

</td></tr>
<tr><td>123.</td><td>Introduzca en el filtro “welcome” y establezca el mensaje que quiere que aparezca en las conexiones directas al host a través de la consola o de vSphere.
<table>
<tr><th>Nombre</th><th>Valor</th></tr>
<tr><td>Annotations.WelcomeMessage</td><td>“Mensaje de seguridad que se adapte a las necesidades de la organización”</td></tr>
<tr><td>UserVars.HostClientWelcomeMessage</td><td>“Mensaje de seguridad que se adapte a las necesidades de la organización”</td></tr>
</table></td></tr>
</table>

Paso	Descripción
124.	Deberá utilizar de nuevo la sesión SSH que activó anteriormente para realizar los pasos que se indican a continuación. Ejecute el script "CCN-STIC-442_ENS_Categoria_Media_Paso_5_Activar_Filtro_BPDU.sh" mediante el siguiente comando y pulse "Enter". **# sh CCN-STIC-442_ENS_Categoria_Media_Paso_5_Activar_Filtro_BPDU.sh** 
125.	Pulse "Enter", de nuevo, para continuar. El Script indicará que ha finalizado. 
126.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Media_Paso_6_Nivel_Aceptacion_SW.sh" mediante el siguiente comando y pulse "Enter". **# sh CCN-STIC-442_ENS_Categoria_Media_Paso_6_Nivel_Aceptacion_SW.sh** 
127.	Pulse "Enter", de nuevo, para continuar. El Script indicará que ha finalizado. 
128.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Media_Paso_7_Configuracion_SSH.sh" mediante el siguiente comando y pulse "Enter". **# sh CCN-STIC-442_ENS_Categoria_Media_Paso_7_Configuracion_SSH.sh**  **Nota:** Antes de realizar este paso, es necesario disponer de una o varias cuentas con acceso a la consola ESXi Shell y que dispongan de los privilegios administrativos adecuados. El script establecerá el mensaje de entrada tanto por consola directa como por consola SSH. El mensaje es el siguiente "Acceso restringido a usuarios autorizados.". En caso de ser necesario, modifique el script y adapte el mensaje a las necesidades del entorno.

Paso	Descripción
129.	Pulse, de nuevo, “Enter” para continuar. El sistema indicará que el Script ha finalizado.  **Nota:** A partir de este momento, al tratar de entrar en la configuración directamente a través del servidor ESXi, solamente aparecerá el mensaje de seguridad que se haya introducido en el script (por defecto “Acceso restringido a usuarios autorizados.”). Aunque no aparezca la opción de pulsar “F2” para iniciar la conexión continúa siendo posible para los usuarios a los que se les haya permitido el acceso de este modo. 
130.	Ejecute el script “CCN-STIC-442_ENS_Categoria_Media_Paso_8_Permisos_de_Ficheros.sh” mediante el siguiente comando y pulse “Enter”. **# sh CCN-STIC-442_ENS_Categoria_Media_Paso_8_Permisos_de_Ficheros.sh** 
131.	Pulse “Enter” para continuar. El Script indicará que ha finalizado. 
132.	A continuación, cierre la sesión SSH abierta contra el servidor ESXi.

2.2.1. CONFIGURACIÓN EN CONMUTADORES VIRTUALES ESTÁNDAR

Las configuraciones descritas a continuación son a nivel de conmutadores estándar. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los conmutadores estándar de cada uno de los hosts ESXi existentes en el servicio de vCenter.

Paso	Descripción
133.	En el menú de la izquierda, seleccione el icono correspondiente a “Hosts y clústeres”. 
134.	En el menú de la izquierda, sitúese sobre el objeto “<FQDN del servidor ESXi>” y, en la pestaña “Configurar”, seleccione “Conmutadores virtuales”. Pulse “Editar” sobre cada conmutador virtual. 
135.	En la ventana emergente, pulse sobre “Seguridad” y compruebe el estado de los siguientes parámetros de seguridad (deberán tener el valor “Rechazar”): – Modo promiscuo – Cambios de dirección MAC – Transmisiones falsificadas 

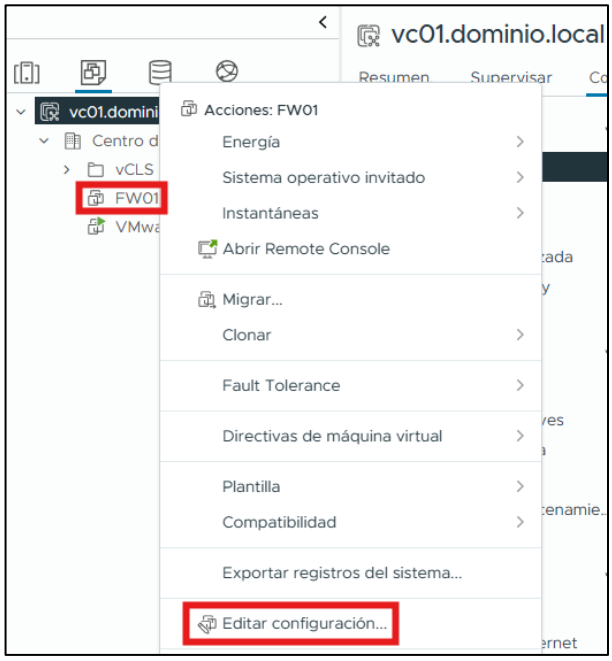
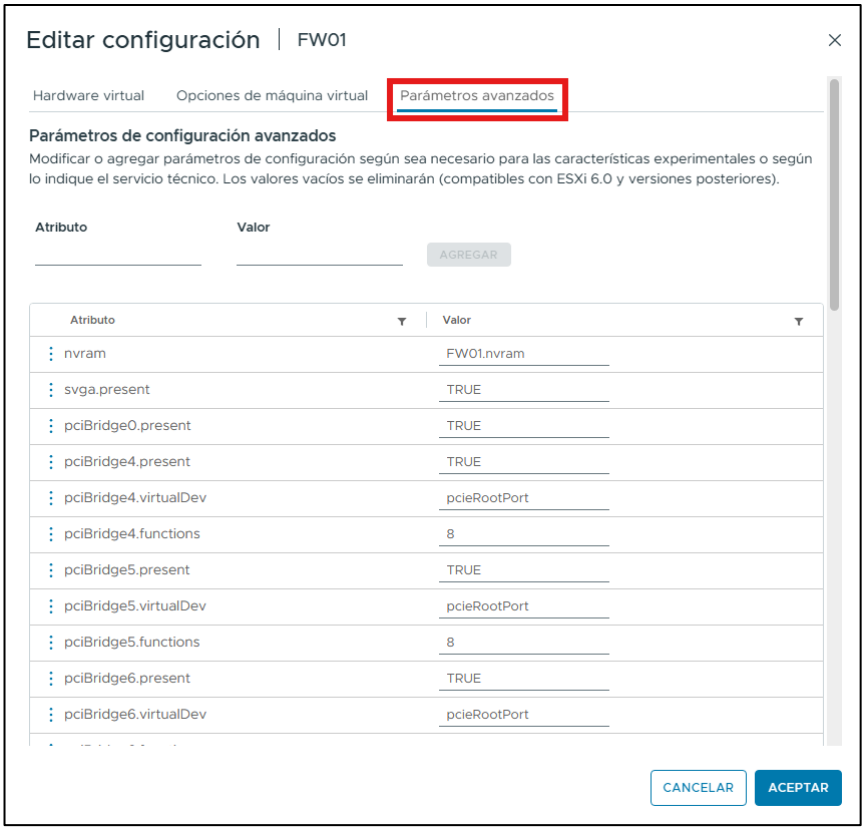
Paso	Descripción
136.	Modifique los parámetros al valor “Rechazar” y pulse “ACEPTAR” para validar la configuración. 

2.2.2. CONFIGURACIÓN DE MÁQUINAS VIRTUALES

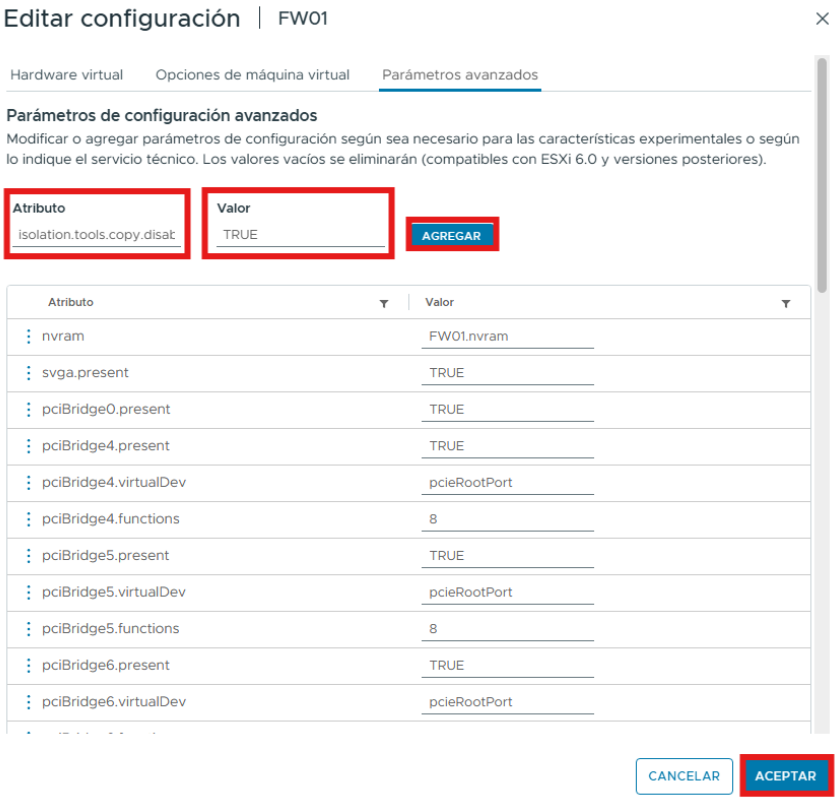
Las configuraciones descritas a continuación son a nivel de máquina virtual. Por tanto, es necesario aplicar estas configuraciones de seguridad a todas las máquinas virtuales que se unan al host de ESXi que se está implementando.

Nota: Existe la posibilidad de convertir las máquinas virtuales configuradas en plantillas, de modo que se utilicen para generar nuevas máquinas, homogeneizando y simplificando las tareas administrativas.

Paso	Descripción
137.	En el menú de la izquierda, pulse el icono correspondiente a “Máquinas virtuales y plantillas”. 

Paso	Descripción
138.	Asegúrese de que la máquina virtual esté apagada. Luego, sitúese sobre la máquina virtual sobre la que va a establecer las configuraciones de seguridad y pulse el botón derecho del ratón para seleccionar “Editar configuración…”. 
139.	Diríjase a la pestaña “Parámetros avanzados”. 

Paso	Descripción
140.	En el campo “Atributo” introduzca “isolation.tools.copy.disable” y en el campo “Valor” introduzca “True”. Pulse “Agregar” y “Aceptar” para guardar los cambios.

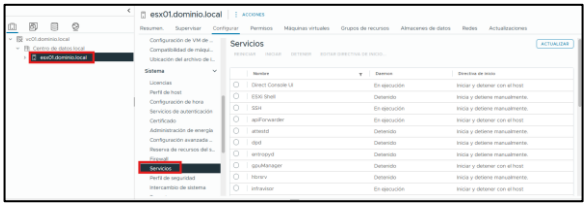
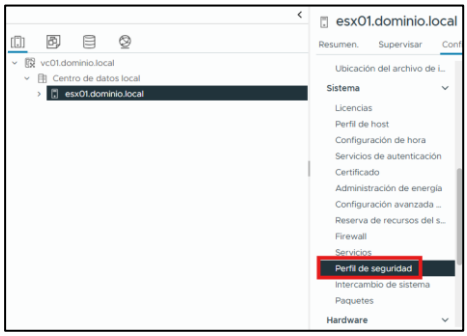
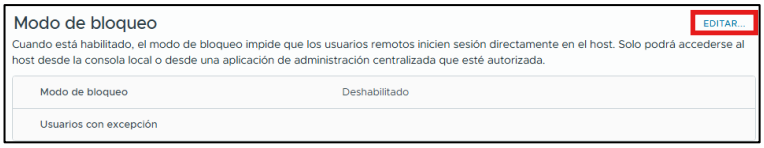


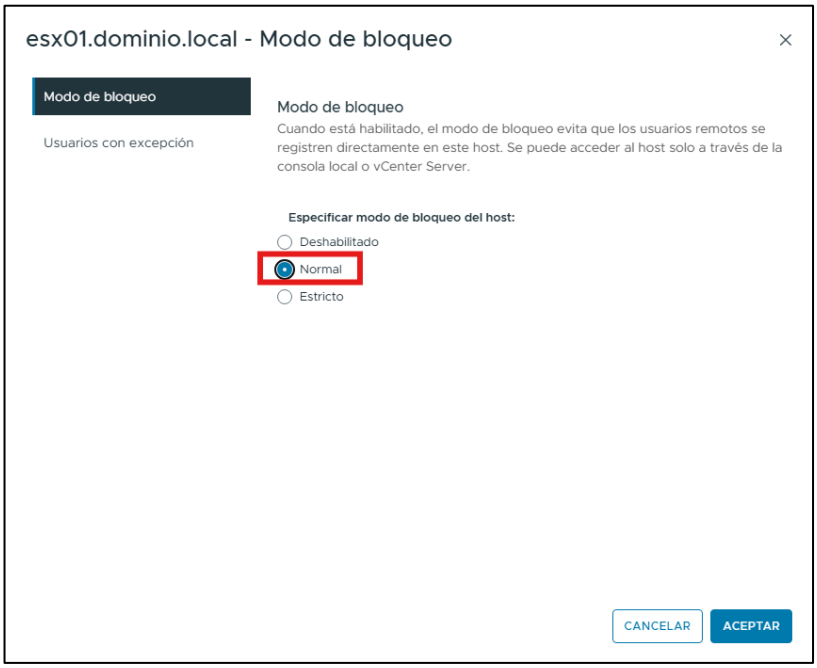
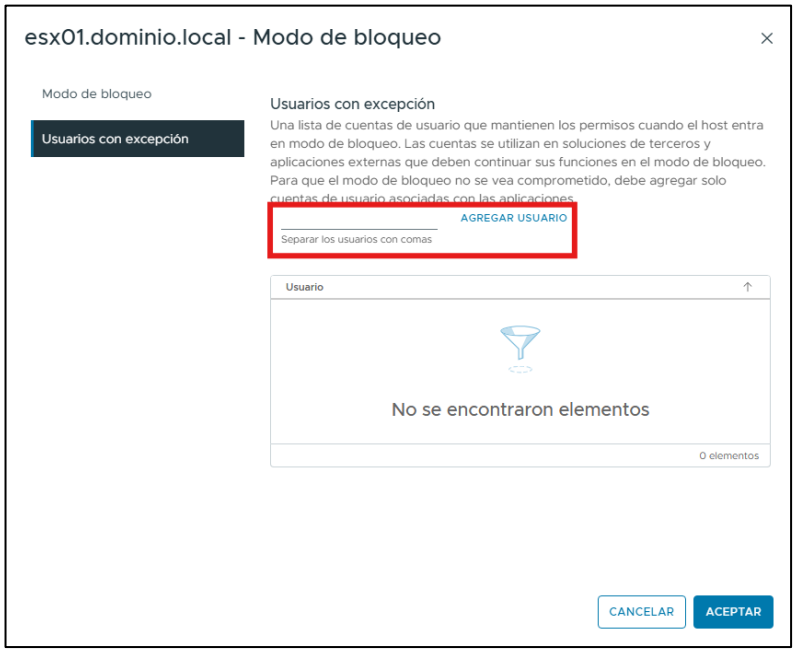
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>141.</td><td>Repita estos últimos pasos para añadir cada uno de los siguientes parámetros de configuración. Una vez haya introducido todos los parámetros, pulse “Aceptar” para continuar.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>isolation.tools.paste.disable</td><td>True</td></tr>
<tr><td>isolation.tools.setGUIOptions.enable</td><td>False</td></tr>
<tr><td>isolation.tools.diskShrink.disable</td><td>True</td></tr>
<tr><td>isolation.tools.diskWiper.disable</td><td>True</td></tr>
<tr><td>isolation.tools.connectable.disable</td><td>True</td></tr>
<tr><td>isolation.device.edit.disable</td><td>True</td></tr>
<tr><td>isolation.tools.setOption.disable</td><td>True</td></tr>
<tr><td>scsiX:Y.mode</td><td>Persistent</td></tr>
<tr><td>mks.enable3d</td><td>False</td></tr>
<tr><td>floppyX.present</td><td>False</td></tr>
<tr><td>parallelX.present</td><td>False</td></tr>
<tr><td>serialX.present</td><td>False</td></tr>
<tr><td>svga.vgaOnly</td><td>True</td></tr>
<tr><td>tools.setInfo.sizeLimit</td><td>1048576</td></tr>
<tr><td>RemoteDisplay.vnc.enabled</td><td>False</td></tr>
<tr><td>tools.guestlib.enableHostInfo</td><td>False</td></tr>
<tr><td>sched.mem.pshare.salt</td><td>Null</td></tr>
<tr><td>ethernetX.filterX. name = filtername</td><td>Null</td></tr>
<tr><td>pciPassthru*.present</td><td>False</td></tr>
<tr><td>Net.BlockGuestBPDU</td><td>1</td></tr>
</table>
Nota: Deberá adaptar la configuración a las necesidades del entorno.</td></tr>
</table>

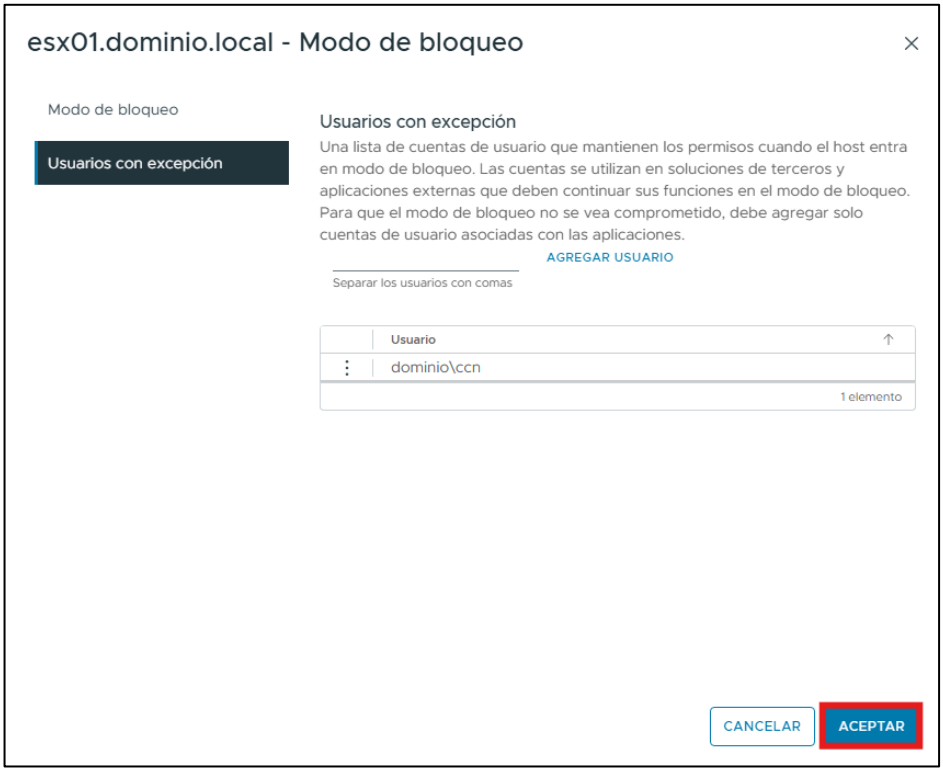
2.2.3. CONFIGURACIÓN DE ESX SHELL Y SSH

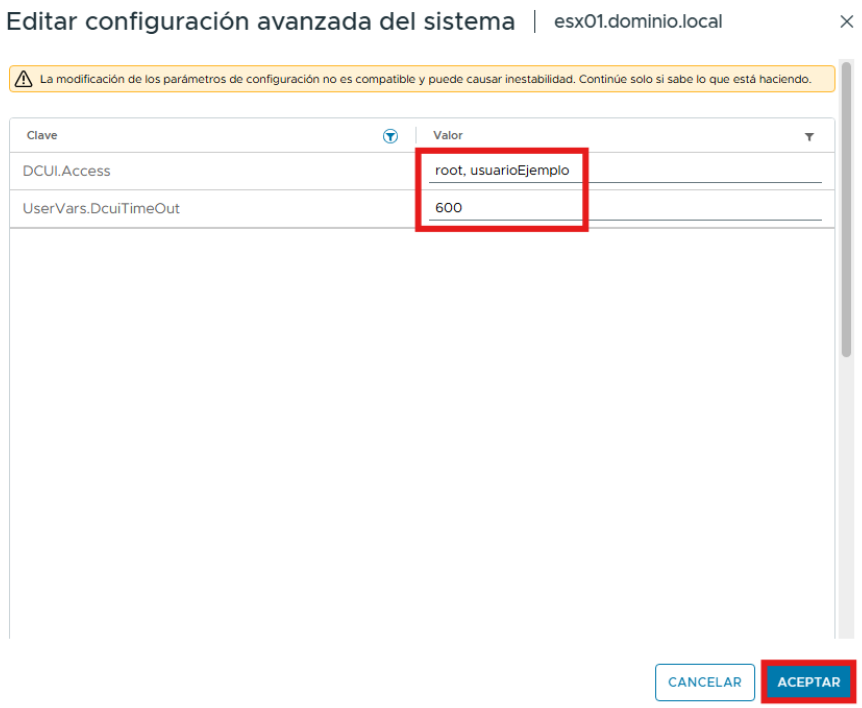
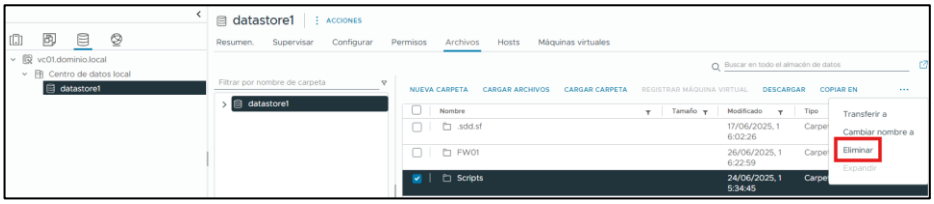
Por último, en el host ESXi, se deshabilitará SSH y la consola ESXi Shell. Así mismo, se activará el modo de bloqueo estricto. A partir de este momento, la administración del host solamente será a través del servidor de vCenter al que haya sido añadido. Se recomienda mantener la configuración de este modo salvo necesidad para resolución de problemas.

Paso	Descripción
142.	En el navegador, pulse sobre el icono que corresponde a “Hosts y clústeres”. 

Paso	Descripción
143.	En el menú de la izquierda, sitúese sobre el objeto “<FQDN del servidor ESXi>” y pulse sobre “Servicios”. 
144.	Seleccione el servicio “ESX Shell” y pulse “Detener”. 
145.	Realice la misma operación con el servicio “SSH”. 
146.	Defina el modo de bloqueo para el acceso a este host en modo “Normal” para que solo se pueda acceder al host de ESXi a través de servidores vCenter o localmente y no a través de clientes vSphere por conexión directa al host. Para ello, sitúese de nuevo sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar”, seleccione “Perfil de seguridad”.  **Nota:** El modo de bloqueo solamente se deberá desactivar, del mismo modo que solo se deberán activar la consola ESXi Shell y SSH, cuando se realicen tareas de resolución de problemas que no puedan ser solucionadas a través del servicio de vCenter o mediante el acceso local.
147.	En “Modo de Bloqueo” seleccione “Editar”. 

Paso	Descripción
148.	En la ventana emergente, seleccione el modo “Normal”. 
149.	En caso de que existan configuraciones y aplicativos que requieran conexión directa hacia el host, se deberán añadir sus usuarios al grupo de excepción para el modo estricto. Seleccione “Usuarios con excepción”, añada los usuarios que deberán tener acceso local al servidor ESXi, separados por “;” y pulse “AGREGAR USUARIO”.  **Nota:** a los usuarios que pertenecen a este grupo de excepción, se les permitirá traspasar el modo de bloqueo y acceder directamente al host. Estos usuarios no deben ser usuarios físicos, sino que deben ser usuarios automáticos que pertenezcan a procesos y aplicaciones. Así mismo, deberán ser auditados periódicamente pudiendo ser consultados mediante los pasos expuestos a continuación.

Paso	Descripción
150.	Los usuarios añadidos aparecerán en la lista. Pulse “ACEPTAR” para cerrar la ventana emergente.  **Nota:** En este paso se ha utilizado un usuario a modo ejemplo, adapte dicho paso a las necesidades de su organización. No se deben añadir a esta lista usuarios que no pertenezcan a aplicaciones o procesos automáticos que necesiten traspasar el modo de bloqueo.
151.	Así mismo, se deberán configurar también los usuarios físicos que podrán tener acceso a la infraestructura incluso cuando el modo de bloqueo está activado. Si esta configuración no contuviera ningún usuario, es posible que se pierda el control del ESXi completamente, no pudiendo volver a ser accesible. Para realizar la configuración, deberá acceder a “Configurar → Configuración avanzada” y pulsar sobre “Editar”. 

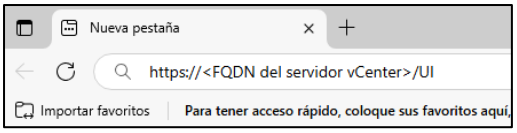
Paso	Descripción
152.	Añada, en el filtro, “DCUI” e introduzca los parámetros deseados añadiendo los usuarios (separados por coma) que podrán acceder por consola directa y el tiempo de bloqueo ante inactividad. Pulse “ACEPTAR” para continuar.  **Nota:** Para cumplir con lo definido en la categoría media del ENS, el tiempo de inactividad deberá ser establecido en 600. VMware desaconseja eliminar al usuario ROOT de esta lista.
153.	Pulse ahora sobre el icono correspondiente a “Almacenamiento”. 
154.	Sitúese sobre el almacén de datos donde alojó la carpeta “Scripts” y seleccione la pestaña “Archivos”. 
155.	Pulse sobre la carpeta “Scripts” y seleccione “Eliminar”. 

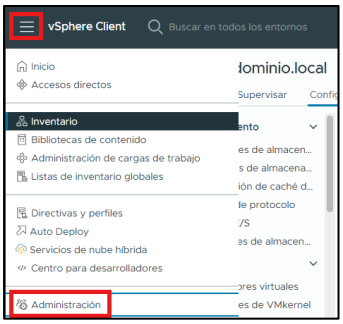
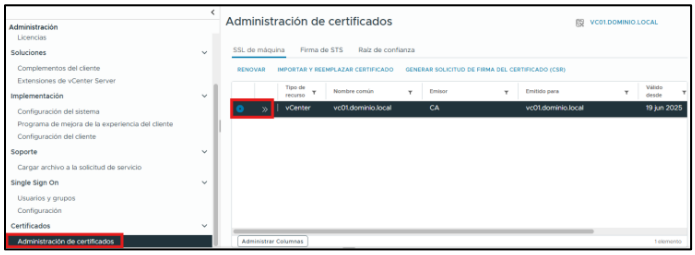
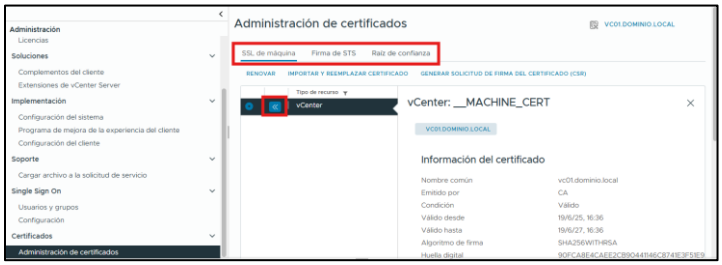
Paso	Descripción
156.	Pulse “ACEPTAR” para confirmar la eliminación. 

ANEXO A.3.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA MEDIA DEL ENS PARA VSPHERE 8.X

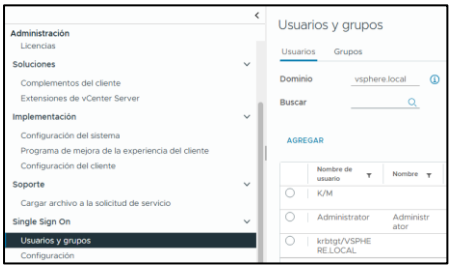
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores que pertenecen a la infraestructura de VMware vSphere 8.x con implementación de seguridad de categoría MEDIA del ENS.

1. SERVIDORES VCENTER

Comprobación	OK/NOK	Como hacerlo
1. Acceso al servidor de vCenter.		Inicie sesión directamente en el host ESXi utilizando el ESXi Host Client a través de su navegador web. Para ello, introduzca la siguiente URL: “ https://<IP-o-FQDN-del-host-ESXi>/UI”.  Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter, pulse sobre las condiciones de acceso y pulse sobre “Iniciar”. 

Comprobación	OK/NOK	Como hacerlo
2. Compruebe los certificados de vCenter.		Compruebe que los certificados que están siendo utilizados en el servidor de vCenter son los correctos (firmados por una entidad certificadora autorizada). Para ello, pulse sobre el icono del menú principal y sobre “Administración” en el menú contextual que se ha desplegado.  Pulse sobre “Administración de certificados y seleccione el servidor de vCenter a comprobar.  Acceda a “Administración de certificados” y compruebe cada uno de ellos.  **Certificado** / **OK/NOK** Certificado de servidor Certificado acceso web a servidor Certificado vsphere-webclient Certificado vpxd Certificado vpxd extensión Certificado raíz de confianza Certificado de entidad subordinada de confianza **Nota:** La lista de certificados puede cambiar dependiendo de los aplicativos instalados y de si se dispone de certificados emitidos por una entidad certificadora subordinada.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>3. Compruebe que el sistema no está unido al programa de mejora de VMware.</td><td></td><td>Pulse sobre “Implementación → Programa de mejora de la experiencia del cliente”.
 

El estado correcto debe ser “No Unido”.
<table><tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Estado del programa</td><td>No unido</td><td></td></tr></table></td></tr>
<tr><td>4. Compruebe que los usuarios y grupos de administración son los correctos.</td><td></td><td>Compruebe que la lista de usuarios y grupos para hacer inicio de sesiones y labores administrativas es la adecuada. Pulse sobre “Usuarios y grupos” y revise la lista de usuarios mediante las pestañas.
 

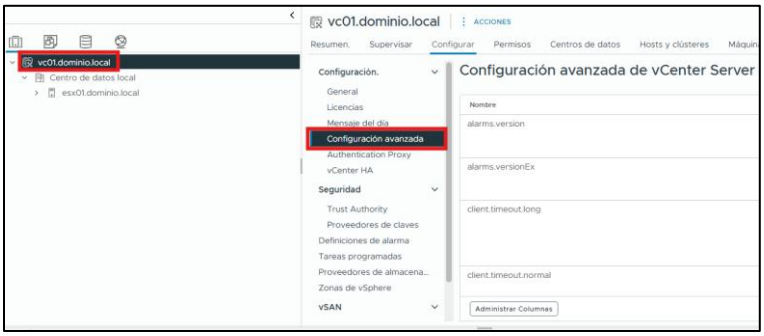
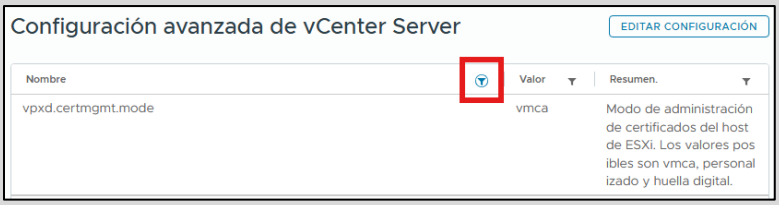
<table><tr><th>Objetos</th><th>OK/NOK</th></tr><tr><td>Lista de usuarios</td><td></td></tr><tr><td>Lista de grupos</td><td></td></tr></table></td></tr>
<tr><td>5. Compruebe la directiva de contraseñas para el servidor de vCenter.</td><td></td><td>Compruebe las directivas de contraseñas. Para ello, pulse sobre “Configuración” y sobre el botón “Directiva de contraseñas”.
 
</td></tr>
<tr><td></td><td></td><td><table><tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Duración máxima</td><td>60</td><td></td></tr><tr><td>Reutilización restringida</td><td>24</td><td></td></tr><tr><td>Longitud mínima</td><td>12</td><td></td></tr><tr><td>Caracteres especiales</td><td>1</td><td></td></tr><tr><td>Caracteres en mayúscula</td><td>1</td><td></td></tr></table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Caracteres en minúscula</td><td>1</td><td></td></tr>
<tr><td>Caracteres numéricos</td><td>1</td><td></td></tr>
</table>
</td></tr>
<tr><td>6. Compruebe la directiva de bloqueo para el servidor de vCenter.</td><td></td><td>Compruebe las directivas de contraseñas. Para ello, pulse sobre el botón “Directiva de bloqueo”.
<table>
<tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cantidad máxima de intentos fallidos de inicio de sesión</td><td>8</td><td></td></tr>
<tr><td>Intervalo de tiempo entre errores</td><td>1800</td><td></td></tr>
<tr><td>Tiempo de desbloqueo</td><td>3600</td><td></td></tr>
</table>
</td></tr>
<tr><td>7. Compruebe que se ha establecido el mensaje de inicio de sesión.</td><td></td><td>Pulse sobre la pestaña “Mensaje de inicio de sesión” y compruebe que el mensaje está configurado, la casilla de consentimiento habilitada y los detalles del mensaje configurados.


<table>
<tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Mensaje de inicio de sesión</td><td>Contiene el mensaje adaptado a sus necesidades</td><td></td></tr>
<tr><td>Casilla de consentimiento</td><td>Habilitado</td><td></td></tr>
<tr><td>Detalles del mensaje de inicio de sesión</td><td>Contiene el mensaje adaptado a sus necesidades</td><td></td></tr>
</table>
</td></tr>
<tr><td>8. Compruebe los parámetros de configuración avanzada del servidor de vCenter.</td><td></td><td>En el menú de la izquierda, a través de la consola de vSphere Client, pulse sobre el icono que corresponde a “Host y clústeres”.

Pulse sobre el objeto con el nombre del servidor de vCenter.

</td></tr>
</table>

Comprobación	OK/NOK	Como hacerlo
		Vaya a la pestaña “Configurar” y seleccione “Configuración Avanzada”.  Localice los siguientes parámetros y confirme que los valores coinciden con los mostrados en la siguiente tabla: **Nota:** Es posible hacer uso del filtro de columna para localizar los parámetros más fácilmente.  **Nombre** | **Valor** | **OK/NOK** vpxd.certmgmt.mode | custom |

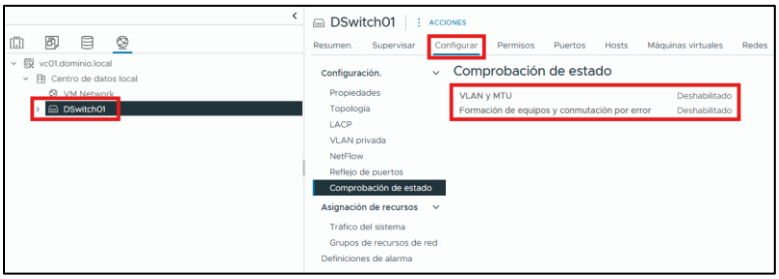
Comprobación	OK/NOK	Como hacerlo
9. Compruebe que los servicios de vCenter son ejecutados por el usuario adecuado.		Revise los servicios principales del vCenter Server Appliance y asegúrese de que los siguientes se encuentren configurados con inicio automático y en estado activo: **Nota:** La disponibilidad de algunos servicios puede variar en función de los componentes habilitados durante la instalación de vCenter. Todos los servicios son gestionados por el gestor de procesos vmon, y se ejecutan bajo el contexto del sistema root en el appliance VCSA basado en Photon OS. Verificación del estado de los servicios Para consultar el estado actual de los servicios en VCSA, utilice el siguiente comando desde una sesión SSH o desde la consola directa del appliance: - **service-control –status** En VCSA, los servicios corren bajo el usuario root y sus configuraciones se encuentran gestionadas desde /etc/init.d/, /usr/lib/vmware/ o mediante systemd. Para revisar permisos de ejecución: - ls -l /etc/init.d/ - ls -l /usr/lib/vmware/

Servicio	Inicio	OK/NOK
VMWareDirectoryService	Automático	
VMWareIdentityMgmtService	Automático	
VMWareCertificateService	Automático	
VMWareDNSService	Automático	
VMWareAfdService	Automático	
VMwareSTS	Automático	
vmon	Automático	
Vmware-cis-config	Automático	

1.1. CONMUTADORES VIRTUALES DISTRIBUIDOS

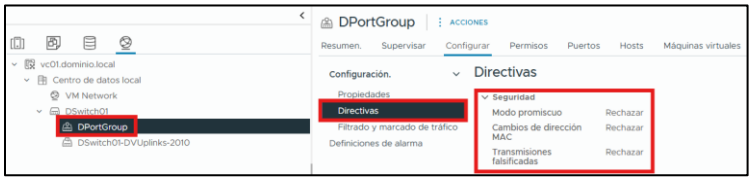
Las comprobaciones descritas a continuación son a nivel de conmutadores virtuales distribuidos. Por tanto, es necesario revisar la seguridad de todos los conmutadores virtuales distribuidos existentes en el servicio de vCenter.

Comprobación	OK/NOK	Como hacerlo
10. Compruebe que la “comprobación de estado” de los conmutadores virtuales		En el menú de la izquierda, seleccione el icono correspondiente a “Redes”.  Sitúese sobre cada conmutador distribuido y en la pestaña “Configurar” pulse sobre el elemento “Comprobación de

Comprobación	OK/NOK	Como hacerlo
distribuidos es correcta.		estado" y compruebe que los valores coinciden con los mostrados en la tabla.  **Parámetro** / **Estado** / **OK/NOK** VLAN y MTU — Deshabilitado — Formación de equipos y conmutación por error — Deshabilitado —

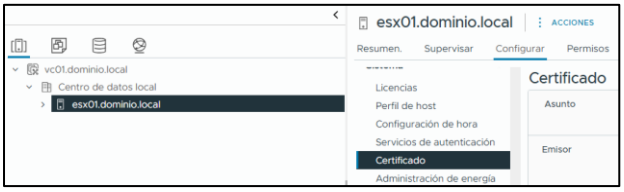
1.2. GRUPOS DE PUERTOS

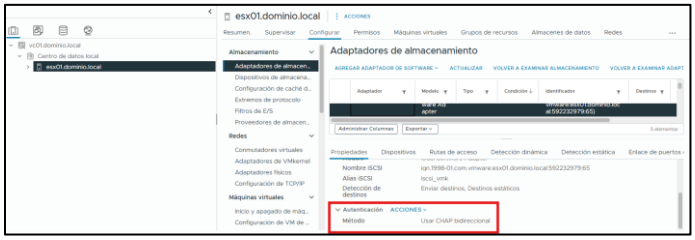
Las comprobaciones descritas a continuación son a nivel de grupos de puertos. Por tanto, es necesario revisar la seguridad de todos los grupos de puertos existentes en los distintos conmutadores presentes en el servicio de vCenter.

Comprobación	OK/NOK	Como hacerlo
11. Compruebe que la seguridad de los grupos de puertos es correcta.		En el menú de la izquierda, seleccione el icono correspondiente a "Redes".  Sitúese sobre cada grupo de puertos (que se encontrarán dentro de la rama de cada conmutador virtual) y, en la pestaña "Configurar", seleccione "Directivas" y compruebe que las siguientes directivas de seguridad tienen el valor "Rechazar"  **Directiva** / **Valor** / **OK/NOK** Modo Promiscuo — Rechazar — Cambios de dirección MAC — Rechazar — Transmisiones falsificadas — Rechazar —

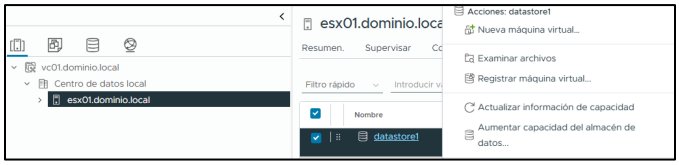
2. SERVIDORES ESXI

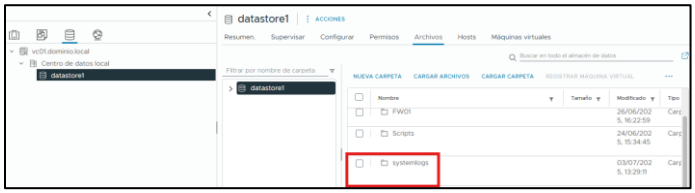
Las comprobaciones descritas a continuación se realizan a nivel de servidor ESXi y deberán ser revisadas en cada uno de los host ESXi que se añadan a cada servidor de vCenter.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>12.Compruebe que el certificado del servidor ESXi es correcto.</td><td></td><td>Pulse sobre el icono que corresponde a “Host y clústeres”.
 
Sitúese sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar” seleccione “Certificado”. Compruebe que el certificado de servidor es el adecuado (emitido por una entidad certificadora autorizada)
 
</td></tr>
<tr><td>13.Compruebe que está establecida la configuración NTP que se adecúa a las necesidades de la organización.</td><td></td><td>Seleccione “Configuración de hora” y compruebe que los valores son los deseados.
 

<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cliente NTP</td><td>Habilitado</td><td></td></tr>
<tr><td>Estado de servicio NTP</td><td>En ejecución</td><td></td></tr>
<tr><td>Servidores NTP</td><td>Configurado con un servidor de NTP válido</td><td></td></tr>
</table></td></tr>
<tr><td>14.Compruebe que el método de autenticación entre el servidor ESXi y el adaptador iSCSI es el adecuado.</td><td></td><td>Sitúese sobre “Adaptadores de almacenamiento” y pulse sobre cada adaptador iSCSI que quiera comprobar. En la pestaña “Propiedades” compruebe en “Autenticación” que el método CHAP está habilitado y la gestión de claves es bidireccional.
 

<table>
<tr><th>Propiedad</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Método</td><td>User CHAP bidireccional</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>15.Compruebe la configuración de logs.</td><td></td><td>Se deberá comprobar que los logs del sistema se encuentran en un almacén de datos persistente y accesible desde el servidor de vCenter. Pulse la pestaña “Almacén de datos” y pulse botón derecho sobre el almacén de datos que debería contener los logs. Seleccione “Examinar Archivos” en el menú contextual que se ha desplegado.
 

Deberá existir una carpeta denominada “systemlogs”.
 

Pulse doble clic sobre dicha carpeta para comprobar que contiene los ficheros de log y que estos se están llenando correctamente.
 
</td></tr>
<tr><td>16.Compruebe que las conexiones permitidas del firewall están filtradas solamente a las redes permitidas.</td><td></td><td>Sitúese sobre “Firewall” y compruebe que las conexiones permitidas no contienen el valor todos en la columna “Direcciones IP permitidas” y, en su lugar, aparecen solamente las redes permitidas.

<table>
<tr><th>Conexión</th><th>Direcciones IP</th><th>OK/NOK</th></tr>
<tr><td>SSH server</td><td>Redes permitidas</td><td></td></tr>
<tr><td>CIM SLP</td><td>Redes permitidas</td><td></td></tr>
<tr><td>DNS client</td><td>Redes permitidas</td><td></td></tr>
<tr><td>Fault tolerance</td><td>Redes permitidas</td><td></td></tr>
<tr><td>Iofiltervp</td><td>Redes permitidas</td><td></td></tr>
<tr><td>NTP client</td><td>Redes permitidas</td><td></td></tr>
<tr><td>Software iSCSI client</td><td>Redes permitidas</td><td></td></tr>
<tr><td>vMotion</td><td>Redes permitidas</td><td></td></tr>
</table>
</td></tr>
</table>

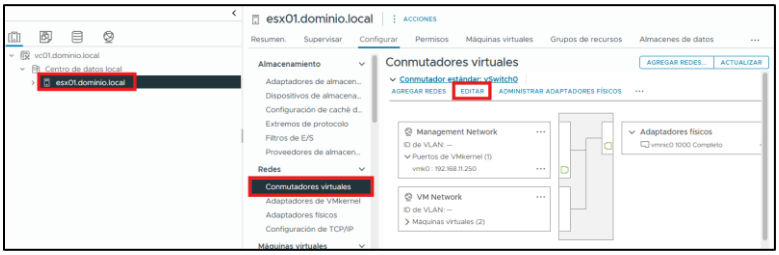
Comprobación	OK/NOK	Como hacerlo
		vSphere Web Access — Redes permitidas Active Directory All — Redes permitidas DHCP client — Redes permitidas DVSsync — Redes permitidas HBR — Redes permitidas NFC — Redes permitidas Rabbitmqproxy — Redes permitidas vCenter Update Manager — Redes permitidas VMware vCenter agent — Redes permitidas vSphere Web client — Redes permitidas
17. Compruebe los parámetros de configuración avanzada en cada servidor de ESXi		Diríjase a "Configurar → Configuración avanzada" y compruebe los parámetros y valores especificados en la tabla.  **Nota:** Puede hacer uso de los filtros de columna para localizar las directivas.

Clave	Valor	OK/NOK
Security.Account.LockFailures	8	
Security.Account.UnlockTime	3600	
Security.PasswordHistory	24	
Security.PasswordMaxDays	90	
Security.PasswordQualitycontrol	retry=3 min=disabled,disabled,disabled, disabled,12	
Config.HostAgent.plugins.solo.enableMOB	false	
Mem.ShareforceShalting	2	
Net.BlockGuestBPDU	1	
Syslog.global.default.rotate	0	
Syslog.global.default.size	8192	
Syslog.global.logDir	"almacén de datos adecuado y persistente"	
UserVars.ESXiShellInteractiveTimeOut	600	
UserVars.ESXiShellTimeOut	600	
Annotations.WelcomeMessage	"Mensaje de seguridad que se adapte a las necesidades de la organización"	
UserVars.HostClientWelcomeMessage	"Mensaje de seguridad que se adapte a las necesidades de la organización"	

Comprobación	OK/NOK	Como hacerlo
		En este momento, aún no se han realizado todas las configuraciones específicas del servidor ESXi. Sin embargo, y dado que el resto de las configuraciones requieren de un acceso directo al host, se comprobarán el resto de los componentes tales como seguridad en las máquinas o conmutadores virtuales contenidos en el host para minimizar el tiempo de exposición del acceso directo o a través de SSH.

2.1. CONMUTADORES VIRTUALES ESTÁNDAR

Las comprobaciones descritas a continuación son a nivel de conmutadores virtuales estándar. Por tanto, es necesario revisar la seguridad de todos los conmutadores virtuales estándar existentes en cada host ESXi contenido en cada servidor de vCenter.

Comprobación	OK/NOK	Como hacerlo
18.Compruebe la seguridad en los conmutadores virtuales estándar de cada servidor ESXi.		Seleccione “Conmutadores virtuales”. Pulse “Editar” sobre cada conmutador virtual.  En la ventana emergente, pulse sobre “Seguridad” y compruebe el estado de los siguientes parámetros de seguridad (deberán tener el valor “Rechazar”).

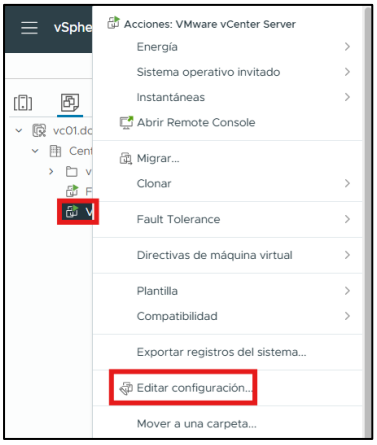
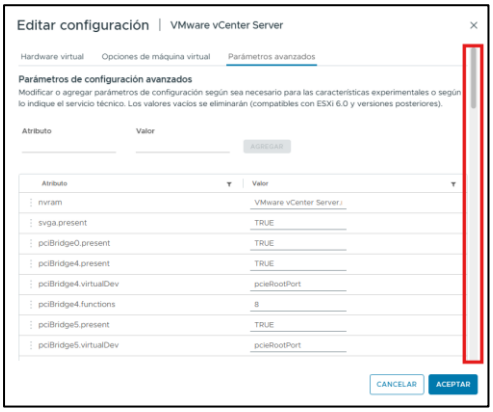
Elemento	Valor	OK/NOK
Modo promiscuo	Rechazar	
Cambios de dirección MAC	Rechazar	
Transmisiones falsificadas	Rechazar	

2.2. MÁQUINAS VIRTUALES

Las comprobaciones descritas a continuación son a nivel de máquina virtual. Por tanto, es necesario aplicar estas configuraciones de seguridad a todas las máquinas virtuales que se unan al host de ESXi que se está implementando.

Nota: Adicionalmente, deberán ser comprobadas las medidas de seguridad aplicadas al sistema operativo invitado siguiendo las listas de comprobación de las guías STIC correspondientes.

Comprobación	OK/NOK	Como hacerlo
19.Compruebe los parámetros de configuración		Pulse el icono correspondiente a “Máquinas virtuales y plantillas”.

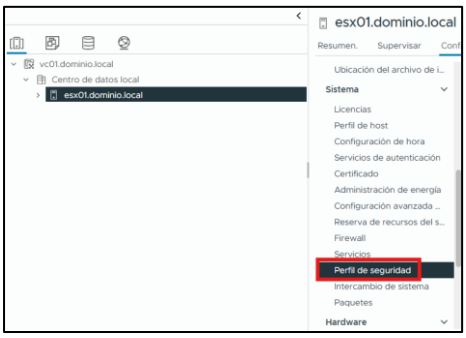
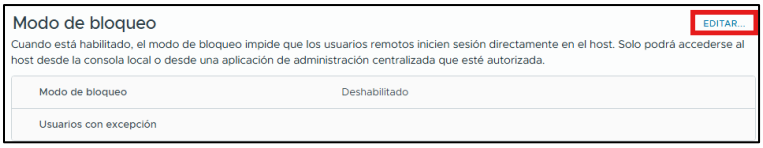
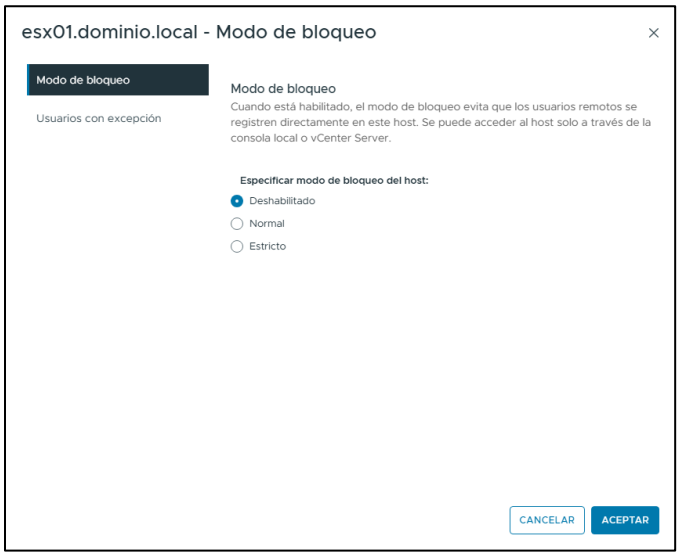
Comprobación	OK/NOK	Como hacerlo
avanzados para las máquinas virtuales.		 Sitúese sobre la máquina virtual sobre la que van a establecer las configuraciones de seguridad y pulse el botón derecho del ratón para seleccionar “Editar configuración…”.  Diríjase a la pestaña “Parámetros avanzados” y utilice la búsqueda por “Atributo”. 
		Localice los diferentes parámetros de configuración y compruebe que los valores coinciden con los indicados en la tabla.

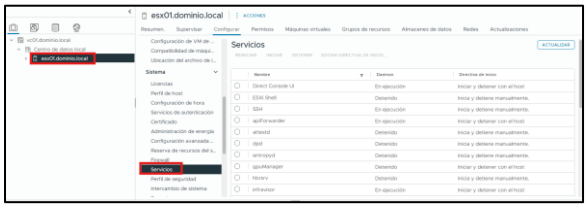
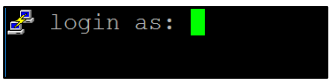
Elemento	Valor	OK/NOK
isolation.tools.copy.disable	True	
isolation.tools.paste.disable	True	
isolation.tools.setGUIOptions.enable	False	
isolation.tools.diskShrink.disable	True	
isolation.tools.diskWiper.disable	True	
isolation.tools.connectable.disable	True	
isolation.device.edit.disable	True	
isolation.tools.setOption.disable	True	

Comprobación	OK/NOK	Como hacerlo		
		scsiX:Y.mode	Persistent	
		mks.enable3d	False	
		floppyX.present	False	
		parallelX.present	False	
		serialX.present	False	
		svga.vgaOnly	True	
		tools.setInfo.sizeLimit	1048576	
		svga.vgaOnly	True	
		RemoteDisplay.vnc.enabled	False	
		tools.guestlib.enableHostInfo	False	
		sched.mem.pshare.salt	Null	
		ethernetX.filterX. name = filtername	Null	
		pciPassthru*.present	False	
		Net.BlockGuestBPDU	1	

2.3. COMPROBACIONES Y PASOS FINALES EN SERVIDOR ESXI

En este momento, se deberá deshabilitar el modo de bloqueo en cada servidor ESXi a comprobar ya que algunas de estas comprobaciones deberán ser realizadas a través de conexión directa al host. En los pasos finales se habilitará de nuevo para forzar el acceso único a través del servidor de vCenter.

Comprobación	OK/NOK	Como hacerlo
20. Deshabilite el modo de bloqueo		Pulse sobre el icono que corresponde a “Host y clústeres”.  Sitúese sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar”, seleccione “Perfil de seguridad”.  En “Modo de Bloqueo” seleccione “Editar”.  En la ventana emergente, seleccione el modo “Deshabilitado” y pulse “ACEPTAR” para continuar. 

Comprobación	OK/NOK	Como hacerlo
21.Habilite la consola ESXi y el acceso SSH		Pulse sobre “Servicios”.  Seleccione el servicio “ESX Shell” y pulse “Iniciar”  Realice la misma operación con el servicio “SSH”.  **Nota:** No cierre aún el navegador web.
22.Realice la conexión al servidor de ESXi a través de SSH.		Utilice un cliente SSH para establecer una conexión al servidor e introduzca las credenciales de un usuario autorizado (no root) con privilegios administrativos para realizar las comprobaciones. 
23.Compruebe el estado los siguientes parámetros de seguridad.		Ejecute los comandos indicados en la tabla y compare los resultados.

Parámetro a comprobar	Valor devuelto	OK/NOK
# esxcli network ip get	IPv6Enable: false	
# esxcli system syslog config get	Local Log output: “Ruta al almacén de datos correcto y persistente”	
	Local Log Output Is Configured: true	
	Local Log Output Is Persistent: true	
	Local Login Default Rotation Size: 8192	
	Local Login Default Rotations: 0	
# esxcli system snmp get	Enable: false	
# esxcli software acceptance get	VMwareCertified	

Comprobación	OK/NOK	Como hacerlo
# grep PermitRootLogin /etc/ssh/sshd_config	PermitRootLogin no	
24.Compruebe los permisos sobre los siguientes ficheros de log		Diríjase a la ruta correspondiente al almacén de datos persistente donde se han alojado los ficheros log mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd "/vmfs/Volumes/<Nombre del almacén>/Syslogs** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l *.log** Compruebe que todos los ficheros con extensión .log tienen los mismos permisos como indica la tabla.

Ficheros	permisos	Propietario	OK/NOK
Todos los ficheros con extensión .log	-rw-------	root	

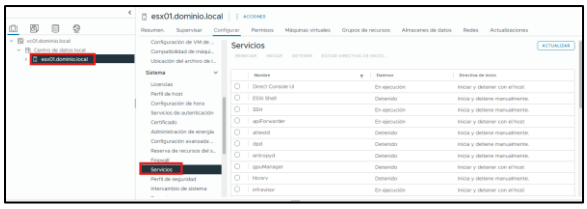
25.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe los permisos sobre la carpeta "/etc" y el propietario.

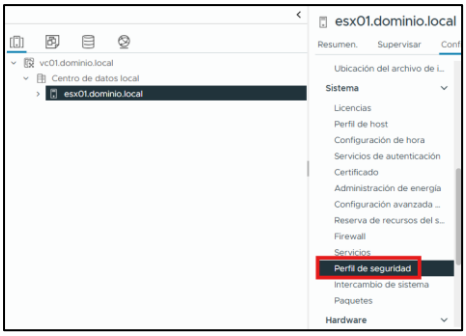
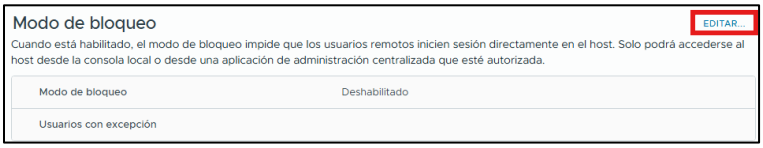
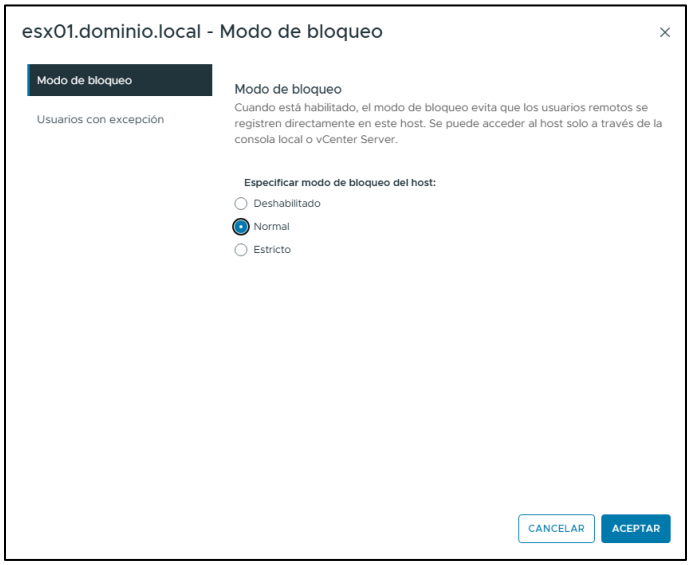
Ficheros	permisos	Propietario	OK/NOK
/etc	-rwxr-xr-x	root	

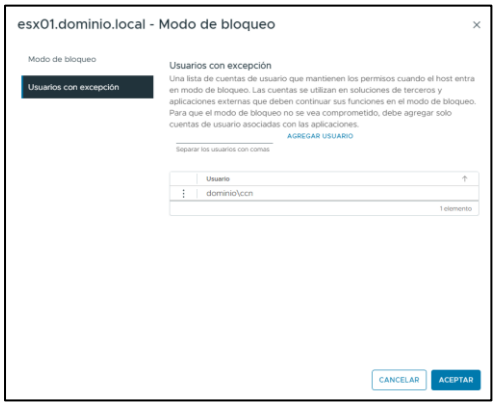
26.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.

Ficheros	permisos	Propietario	OK/NOK
/etc/profile	-rw-r--r--	root	
/etc/krb5.conf	-rw-r--r--	root	
/etc/krb5.realms	-rw-r--r--	root	
/etc/nscd.conf	-rw-r--r--	root	
/etc/resolv.conf	-rw-r--r--	root	
/etc/nsswitch.conf	-rw-r--r--	root	
/etc/ntp.conf	-rw-r--r--	root	
/etc/passwd	-rw-r--r--	root	

Comprobación	OK/NOK	Como hacerlo			
/etc/group			-rw-r--r--	root	
/etc/shadow			-r---------	root	
/etc/vmware/			-rwxr-xr-x	root	
27.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/ssh" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/ssh** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
/etc/ssh/sshd_config			-rw-------	root	
28.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/usr/sbin" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /usr/sbin** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l esxcfg*** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
Todos los ficheros que comienzan por esxcfg			-r-x------	root	
29.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/vmware" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/vmware** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
/etc/vmware/config			-rw-r--r--	root	
/etc/vmware/configrules			-rw-r--r--	root	
/etc/vmware/esx.conf			-rw-r--r--	root	
/etc/vmware/firewall			-rwxr-xr-x	root	
/etc/vmware/hostd			-rwxr-xr-x	root	
/etc/vmware/ima_plugin.conf			-rw-r--r--	root	
/etc/vmware/license.cfg			-rw-r--r--	root	

Comprobación	OK/NOK	Como hacerlo			
/etc/vmware/logfilters			-rw-r--r--	root	
/etc/vmware/pciid			-rwxr-xr-x	root	
/etc/vmware/pci.ids			-rw-r--r--	root	
/etc/vmware/service			-rwxr-xr-x	root	
/etc/vmware/snmp.xml			-rw-r--r--	root	
/etc/vmware/ssl			-rwxr-xr-x	root	
30.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/vmware/ssl" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/vmware/ssl** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
/etc/vmware/ssl/rui.crt			-rw-r—r--	root	
/etc/vmware/ssl/rui.key			-r--------		
31.Cierre la sesión SSH.		Cierre la sesión SSH.			
32.Una vez realizado, deshabilite SSH y la consola ESXi Shell (en caso de que no se hayan deshabilitado de forma automática).		En el navegador, pulse sobre el icono que corresponde a "Hosts y clústeres".  En el menú de la izquierda, sitúese sobre el objeto "<FQDN del servidor ESXi>" y pulse sobre "Servicios".  Sitúese sobre el servicio "ESX Shell" y pulse "Detener".  Realice la misma operación con el servicio "SSH".  			

Comprobación	OK/NOK	Como hacerlo
33.Vuelva a habilitar el modo de bloqueo.		Defina el modo de bloqueo para el acceso a este host en modo “Normal” para que solo se pueda acceder al host de ESXi a través de servidores vCenter o mediante acceso local y no a través de clientes vSphere por conexión directa al. Para ello, sitúese de nuevo sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar”, seleccione “Perfil de seguridad”.  En “Modo de Bloqueo” seleccione “Editar”.  En la ventana emergente, seleccione el modo “Normal”. 
34.Compruebe la lista de usuarios autorizados para acceder directamente al host con		Compruebe la lista de usuarios autorizados pulsando sobre “Usuarios con excepción” y pulse “ACEPTAR” para finalizar.

Comprobación	OK/NOK	Como hacerlo
modo de bloqueo activo.		 **Nota:** Esta lista debería ser revisada periódicamente para evitar que haya usuarios no autorizados añadidos a ella.

ANEXO A.4. CATEGORÍA ALTA / DIFUSIÓN LIMITADA

ANEXO A.4.1. IMPLEMENTACIÓN DE SEGURIDAD EN VMWARE VSPHERE 8.X SOBRE SERVIDORES QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS / DIFUSIÓN LIMITADA

El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores del entorno de virtualización VMware vSphere 8.x con una categorización de seguridad alta - DL según los criterios del Esquema Nacional de Seguridad.

Antes de realizar la implementación de este Anexo, la organización deberá haber realizado la categorización de los sistemas con objeto de determinar el nivel de cada una de las dimensiones de seguridad según se establece en el Anexo II del RD 311/2022. Si algún elemento del conjunto resultante para todos los servicios e información manejada por la organización correspondiera a la categoría alta - DL, deberá realizar las implementaciones según se referencian en el presente anexo.

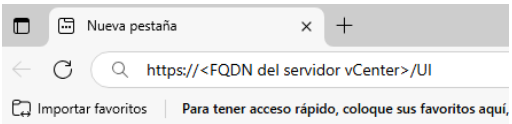
Este anexo será de igual aplicación cuando el sistema sobre el que se esté aplicando seguridad necesite cumplir los requisitos para una red clasificada con grado de clasificación Difusión Limitada.

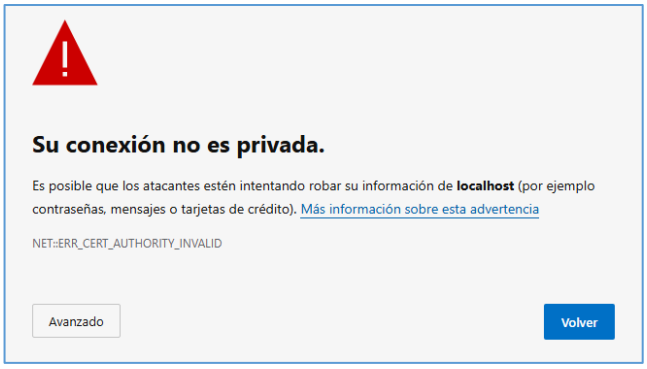
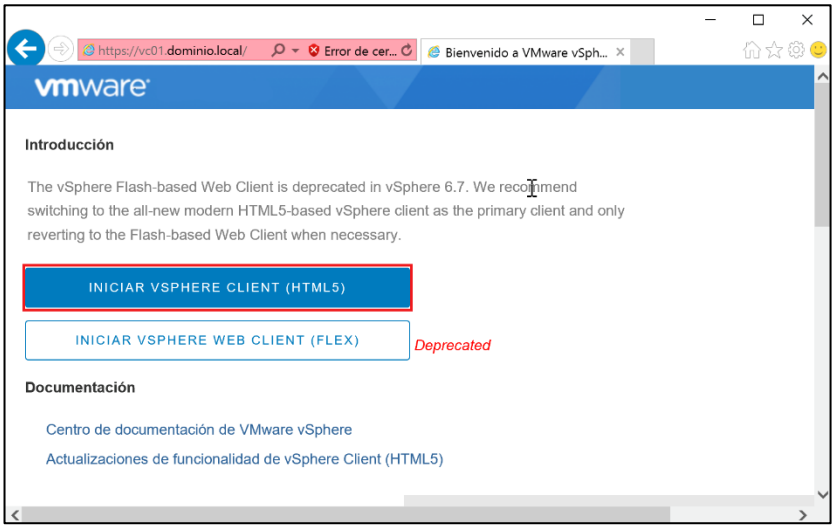
Nota: Tenga en cuenta que en el caso de una red clasificada con grado de clasificación Difusión Limitada se hará usó de la aplicación de seguridad descrita en este anexo, pero deberá atender adicionalmente a los requisitos establecidos por la normativa de aplicación sobre sistemas clasificados para dicho caso.

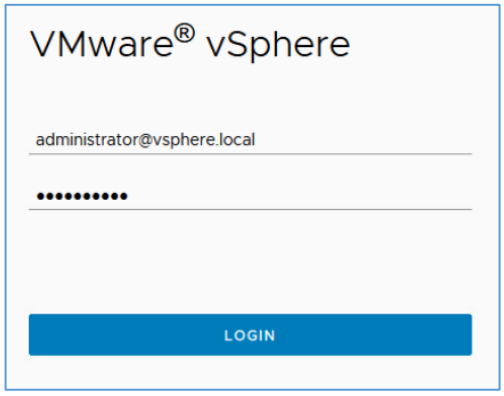
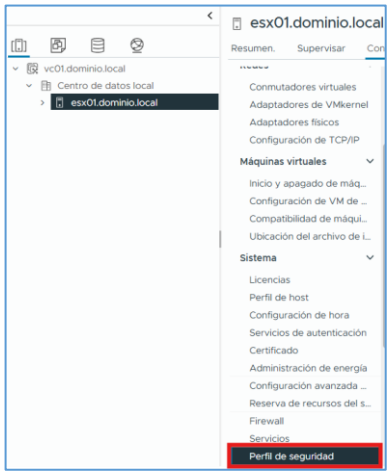
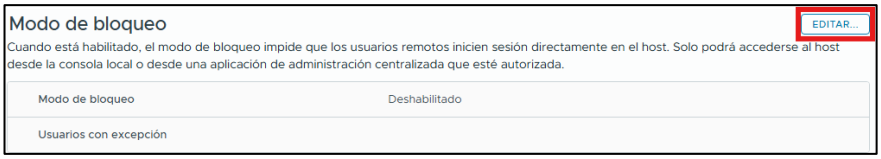
Debe tener en consideración que antes de realizar la puesta en producción de los mecanismos descritos en la presente guía, deberá realizar pruebas en un entorno de preproducción con objeto de familiarizarse con el escenario y realizar pruebas de funcionalidad.

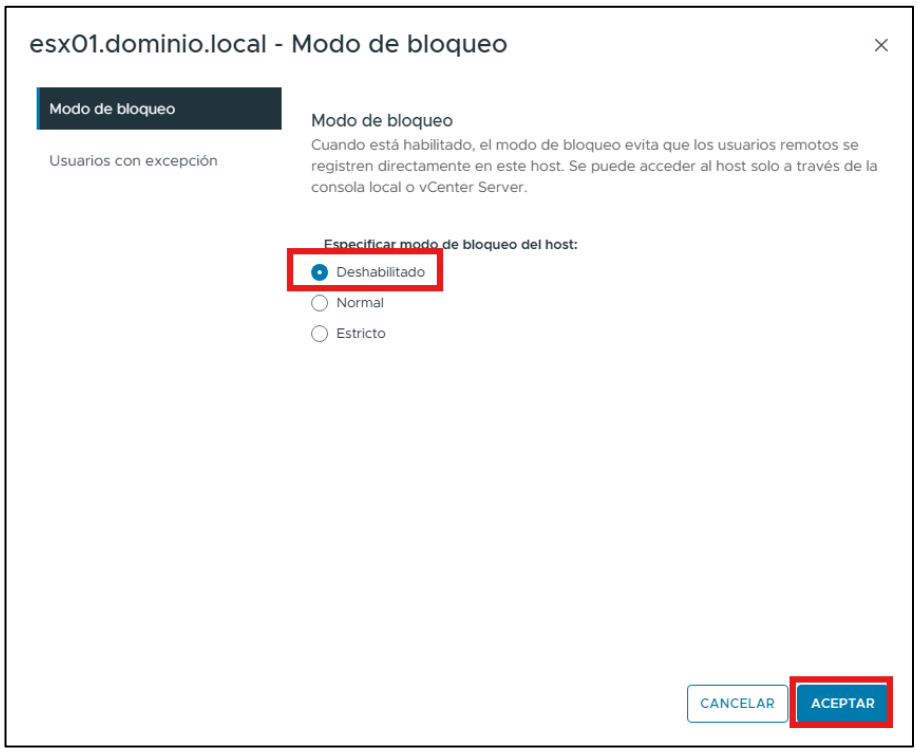
1. PREPARACIÓN DEL SERVIDOR ESXI

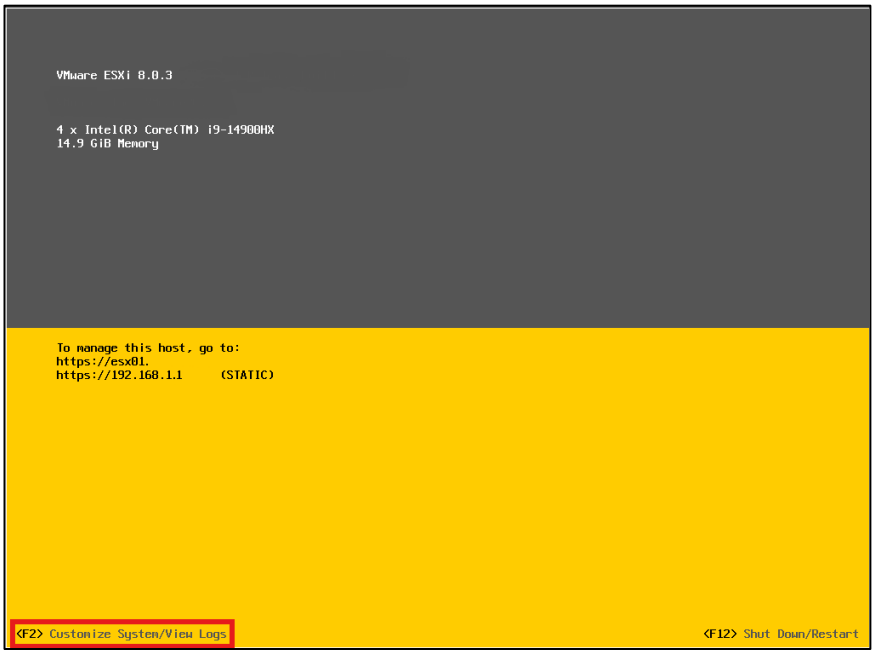
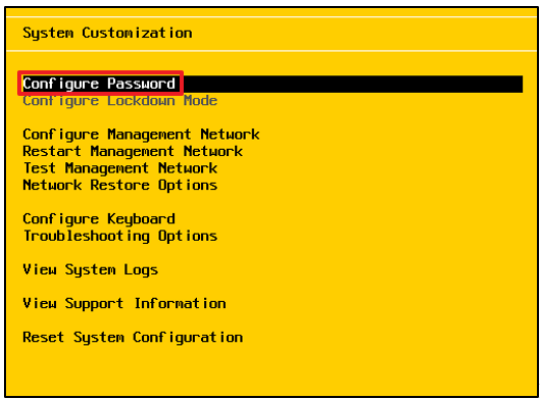
En caso de que esté habilitado, se deberá deshabilitar temporalmente el modo de bloqueo en cada servidor ESXi al que se le va a aplicar la seguridad ya que algunas de estas configuraciones deberán ser realizadas a través de conexión directa al host. En los pasos finales se habilitará de nuevo para forzar el acceso único a través del servidor de vCenter.

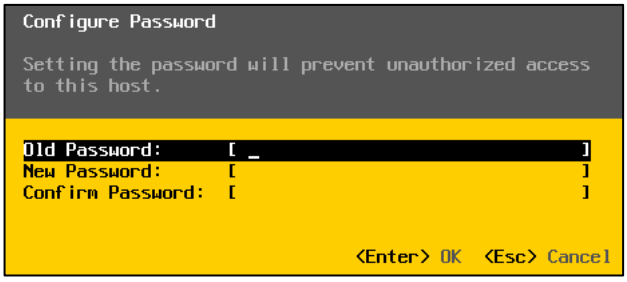
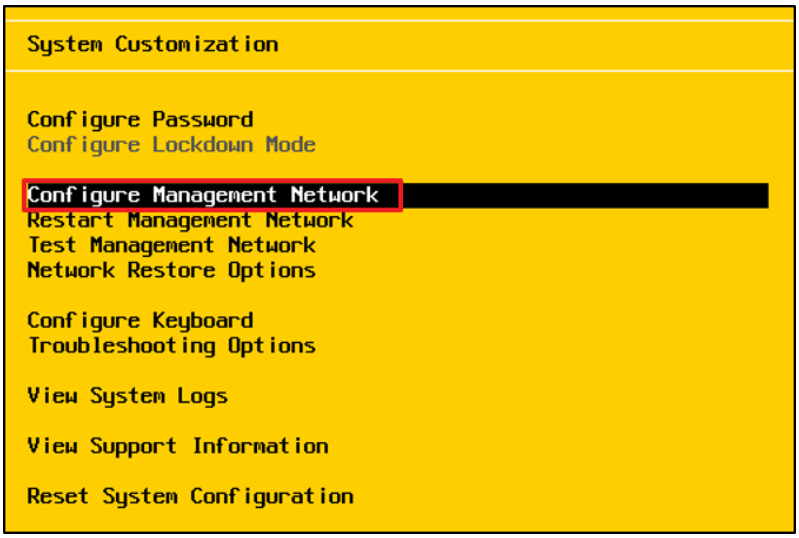
Paso	Descripción
1.	Inicie sesión directamente en el host ESXi utilizando el ESXi Host Client a través de su navegador web. Para ello, introduzca la siguiente URL: “ https://<IP-o-FQDN-del-host-ESXi>/UI”. 

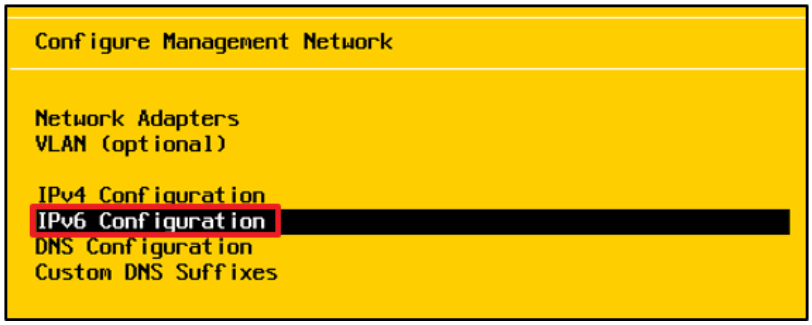
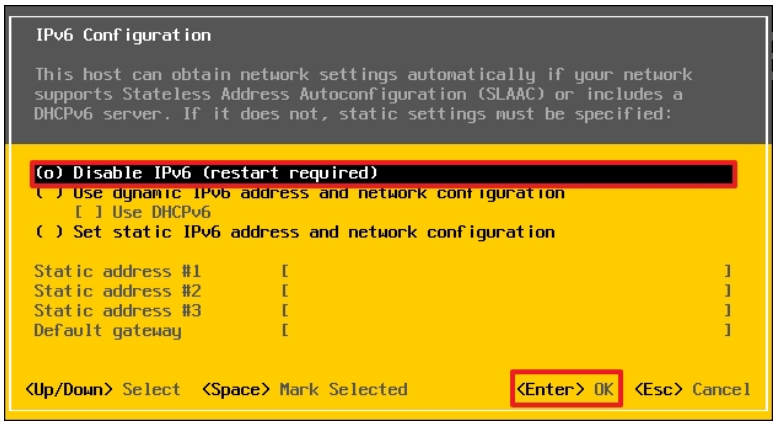
Paso	Descripción
2.	En caso de que aparezca una advertencia en el navegador que indica que el sitio no es seguro ignórela. Esto es debido a que en este momento se está empleando un certificado auto firmado que posteriormente deberá ser sustituido por un certificado válido emitido por una entidad certificadora autorizada. Pulse sobre la opción de ir al sitio web.  **Nota:** La captura y la opción a escoger podrían ser diferentes según el navegador que se esté empleando. En el ejemplo se ha utilizado Microsoft Edge.
3.	En caso de que aparezca un mensaje permitiendo elegir entre “vSphere Client (HTML5)” y “vSphere Web Client”, deberá seleccionar la primera opción. 

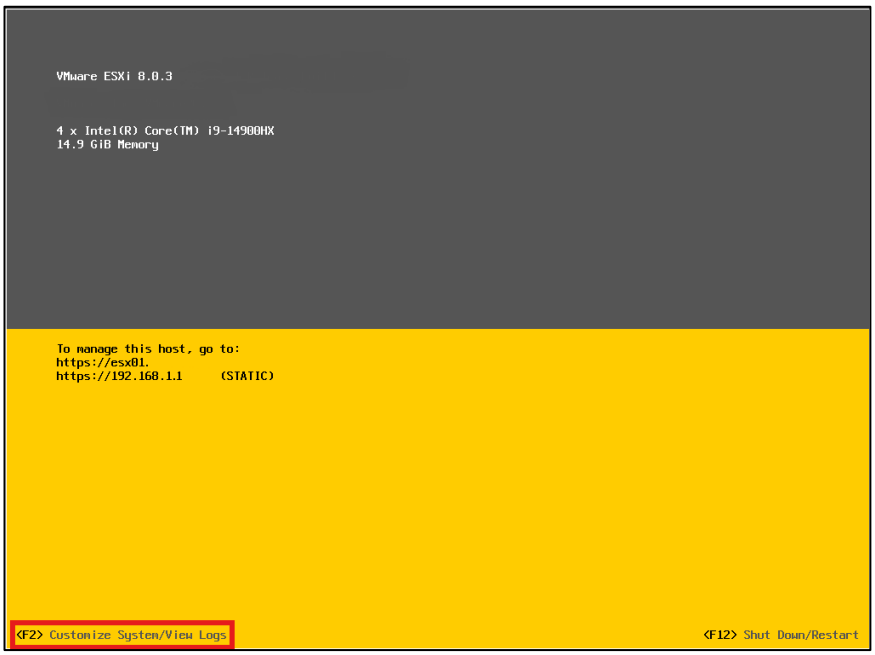
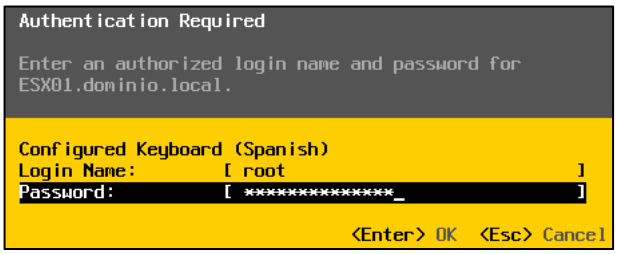
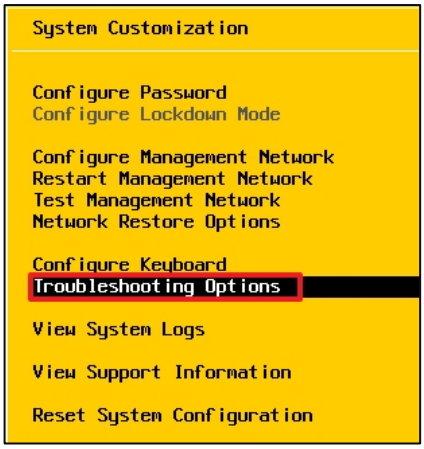
Paso	Descripción
4.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”.  **Nota:** Según los métodos de autenticación empleados, la pantalla podría diferir de la captura mostrada.
5.	En el menú de la izquierda, pulse sobre el icono que corresponde a “Host y clústeres”. 
6.	Sitúese sobre el objeto “<FQDN del servidor ESXi>” sobre el que quiere aplicar la seguridad y en la pestaña “Configurar”, seleccione “Perfil de seguridad”. 
7.	En “Modo de Bloqueo” seleccione “Editar”.  **Nota:** En caso de que el modo de bloqueo figure como “Deshabilitado” puede este paso.

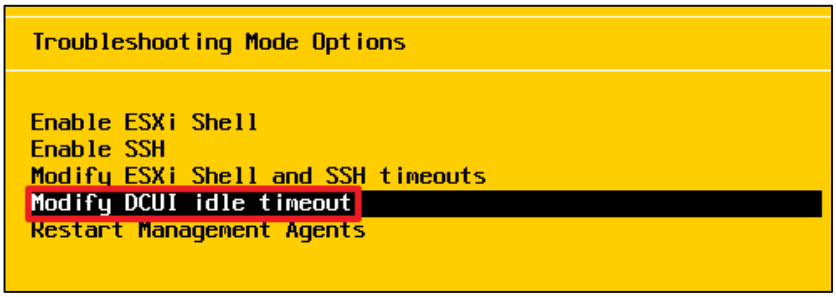
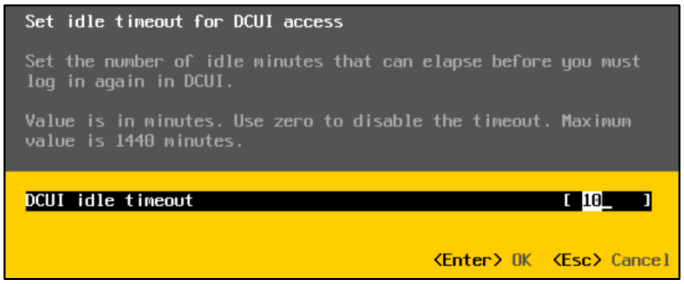
Paso	Descripción
8.	En la ventana emergente, seleccione el modo “Deshabilitado” y pulse “ACEPTAR” para continuar.  **Nota:** En caso de que el modo de bloqueo figure como “Deshabilitado” puede obviar este paso.
9.	Los siguientes pasos descritos a continuación se realizarán en el servidor ESXi para terminar de configurar el hipervisor de forma local. **Nota:** Los pasos que se detallan a continuación, se deberán realizar en cada host ESXi que se implemente en la infraestructura de VMware vSphere 8.x que se está implementando.
10.	Es recomendable establecer una contraseña para el BIOS del propio servidor de ESXi de modo que se eviten posibles ataques basados en el acceso al equipo, de forma física, ya que se puede manipular la secuencia de arranque y los elementos de configuración del propio BIOS del servidor. **Nota:** En esta guía no se explica cómo hacerlo ya que el modo de establecer una contraseña en el BIOS del servidor variará dependiendo del fabricante y modelo de este.
11.	Así mismo, sería conveniente establecer, a través del BIOS, la secuencia de arranque y la lista de dispositivos de arranque permitidos. En caso de no establecer dicha configuración, sería posible arrancar desde un medio extraíble no autorizado pudiendo acceder a la información del servidor.

Paso	Descripción
12.	En el servidor de ESXi, pulse “F2” para realizar las tareas de configuración inicial. 
13.	El sistema solicitará credenciales. Introduzca la contraseña y pulse “Enter” para continuar. 
14.	En caso de que la contraseña suministrada durante la instalación no cumpliera con los requisitos de complejidad necesarios, seleccione “Configure Password” situándose sobre él mediante las teclas de dirección y presione “Enter”. 

Paso	Descripción
15.	Introduzca en el primer campo la contraseña suministrada durante la instalación y, a continuación, introduzca dos veces la contraseña deseada. Pulse "Enter" para validar la configuración y salir.  **Nota:** Recuerde que en esta categoría el nivel de complejidad y longitud de la contraseña deberá cumplir con los siguientes requisitos: - Mínimo 14 caracteres - Al menos 1 mayúscula - Al menos 1 minúscula - Al menos 1 carácter especial - Al menos 1 número
16.	Seleccione "Configure Management Network" para deshabilitar TCP/IPv6. Para ello, sitúese sobre la opción mediante las teclas de dirección y pulse "Enter".  **Nota:** Esta guía paso a paso asume que se está aplicando la seguridad sobre una infraestructura de VMware vSphere 8.x previamente operativa, por lo que no tendrán en cuenta parámetros de configuración e implementación y se ocupará de modificar las configuraciones relativas a la seguridad del sistema para alcanzar el nivel de seguridad deseado.

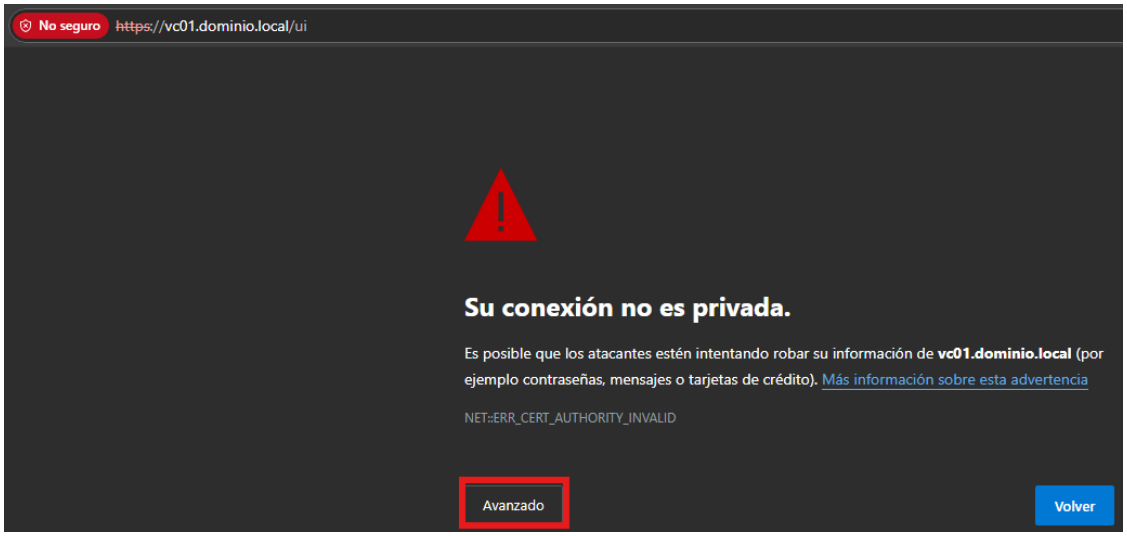
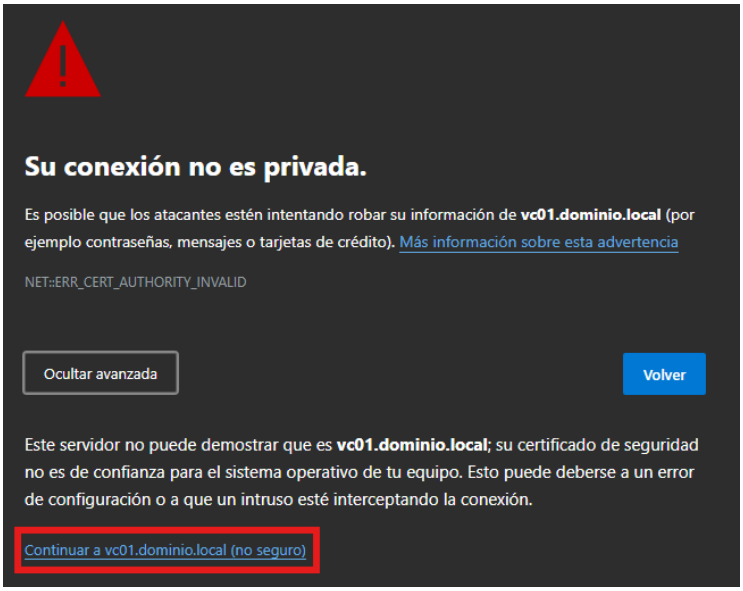
Paso	Descripción
17.	Seleccione “IPv6 Configuration” situándose sobre la opción, mediante las teclas de dirección, y presione “Enter”. 
18.	Sitúese sobre “Disable IPv6 (restart required)” y utilice la barra espaciadora para seleccionarlo. Pulse “Enter” para guardar los cambios. 
19.	Pulse “Esc” para salir de la configuración de red.
20.	Ante la solicitud de aplicar los cambios y reiniciar el host seleccione "Yes" pulsando la tecla "Y". El servidor se reiniciará. 

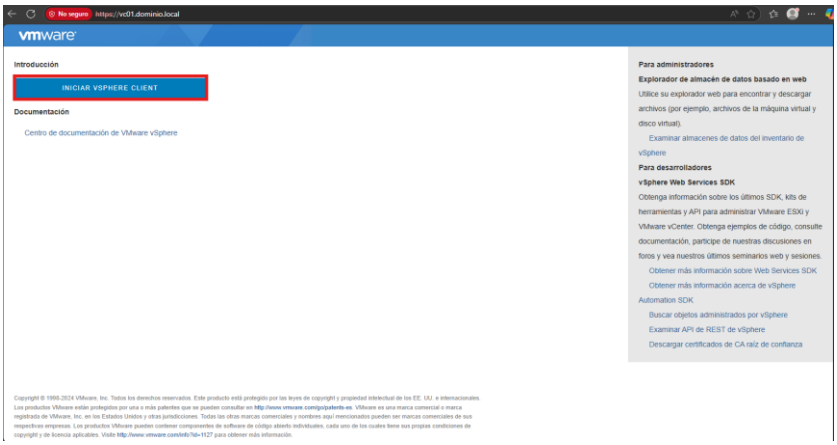
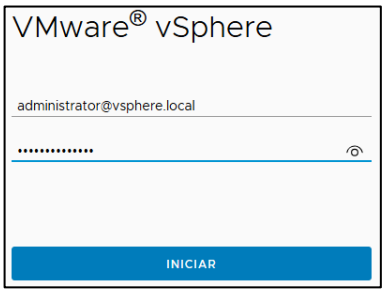
Paso	Descripción
21.	Una vez reiniciado el servidor, se procede a definir el tiempo de desconexión por inactividad. Pulse “F2” para abrir las herramientas de configuración del servidor ESXi. 
22.	El sistema solicitará credenciales. Introduzca la contraseña y pulse “Enter” para continuar. 
23.	Seleccione la opción “Troubleshooting options” y pulse “Enter” para continuar. 

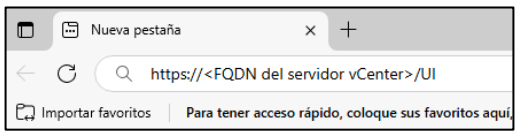
Paso	Descripción
24.	Pulse sobre “Modify DCUI idle timeouts” para establecer el tiempo de bloqueo de uso de la consola directa DCUI. 
25.	Introduzca el valor “10” y pulse “Enter” para registrarlo. Pulse “Esc” para salir al menú inicial. 
26.	Pulse “Esc” de nuevo para salir a la pantalla principal.

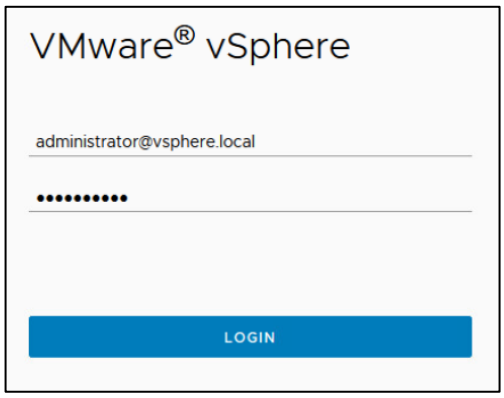
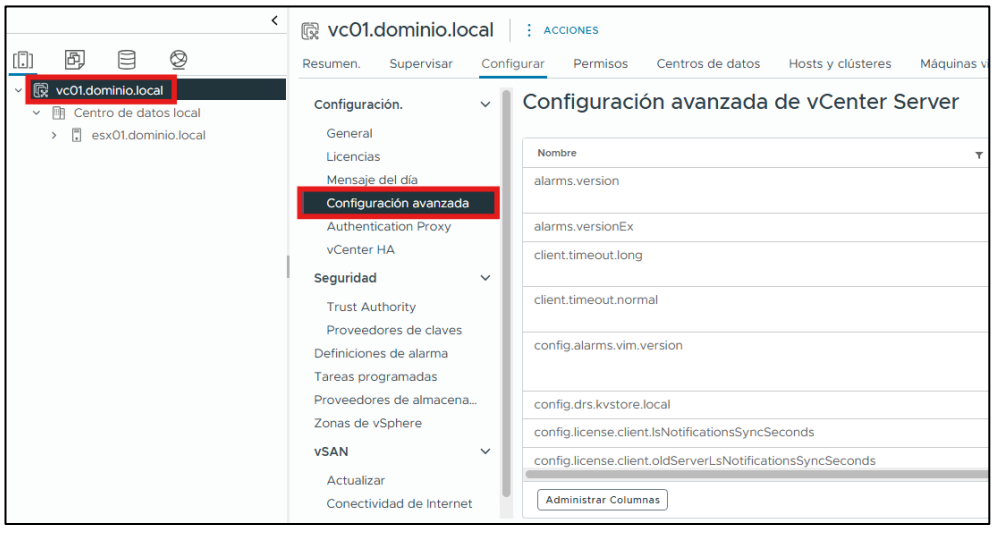
2. CONFIGURACIÓN DE SEGURIDAD EN VCENTER

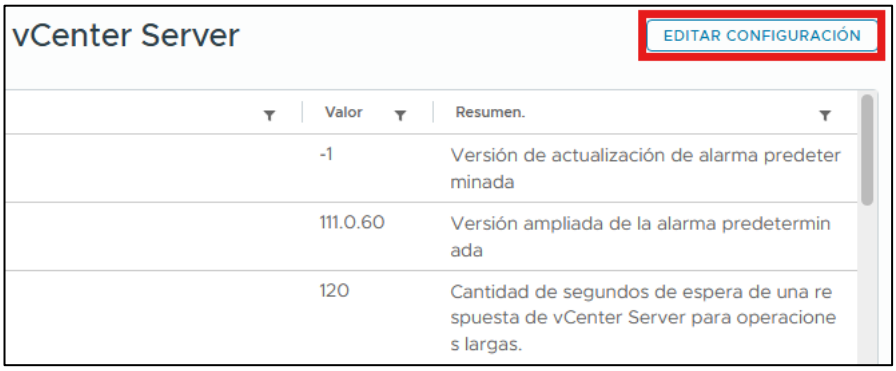
El resto de las configuraciones de seguridad que aplicarán al servidor de ESXi se realizarán a través del servidor de vCenter. Previamente se va a aplicar la configuración de seguridad de los propios servidores de vCenter. Deberá realizar los siguientes pasos en cada servidor de vCenter que pertenezca a la infraestructura.

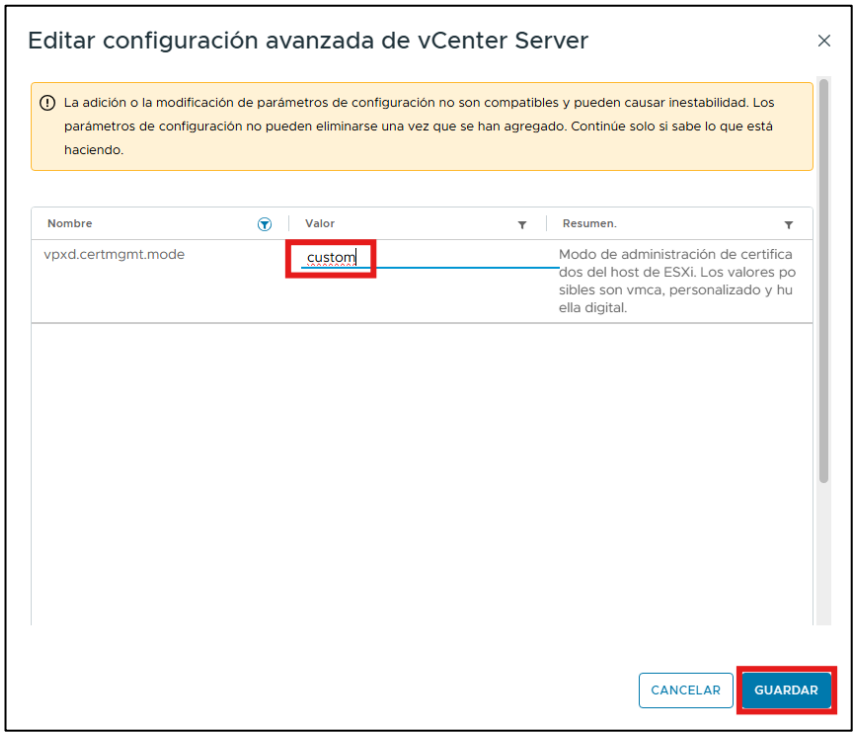
Paso	Descripción
27.	Inicie sesión, a través del vSphere client mediante html5, en el servidor de vCenter. Para ello, en su navegador, introduzca la url “https://<FQDN del servidor vCenter>/UI”. Si el navegador muestra una advertencia indicando que el sitio no es seguro, puede ignorarla. Esto se debe a que se está utilizando un certificado autofirmado. Haga clic en la opción "Avanzado". 
28.	Haga clic en la opción “Continuar al sitio”.  **Nota:** La apariencia de la advertencia de seguridad y las opciones disponibles pueden variar según el navegador utilizado. En este ejemplo se ha utilizado Microsoft Edge.

Paso	Descripción
29.	El cliente basado en Flash (vSphere Web Client - Flex) ha sido retirado oficialmente y ya no es compatible en vSphere 8. Utilizaremos exclusivamente el vSphere Client (HTML5) para acceder y gestionar el entorno. 
30.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”.  **Nota:** Según los métodos de autenticación empleados, la pantalla podría diferir de la captura mostrada.
31.	Se va a realizar una serie de pasos previos en el propio servidor de vCenter. Estas configuraciones deberán ser realizadas en los diferentes servidores de vCenter que pertenezcan a la organización. **Nota:** No es objeto de esta guía especificar los métodos de emisión de los certificados. Los pasos descritos a continuación, se realizan en el servidor de vCenter y tendrán que ser aplicados en cada servidor de vCenter implementado en la infraestructura.

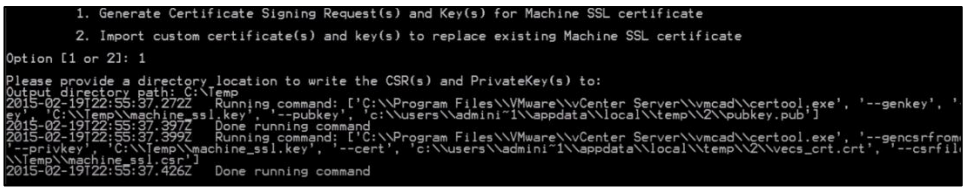
Paso	Descripción
32.	Los siguientes pasos consistirán en añadir y publicar en la infraestructura el certificado de la entidad de certificación raíz y el certificado de la subordinada. Una vez realizado esto, será posible añadir certificados de servidor a los servidores de ESXi. **Nota:** Antes de realizar este proceso, el servidor de vCenter no debe tener conectados los servidores de ESXi. En caso de haber añadido el servidor ESXi se deberá desconectar y se reconectará una vez realizados los pasos siguientes hasta el reinicio del servidor (Paso 56). Para desconectar el servidor ESXi, selecciónelo en el menú de la izquierda y con el botón derecho del ratón seleccione **"Conexión → Desconectar"** en el menú contextual que se ha desplegado. 
33.	El siguiente paso debe realizarse en el vCenter Server Appliance (VCSA), y consiste en publicar los certificados de la Entidad Certificadora (CA) raíz y, si aplica, de la Entidad Certificadora subordinada (SubCA) en el almacén de confianza del dominio de SSO (vsphere.local). Para ello, se utilizará el siguiente comando desde la consola del **appliance de vCenter (VCSA)**: **/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert <ruta_al_certificado_CA_base64>** **Nota:** Si el certificado fue firmado por una entidad certificadora subordinada, será necesario ejecutar, también, el siguiente comando: - **/usr/lib/vmware-vmafd/bin/dir-cli trustedcert publish --chain --cert <ruta_al_certificado_CA_subordinada_base64>** Asegúrese de que el certificado esté exportado en formato Base64 codificado (PEM).
34.	En caso de haber cerrado el navegador, inicie sesión, a través del vSphere client mediante html5, en el servidor de vCenter. Para ello, en su navegador, introduzca la url "https://<FQDN del servidor>/UI". 

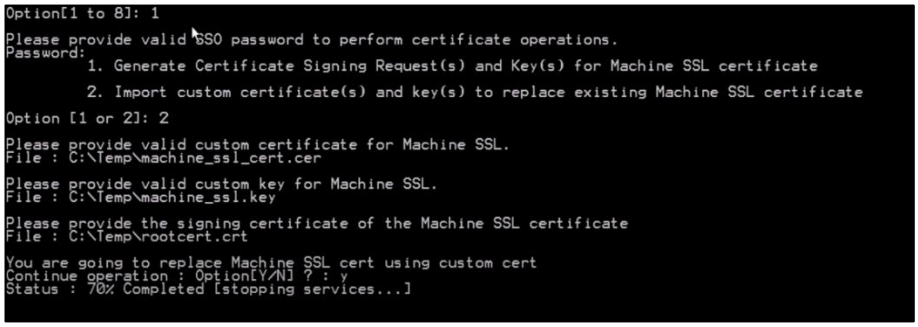
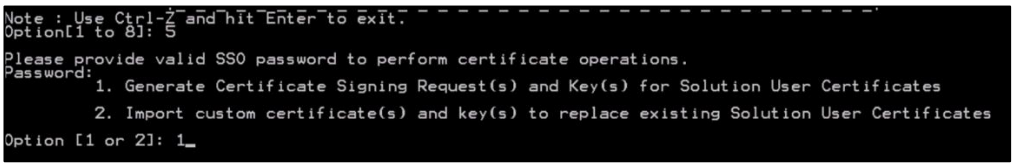
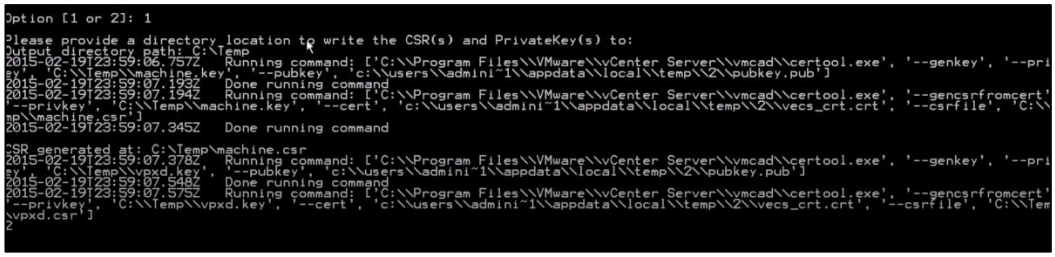
Paso	Descripción
35.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”. 
36.	A continuación, será necesario cambiar el modo de uso del certificado al modo personalizado. Para ello, a través de la consola de vSphere Client, pulse sobre el icono que corresponde a “Host y clústeres”. 
37.	En el menú de la izquierda, pulse sobre el objeto con el nombre del servidor de vCenter. 
38.	Vaya a la pestaña “Configurar” y seleccione “Configuración Avanzada”. 

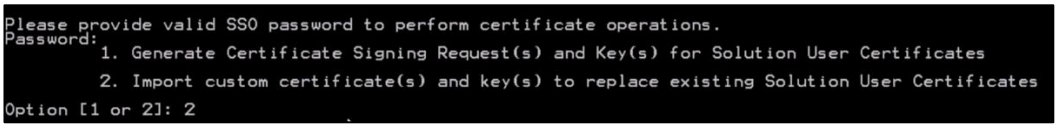
Paso	Descripción
39.	Pulse sobre “Editar configuración” en la zona superior derecha. 
40.	Pulse sobre la flecha a la derecha del título de la columna “Nombre”. 
41.	Teclee “vpxd.certmgmt.mode” y pulse la “X” de la zona superior para cerrar la ventana emergente. 

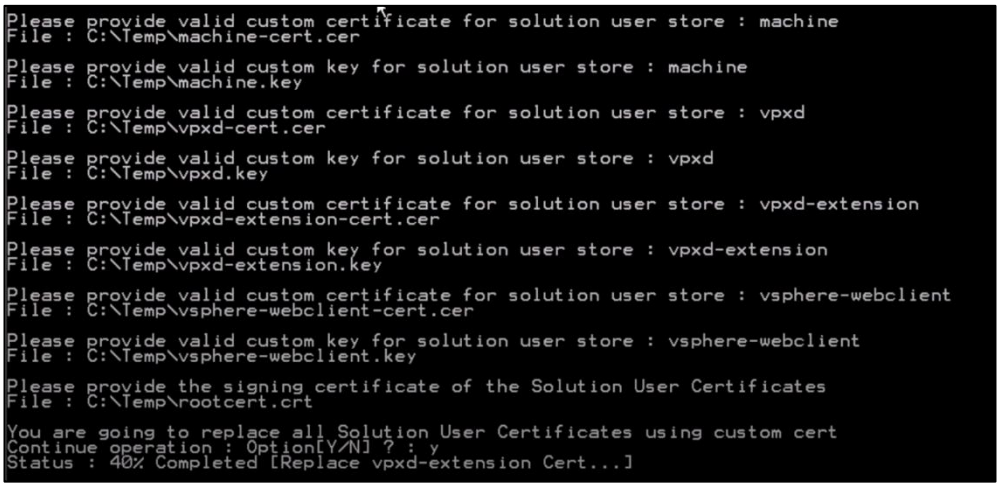
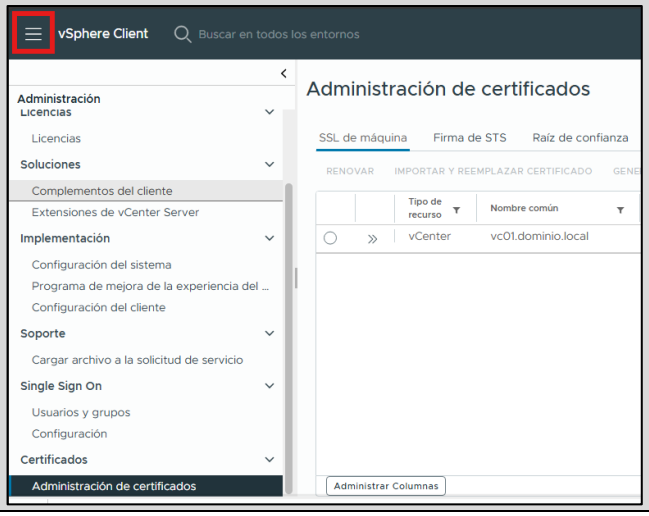
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>42.</td><td>Sustituya el valor “vmca” por “custom” y pulse “Guardar”
 
</td></tr>
<tr><td>43.</td><td>Se sustituirá, en este momento, el certificado de equipo existente por uno emitido por la entidad certificadora de terceros autorizada. El fichero de solicitud CSR que se deberá generar deberá responder a las siguientes características (es posible generar el fichero de solicitud CSR mediante una aplicación en el servidor de vCenter):
<table>
<tr><th>Elemento</th><th>Valor</th></tr>
<tr><td>Tamaño de clave</td><td>2048 bits o más</td></tr>
<tr><td>Formato</td><td>PEM / clave pública en formato CRT</td></tr>
<tr><td>SubjectAltName -> DNS Name</td><td>=<FQDN de la máquina></td></tr>
<tr><td>Usos permitidos</td><td>Firma digital, no repudio, cifrado de clave</td></tr>
<tr><td>Momento de validez</td><td>Un día antes del tiempo de solicitud</td></tr>
<tr><td>CN (y SubjectAltName)</td><td>Nombre del Host o dirección IP (debe coincidir con el nombre con el que se ha registrado el servidor de vCenter)</td></tr>
</table>
Así mismo, deberá emitir certificados para las aplicaciones web que vaya a utilizar (vpxd, vsphere-webclient, etc.).

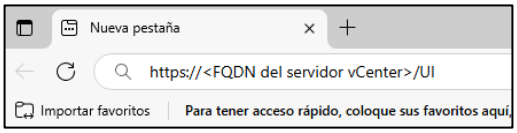
Nota: No es objeto de esta guía especificar los métodos de emisión de los certificados.</td></tr>
</table>

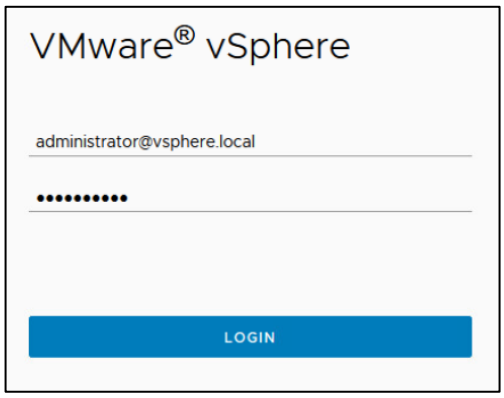
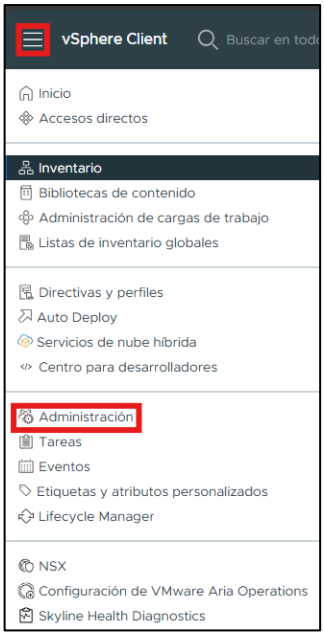
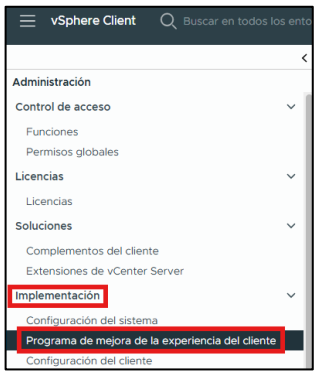
Paso	Descripción
44.	En el ejemplo se ha ejecutado la aplicación “certificate-manager” desde un servidor de vCenter sobre plataforma Windows. La ruta donde se encuentra dicha aplicación es “C:\Archivos de programa\VMware\vCenter Server\vmcad\certificate-manager.bat”. Pulse botón derecho sobre el ejecutable y seleccione “Ejecutar como administrador” en el menú contextual que se ha desplegado.  **Nota:** Si se desea instalar la aplicación desde un vCenter Appliance sobre Linux la ruta es **“/usr/lib/vmware-/vmca/bin/certificate-manager”**
45.	Seleccione la opción “1” en el menú principal de la aplicación, pulse “Enter” e introduzca un usuario con permisos para la gestión de certificados en el servidor. 
46.	Seleccione la opción “1” para generar el fichero de solicitud de certificado CSR (y el fichero de clave “.key”), pulse “Enter” y especifique la ruta donde almacenará el fichero de solicitud, pulse “Enter” de nuevo.  **Nota:** Se le solicitará la inclusión de datos para la emisión del certificado (Country, Name, Organization, etc.).
47.	Envíe el fichero CSR generado a una entidad certificadora autorizada para que genere el certificado a partir de la solicitud. **Nota:** No es objeto de esta guía especificar los métodos de emisión de los certificados.

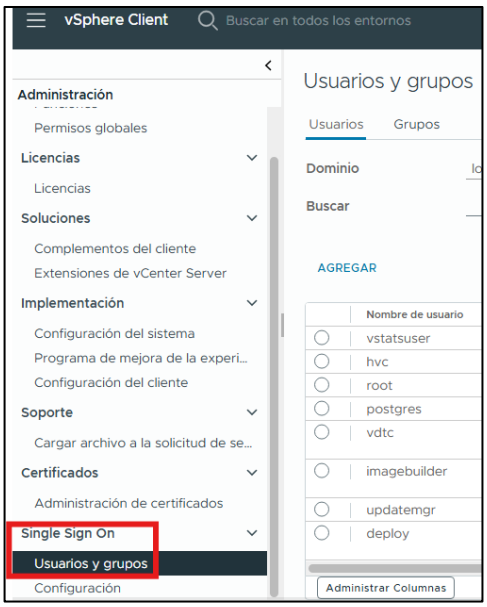
Paso	Descripción
48.	En caso de haber cerrado la sesión, vuelva a ejecutar la aplicación y seleccione la opción “1” en el menú principal (introduzca credenciales válidas), pulse “Enter” e introduzca un usuario con permisos para la gestión de certificados en el servidor. 
49.	Seleccione la opción “2” para importar el certificado generado, pulse “Enter” y especifique la ruta donde se encuentra el fichero generado por la entidad certificadora, la clave “.key” y el certificado de la entidad certificadora, pulse “Enter” de nuevo. Pulse “y” finalmente para confirmar la operación.  **Nota:** La ruta debe incluir también el fichero “.key” generado durante la fase de solicitud y el certificado de la entidad certificadora autorizada. De igual modo, la lista de certificados revocados (CRL) deberá ser accesible desde el servidor de vCenter para que este proceso pueda validar el certificado.
50.	Seleccione la opción “5”, “Enter” y “1” para generar los ficheros de solicitud de certificado CSR (y los ficheros de clave “.key”) de las diferentes soluciones web. Pulse “Enter” de nuevo. 
51.	Pulse “Enter” y especifique la ruta donde almacenarán los ficheros de solicitud, pulse “Enter” de nuevo.  **Nota:** Se generarán varios ficheros correspondientes a las claves y solicitudes de cada aplicación.

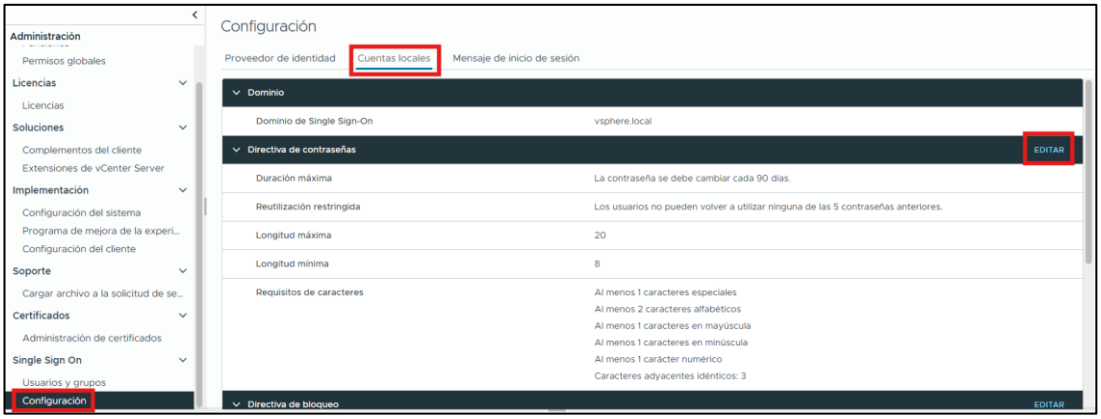
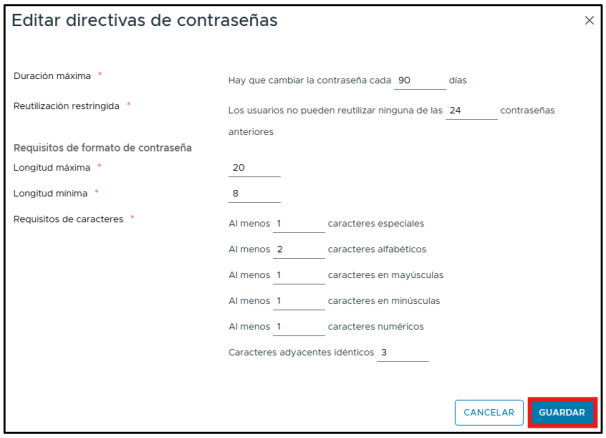
Paso	Descripción
52.	En caso de haber cerrado la sesión, vuelva a ejecutar la aplicación y seleccione la opción “5” en el menú principal (introduzca credenciales válidas), pulse “Enter” e introduzca un usuario con permisos para la gestión de certificados en el servidor. 
53.	Seleccione la opción “2” para importar los certificados generados y pulse “Enter.  **Nota:** La ruta debe incluir también los ficheros “.key” generados durante la fase de solicitud y el certificado de la entidad certificado.

Paso	Descripción
54.	Especifique las rutas donde se encuentran los ficheros generados por la entidad certificadora, las claves ".key" y el certificado de la entidad certificadora, pulse "Enter" de nuevo. Pulse "y" finalmente para confirmar la operación.  **Nota:** Es posible gestionar la importación de los certificados, también, a través de vSphere client mediante el **"Menú principal → Administración → Administración de certificados"**. 

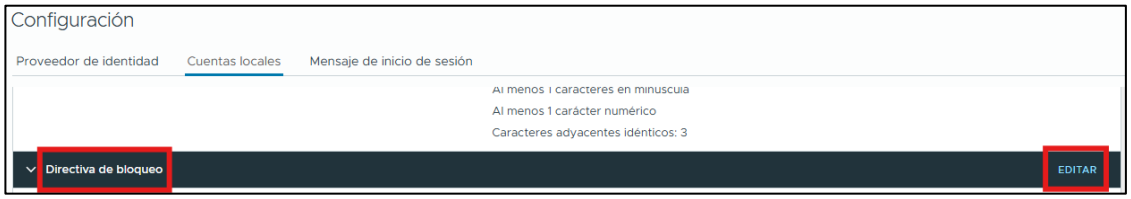
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>55.</td><td>Revise los servicios principales del vCenter Server Appliance y asegúrese de que los siguientes se encuentren configurados con inicio automático y en estado activo:
<table>
<tr><th>Servicio</th><th>Inicio</th><th>OK/NOK</th></tr>
<tr><td>VMWareDirectoryService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareIdentityMgmtService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareCertificateService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareDNSService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareAfdService</td><td>Automático</td><td></td></tr>
<tr><td>VMwareSTS</td><td>Automático</td><td></td></tr>
<tr><td>vmon</td><td>Automático</td><td></td></tr>
<tr><td>Vmware-cis-config</td><td>Automático</td><td></td></tr>
</table>
Nota: La disponibilidad de algunos servicios puede variar en función de los componentes habilitados durante la instalación de vCenter. Todos los servicios son gestionados por el gestor de procesos vmon, y se ejecutan bajo el contexto del sistema root en el appliance VCSA basado en Photon OS.
Verificación del estado de los servicios
Para consultar el estado actual de los servicios en VCSA, utilice el siguiente comando desde una sesión SSH o desde la consola directa del appliance:
- service-control –status
En VCSA, los servicios corren bajo el usuario root y sus configuraciones se encuentran gestionadas desde /etc/init.d/, /usr/lib/vmware/ o mediante systemd.
Para revisar permisos de ejecución:
- ls -l /etc/init.d/
- ls -l /usr/lib/vmware/</td></tr>
<tr><td>56.</td><td>Reinicie el servidor de vCenter server para aplicar los cambios.</td></tr>
<tr><td>57.</td><td>Una vez reiniciado el servicio, inicie sesión a través del vSphere client mediante html5, en el servidor de vCenter. Para ello, en su navegador, introduzca la url “https://<FQDN del servidor vCenter>/UI”.

</td></tr>
</table>

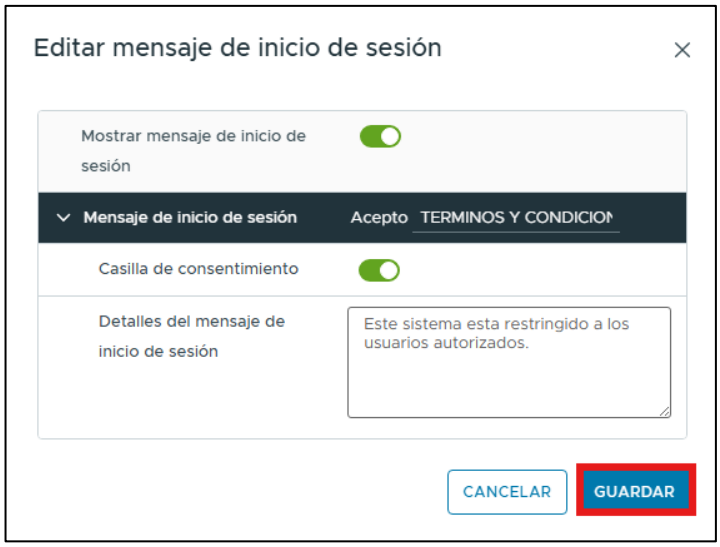
Paso	Descripción
58.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre “Iniciar”.  **Nota:** Según los métodos de autenticación empleados, la pantalla podría diferir de la captura mostrada.
59.	Pulse sobre el menú principal (☰) para acceder a la configuración del servidor de vCenter y seleccione “Administración” en el menú contextual que se ha desplegado. 
60.	Pulse sobre “Implementación → Programa de mejora de la experiencia del cliente”. 

Paso	Descripción
61.	El estado correcto debe ser “No Unido”. En caso de que el estado sea “Unido”, pulse sobre “Abandonar” en la zona inferior de la pantalla central. 
62.	Confirme pulsando sobre “Abandonar el programa”. 
63.	En el apartado “SingleSignOn” podrá añadir los “Usuarios y grupos que tendrán acceso al servicio de VMware vSphere 8.x y los privilegios que se les otorgarán.  **Nota:** Adapte los usuarios, grupos y permisos a las necesidades de la organización y rigiéndose por los criterios indicados en la presente guía. A partir de esta categoría del ENS será necesario el uso de grupos personalizados con permisos administrativos específicos y usuarios únicos para responder a la necesidad de segregación de roles y trazabilidad de actuaciones.

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>64.</td><td>Así mismo, en el apartado “SingleSignOn”, pulse sobre “Configuración” y en la pestaña “Cuentas locales”, pulse sobre “Directiva de contraseñas” y sobre “Editar”.
 
</td></tr>
<tr><td>65.</td><td>En la ventana emergente, establezca los siguientes parámetros y pulse “Guardar”.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Duración máxima</td><td>Hay que cambiar la contraseña cada “60” días</td></tr>
<tr><td>Reutilización restringida</td><td>Los usuarios no pueden reutilizar ninguna de las “24” contraseñas anteriores</td></tr>
<tr><td>Longitud mínima</td><td>“14”</td></tr>
<tr><td colspan="2">Al menos “1” caracteres especiales</td></tr>
<tr><td colspan="2">Al menos “1” caracteres en mayúsculas</td></tr>
<tr><td colspan="2">Al menos “1” caracteres en minúsculas</td></tr>
<tr><td colspan="2">Al menos “1” caracteres numéricos</td></tr>
</table>


Nota: Estos parámetros corresponden a la complejidad mínima a establecer, el resto de las configuraciones refuerzan dicha complejidad. Mantenerlos con los valores indicados es una acción correcta de cara a mejorar la seguridad.</td></tr>
</table>

Paso	Descripción
66.	Sitúese sobre “Directiva de bloqueo” y pulse sobre “Editar”. 
67.	En la ventana emergente, establezca los siguientes parámetros y pulse “Guardar”. – Cantidad máxima de intentos fallidos de inicio de sesión: “8”. – Intervalo de tiempo entre errores: 1800 segundos. – Tiempo de desbloqueo: 5400 segundos. 
68.	Pulse sobre la pestaña “Mensaje de inicio de sesión” y sobre “Editar”. 

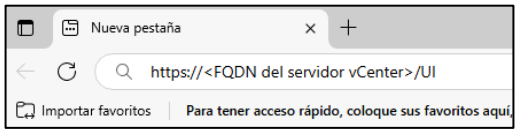
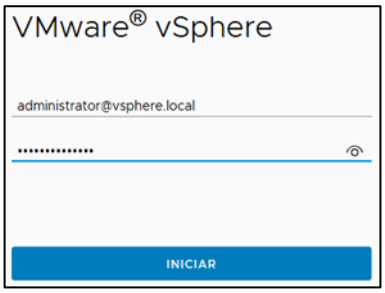
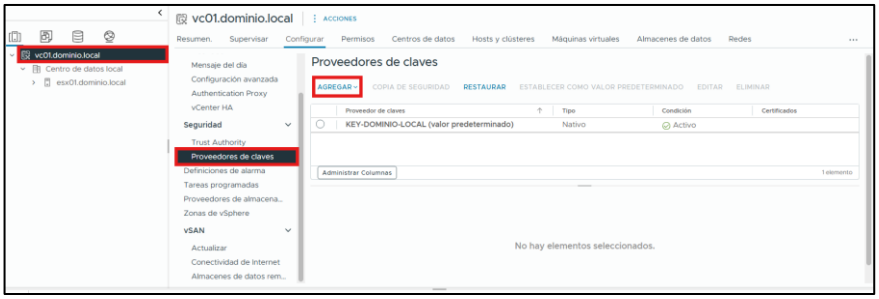
Paso	Descripción
69.	Pulse sobre los botones correspondientes a “Mostrar mensaje de inicio de sesión” y “Casilla de consentimiento” para habilitarlos y establezca un mensaje de seguridad. Pulse “Guardar” para continuar.  **Nota:** Adaptar el mensaje a las necesidades de su organización. A partir de este momento. El sistema, además de solicitar credenciales obliga a revisar las condiciones de acceso para marcar la aceptación de entrada a la aplicación. Podrán implementarse factores adicionales tal como autenticación por tarjeta inteligente o RSA secure ID. 

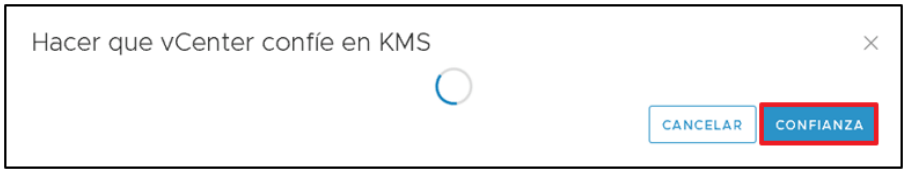
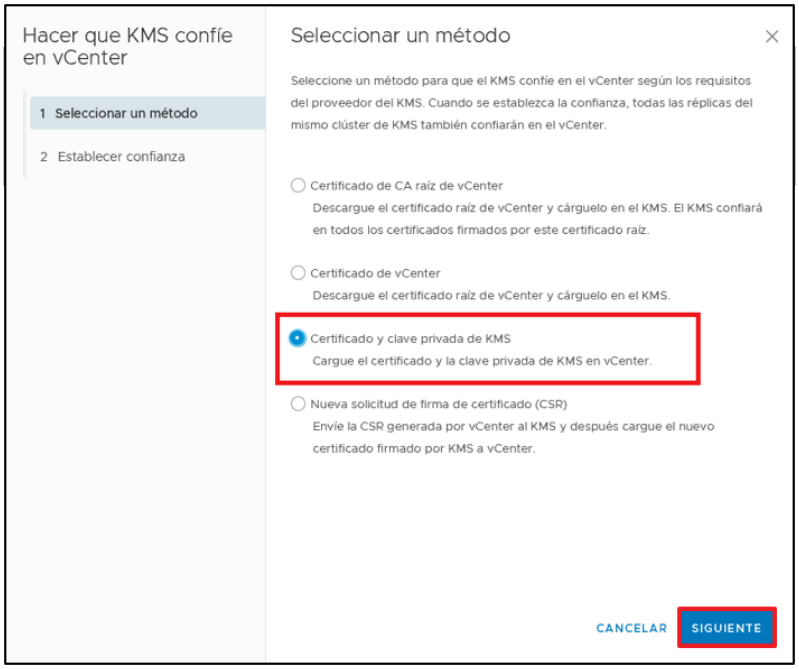
2.1. CONFIGURACIÓN DE SERVIDOR KMS

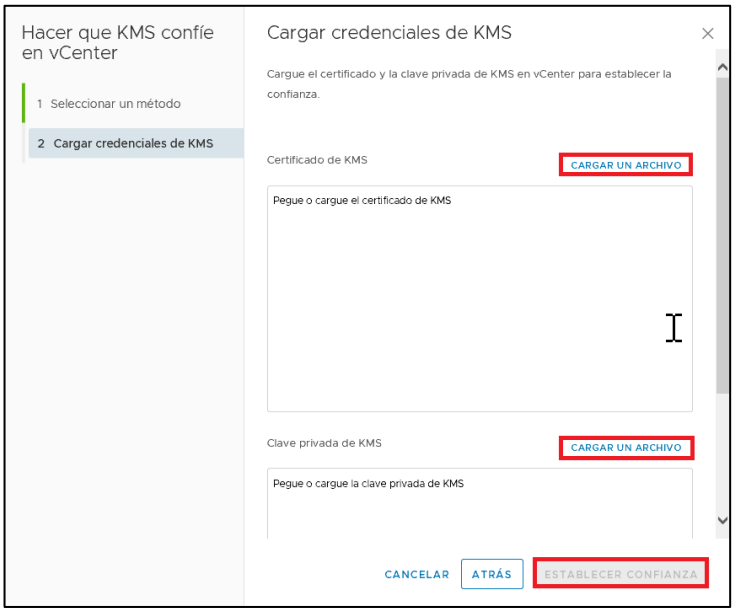
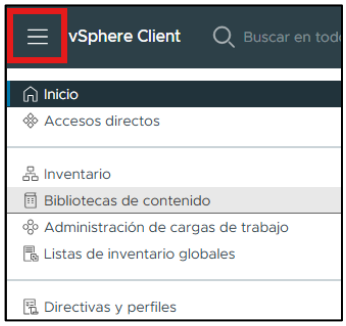
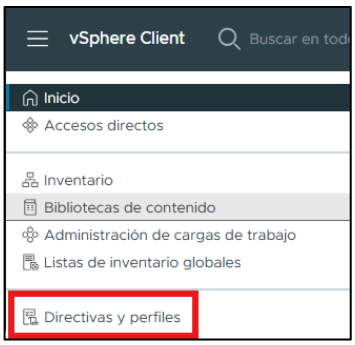
El ENS en su categorización Alta – Difusión Limitada requiere mecanismos que permitan el cifrado de la información. Existe un mecanismo específico proporcionado por VMware vSphere 8.x que posibilita el cifrado de aquellas máquinas virtuales en las que sea de necesidad proteger la información que contienen.

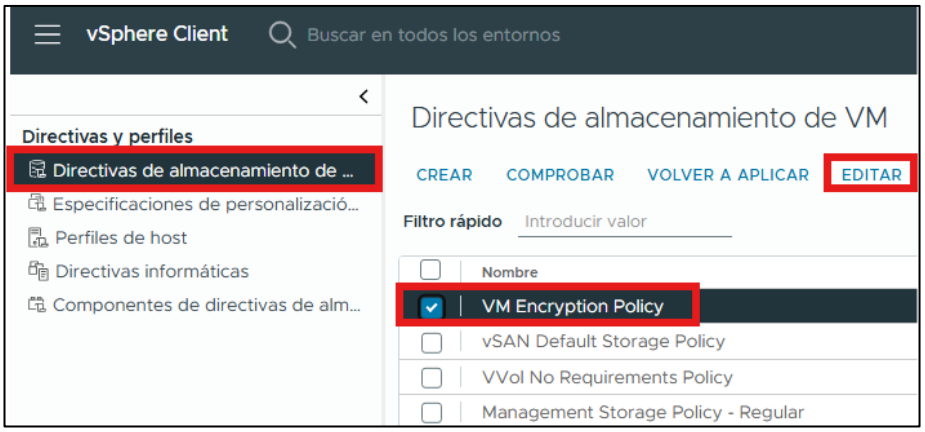
Para hacer uso del servicio de cifrado será necesario disponer de un servidor KMS (Key Management Service). No es objeto de esta guía paso a paso la instalación de un servicio de KMS, sin embargo, se especifican los pasos para añadirlo a la infraestructura.

Nota: Adapte las configuraciones a las necesidades del entorno.

Paso	Descripción
70.	Inicie sesión directamente en el host ESXi utilizando el ESXi Host Client a través de su navegador web. Para ello, introduzca la siguiente URL: " https://<IP-o-FQDN-del-host-ESXi>/UI". 
71.	Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter y pulse sobre "Iniciar". 
72.	A continuación, será necesario cambiar el modo de uso del certificado al modo personalizado. Para ello, a través de la consola de vSphere Client, pulse sobre el icono que corresponde a "Host y clústeres". 
73.	En el menú de la izquierda, pulse sobre el objeto con el nombre del servidor de vCenter. 
74.	En la pestaña "Configurar", sitúese sobre "Proveedores de claves" y pulse sobre "Agregar". 

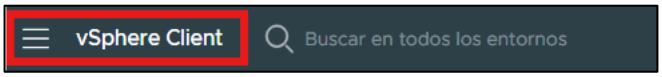
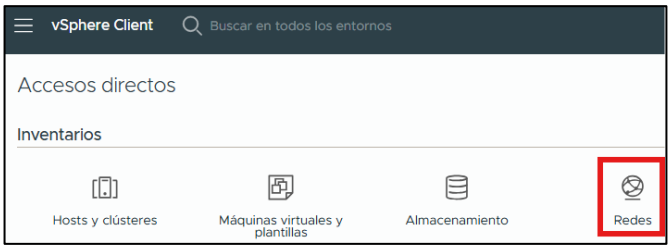
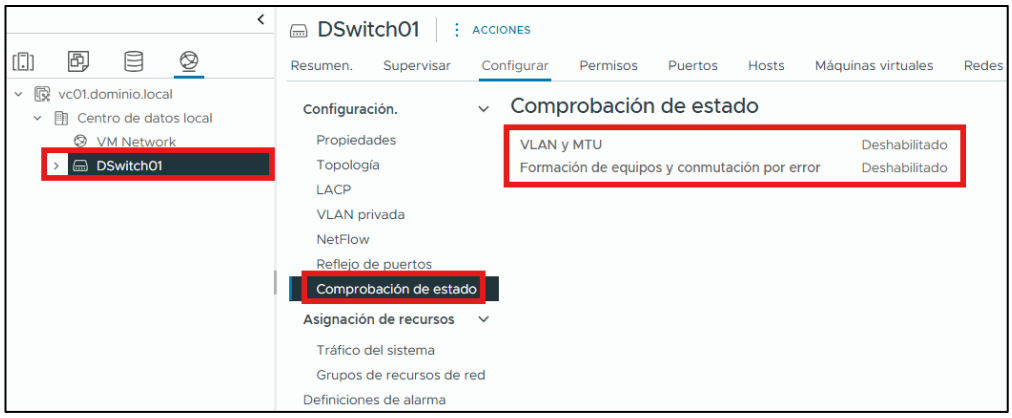
Paso	Descripción
75.	En la ventana emergente, introduzca los siguientes datos relativos al servidor de KMS y pulse “Añadir". Una vez añadido el servidor, se establecerá la confianza entre el servidor vCenter y el servidor de KMS. Para ello, deberá pulsar sobre “Confianza” cuando aparezcan los datos del servidor. 
76.	Por último, deberá establecer la confianza desde el servidor de KMS hacia el servidor de vCenter. Para ello, sitúese sobre “Establecer confianza” y pulse sobre “Hacer que KMS confíe en vCenter” a través del menú que se ha desplegado. 
77.	La opción de relación de confianza se realizará dependiendo de las necesidades del entorno. En el ejemplo se ha seleccionado “Certificado y clave privada de KMS”. Pulse “Siguiente” para continuar.  **Nota:** Deberá adaptar este paso a las necesidades de la organización.

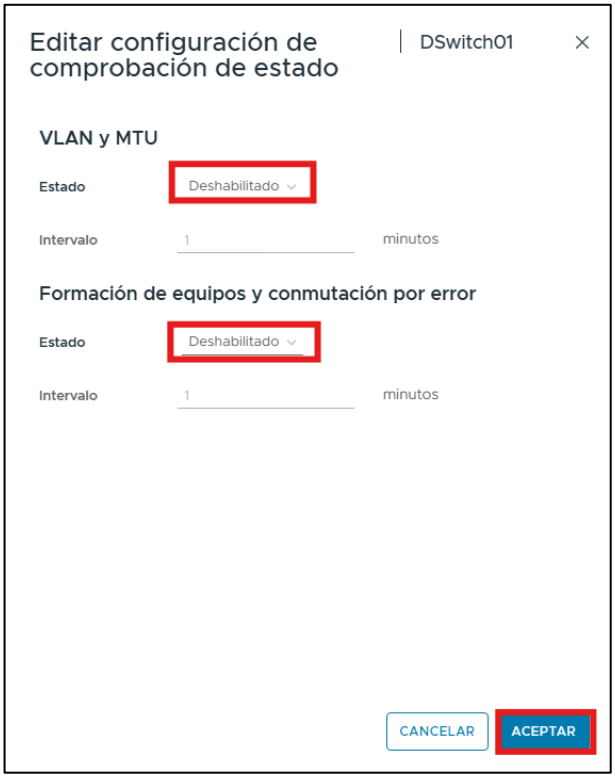
Paso	Descripción
78.	Pulse sobre “Cargar un archivo” tanto para cargar el certificado del servidor KMS como la clave privada. Pulse “Establecer confianza” para finalizar.  **Nota:** Deberá adaptar este paso a las necesidades de la organización.
79.	En caso de requerirlo, se puede personalizar la política de cifrado que se aplicará a los distintos servidores ESXi, al almacenamiento y a las máquinas virtuales. En la parte superior izquierda pulse (☰) y seleccione “Inicio” en el menú que se ha desplegado. 
80.	Seleccione “Directivas y perfiles”. 

Paso	Descripción
81.	Pulse sobre “Directivas de almacenamiento” y cree una nueva directiva pulsando sobre “Crear directiva de almacenamiento de máquina virtual” o edite la directiva “VM Encryption Policy” seleccionándola y pulsando “Editar”. En el ejemplo se ha editado la directiva “VM Encryption Policy”. 
82.	Personalice los parámetros pulsando “Siguiente” para navegar por los diferentes elementos de configuración, los cuales permiten aplicar cifrado a nivel de máquinas virtuales, hosts o almacenes y establecer propiedades de cifrado personalizadas.  **Nota:** Deberá adaptar este paso a las necesidades de la organización.
83.	Pulse “Finalizar” para guardar los cambios.

2.2. CONFIGURACIÓN EN CONMUTADORES VIRTUALES DISTRIBUIDOS

Las configuraciones descritas a continuación son a nivel de conmutadores virtuales distribuidos. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los conmutadores virtuales distribuidos existentes en el servicio de vCenter.

Paso	Descripción
84.	Haga clic sobre el icono “vSphere Client” para ir al menú principal. 
85.	En el menú de la izquierda, seleccione el icono correspondiente a “Redes”. 
86.	Sitúese sobre cada conmutador distribuido y en la pestaña “Configurar” pulse sobre el elemento “Comprobación de estado”. A continuación, en caso de que esté habilitado alguno de estos dos elementos, deberá deshabilitarlos: – VLAN y MTU. – Formación de equipos y conmutación por error.  **Nota:** Estas opciones solamente deberían ser habilitadas en momentos de resolución de problemas y de forma temporal.
87.	Para ello, pulse sobre “Editar”. 

Paso	Descripción
88.	En la ventana emergente, modifique los campos de estado a “Deshabilitado” y pulse “Aceptar”. 

2.2.1. CONFIGURACIÓN EN GRUPO DE PUERTOS

Las configuraciones descritas a continuación son a nivel de grupos de puertos. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los grupos de puertos existentes en los distintos conmutadores presentes en el servicio de vCenter.

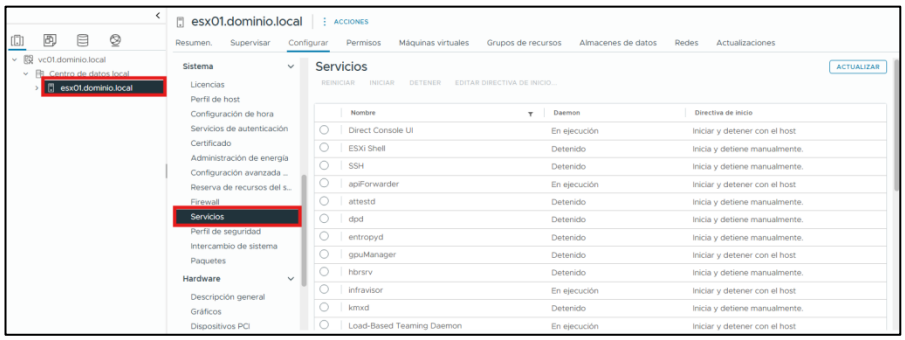
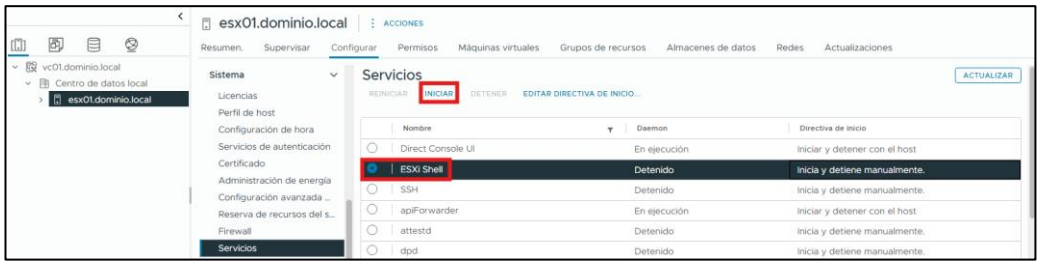
Paso	Descripción
89.	En el menú de la izquierda, seleccione el icono correspondiente a “Redes”. 

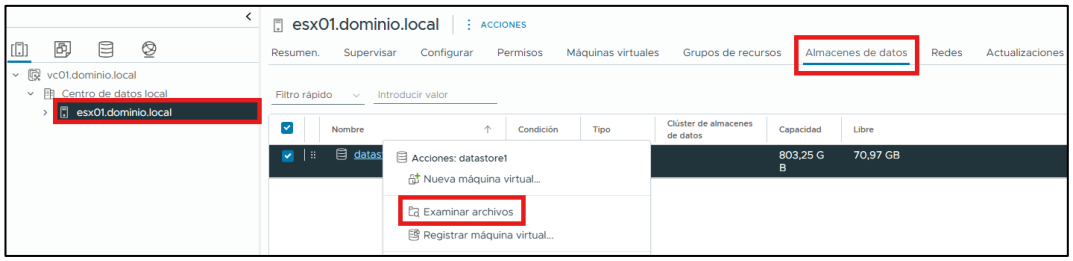
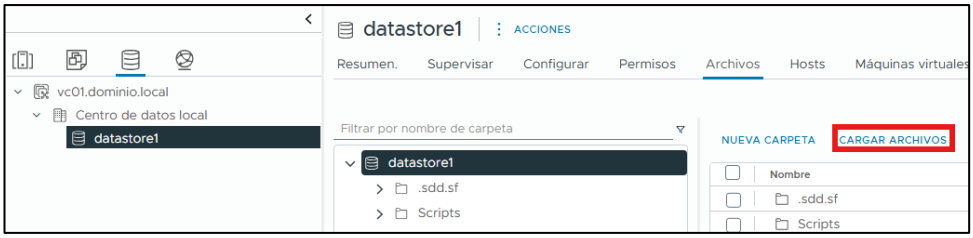
Paso	Descripción
90.	Sitúese sobre cada grupo de puertos (que se encontrarán dentro de la rama de cada conmutador virtual) y en la pestaña “Configurar”, seleccione “Directivas” y compruebe que las siguientes directivas de seguridad tienen el valor “Rechazar” y si no es así se deberá modificar el valor de las directivas: – Modo promiscuo – Cambios de dirección MAC – Transmisiones falsificadas 
91.	Para modificar las directivas pulse sobre “Editar”. 
92.	En la ventana emergente pulse sobre “Seguridad”, modifique las directivas deseadas y pulse “ACEPTAR” para validar la configuración. 

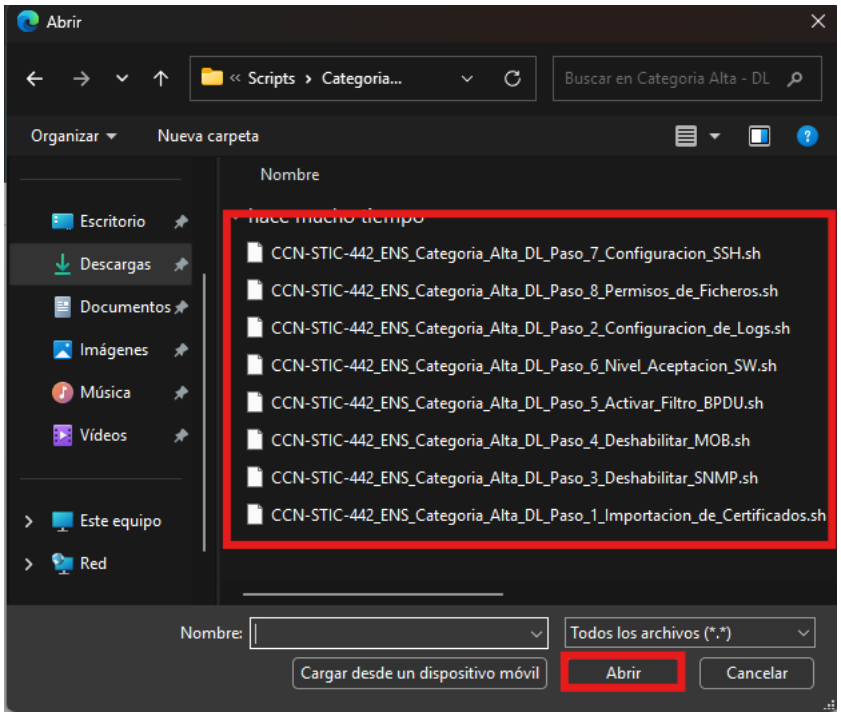
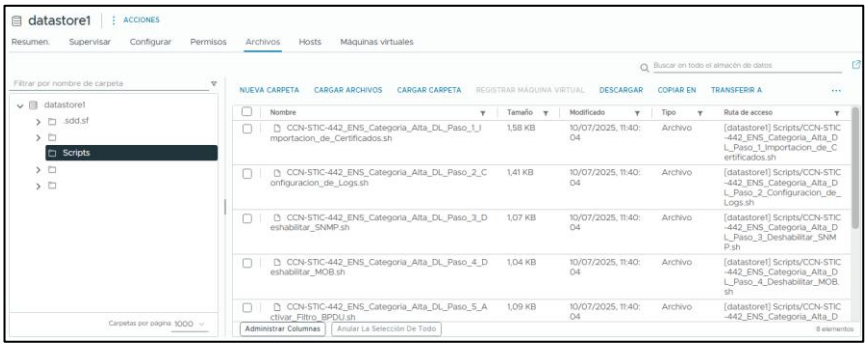
2.3. CONFIGURACIÓN DE SEGURIDAD EN SERVIDORES ESXI

Los pasos descritos a continuación se realizan a nivel de servidor ESXi y deberán ser aplicados en cada uno de los host ESXi que se añadan al servidor de vCenter. Existe la posibilidad de establecer perfiles de host para definir las configuraciones, a modo de plantilla, de modo que se homogenice y automatice el proceso de implementación de los servidores de ESXi.

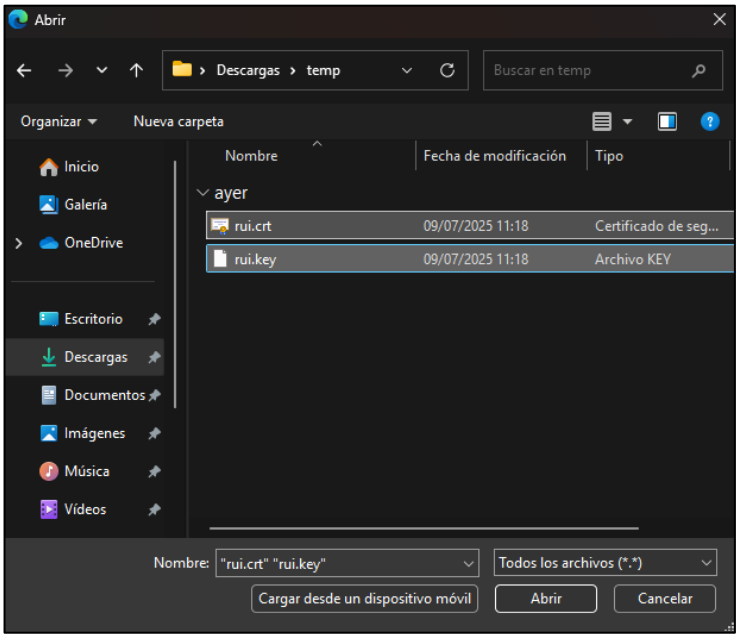
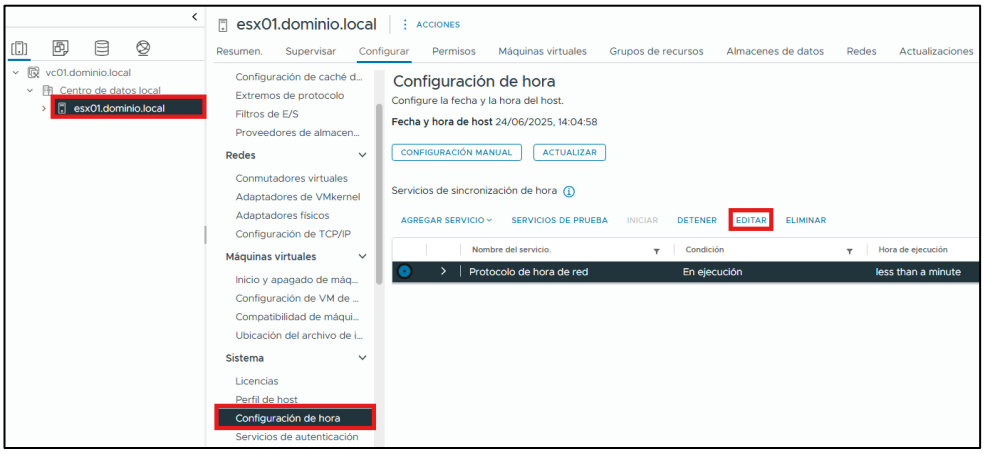
Muchos de los pasos se continúan realizando a través del cliente de vSphere pero la ejecución de scripts se realizará mediante una conexión directa por SSH a la consola ESXi Shell del host al que queremos aplicarle seguridad. Por tanto, será necesario activar los servicios de SSH y ESXi Shell en el host ESXi y, una vez completadas las configuraciones, se volverán a deshabilitar ambos servicios.

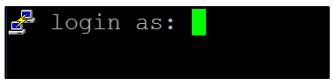
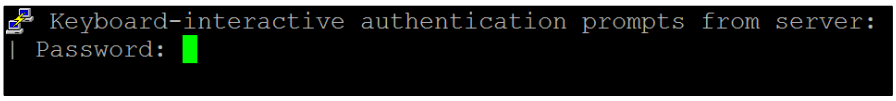
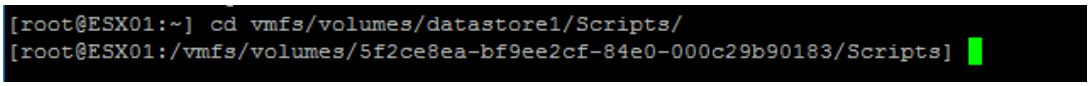
Paso	Descripción
93.	En el menú de la izquierda, pulse sobre el icono que corresponde a “Host y clústeres”. 
94.	Sitúese sobre el objeto “<FQDN del servidor ESXi>” sobre el que quiere aplicar la seguridad y en la pestaña “Configurar”, seleccione “Servicios”. 
95.	Sitúese sobre el servicio “ESX Shell” y pulse el botón “Iniciar”.  **Nota:** Si el servicio ya se encuentra activo no será necesario realizar ninguna acción.
96.	Realice la misma operación con el servicio “SSH”.  **Nota:** Si el servicio ya se encuentra activo no será necesario realizar ninguna acción.

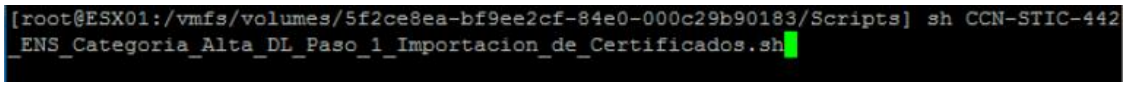
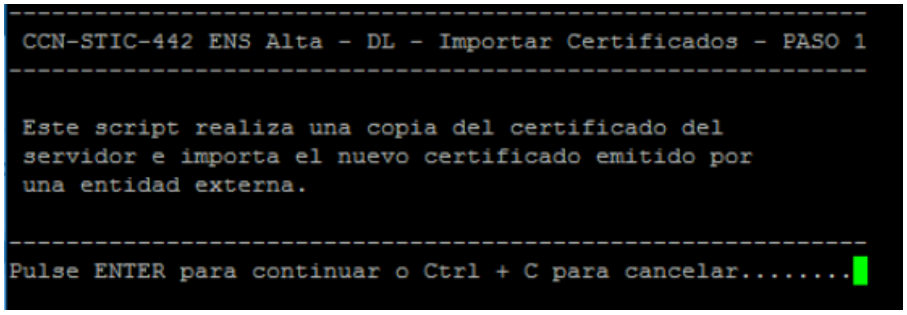
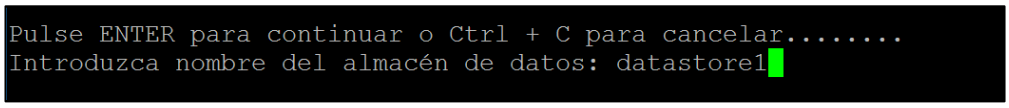
Paso	Descripción
97.	Sitúese sobre el objeto <FQDN del Servidor ESXi> y en la pestaña “Almacenes de datos”, seleccione, con el botón derecho del ratón, el almacén donde alojará los Scripts de configuración de seguridad de la presente guía y pulse sobre “Examinar archivos”.  **Nota:** En el ejemplo se ha utilizado el almacén que se ha creado por defecto al añadir el host a vCenter. Adapte la configuración a las necesidades de su entorno.
98.	Seleccione “Nueva Carpeta” para crear la carpeta que contendrá los Scripts. 
99.	Establezca el nombre “Scripts” a la carpeta y pulse “Aceptar”. 
100.	Haga clic sobre la carpeta “Scripts” recién creada y seleccione “Cargar archivos”. 

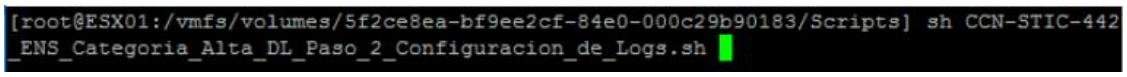
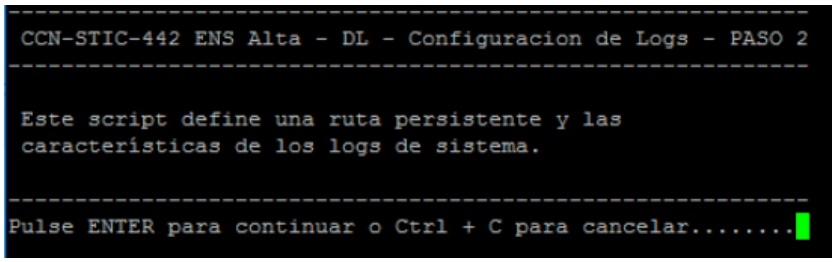
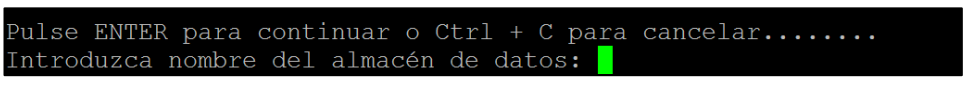
Paso	Descripción
101.	Localice los scripts que se aplican en este anexo, selecciónelos todos y pulse “Abrir”. 
102.	Los scripts quedarán almacenados en el almacén de datos. 

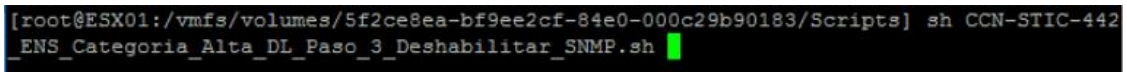
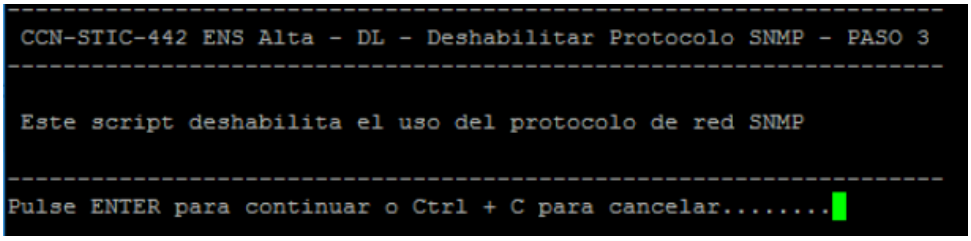
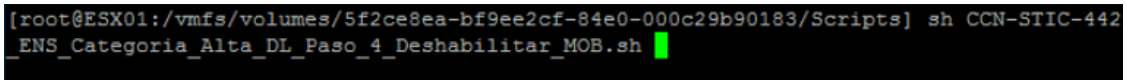
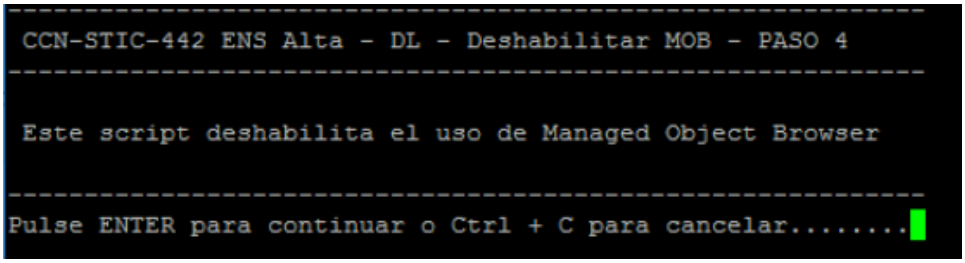
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>103.</td><td>Para establecer comunicaciones seguras entre el servidor de vCenter, y el servidor ESXi, se deberán generar y añadir certificados válidos emitidos y firmados por una entidad certificadora válida y confiable. El fichero CSR que se deberá generar deberá responder a las siguientes características:
<table>
<tr><th>Elemento</th><th>Valor</th></tr>
<tr><td>Tamaño de clave</td><td>2048 bits o más</td></tr>
<tr><td>Formato</td><td>PEM / clave pública en formato CRT</td></tr>
<tr><td>SubjectAltName -> DNS Name</td><td>=<FQDN de la máquina ESXi></td></tr>
<tr><td>Usos permitidos</td><td>Firma digital, no repudio, cifrado de clave</td></tr>
<tr><td>Momento de validez</td><td>Un día antes del tiempo de solicitud</td></tr>
<tr><td>CN (y SubjectAltName)</td><td>Nombre del Host o dirección IP (debe coincidir con el nombre con el que se ha registrado el servidor de ESXi)</td></tr>
</table>
Nota: No es objeto de esta guía especificar los métodos de emisión de los certificados.</td></tr>
<tr><td>104.</td><td>Una vez se disponga del fichero “.crt” firmado por la entidad certificadora autorizada y el fichero “.key” con la clave privada del certificado, se deberán renombrar a “rui.crt” y “rui.key” para posteriormente almacenarlos en la carpeta “Scripts” creada en pasos anteriores.</td></tr>
<tr><td>105.</td><td>Sitúese, de nuevo, sobre el objeto <FQDN del Servidor> y en la pestaña “Archivos”, seleccione y haga clic en el almacén donde alojará los Scripts de configuración de seguridad de la presente guía.
 
</td></tr>
<tr><td>106.</td><td>Pulse doble clic sobre la carpeta “Scripts” y seleccione “Cargar archivos”.
 
</td></tr>
</table>

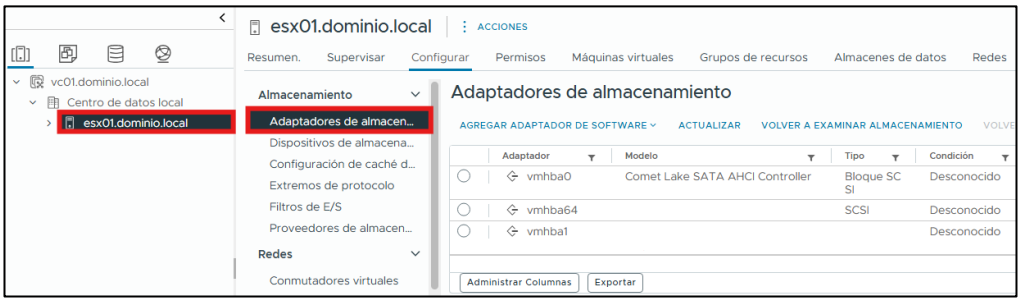
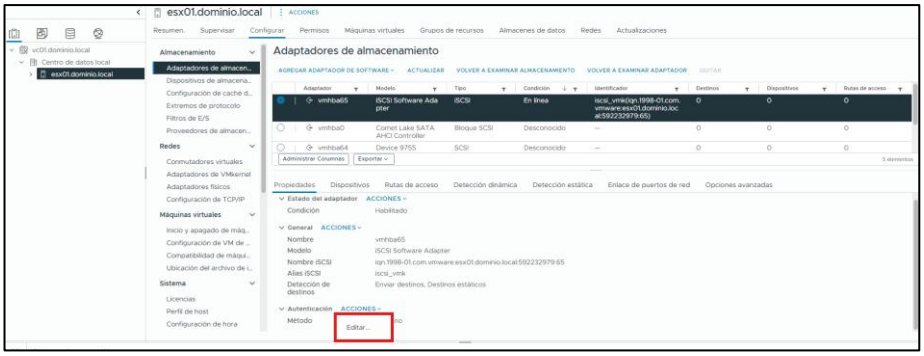
Paso	Descripción
107.	Localice los dos ficheros y cárguelos en el servidor seleccionándolos y pulsando “Abrir”.  **Nota:** No cierre el navegador y manténgalo en segundo plano mientras realiza los pasos siguientes.
108.	El siguiente paso consiste en configurar el servidor para que sincronice la hora con la del servidor NTP. De nuevo, a través del navegador, pulse sobre el icono correspondiente a “Hosts y clústeres”. 
109.	Sitúese sobre el objeto <FQDN del Servidor ESXi> y en la pestaña “Configurar”, seleccione “Configuración de hora”, “Protocolo de hora de red” y pulse “Editar”. 

Paso	Descripción
110.	Introduzca la dirección o direcciones IP del servidor o servidores NTP que quiera utilizar para la sincronización. Pulse “Aceptar” para guardar la configuración.  **Nota:** Deberá adaptar las configuraciones a las necesidades del entorno y, en caso de utilizar el protocolo NTP, se deberán habilitar las configuraciones que lo permitan. No cierre el navegador y manténgalo en segundo plano mientras realiza los pasos siguientes.
111.	Para los siguientes pasos, deberá conectarse al host a través de un cliente SSH. Se le solicitarán credenciales de acceso. Introduzca el usuario que configuró en el servidor de ESXi en los pasos iniciales del presente apartado.  **Nota:** para establecer una conexión SSH hacia el servidor ESXi, se deberá permitir el tráfico correspondiente. El cliente utiliza, por defecto, el puerto 22 para realizar la conexión. Deberá adaptar estos pasos a las necesidades de su entorno. Al no estar utilizando certificados confiables, es posible que el cliente SSH muestra una advertencia. Puede continuar la conexión.
112.	Introduzca la contraseña definida para dicho usuario. 
113.	Acceda a la ruta del almacén de datos que ha configurado en los pasos anteriores a través de la siguiente línea de comandos: **# cd /vmfs/volumes/<almacén de datos>/Scripts**  **Nota:** La ruta seleccionada es la ruta en la que se almacenan por defecto los almacenes de datos. Deberá adaptar estos pasos a las necesidades de su entorno.

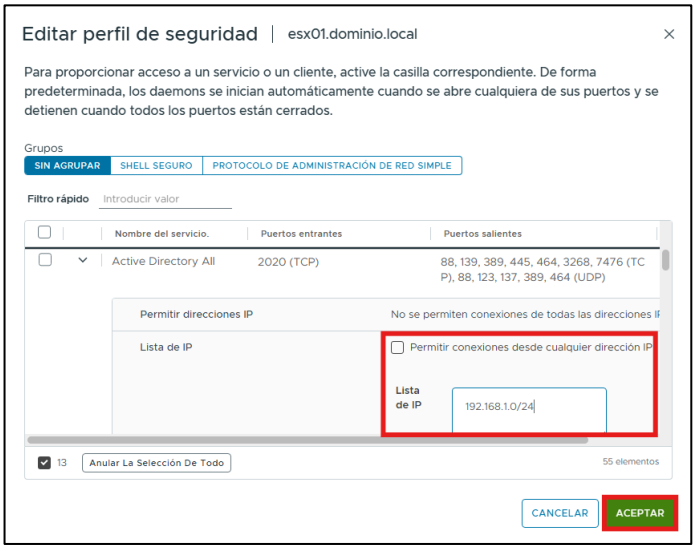
Paso	Descripción
114.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_1_Importacion_de_Certificados.sh" mediante el siguiente comando y pulse "Enter" para continuar: **# sh CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_1_Importacion_de_Certificados.sh** 
115.	Pulse "Enter", de nuevo, para continuar. 
116.	El sistema le solicitará el nombre del almacén de datos donde se encuentra la carpeta Scripts. Introduzca el nombre del almacén respetando mayúsculas, minúsculas, puntuación, espacios, etc. y pulse "Enter" para continuar.  **Nota:** En el ejemplo, el almacén de datos se llama "datastore1". Este script asume que la ruta donde se encuentran los ficheros de origen es "/vmfs/volumes/<nombre de almacén de datos>/Scripts" y los ficheros de destino en "/etc/vmware/ssl/". En caso de que las rutas sean distintas se deberá modificar en el script.

Paso	Descripción
117.	En este momento y si fuera posible, sería recomendable aplicar las actualizaciones sobre el servidor de ESXi. Para llevar a cabo esta acción y teniendo en cuenta que el entorno puede o no disponer de conectividad a internet, se puede hacer uso de un repositorio centralizado por medio de vSphere Update Manager, un plugin que puede ser añadido a la configuración de vCenter Server. **Nota:** Una vez las actualizaciones son accesibles, los comandos a utilizar, a través del CLI de ESXi, serían los siguientes: - **# esxcli software profile get** (para consultar el estado de las actualizaciones) - **# esxcli software vib get** (para consultar el estado de las actualizaciones) - **# esxcli software profile update** (para aplicar las actualizaciones) - **# esxcli software vib update** (para aplicar las actualizaciones) Recuerde que para poder ejecutar estos comandos deberá realizarlos desde la consola directa o activando el acceso SSH. En caso de haber aplicado las configuraciones de la guía, adicionalmente deberá pertenecer al grupo de excepciones en el modo de bloqueo o rebajar el nivel de bloqueo temporalmente siguiendo los pasos inversos a los descritos. **Nota:** No cierre la sesión SSH y manténgala en segundo plano mientras realiza los pasos siguientes.
118.	A continuación, se modificarán los parámetros relativos a los registros de auditoría o ficheros log. Para ello, deberá utilizar de nuevo la sesión SSH que activó para realizar los pasos anteriores. Ejecute el script "CCN-STIC-442_ENS_Categoria_Alta_DL _Paso_2_Configuracion_de_Logs.sh" mediante el siguiente comando y pulse "Enter". **# sh CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_2_Configuracion_de_Logs.sh** 
119.	Pulse "Enter", de nuevo, para continuar. 
120.	El sistema le solicitará el nombre del almacén de datos donde se encuentra la carpeta Scripts. Introduzca el nombre del almacén respetando mayúsculas, minúsculas, puntuación, espacios, etc. Pulse "Enter" para continuar.  **Nota:** En el ejemplo, el almacén de datos se llama "datastore1".

Paso	Descripción
121.	Es recomendable también el uso de un servidor de logs externo al que se exporten los logs del servidor. Para establecer dicha configuración, a través del vSphere Client, puede situarse en el servidor ESXi y seleccionar "Configuración → Configuración avanzada". Los campos a modificar son los siguientes: – "Syslog.global.logHost" → "<Nombre del Host>". – "Syslog.global.logDirUnique" → "True".
122.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_3_Deshabilitar_SNMP.sh" mediante el siguiente comando y pulse "Enter" para continuar. **# sh CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_3_Deshabilitar_SNMP.sh**  **Nota:** En caso de que se haga uso del protocolo SNMP, no se debería ejecutar este paso. En su lugar, se debería ejecutar lo siguiente para establecer la seguridad adecuada en el uso del protocolo y evitar que elementos externos puedan extraer información de datos SNMP: - **# esxcli conn_options system snmp set --communities [COMMUNITY]** - **# esxcli conn_options system snmp set --targets [TARGET]@[PORT]/[COMMUNITY]** - **# esxcli conn_options system snmp set --enable true**
123.	Pulse "Enter", de nuevo, para continuar. El Script indicará que ha finalizado. 
124.	Ejecute el script "CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_4_Deshabilitar_MOB.sh" mediante el comando siguiente y pulse "Enter" para continuar. **# sh CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_4_Deshabilitar_MOB.sh** 
125.	Pulse "Enter", de nuevo, para continuar. El Script indicará que ha finalizado.  **Nota:** No cierre la sesión SSH y manténgala en segundo plano mientras realiza los pasos siguientes.

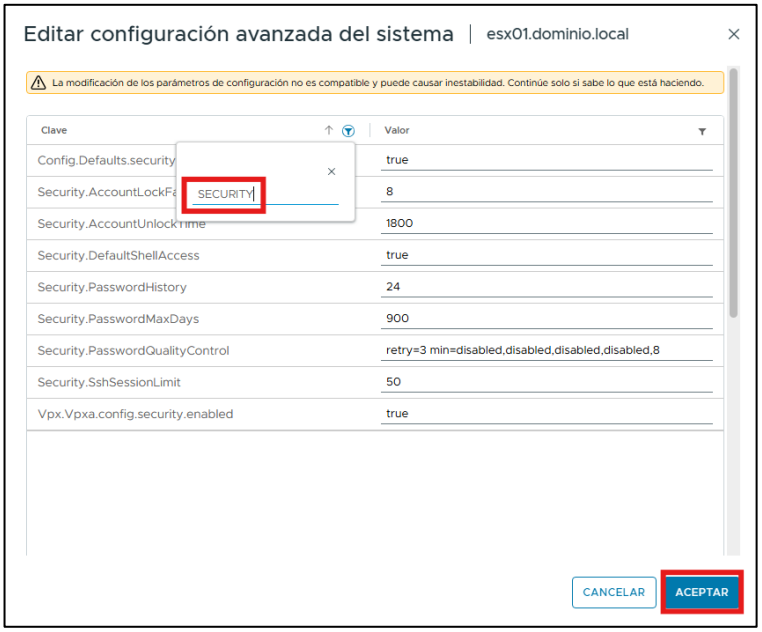
Paso	Descripción
126.	Todos los adaptadores y servidores de destino iSCSI deberán ser configurados con autenticación CHAP para asegurar la conexión. De nuevo, a través del navegador, pulse sobre el icono correspondiente a “Hosts y clústeres”. 
127.	Pulse sobre el objeto del menú de la izquierda “<FQDN de servidor ESXi>” y en la pestaña “Configuración” seleccione “Adaptadores de almacenamiento”. 
128.	Pulse sobre el adaptador o adaptadores iSCSI mediante el cual se entrega el almacenamiento para el host ESXi. Diríjase ahora a la pestaña “Propiedades” y en el apartado “Autenticación” pulse sobre “Editar”. 

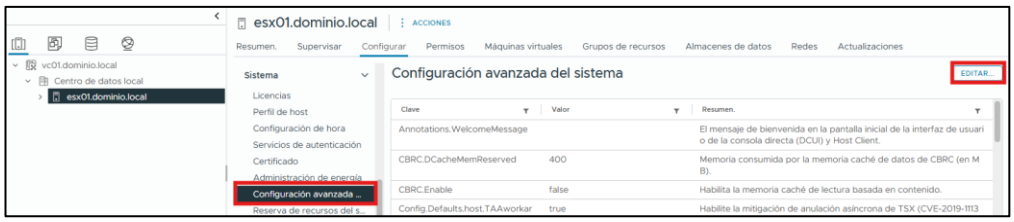
Paso	Descripción
129.	Seleccione, en el menú contextual que se despliega al pulsar sobre el campo “Método de autenticación”, la opción “Usar CHAP bidireccional”. Establezca “Nombre” y “Secreto” para las credenciales CHAP salientes y entrantes. Una vez establecidos los parámetros pulse “Aceptar”.  **Nota:** Puede marcar “Usar nombre del iniciador” para establecer como nombre el iniciador iSCSI que se ha generado al crear el adaptador. Tenga en cuenta que el nombre no puede exceder los 255 caracteres y que el secreto no puede exceder los 100 caracteres (el secreto CHAP saliente no debe coincidir con el secreto CHAP entrante).
130.	A continuación, modifique el estado del cortafuegos del ESXi para que limite el tráfico a la red o redes específicas del entorno. Para ello, en la pestaña “Configurar”, seleccione “Firewall” y pulse sobre “Editar”. 

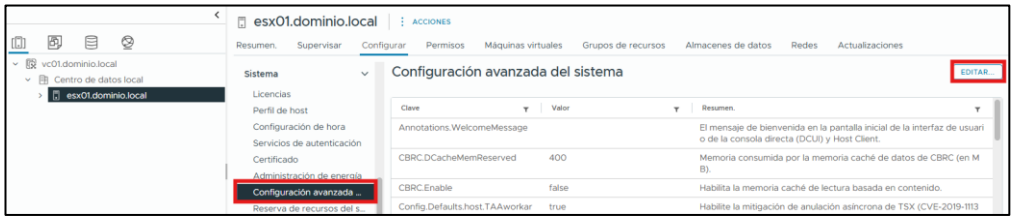
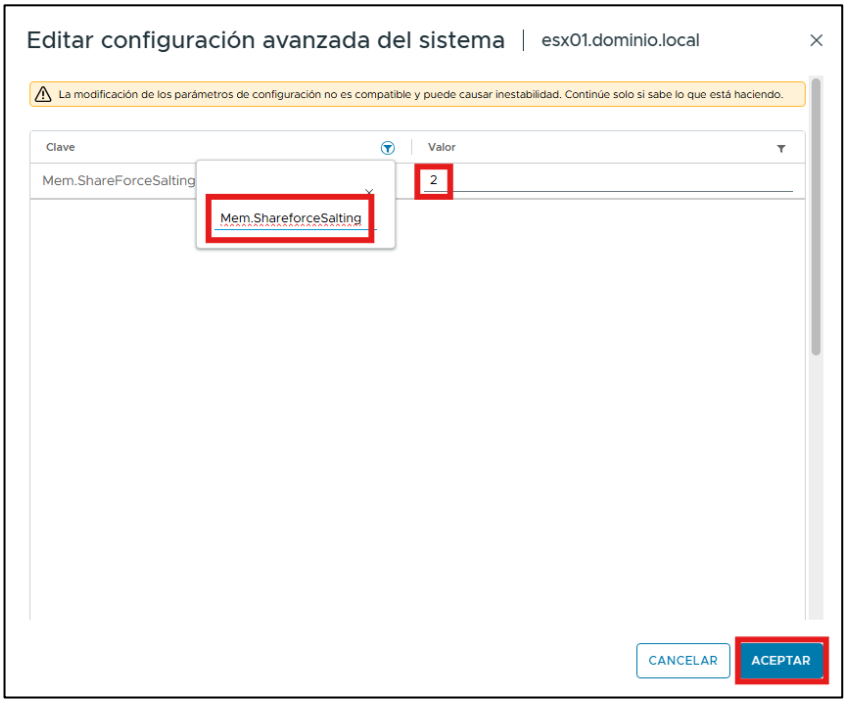
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>131.</td><td>Modifique cada uno de los parámetros siguientes y desmarque “Permitir conexiones desde cualquier dirección IP” para, a continuación, añadir la red o redes (separadas por comas) en las que se permitirá la comunicación. Pulse “Aceptar”.
<table>
<tr><th colspan="2">Protocolos</th></tr>
<tr><td>SSH server</td><td>Active Directory All</td></tr>
<tr><td>CIM SLP</td><td>DHCP client</td></tr>
<tr><td>DNS client</td><td>DVSsync</td></tr>
<tr><td>Fault tolerance</td><td>HBR</td></tr>
<tr><td>Iofiltervp</td><td>NFC</td></tr>
<tr><td>NTP client</td><td>Rabbitmqproxy</td></tr>
<tr><td>Software iSCSI client</td><td>vCenter Update Manager</td></tr>
<tr><td>vMotion</td><td>VMware vCenter agent</td></tr>
<tr><td>vSphere Web Access</td><td>vSphere Web client</td></tr>
</table>


Nota: En caso de instalar y utilizar más servicios, del mismo modo, estos tendrán que ser modificados. Deberá adaptar esta configuración a las necesidades del entorno.</td></tr>
<tr><td>132.</td><td>En este momento se definirán los criterios relativos a complejidad y comportamiento de contraseñas. Para configurar estos parámetros diríjase a “Configurar → Configuración avanzada” y pulse “Editar”.

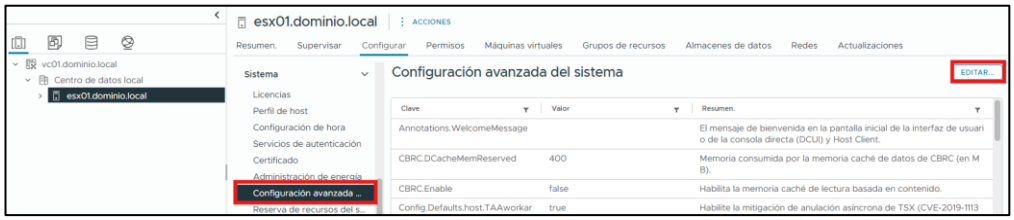
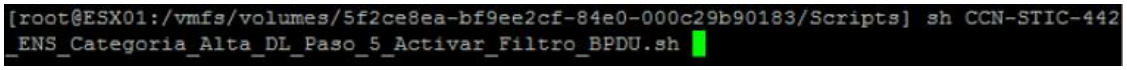
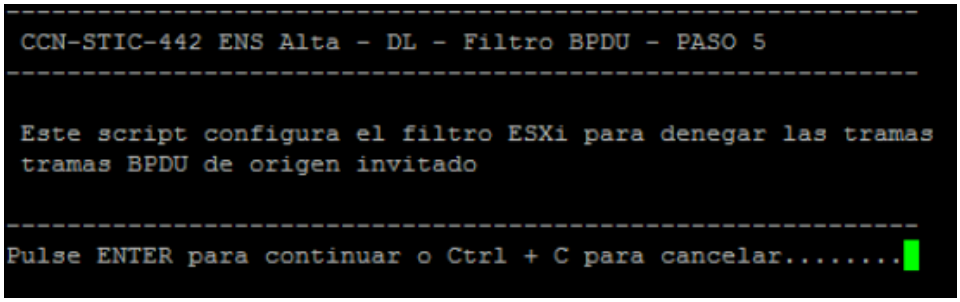
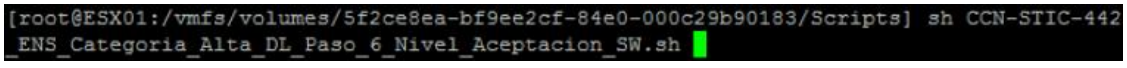
</td></tr>
</table>

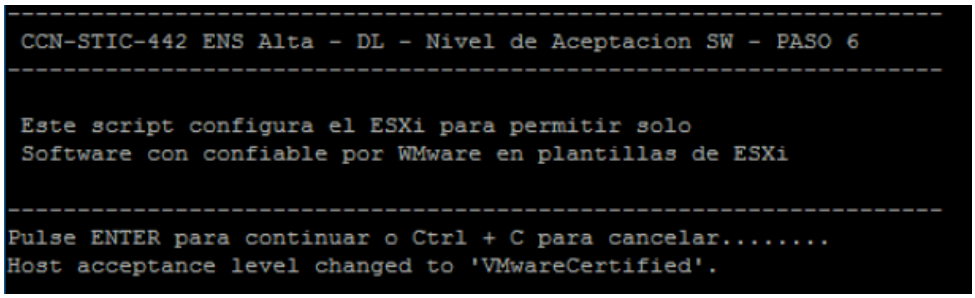
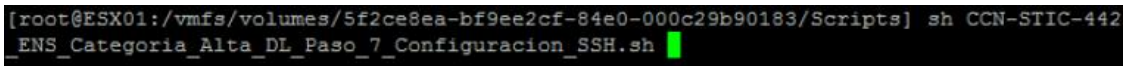
<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>133.</td><td>Introduzca en el filtro “Security” los objetos definidos a continuación y establezca los valores adecuados:
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Security.Account.LockFailures</td><td>8</td></tr>
<tr><td>Security.Account.UnlockTime</td><td>3600</td></tr>
<tr><td>Security.PasswordHistory</td><td>24</td></tr>
<tr><td>Security.PasswordMaxDays</td><td>60</td></tr>
<tr><td>Security.PasswordQualitycontrol</td><td>retry=3 min=disabled,disabled,disabled, disabled,14</td></tr>
</table>
Pulse “Aceptar” para continuar.


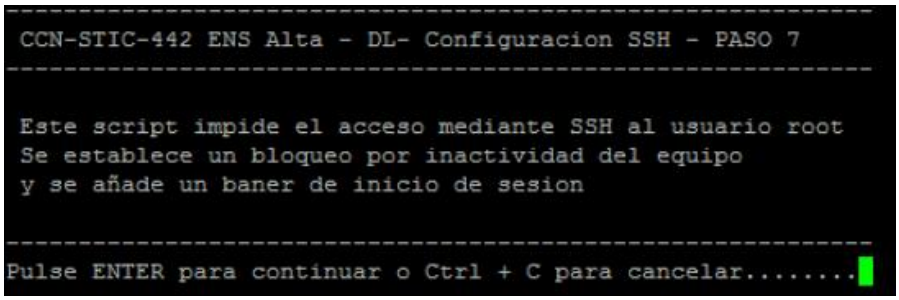
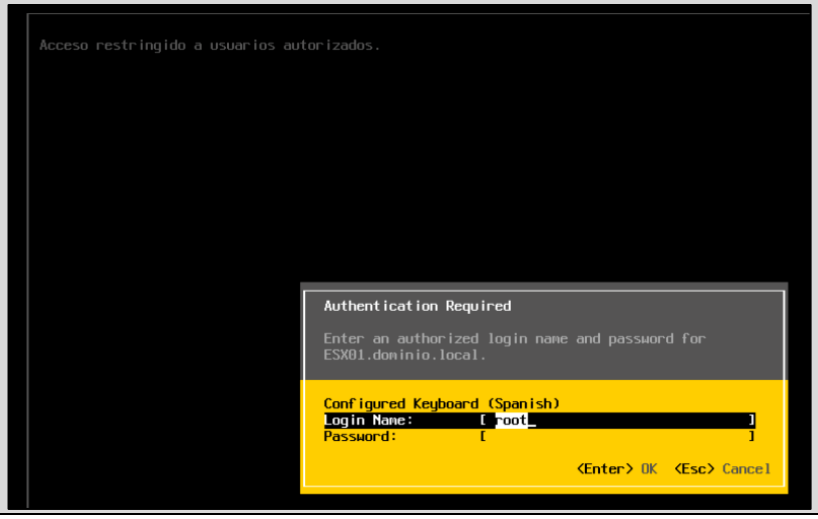
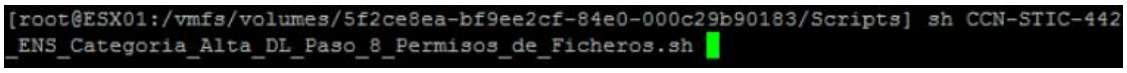
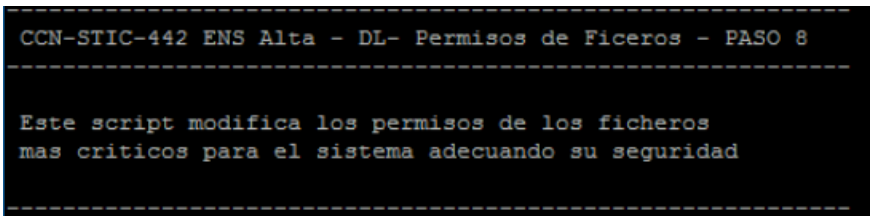
Nota: En caso de necesitar desbloquear, antes del tiempo definido, una cuenta que ha superado los intentos de introducción de contraseña, se puede hacer uso del comando siguiente a través de la consola ESXi Shell:
- # pam_tally –user <Usuario bloqueado> --reset</td></tr>
<tr><td>134.</td><td>A continuación, se va a deshabilitar el servicio que permite hacer uso de los puertos USB del servidor ESXi. Pulse sobre “Editar” de nuevo.

</td></tr>
</table>

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>135.</td><td>Introduzca en el filtro “Misc.Usb” y establezca el valor deseado. Pulse “Aceptar” para continuar.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Misc.UsbArbitratorAutostartDisabled</td><td>1</td></tr>
</table>
Nota: Para hacer uso de los puertos USB del ESXi se deberá iniciar manualmente el servicio mediante el siguiente comando (a través de SSH a la consola ESXi Shell):
- # /etc/init.d/usbarbitrator start
Una vez utilizado y para detener de nuevo el servicio, se puede ejecutar lo siguiente:
- # /etc/init.d/usbarbitrator stop</td></tr>
<tr><td>136.</td><td>Pulse sobre “Editar” de nuevo.
 
</td></tr>
<tr><td>137.</td><td>Introduzca en el filtro “Mem.ShareforceShalting” y establezca el valor en “2”. Pulse “Aceptar” para continuar.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>Mem.ShareforceShalting</td><td>2</td></tr>
</table>


Nota: No cierre el navegador y manténgalo en segundo plano mientras realiza los pasos siguientes.</td></tr>
</table>

<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>138.</td><td>Pulse sobre “Editar” de nuevo.
 
</td></tr>
<tr><td>139.</td><td>Introduzca en el filtro “welcome” y establezca el mensaje que quiere que aparezca en las conexiones directas al host a través de la consola o de vSphere.
<table>
<tr><th>Nombre</th><th>Valor</th></tr>
<tr><td>Annotations.WelcomeMessage</td><td>“Mensaje de seguridad que se adapte a las necesidades de la organización”</td></tr>
<tr><td>UserVars.HostClientWelcomeMessage</td><td>“Mensaje de seguridad que se adapte a las necesidades de la organización”</td></tr>
</table></td></tr>
<tr><td>140.</td><td>Deberá utilizar de nuevo la sesión SSH que activó anteriormente para realizar los pasos que se indican a continuación. Ejecute el script “CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_5_Activar_Filtro_BPDU.sh” mediante el siguiente comando y pulse “Enter”.
sh CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_5_Activar_Filtro_BPDU.sh
 
</td></tr>
<tr><td>141.</td><td>Pulse “Enter”, de nuevo, para continuar. El Script indicará que ha finalizado.
 
</td></tr>
<tr><td>142.</td><td>Ejecute el script “CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_6_Nivel_Aceptacion_SW.sh” mediante el siguiente comando y pulse “Enter”.
sh CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_6_Nivel_Aceptacion_SW.sh
 
</td></tr>
</table>

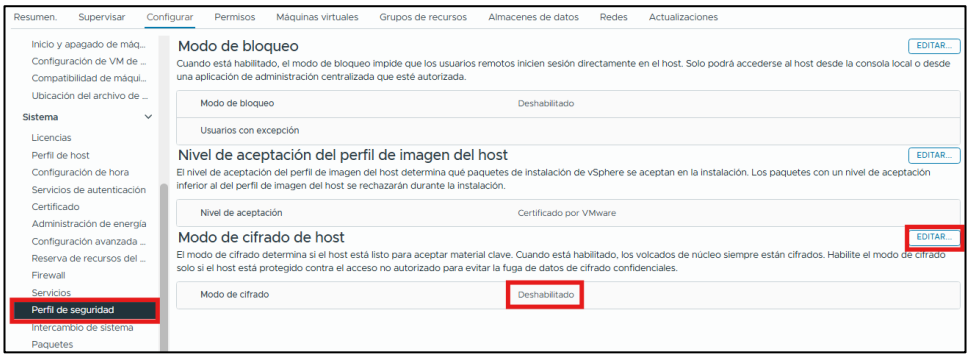
Paso	Descripción
143.	Pulse “Enter”, de nuevo, para continuar. El Script indicará que ha finalizado. 
144.	Ejecute el script “CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_7_Configuracion_SSH.sh” mediante el siguiente comando y pulse “Enter”. **# sh CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_7_Configuracion_SSH.sh**  **Nota:** Antes de realizar este paso, es necesario disponer de una o varias cuentas con acceso a la consola ESXi Shell y que dispongan de los privilegios administrativos adecuados. El script establecerá el mensaje de entrada tanto por consola directa como por consola SSH. El mensaje es el siguiente “Acceso restringido a usuarios autorizados.”. En caso de ser necesario, modifique el script y adapte el mensaje a las necesidades del entorno.

Paso	Descripción
145.	Pulse, de nuevo, “Enter” para continuar. El sistema indicará que el Script ha finalizado.  **Nota:** A partir de este momento, al tratar de entrar en la configuración directamente a través del servidor ESXi, solamente aparecerá el mensaje de seguridad que se haya introducido en el script (por defecto “Acceso restringido a usuarios autorizados.”). Aunque no aparezca la opción de pulsar “F2” para iniciar la conexión continúa siendo posible para los usuarios a los que se les haya permitido el acceso de este modo. 
146.	Ejecute el script “CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_8_Permisos_de_Ficheros.sh” mediante el siguiente comando y pulse “Enter”. **# sh CCN-STIC-442_ENS_Categoria_Alta_DL_Paso_8_Permisos_de_Ficheros.sh** 
147.	Pulse “Enter” para continuar. El Script indicará que ha finalizado. 
148.	A continuación, cierre la sesión SSH abierta contra el servidor ESXi.

2.3.1. ACTIVAR USO DE CIFRADO EN HOST ESXI

Si bien es cierto que es posible que el resto de las medidas de seguridad inherentes a un escenario de red clasificada probablemente haga innecesario el empleo de la posibilidad de cifrar los discos duros virtuales de las máquinas, existe un mecanismo específico proporcionado por VMware vSphere 8.x que posibilita el cifrado de aquellas máquinas virtuales en las que sea de necesidad cifrar la información que contienen.

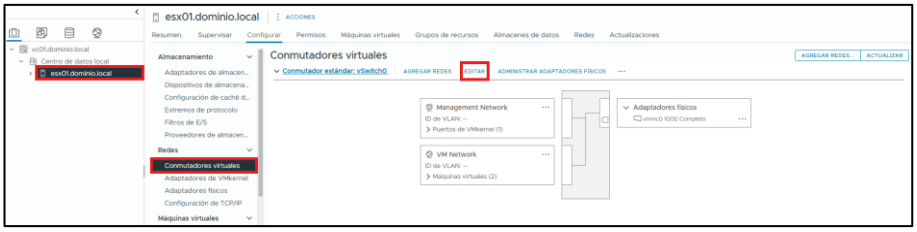
Para hacer uso del servicio de virtualización será necesario activar el modo cifrado en el servidor host ESXI.

Paso	Descripción
149.	En el menú de la izquierda, seleccione el icono correspondiente a “Hosts y clústeres”. 
150.	Pulse sobre el objeto <FQDN del servidor ESXi> y seleccione, en la pestaña “Configurar”, la opción “Perfil de seguridad” y establezca como “Habilitado ”·el “Modo de cifrado del host” por medio del botón “Editar…”. 

2.3.2. CONFIGURACIÓN EN CONMUTADORES VIRTUALES ESTÁNDAR

Las configuraciones descritas a continuación son a nivel de conmutadores estándar. Por tanto, es necesario aplicar estas configuraciones de seguridad a todos los conmutadores estándar de cada uno de los hosts ESXi existentes en el servicio de vCenter.

Paso	Descripción
151.	En el menú de la izquierda, seleccione el icono correspondiente a “Hosts y clústeres”. 

Paso	Descripción
152.	En el menú de la izquierda, sitúese sobre el objeto “<FQDN del servidor ESXi>” y, en la pestaña “Configurar”, seleccione “Conmutadores virtuales”. Pulse “Editar” sobre cada conmutador virtual. 
153.	En la ventana emergente, pulse sobre “Seguridad” y compruebe el estado de los siguientes parámetros de seguridad (deberán tener el valor “Rechazar”): – Modo promiscuo – Cambios de dirección MAC – Transmisiones falsificadas 

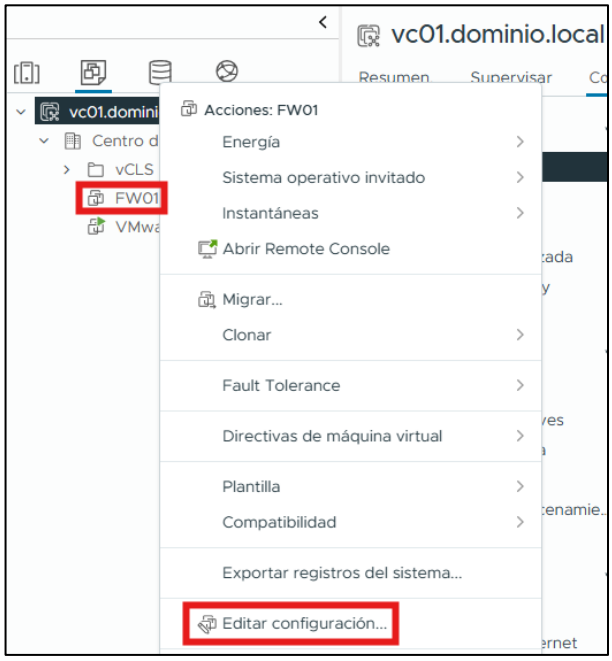
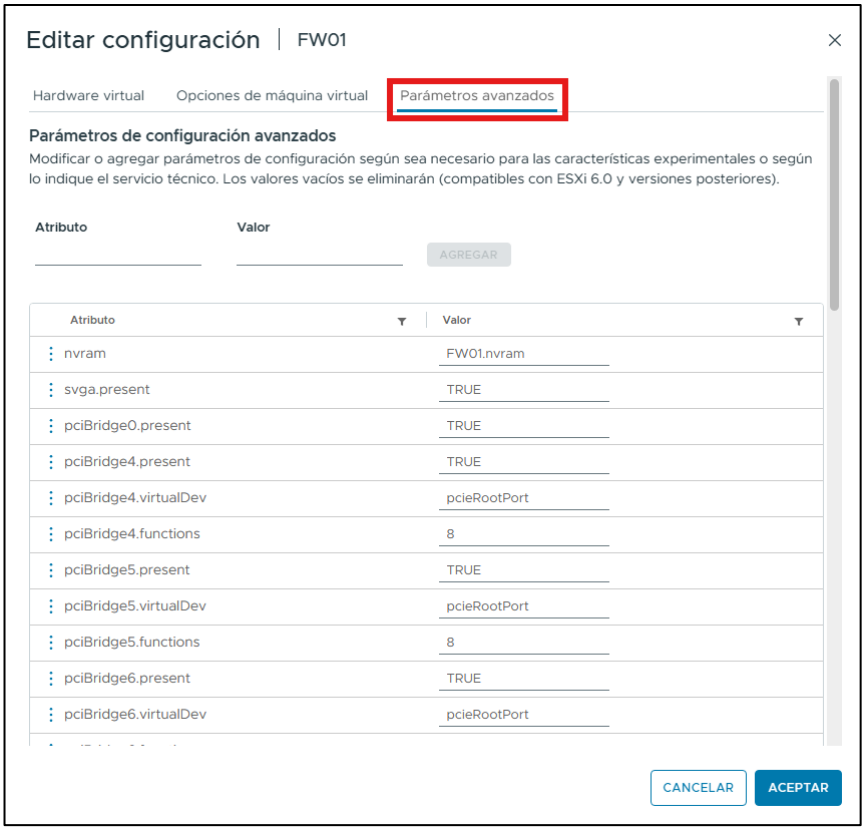
Paso	Descripción
154.	Modifique los parámetros al valor “Rechazar” y pulse “ACEPTAR” para validar la configuración. 

2.3.3. CONFIGURACIÓN EN MÁQUINAS VIRTUALES

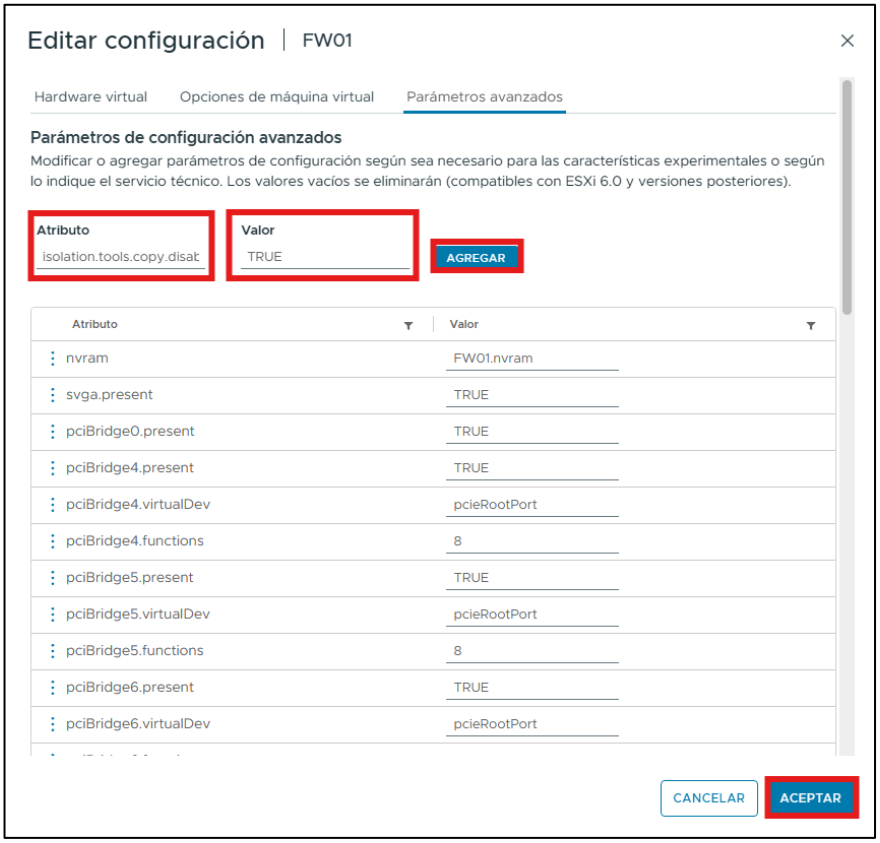
Las configuraciones descritas a continuación son a nivel de máquina virtual. Por tanto, es necesario aplicar estas configuraciones de seguridad a todas las máquinas virtuales que se unan al host de ESXi que se está implementando.

Nota: Existe la posibilidad de convertir las máquinas virtuales configuradas en plantillas, de modo que se utilicen para generar nuevas máquinas, homogeneizando y simplificando las tareas administrativas.

Paso	Descripción
155.	En el menú de la izquierda, pulse el icono correspondiente a “Máquinas virtuales y plantillas”. 

Paso	Descripción
156.	Asegúrese de que la máquina virtual esté apagada. Luego, sitúese sobre la máquina virtual sobre la que va a establecer las configuraciones de seguridad y pulse el botón derecho del ratón para seleccionar “Editar configuración…”. 
157.	Diríjase a la pestaña “Parámetros avanzados”. 

Paso	Descripción
158.	En el campo “Atributo” introduzca “isolation.tools.copy.disable” y en el campo “Valor” introduzca “True”. Pulse “Agregar” y “Aceptar” para guardar los cambios.

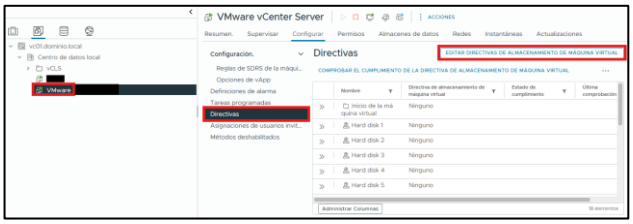
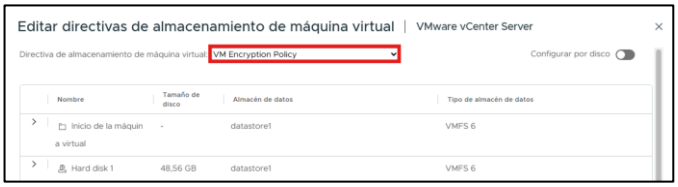


<table>
<tr><th>Paso</th><th>Descripción</th></tr>
<tr><td>159.</td><td>Repita estos últimos pasos para añadir cada uno de los siguientes parámetros de configuración. Una vez haya introducido todos los parámetros, pulse “Aceptar” para continuar.
<table>
<tr><th>Directiva</th><th>Valor</th></tr>
<tr><td>isolation.tools.paste.disable</td><td>True</td></tr>
<tr><td>isolation.tools.setGUIOptions.enable</td><td>False</td></tr>
<tr><td>isolation.tools.diskShrink.disable</td><td>True</td></tr>
<tr><td>isolation.tools.diskWiper.disable</td><td>True</td></tr>
<tr><td>isolation.tools.connectable.disable</td><td>True</td></tr>
<tr><td>isolation.device.edit.disable</td><td>True</td></tr>
<tr><td>isolation.tools.setOption.disable</td><td>True</td></tr>
<tr><td>scsiX:Y.mode</td><td>Persistent</td></tr>
<tr><td>mks.enable3d</td><td>False</td></tr>
<tr><td>floppyX.present</td><td>False</td></tr>
<tr><td>parallelX.present</td><td>False</td></tr>
<tr><td>serialX.present</td><td>False</td></tr>
<tr><td>svga.vgaOnly</td><td>True</td></tr>
<tr><td>tools.setInfo.sizeLimit</td><td>1048576</td></tr>
<tr><td>RemoteDisplay.vnc.enabled</td><td>False</td></tr>
<tr><td>tools.guestlib.enableHostInfo</td><td>False</td></tr>
<tr><td>sched.mem.pshare.salt</td><td>Null</td></tr>
<tr><td>ethernetX.filterX. name = filtername</td><td>Null</td></tr>
<tr><td>pciPassthru*.present</td><td>False</td></tr>
<tr><td>Net.BlockGuestBPDU</td><td>1</td></tr>
</table>
Nota: Deberá adaptar la configuración a las necesidades del entorno.</td></tr>
</table>

2.3.3.1. CIFRADO DE DISCOS EN MÁQUINAS VIRTUALES

Si bien es cierto que es posible que el resto de las medidas de seguridad inherentes a un escenario de red clasificada probablemente haga innecesario el empleo de la posibilidad de cifrar los discos duros virtuales de las máquinas, existe un mecanismo específico proporcionado por VMware vSphere 8.x que posibilita el cifrado de aquellas máquinas virtuales en las que sea de necesidad cifrar la información que contienen.

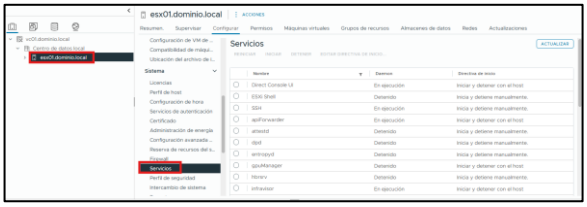
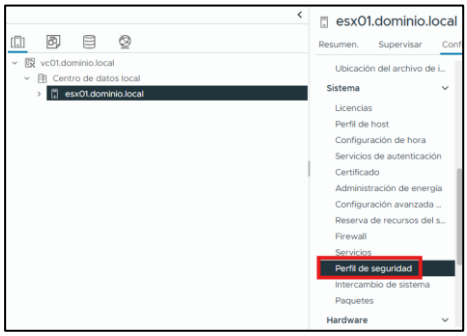
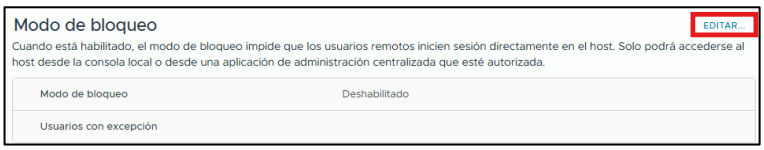
Paso	Descripción
160.	En el menú de la izquierda, pulse el icono correspondiente a “Máquinas virtuales y plantillas”. 

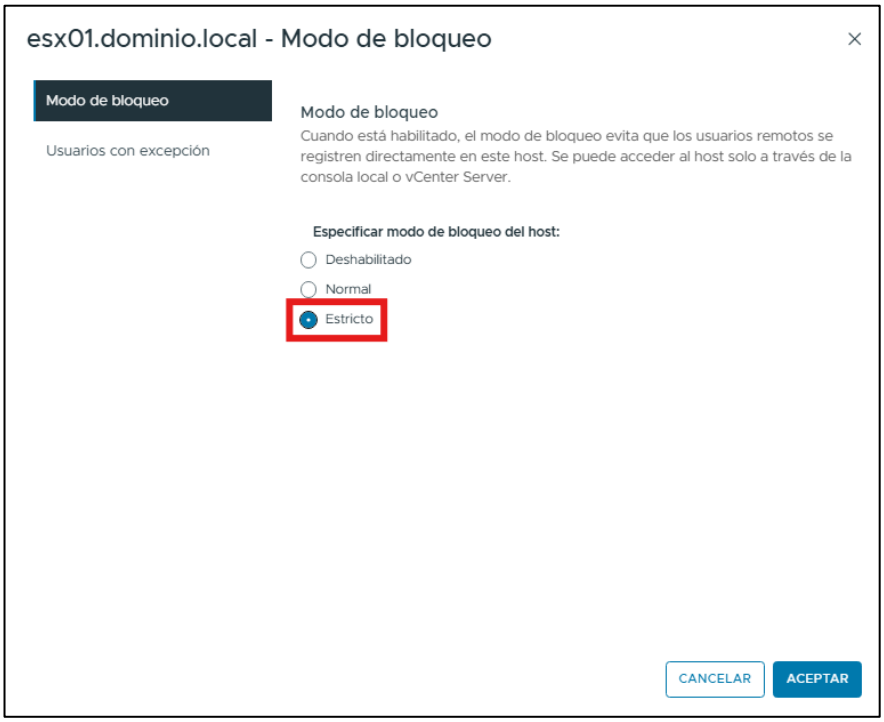
Paso	Descripción
161.	Seleccione la máquina virtual y pulse sobre “Directivas”. Seguidamente pulse sobre “Editar directivas de almacenamiento de máquina”.  **Nota:** La máquina virtual debe estar apagada.
162.	Si quiere cifrar todo el almacenamiento de la máquina virtual, sustituya la opción “Valor predeterminado de almacén de datos” por la directiva de cifrado que creó o configuró en el servidor de vCenter en el apartado “2.1 CONFIGURACIÓN DE SERVIDOR KMS” de la presente guía. Para ello seleccione la directiva a través del menú desplegable y pulse “Aceptar”.  **Nota:** En caso de querer cifrar solo alguno de los discos de la máquina virtual y no la totalidad, puede marcar la opción “Configurar por disco” y se podrá establecer la política de forma individual en cada almacén virtual. 

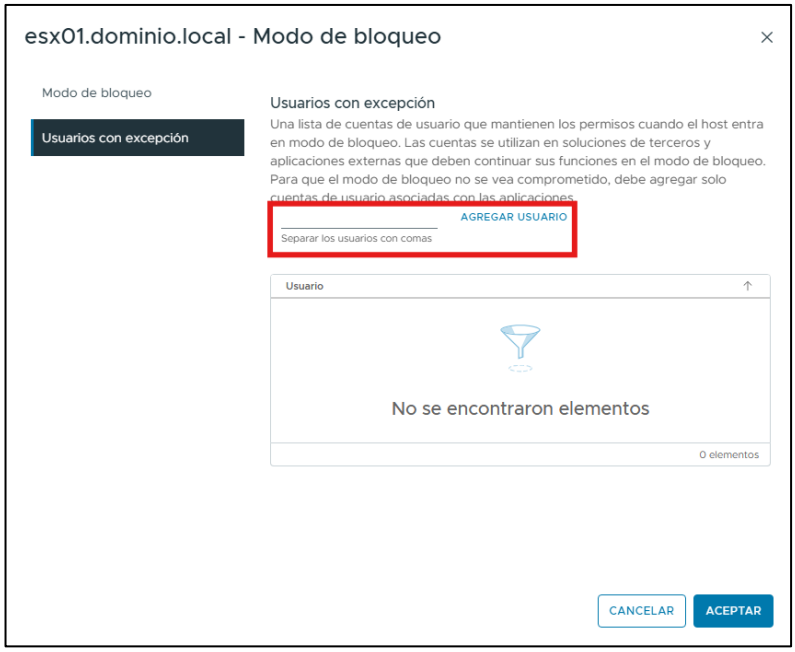
2.3.4. CONFIGURACIÓN DE ESX SHELL Y SSH

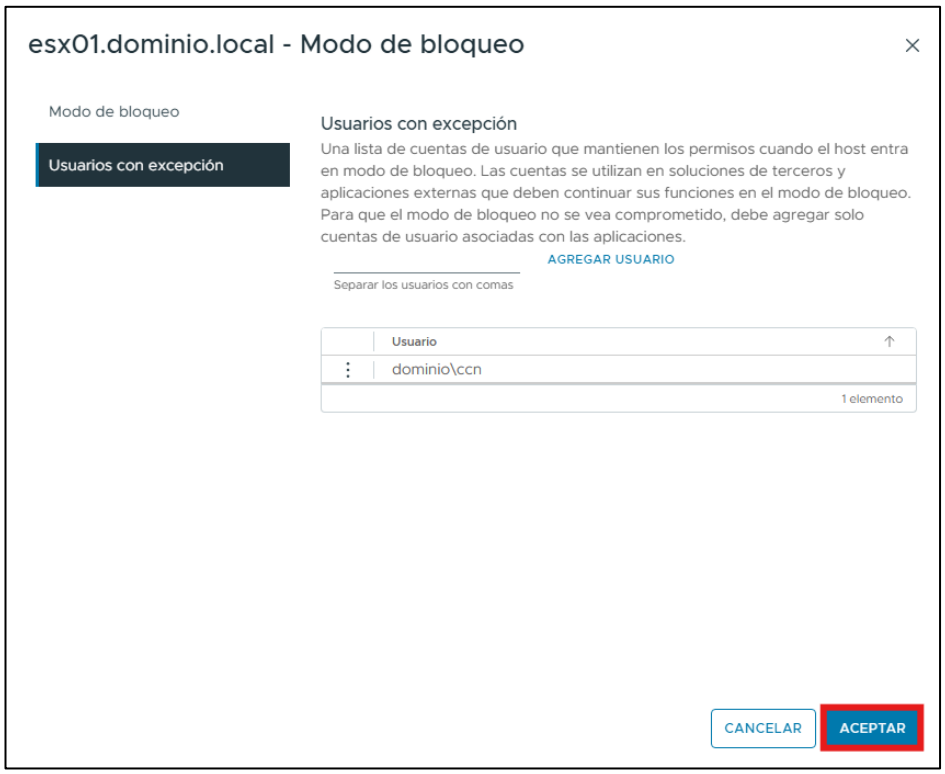
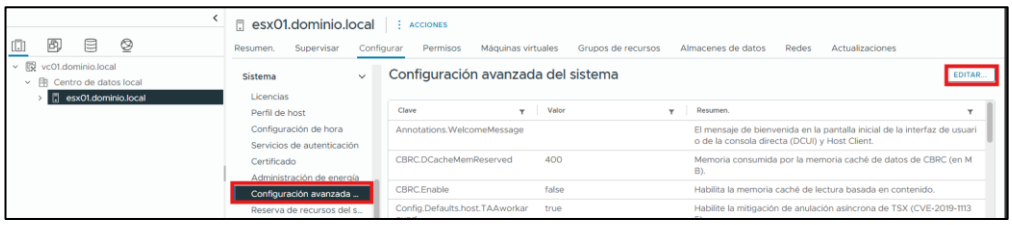
Por último, en el host ESXi, se deshabilitará SSH y la consola ESXi Shell. Así mismo, se activará el modo de bloqueo estricto. A partir de este momento, la administración del host solamente será a través del servidor de vCenter al que haya sido añadido. Se recomienda mantener la configuración de este modo salvo necesidad para resolución de problemas.

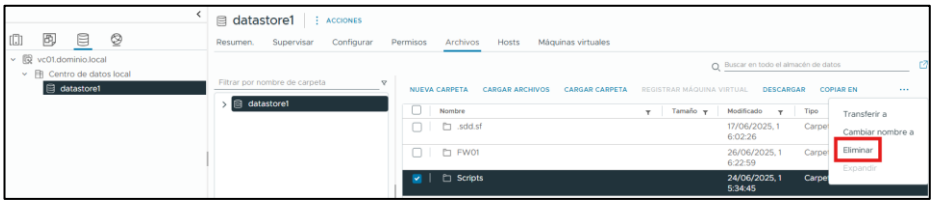
Paso	Descripción
163.	En el navegador, pulse sobre el icono que corresponde a “Hosts y clústeres”. 

Paso	Descripción
164.	En el menú de la izquierda, sitúese sobre el objeto “<FQDN del servidor ESXi>” y pulse sobre “Servicios”. 
165.	Seleccione el servicio “ESX Shell” y pulse “Detener”. 
166.	Realice la misma operación con el servicio “SSH”. 
167.	Defina el modo de bloqueo para el acceso a este host en modo “Estricto” para que solo se pueda acceder al host de ESXi a través de servidores vCenter y no a través de clientes vSphere por conexión directa al host o a través de la consola local. Para ello, sitúese de nuevo sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar”, seleccione “Perfil de seguridad”.  **Nota:** El modo de bloqueo solamente se deberá desactivar, del mismo modo que solo se deberán activar la consola ESXi Shell y SSH, cuando se realicen tareas de resolución de problemas que no puedan ser solucionadas a través del servicio de vCenter.
168.	En “Modo de Bloqueo” seleccione “Editar”. 

Paso	Descripción
169.	En la ventana emergente, seleccione el modo “Estricto”. 

Paso	Descripción
170.	En caso de que existan configuraciones y aplicativos que requieran conexión directa hacia el host, se deberán añadir sus usuarios al grupo de excepción para el modo estricto. Seleccione “Usuarios con excepción” , añada los usuarios que deberán tener acceso local al servidor ESXi, separados por “;” y pulse “AGREGAR USUARIO”.  **Nota:** a los usuarios que pertenecen a este grupo de excepción, se les permitirá traspasar el modo de bloqueo y acceder directamente al host. Estos usuarios no deben ser usuarios físicos, sino que deben ser usuarios automáticos que pertenezcan a procesos y aplicaciones. Así mismo, deberán ser auditados periódicamente pudiendo ser consultados mediante los pasos expuestos a continuación.

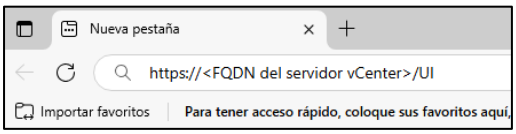
Paso	Descripción
171.	Los usuarios añadidos aparecerán en la lista. Pulse “ACEPTAR” para cerrar la ventana emergente.  **Nota:** En este paso se ha utilizado un usuario a modo ejemplo, adapte dicho paso a las necesidades de su organización. No se deben añadir a esta lista usuarios que no pertenezcan a aplicaciones o procesos automáticos que necesiten traspasar el modo de bloqueo.
172.	Así mismo, se deberán configurar también los usuarios físicos que podrán tener acceso a la infraestructura incluso cuando el modo de bloqueo está activado. Si esta configuración no contuviera ningún usuario, es posible que se pierda el control del ESXi completamente, no pudiendo volver a ser accesible. Para realizar la configuración, deberá acceder a “Configurar → Configuración avanzada” y pulsar sobre “Editar”. 
173.	Añada, en el filtro, “DCUI” e introduzca los parámetros deseados añadiendo los usuarios (separados por coma) que podrán acceder por consola directa y el tiempo de bloqueo ante inactividad. Pulse “Aceptar” para continuar. **Nota:** Para cumplir con lo definido en la categoría alta del ENS, el tiempo de inactividad deberá ser establecido en 600. VMware desaconseja eliminar al usuario ROOT de esta lista.

Paso	Descripción
174.	Pulse ahora sobre el icono correspondiente a “Almacenamiento”. 
175.	Sitúese sobre el almacén de datos donde alojó la carpeta “Scripts” y seleccione la pestaña “Archivos”. 
176.	Pulse sobre la carpeta “Scripts” y seleccione “Eliminar”. 
177.	Pulse “Sí” para confirmar la eliminación. 

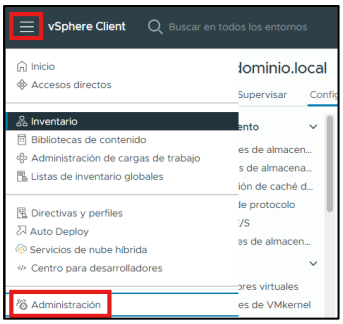
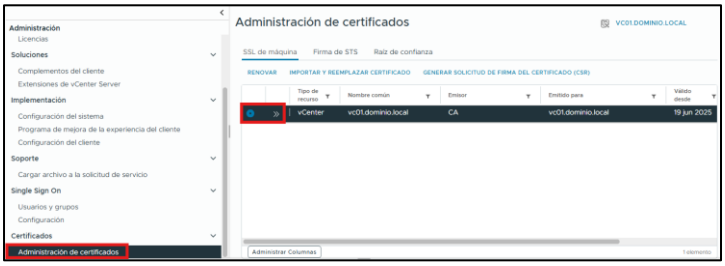
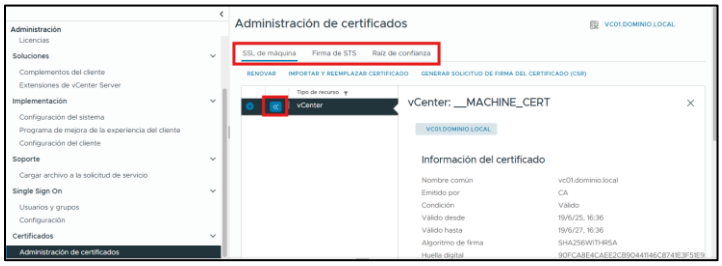
ANEXO A.4.2. LISTA DE COMPROBACIÓN DE IMPLEMENTACIÓN DE SEGURIDAD DE CATEGORÍA ALTA / DIFUSIÓN LIMITADA DEL ENS PARA VSPHERE 8.X

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores que pertenecen a la infraestructura de VMware vSphere 8.x con implementación de seguridad de categoría ALTA / DIFUSIÓN LIMITADA del ENS.

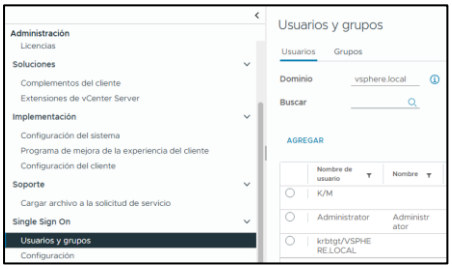
1. SERVIDORES VCENTER

Comprobación	OK/NOK	Como hacerlo
1. Acceso al servidor de vCenter.		Inicie sesión directamente en el host ESXi utilizando el ESXi Host Client a través de su navegador web. Para ello, introduzca la siguiente URL: “ https://<IP-o-FQDN-del-host-ESXi>/UI”. 

Comprobación	OK/NOK	Como hacerlo
		Introduzca credenciales válidas y con los privilegios adecuados para acceder al entorno de vCenter, pulse sobre las condiciones de acceso y pulse sobre “Iniciar”. 

Comprobación	OK/NOK	Como hacerlo
2. Compruebe los certificados de vCenter.		Compruebe que los certificados que están siendo utilizados en el servidor de vCenter son los correctos (firmados por una entidad certificadora autorizada). Para ello, pulse sobre el icono del menú principal y sobre “Administración” en el menú contextual que se ha desplegado.  Pulse sobre “Administración de certificados” y seleccione el servidor de vCenter a comprobar.  Acceda a “Administración de certificados” y compruebe cada uno de ellos.  **Certificado** / **OK/NOK** Certificado de servidor Certificado acceso web a servidor Certificado vsphere-webclient Certificado vpxd Certificado vpxd extensión Certificado raíz de confianza Certificado de entidad subordinada de confianza **Nota:** La lista de certificados puede cambiar dependiendo de los aplicativos instalados y de si se dispone de certificados emitidos por una entidad certificadora subordinada.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>3. Compruebe que el sistema no está unido al programa de mejora de VMware.</td><td></td><td>Pulse sobre “Implementación → Programa de mejora de la experiencia del cliente”.
 

El estado correcto debe ser “No unido”.
<table><tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Estado del programa</td><td>No unido</td><td></td></tr></table></td></tr>
<tr><td>4. Compruebe que los usuarios y grupos de administración son los correctos.</td><td></td><td>Compruebe que la lista de usuarios y grupos para hacer inicio de sesiones y labores administrativas es la adecuada. Pulse sobre “Usuarios y grupos” y revise la lista de usuarios mediante las pestañas.
 

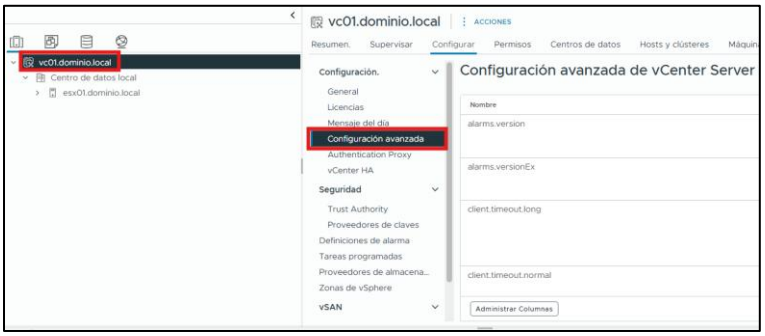
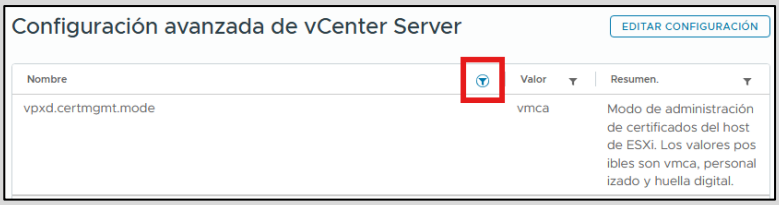
<table><tr><th>Objetos</th><th>OK/NOK</th></tr><tr><td>Lista de usuarios</td><td></td></tr><tr><td>Lista de grupos</td><td></td></tr></table></td></tr>
<tr><td>5. Compruebe la directiva de contraseñas para el servidor de vCenter.</td><td></td><td>Compruebe las directivas de contraseñas. Para ello, pulse sobre “Configuración” y sobre el botón “Directiva de contraseñas”.
 
</td></tr>
<tr><td></td><td></td><td><table><tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr><tr><td>Duración máxima</td><td>60</td><td></td></tr><tr><td>Reutilización restringida</td><td>24</td><td></td></tr><tr><td>Longitud mínima</td><td>14</td><td></td></tr><tr><td>Caracteres especiales</td><td>1</td><td></td></tr><tr><td>Caracteres en mayúscula</td><td>1</td><td></td></tr></table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>Caracteres en minúscula</td><td>1</td><td></td></tr>
<tr><td>Caracteres numéricos</td><td>1</td><td></td></tr>
</table>
</td></tr>
<tr><td>6. Compruebe la directiva de bloqueo para el servidor de vCenter.</td><td></td><td>Compruebe las directivas de contraseñas. Para ello, pulse sobre el botón “Directiva de bloqueo”.
<table>
<tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cantidad máxima de intentos fallidos de inicio de sesión</td><td>8</td><td></td></tr>
<tr><td>Intervalo de tiempo entre errores</td><td>1800</td><td></td></tr>
<tr><td>Tiempo de desbloqueo</td><td>5400</td><td></td></tr>
</table>
</td></tr>
<tr><td>7. Compruebe que se ha establecido el mensaje de inicio de sesión.</td><td></td><td>Pulse sobre la pestaña “Mensaje de inicio de sesión” y compruebe que el mensaje está configurado, la casilla de consentimiento habilitada y los detalles del mensaje configurados.


<table>
<tr><th>Parámetro</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Mensaje de inicio de sesión</td><td>Contiene el mensaje adaptado a sus necesidades</td><td></td></tr>
<tr><td>Casilla de consentimiento</td><td>Habilitado</td><td></td></tr>
<tr><td>Detalles del mensaje de inicio de sesión</td><td>Contiene el mensaje adaptado a sus necesidades</td><td></td></tr>
</table>
</td></tr>
<tr><td>8. Compruebe los parámetros de configuración avanzada del servidor de vCenter.</td><td></td><td>En el menú de la izquierda, a través de la consola de vSphere Client, pulse sobre el icono que corresponde a “Host y clústeres”.

Pulse sobre el objeto con el nombre del servidor de vCenter.

</td></tr>
</table>

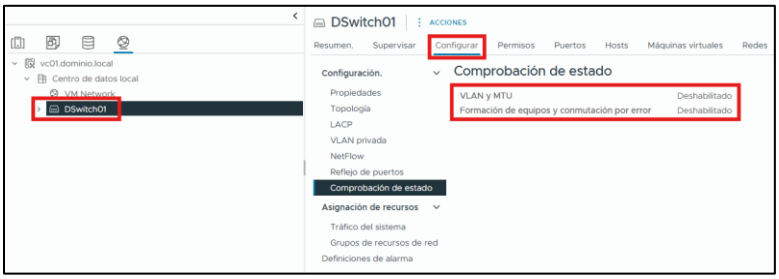
Comprobación	OK/NOK	Como hacerlo
		Vaya a la pestaña “Configurar” y seleccione “Configuración Avanzada”.  Localice los siguientes parámetros y confirme que los valores coinciden con los mostrados en la siguiente tabla: **Nota:** Es posible hacer uso del filtro de columna para localizar los parámetros más fácilmente.  **Nombre** | **Valor** | **OK/NOK** vpxd.certmgmt.mode | custom |

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>9. Compruebe que los servicios de vCenter son ejecutados por el usuario adecuado.</td><td></td><td>Revise los servicios principales del vCenter Server Appliance y asegúrese de que los siguientes se encuentren configurados con inicio automático y en estado activo:
<table>
<tr><th>Servicio</th><th>Inicio</th><th>OK/NOK</th></tr>
<tr><td>VMWareDirectoryService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareIdentityMgmtService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareCertificateService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareDNSService</td><td>Automático</td><td></td></tr>
<tr><td>VMWareAfdService</td><td>Automático</td><td></td></tr>
<tr><td>VMwareSTS</td><td>Automático</td><td></td></tr>
<tr><td>vmon</td><td>Automático</td><td></td></tr>
<tr><td>Vmware-cis-config</td><td>Automático</td><td></td></tr>
</table>
Nota: La disponibilidad de algunos servicios puede variar en función de los componentes habilitados durante la instalación de vCenter. Todos los servicios son gestionados por el gestor de procesos vmon, y se ejecutan bajo el contexto del sistema root en el appliance VCSA basado en Photon OS.
Verificación del estado de los servicios
Para consultar el estado actual de los servicios en VCSA, utilice el siguiente comando desde una sesión SSH o desde la consola directa del appliance:
- service-control –status
En VCSA, los servicios corren bajo el usuario root y sus configuraciones se encuentran gestionadas desde /etc/init.d/, /usr/lib/vmware/ o mediante systemd.
Para revisar permisos de ejecución:
- ls -l /etc/init.d/
- ls -l /usr/lib/vmware/</td></tr>
</table>

1.1. CONMUTADORES VIRTUALES DISTRIBUIDOS

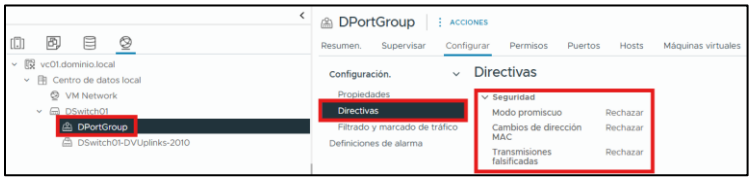
Las comprobaciones descritas a continuación son a nivel de conmutadores virtuales distribuidos. Por tanto, es necesario revisar la seguridad de todos los conmutadores virtuales distribuidos existentes en el servicio de vCenter.

Comprobación	OK/NOK	Como hacerlo
10. Compruebe que la “comprobación de estado” de los conmutadores virtuales		En el menú de la izquierda, seleccione el icono correspondiente a “Redes”.  Sitúese sobre cada conmutador distribuido y en la pestaña “Configurar” pulse sobre el elemento “Comprobación de

Comprobación	OK/NOK	Como hacerlo
distribuidos es correcta.		estado" y compruebe que los valores coinciden con los mostrados en la tabla.  **Parámetro** / **Estado** / **OK/NOK** VLAN y MTU — Deshabilitado Formación de equipos y conmutación por error — Deshabilitado

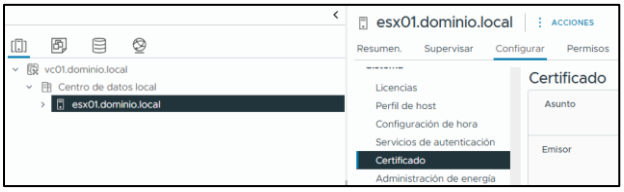
1.2. GRUPOS DE PUERTOS

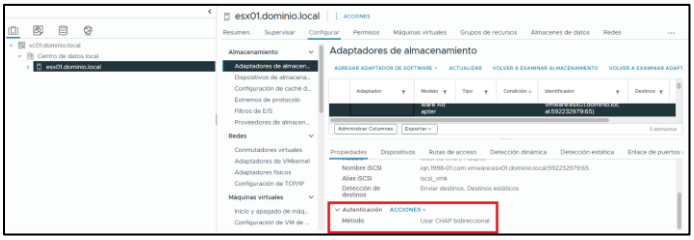
Las comprobaciones descritas a continuación son a nivel de grupos de puertos. Por tanto, es necesario revisar la seguridad de todos los grupos de puertos existentes en los distintos conmutadores presentes en el servicio de vCenter.

Comprobación	OK/NOK	Como hacerlo
11. Compruebe que la seguridad de los grupos de puertos es correcta.		En el menú de la izquierda, seleccione el icono correspondiente a "Redes".  Sitúese sobre cada grupo de puertos (que se encontrarán dentro de la rama de cada conmutador virtual) y, en la pestaña "Configurar", seleccione "Directivas" y compruebe que las siguientes directivas de seguridad tienen el valor "Rechazar"  **Directiva** / **Valor** / **OK/NOK** Modo Promiscuo — Rechazar Cambios de dirección MAC — Rechazar Transmisiones falsificadas — Rechazar

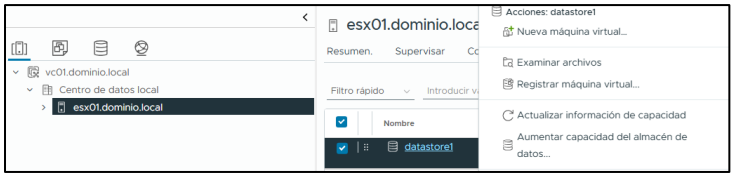
2. SERVIDORES ESXI

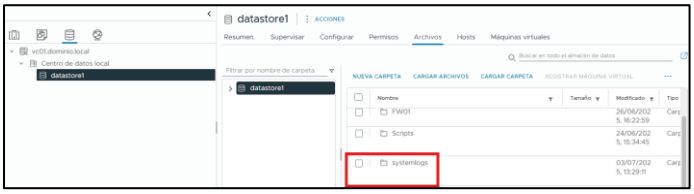
Las comprobaciones descritas a continuación se realizan a nivel de servidor ESXi y deberán ser revisadas en cada uno de los host ESXi que se añadan a cada servidor de vCenter.

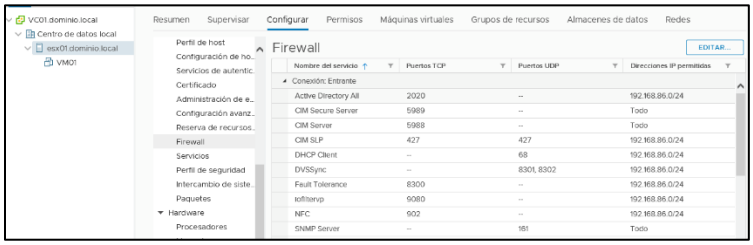
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>12.Compruebe que el certificado del servidor ESXi es correcto.</td><td></td><td>Pulse sobre el icono que corresponde a “Host y clústeres”.
 
Sitúese sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar” seleccione “Certificado”. Compruebe que el certificado de servidor es el adecuado (emitido por una entidad certificadora autorizada)
 
</td></tr>
<tr><td>13.Compruebe que está establecida la configuración NTP que se adecúa a las necesidades de la organización.</td><td></td><td>Seleccione “Configuración de hora” y compruebe que los valores son los deseados.
 

<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Cliente NTP</td><td>Habilitado</td><td></td></tr>
<tr><td>Estado de servicio NTP</td><td>En ejecución</td><td></td></tr>
<tr><td>Servidores NTP</td><td>Configurado con un servidor de NTP válido</td><td></td></tr>
</table></td></tr>
<tr><td>14.Compruebe que el método de autenticación entre el servidor ESXi y el adaptador iSCSI es el adecuado.</td><td></td><td>Sitúese sobre “Adaptadores de almacenamiento” y pulse sobre cada adaptador iSCSI que quiera comprobar. En la pestaña “Propiedades” compruebe en “Autenticación” que el método CHAP está habilitado y la gestión de claves es bidireccional.
 

<table>
<tr><th>Propiedad</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Método</td><td>User CHAP bidireccional</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>15.Compruebe la configuración de logs.</td><td></td><td>Se deberá comprobar que los logs del sistema se encuentran en un almacén de datos persistente y accesible desde el servidor de vCenter. Pulse la pestaña “Almacén de datos” y pulse botón derecho sobre el almacén de datos que debería contener los logs. Seleccione “Examinar Archivos” en el menú contextual que se ha desplegado.
 

Deberá existir una carpeta denominada “systemlogs”.
 

Pulse doble clic sobre dicha carpeta para comprobar que contiene los ficheros de log y que estos se están llenando correctamente.
 
</td></tr>
<tr><td>16.Compruebe que las conexiones permitidas del firewall están filtradas solamente a las redes permitidas.</td><td></td><td>Sitúese sobre “Firewall” y compruebe que las conexiones permitidas no contienen el valor todos en la columna “Direcciones IP permitidas” y, en su lugar, aparecen solamente las redes permitidas.
 

<table><tr><th>Conexión</th><th>Direcciones IP</th><th>OK/NOK</th></tr><tr><td>SSH server</td><td>Redes permitidas</td><td></td></tr><tr><td>CIM SLP</td><td>Redes permitidas</td><td></td></tr><tr><td>DNS client</td><td>Redes permitidas</td><td></td></tr></table></td></tr>
</table>

Comprobación	OK/NOK	Como hacerlo
		Fault tolerance — Redes permitidas Iofiltervp — Redes permitidas NTP client — Redes permitidas Software iSCSI client — Redes permitidas vMotion — Redes permitidas vSphere Web Access — Redes permitidas Active Directory All — Redes permitidas DHCP client — Redes permitidas DVSsync — Redes permitidas HBR — Redes permitidas NFC — Redes permitidas Rabbitmqproxy — Redes permitidas vCenter Update Manager — Redes permitidas VMware vCenter agent — Redes permitidas vSphere Web client — Redes permitidas
17. Compruebe los parámetros de configuración avanzada en cada servidor de ESXi		Diríjase a "Configurar → Configuración avanzada" y compruebe los parámetros y valores especificados en la tabla.  **Nota:** Puede hacer uso de los filtros de columna para localizar las directivas.

Clave	Valor	OK/NOK
Security.Account.LockFailures	8	
Security.Account.UnlockTime	3600	
Security.PasswordHistory	24	
Security.PasswordMaxDays	60	
Security.PasswordQualitycontrol	retry=3 min=disabled,disabled,disabled, disabled,14	
Misc.UsbArbitratorAutostartDisabled	1	
Config.HostAgent.plugins.solo.enableMOB	false	
Mem.ShareforceShalting	2	
Net.BlockGuestBPDU	1	
Syslog.global.default.rotate	0	
Syslog.global.default.size	8192	
Syslog.global.logDir	"almacén de datos adecuado y persistente"	
UserVars.ESXiShellInteractiveTimeOut	600	
UserVars.ESXiShellTimeOut	600	

Comprobación	OK/NOK	Como hacerlo	
Annotations.WelcomeMessage		"Mensaje de seguridad que se adapte a las necesidades de la organización"	
UserVars.HostClientWelcomeMessage		"Mensaje de seguridad que se adapte a las necesidades de la organización"	
		En este momento, aún no se han realizado todas las configuraciones específicas del servidor ESXi. Sin embargo, y dado que el resto de las configuraciones requieren de un acceso directo al host, se comprobarán el resto de los componentes tales como seguridad en las máquinas o conmutadores virtuales contenidos en el host para minimizar el tiempo de exposición del acceso directo o a través de SSH.	

2.1. CONMUTADORES VIRTUALES ESTÁNDAR

Las comprobaciones descritas a continuación son a nivel de conmutadores virtuales estándar. Por tanto, es necesario revisar la seguridad de todos los conmutadores virtuales estándar existentes en cada host ESXi contenido en cada servidor de vCenter.

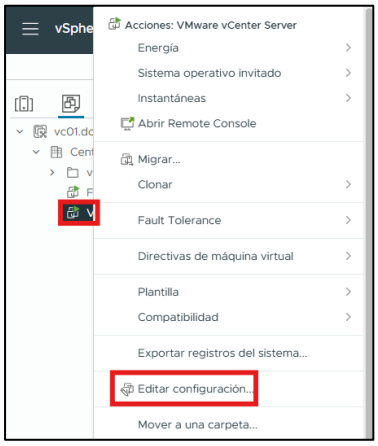
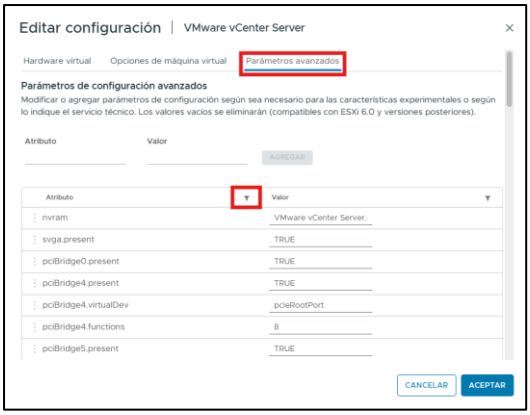
Comprobación	OK/NOK	Como hacerlo
18. Compruebe la seguridad en los conmutadores virtuales estándar de cada servidor ESXi.		Seleccione "Conmutadores virtuales". Pulse "Editar" sobre cada conmutador virtual.  En la ventana emergente, pulse sobre "Seguridad" y compruebe el estado de los siguientes parámetros de seguridad (deberán tener el valor "Rechazar").

Elemento	Valor	OK/NOK
Modo promiscuo	Rechazar	
Cambios de dirección MAC	Rechazar	
Transmisiones falsificadas	Rechazar	

2.2. MÁQUINAS VIRTUALES

Las comprobaciones descritas a continuación son a nivel de máquina virtual. Por tanto, es necesario aplicar estas configuraciones de seguridad a todas las máquinas virtuales que se unan al host de ESXi que se está implementando.

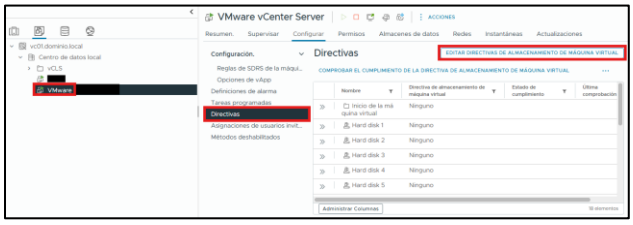
Nota: Adicionalmente, deberán ser comprobadas las medidas de seguridad aplicadas al sistema operativo invitado siguiendo las listas de comprobación de las guías STIC correspondientes.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td>19. Compruebe los parámetros de configuración avanzados para las máquinas virtuales.</td><td></td><td>Pulse el icono correspondiente a “Máquinas virtuales y plantillas”.
 
Sitúese sobre la máquina virtual sobre la que van a establecer las configuraciones de seguridad y pulse el botón derecho del ratón para seleccionar “Editar configuración…”.
 
Diríjase a la pestaña “Parámetros avanzados” y utilice la búsqueda por “Atributo”.
  </td></tr>
<tr><td></td><td></td><td>Localice los diferentes parámetros de configuración y compruebe que los valores coincides con los indicados en la tabla.
<table>
<tr><th>Elemento</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>isolation.tools.copy.disable</td><td>True</td><td></td></tr>
<tr><td>isolation.tools.paste.disable</td><td>True</td><td></td></tr>
<tr><td>isolation.tools.setGUIOptions.enable</td><td>False</td><td></td></tr>
</table></td></tr>
</table>

Comprobación	OK/NOK	Como hacerlo		
		isolation.tools.diskShrink.disable	True	
		isolation.tools.diskWiper.disable	True	
		isolation.tools.connectable.disable	True	
		isolation.device.edit.disable	True	
		isolation.tools.setOption.disable	True	
		scsiX:Y.mode	Persistent	
		mks.enable3d	False	
		floppyX.present	False	
		parallelX.present	False	
		serialX.present	False	
		svga.vgaOnly	True	
		tools.setInfo.sizeLimit	1048576	
		svga.vgaOnly	True	
		RemoteDisplay.vnc.enabled	False	
		tools.guestlib.enableHostInfo	False	
		sched.mem.pshare.salt	Null	
		ethernetX.filterX. name = filtername	Null	
		pciPassthru*.present	False	
		Net.BlockGuestBPDU	1	

2.2.1. CIFRADO DE MÁQUINAS VIRTUALES

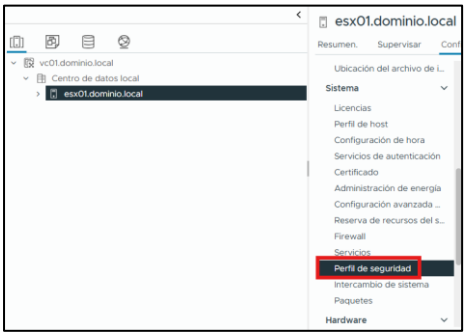
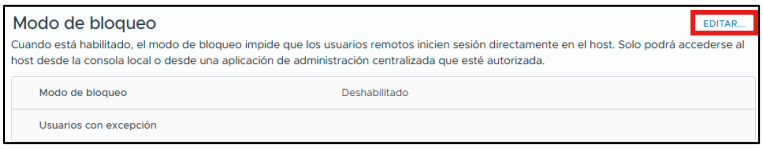
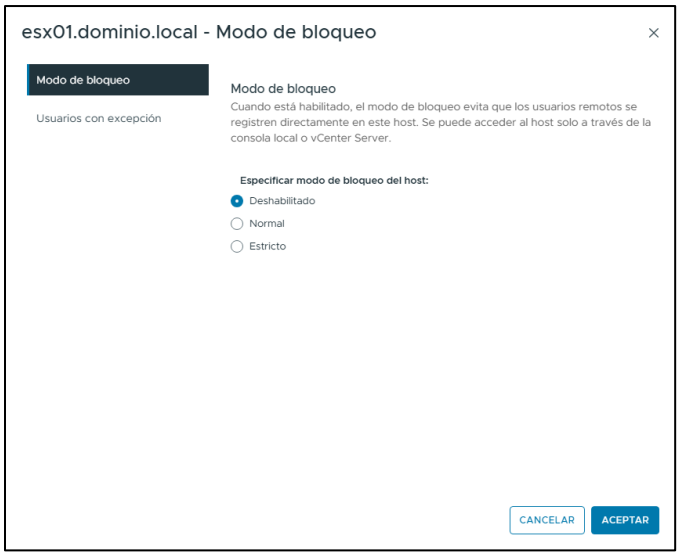
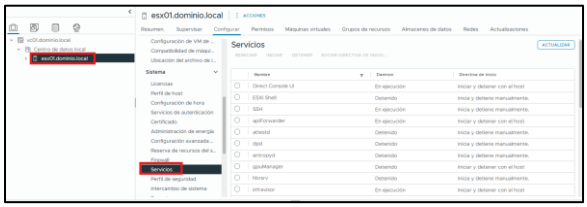
Compruebe en aquellas máquinas virtuales que se hayan cifrado que les aplica la política correcta de cifrado de almacenamiento.

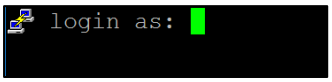
Comprobación	OK/NOK	Como hacerlo
20. Compruebe los parámetros de configuración avanzados para las máquinas virtuales.		Pulse el icono correspondiente a "Máquinas virtuales y plantillas".  Seleccione la máquina virtual y pulse sobre "Directivas". Seguidamente pulse sobre "Editar directivas de almacenamiento de máquina".  Compruebe que la política asignada al almacenamiento de la máquina virtual es la que se creó en el apartado "2.1 CONFIGURACIÓN DE SERVIDOR KMS" o, en caso de que no todos los discos estén cifrados, que la política asignada a cada uno sea la adecuada.  Pulse "Aceptar" para continuar.

2.3. COMPROBACIONES Y PASOS FINALES EN SERVIDOR ESXI

En este momento, se deberá deshabilitar el modo de bloqueo en cada servidor ESXi a comprobar ya que algunas de estas comprobaciones deberán ser realizadas a través de conexión directa al host. En los pasos finales se habilitará de nuevo para forzar el acceso único a través del servidor de vCenter.

Comprobación	OK/NOK	Como hacerlo
21. Deshabilite el modo de bloqueo		Pulse sobre el icono que corresponde a "Host y clústeres".  Sitúese sobre el objeto "<FQDN del servidor ESXi>" y en la pestaña "Configurar", seleccione "Perfil de seguridad".

Comprobación	OK/NOK	Como hacerlo
		 En “Modo de Bloqueo” seleccione “Editar”.  En la ventana emergente, seleccione el modo “Deshabilitado” y pulse “ACEPTAR” para continuar. 
22.Habilite la consola ESXi y el acceso SSH		Pulse sobre “Servicios”.  Seleccione el servicio “ESX Shell” y pulse “Iniciar”.  Realice la misma operación con el servicio “SSH”.

Comprobación	OK/NOK	Como hacerlo
		 **Nota:** No cierre aún el navegador web.
23. Realice la conexión al servidor de ESXi a través de SSH.		Utilice un cliente SSH para establecer una conexión al servidor e introduzca las credenciales de un usuario autorizado (no root) con privilegios administrativos para realizar las comprobaciones. 
24. Compruebe el estado los siguientes parámetros de seguridad.		Ejecute los comandos indicados en la tabla y compare los resultados.

Parámetro a comprobar	Valor devuelto	OK/NOK
# esxcli network ip get	IPv6Enable: false	
# esxcli system syslog config get	Local Log output: "Ruta al almacén de datos correcto y persistente"	
	Local Log Output Is Configured: true	
	Local Log Output Is Persistent: true	
	Local Login Default Rotation Size: 8192	
	Local Login Default Rotations: 0	
# esxcli system snmp get	Enable: false	
# esxcli software acceptance get	VMwareCertified	
# grep PermitRootLogin /etc/ssh/sshd_config	PermitRootLogin no	

25. Compruebe los permisos sobre los siguientes ficheros de log		Diríjase a la ruta correspondiente al almacén de datos persistente donde se han alojado los ficheros log mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd "/vmfs/Volumes/<Nombre del almacén>/Syslogs** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l *.log** Compruebe que todos los ficheros con extensión .log tienen los mismos permisos como indica la tabla.

Comprobación	OK/NOK	Como hacerlo			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
Todos los ficheros con extensión .log			-rw-------	root	
26.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe los permisos sobre la carpeta "/etc" y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
/etc			-rwxr-xr-x	root	
27.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.			
Ficheros			**permisos**	**Propietario**	**OK/NOK**
/etc/profile			-rw-r--r--	root	
/etc/krb5.conf			-rw-r--r--	root	
/etc/krb5.realms			-rw-r--r--	root	
/etc/nscd.conf			-rw-r--r--	root	
/etc/resolv.conf			-rw-r--r--	root	
/etc/nsswitch.conf			-rw-r--r--	root	
/etc/ntp.conf			-rw-r--r--	root	
/etc/passwd			-rw-r--r--	root	
/etc/group			-rw-r--r--	root	
/etc/shadow			-r---------	root	
/etc/vmware/			-rwxr-xr-x	root	
28.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/ssh" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/ssh** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l**			

Comprobación	OK/NOK	Como hacerlo
		Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.

Ficheros	permisos	Propietario	OK/NOK
/etc/ssh/sshd_config	-rw-------	root	

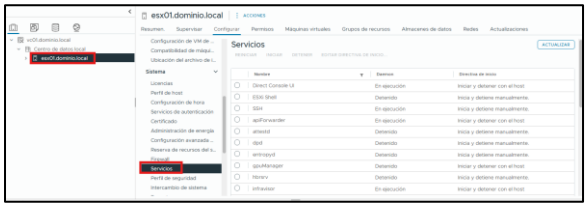
29.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/usr/sbin" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /usr/sbin** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l esxcfg*** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.

Ficheros	permisos	Propietario	OK/NOK
Todos los ficheros que comienzan por esxcfg	-r-x------	root	

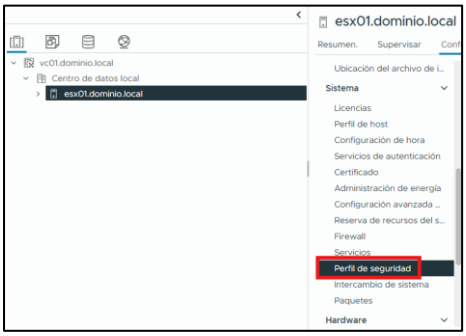
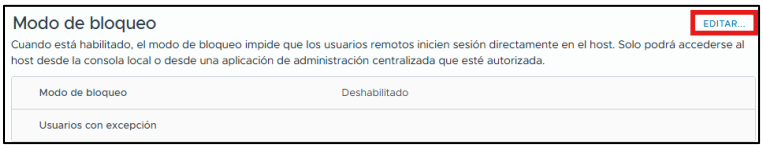
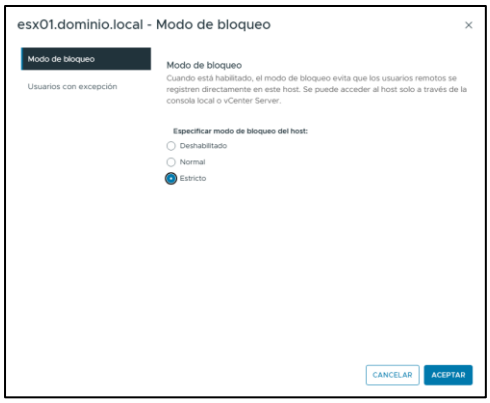
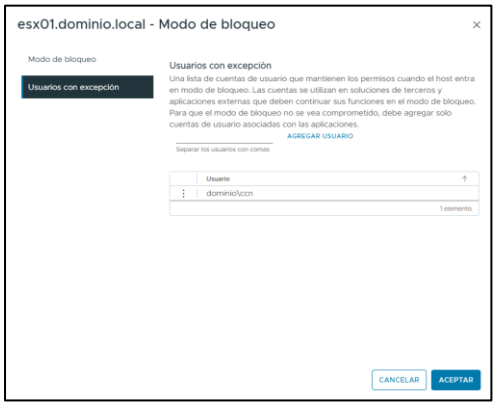
30.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/vmware" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/vmware** Introduzca el siguiente comando y pulse "Enter" para ejecutarlo. **# ls -l** Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.

Ficheros	permisos	Propietario	OK/NOK
/etc/vmware/config	-rw-r--r--	root	
/etc/vmware/configrules	-rw-r--r--	root	
/etc/vmware/esx.conf	-rw-r--r--	root	
/etc/vmware/firewall	-rwxr-xr-x	root	
/etc/vmware/hostd	-rwxr-xr-x	root	
/etc/vmware/ima_plugin.conf	-rw-r--r--	root	
/etc/vmware/license.cfg	-rw-r--r--	root	
/etc/vmware/logfilters	-rw-r--r--	root	
/etc/vmware/pciid	-rwxr-xr-x	root	
/etc/vmware/pci.ids	-rw-r--r--	root	
/etc/vmware/service	-rwxr-xr-x	root	
/etc/vmware/snmp.xml	-rw-r--r--	root	
/etc/vmware/ssl	-rwxr-xr-x	root	

31.Compruebe los permisos sobre los ficheros siguientes.		Diríjase a la ruta "/etc/vmware/ssl" mediante el siguiente comando y pulse "Enter" para ejecutarlo. **# cd /etc/vmware/ssl**

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Como hacerlo</th></tr>
<tr><td></td><td></td><td>Introduzca el siguiente comando y pulse “Enter” para ejecutarlo.
ls -l
Compruebe todos los ficheros y carpetas que aparecen en la tabla, sus permisos y el propietario.</td></tr>
<tr><td colspan="3"><table>
<tr><th>Ficheros</th><th>permisos</th><th>Propietario</th><th>OK/NOK</th></tr>
<tr><td>/etc/vmware/ssl/rui.crt</td><td>-rw-r—r--</td><td>root</td><td></td></tr>
<tr><td>/etc/vmware/ssl/rui.key</td><td>-r--------</td><td></td><td></td></tr>
</table></td></tr>
<tr><td>32.Cierre la sesión SSH.</td><td></td><td>Cierre la sesión SSH.</td></tr>
<tr><td>33.Una vez realizado, deshabilite SSH y la consola ESXi Shell (en caso de que no se hayan deshabilitado de forma automática).</td><td></td><td>En el navegador, pulse sobre el icono que corresponde a “Hosts y clústeres”.
 
En el menú de la izquierda, sitúese sobre el objeto “<FQDN del servidor ESXi>” y pulse sobre “Servicios”.
 
Seleccione el servicio “ESX Shell” y pulse “Detener”.
 

Realice la misma operación con el servicio “SSH”.
 
</td></tr>
<tr><td>34.Vuelva a habilitar el modo de bloqueo.</td><td></td><td>Defina el modo de bloqueo para el acceso a este host en modo “Estricto” para que solo se pueda acceder al host de ESXi a través de servidores vCenter y no a través de clientes vSphere por conexión directa al host o a través de la consola local. Para ello, sitúese de nuevo sobre el objeto “<FQDN del servidor ESXi>” y en la pestaña “Configurar”, seleccione “Perfil de seguridad”.</td></tr>
</table>

Comprobación	OK/NOK	Como hacerlo
		 En “Modo de Bloqueo” seleccione “Editar”.  En la ventana emergente, seleccione el modo “Estricto”. 
35. Compruebe la lista de usuarios autorizados para acceder directamente al host con modo de bloqueo activo.		Compruebe la lista de usuarios autorizados pulsando sobre “Usuarios con excepción” y pulse “ACEPTAR” para finalizar.  **Nota:** Esta lista debería ser revisada periódicamente para evitar que haya usuarios no autorizados añadidos a ella.