Guía de Seguridad de las TIC
CCN-STIC 826

IMPLEMENTACIÓN DEL ENS EN NEXTCLOUD 15

NOVIEMBRE 2019

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES

NIPO: 083-19-272-3
Fecha de Edición: noviembre de 2019
Sidertia solutions S.L. ha participado en la realización y modificación del presente documento y sus anexos.

PRÓLOGO

El uso masivo de las tecnologías de la información y las telecomunicaciones (TIC), en todos los ámbitos de la sociedad, ha creado un nuevo espacio, el ciberespacio, donde se producirán conflictos y agresiones, y donde existen ciberamenazas que atentarán contra la seguridad nacional, el estado de derecho, la prosperidad económica, el estado de bienestar y el normal funcionamiento de la sociedad y de las administraciones públicas.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información en su artículo 4.e), y de protección de la información clasificada en su artículo 4.f), a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN) en su artículo 9.2.f).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través de su Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, a la aplicación de políticas y procedimientos de seguridad, y al empleo de tecnologías de seguridad adecuadas.

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica (ENS, en adelante), al que se refiere el apartado segundo del artículo 156 de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público, establece la política de seguridad en la utilización de medios electrónicos que permita una protección adecuada de la información.

Precisamente el Real Decreto 3/2010 de 8 de Enero, actualizado por el Real Decreto 951/2015, de 23 de octubre, fija los principios básicos y requisitos mínimos así como las medidas de protección a implantar en los sistemas de la Administración, y promueve la elaboración y difusión de guías de seguridad de las tecnologías de la información y las comunicaciones (STIC) por parte de CCN para facilitar un mejor cumplimiento de dichos requisitos mínimos.

En definitiva, la serie de documentos CCN-STIC se elabora para dar cumplimiento a los cometidos del Centro Criptológico Nacional y a lo reflejado en el Esquema Nacional de Seguridad, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo su difícil, y en ocasiones, ingrata tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

julio de 2019

Félix Sanz Roldán
Secretario de Estado
Director del Centro Criptológico Nacional

ANEXOS

ANEXO A. CONFIGURACIÓN SEGURA DE NEXTCLOUD 15 EN EL ENS

Este apartado detalla las características y configuraciones específicas que van a ser aplicadas sobre un servidor de alojamiento de archivos con el sistema operativo CentOS 7.4 Linux según criterios del ENS.

Debido a las características de los puestos de trabajo a los que van dirigidas las guías de la serie 600 se toma la determinación de establecer la versión CentOS 7.4 Linux de la distribución, con la opción de instalación "servidor con GUI" como la más adecuada para su implementación. Esto se basa en los siguientes condicionantes:

a) Estos equipos pueden estar conectados a Internet por lo cual determinadas funcionalidades como el instalador de aplicaciones o los entornos de escritorio GNOME o KDE, pueden ser utilizados o no, en función de las necesidades de cada organización.

b) El anterior hecho redunda en dos principios base de la seguridad: mínima funcionalidad y menor exposición.

c) La opción de "servidor con GUI" de CentOS 7.4 Linux permite garantizar la funcionalidad del sistema para aquellas infraestructuras implementadas con CentOS 7.4 Linux. No obstante, deben considerarse siempre las actualizaciones de seguridad tanto del propio sistema operativo como de los servidores LAMP y Nextcloud un elemento esencial para garantizar la seguridad de los puestos de trabajo en cualquier infraestructura.

Además de esta determinación existen varias configuraciones adicionales en el "ANEXO A.6 TAREAS ADICIONALES DE SEGURIDAD" para garantizar la securización del sistema. Dichas características son:

a) Integración de usuarios con LDAP. Este componente se establece de manera predeterminada en Nextcloud, debiendo configurarlo correctamente con los parámetros de su organización.

b) Servidor de redis caché: Este componente puede mejorar significativamente el rendimiento del servidor Nextcloud con el almacenamiento en memoria caché, donde los objetos solicitados con frecuencia se almacenan en la memoria para una recuperación más rápida.

c) Configuración adicional de seguridad, Selinux. SELinux (Linux con seguridad mejorada: «Security Enhanced Linux») es un sistema de control obligatorio de acceso («Mandatory Access Control») basado en la interfaz LSM (módulos de seguridad de Linux: «Linux Security Modules»). En la práctica, el núcleo pregunta a SELinux antes de cada llamada al sistema para saber si un proceso está autorizado a realizar dicha operación.

SELinux utiliza una serie de reglas, conocidas en conjunto como una política («policy»), para autorizar o denegar operaciones. Puesto que estas reglas son difíciles de crear, en este apartado se recoge una configuración mínima de las mismas para mayor seguridad del sistema.

No obstante, las diferentes organizaciones deberán tener en consideración el hecho de que las plantillas definidas, puedan ser modificadas para adaptarlas a sus necesidades operativas.

La aplicación de esta guía se debe realizar en un sistema operativo CentOS 7.4 Linux que se acaba de instalar en un equipo que se encontraba formateado (sin datos).

ANEXO A.1. CONFIGURACIÓN DE SEGURIDAD DE NEXTCLOUD 15 PARA ENS

1. APLICACIÓN DE MEDIDAS EN NEXTCLOUD 15

Atendiendo a la necesidad de aplicar medidas de seguridad en aquellos escenarios donde sea necesaria la implementación de servidores con Nextcloud 15 y que les sea de aplicación el ENS, se establecerán a través de la presente guía las condiciones necesarias de aplicación. Estas se materializarán bien en la aplicación de configuraciones de seguridad o bien en procedimientos para garantizar la seguridad, cuando así se demande.

La aplicación de medidas de seguridad atenderá a las siguientes condiciones de implantación de infraestructuras.

a) Aplicación de seguridad en el entorno de Servidor de alojamiento de archivos sobre CentOS 7.4 Linux como servidor independiente.

b) Aplicación de seguridad en servidores independientes que se encontrarán implementados con CentOS 7.4 Linux implementados siguiendo la guía CCN-STIC-619 – IMPLEMENTACIÓN DE SEGURIDAD SOBRE CENTOS 7 LINUX (CLIENTE INDEPENDIENTE).

Para el análisis y desarrollo de las plantillas a aplicar, así como las tareas administrativas que sean necesarias para el cumplimiento de las medidas dispuestas en el ENS, se tienen en consideración los propios elementos técnicos que aporta CentOS 7 Linux y el propio servidor Nextcloud, así como otras medidas que puedan ser fácilmente aplicables mediante condiciones de seguridad válidas. Por ejemplo, todas aquellas medidas que puedan ser aplicadas a través de políticas de seguridad en instalación o las innatas a la gestión del sistema.

Esta guía por lo tanto no referenciará aquellas medidas que, aunque sean de aplicación y de obligado cumplimiento, no sean nativas al sistema operativo o del propio servidor de alojamiento de ficheros. Es factible en ello que se realicen referencias a soluciones de seguridad que como en el caso de CentOS 7 Linux vienen implementadas por el propio Sistema Operativo a través del software SELinux. No obstante, tal y como es lógico referenciar dicha implementación, y atendiendo a los requerimientos del ENS, requiere una administración centralizada que no aporta esta solución, cubriendo además solo uno de los aspectos requeridos por la medida de protección frente a código dañino.

Para un mejor entendimiento de las medidas éstas van a ser explicadas y además van a ser definidos los mecanismos que proporcione el sistema atendiendo a los criterios de categorización. Así se irá delimitando cada una de las medidas y estableciendo en base a las categorías que mecanismos se deberán habilitar para su cumplimiento. Habida cuenta de esta información a continuación se detallarán las diferentes plantillas de seguridad aplicables en función de las diferentes categorías de seguridad.

1.1. MARCO OPERACIONAL

1.1.1. CONTROL DE ACCESO

El control de acceso abarca todo el conjunto de acciones que bien preparatorias o ejecutivas 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 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 comodidad de uso y la protección del sistema, de tal forma que la seguridad se irá incrementando en base a la categoría exigida. Así en la categoría básica se prima la comodidad y en la categoría alta se prima la protección.

1.1.1.1. OP. ACC. 1. IDENTIFICACIÓN

Desde las categorías básicas debe especificarse mecanismos para garantizar la autenticidad y trazabilidad de las diferentes entidades. Esto se transforma generando una identificación singular para cada entidad: usuario, proceso o servicio. De esta manera siempre se podrá conocer quién recibe qué derechos y se puede saber qué ha hecho.

La identificación de usuario se traduce en la necesidad de crear cuentas únicas e inequívocas para cada usuario y servicio, a través de cuentas locales en los puestos de trabajo. Dichas cuentas deberán ser gestionadas de tal forma que deberán ser inhabilitadas cuando se dieran una serie de condicionantes:

a) El usuario deja la organización.

b) Cesa en la función para la cual se requería dicha cuenta.

c) La persona que lo autorizó emite una orden en contra.

Debe tenerse en consideración que nunca deberán existir dos cuentas iguales de forma que estas no puedan confundirse o bien imputarse acciones a usuarios diferentes.

1.1.1.2. OP. ACC. 2. REQUISITOS DE ACCESO

Los requisitos de acceso se aplican desde la categoría básica y atenderán a la necesidad que los recursos del sistema queden protegidos con algún mecanismo que impida su utilización, salvo a las entidades que disfruten de los derechos de acceso suficientes.

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

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. 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.

La plantilla de seguridad recoge una serie de permisos que serán asignados con objeto de limitar las acciones por parte de usuarios y administradores. De esta forma y controlando los requisitos de acceso, se reducirán todos aquellos riesgos del uso habitual de administración de un puesto de trabajo.

Es necesario en este sentido que el operador conozca los requerimientos y procesos para la asignación de las listas de control de acceso (ACL), teniendo en consideración que es la base en las infraestructuras Linux para la concesión o no de acceso, así como el que estará permitido o denegado en cada circunstancia.

1.1.1.3. 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 establece 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.

Dichos procesos de segregación son factibles realizarlos a través de los propios mecanismos que proporciona CentOS 7 Linux y Nextcloud, así como las funcionalidades implicadas en la presente guía.

Con respecto a los controles de auditoría o supervisión, se recomienda al operador de aquellas organizaciones que no contaran con sistemas de recolección, consolidación y tratamiento de eventos, la lectura de documentación sobre la herramienta Audit incluida en CentOS 7 Linux además del propio servidor de alojamiento de archivos Nextcloud, a través de su aplicación **Nextcloud Activity**. Aunque serán mencionadas a lo largo de la presente guía en relación a todas las acciones enfocadas a garantizar la trazabilidad, se recoge específicamente la capacidad para la segregación de auditoría de registros empleados en CentOS 7 Linux a través de la herramienta Audit y la trazabilidad que se consigue mediante la aplicación Nextcloud Activity.

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

Altamente vinculado al punto 1.1.1.2 OP. ACC. 2. REQUISITOS DE ACCESO, estas medidas requieren consolidación de los derechos de acceso, de tal forma que:

a) Exista la aplicación del mínimo privilegio. Los privilegios de cada usuario 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.

Como ya se comentó previamente, tanto CentOS 7 Linux como el servidor Nextcloud se encuentran facultados para establecer diferentes mecanismos de control de acceso, proporcionando así la gestión de derechos de acceso.

Adicionalmente y siguiendo uno de los principios fundamentales de mínimo privilegio posible, a través de la aplicación de la presente guía se configurarán diferentes permisos a las cuentas de usuario, limitando la utilización de la cuentas de administradores locales, para tareas específicas que necesiten un nivel de privilegios elevado, ésta configuración debe entenderse como un mecanismo para impedir que el trabajo directo con usuarios con privilegios de administrador, repercuta negativamente en la seguridad, a acometer todas las acciones con el máximo privilegio cuando este no es siempre requerido.

En la navegación a Internet, acceso a recurso o tratamientos ofimáticos por citar algunos ejemplos frecuentes, un usuario no requiere del privilegio de administración para desempeñarlo. Así y sin darse cuenta podría estar poniendo en grave riesgo la seguridad del sistema al tratar ficheros, ejecutables, componentes y otros, que 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 de ACL para permitir la visualización de contenido o edición del mismo 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 para 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 el permiso total sobre ella. Con la concesión permisos de este tipo, se le estarían otorgando permisos más allá de las necesidades que requiere dicho usuario. Concederle el permiso de modificar se debe considerar como la opción más óptima desde el punto de vista del ENS.

1.1.1.5. OP. ACC. 5. MECANISMOS DE AUTENTICACIÓN

Dentro de los procesos habituales en el manejo de los sistemas de la información, el correspondiente a la autenticación, corresponde al primero a llevar a efecto. Antes de acceder a datos, gestionar recursos o tratar servicios es necesario indicar al sistema “quién eres”.

El sistema de autenticación se puede traducir tecnológicamente mediante múltiples mecanismos, siendo el del empleo de una contraseña el más habitual pero no por ello el más seguro, sino todo lo contrario. Los mecanismos de autenticación se deberán adecuar en función del nivel de criticidad de la información o el servicio atendiendo lógicamente a diferentes criterios.

Según establece el propio Esquema Nacional de Seguridad, a grandes generalidades estos serán:

a) Para la categoría básica se admitirá el uso de cualquier mecanismo de autenticación: claves concertadas, dispositivos físicos (en inglés “Tokens”), sistemas de biometría o certificados digitales entre otros.

b) Para la categoría media se desaconseja el empleo de passwords o claves concertadas, siendo recomendable el uso de sistemas físicos (Tokens), biométricos o certificados digitales.

c) Para la categoría alta, se prohíbe el uso de autenticadores basados en el empleo de claves concertadas. Se exige para ello el uso de dispositivos físicos o de biometría. Para ello deberán emplearse algoritmos acreditados por el Centro Criptológico Nacional, recogidos en la guía CCN-STIC-807 de criptología de empleo en el ENS.

Conforme a las necesidades establecidas por el Esquema Nacional de Seguridad se deberá tener también en consideración lo establecido en la guía CCN-STIC-804 para los mecanismos de autenticación y que se encuentra recogido en el punto 4.2.5.

La presente guía tiene en consideración los siguientes aspectos, para el desarrollo de plantillas de seguridad por categorías, enfocados en los procesos de autenticación:

a) Gestión y definición de política de contraseñas.

b) Implementación de algoritmos para el almacenamiento de contraseñas cifradas.

c) Implementación de mecanismos para el bloqueo de cuentas de usuario y de servicio.

d) Permisividad para el empleo de mecanismos de algoritmos y criptografía basados en biometría, certificados o tarjetas inteligentes.

Nextcloud 15 tiene la capacidad de implementar sistemas de autenticación que se adapten a cualquiera de las necesidades que puedan existir tanto ahora como en el futuro. Pudiendo emplear actualmente mecanismos de autenticación basados en el empleo de contraseñas, así como mecanismos basados en Kerberos.

1.1.1.6. OP. ACC. 6. ACCESO LOCAL

Se considera acceso local aquel que se ha realizado desde los puestos dentro de las propias instalaciones que tiene la organización.

El Esquema Nacional de Seguridad, tiene en cuenta la aplicación de medidas diferentes atendiendo a la criticidad de servicios y sistemas. Así en función de la categoría de seguridad deberán aplicarse medidas para:

a) En la categoría básica, se prevendrán ataques para evitar intentos de ataques reiterados contra los sistemas de autenticación. Adicionalmente la información proporcionada en caso de fallo en el acceso deberá ser mínima, siendo este hecho especialmente crítico en las aplicaciones web. También deberán registrarse los intentos satisfactorios y erróneos, así como la de informar a los usuarios de las obligaciones.

b) En la categoría media será exigencia el proporcionar al usuario el detalle de la última vez que se ha autenticado.

c) En la categoría alta deberán existir limitaciones para la fecha y hora en la que se accede. También se facilitará mediante identificación singular la renovación de la autenticación, no bastando el hecho de hacerlo en la sesión iniciada.

Nextcloud a través de aplicaciones específicas, así como CentOS 7 Linux por medio de ficheros de configuración y módulos PAM, permiten establecer mecanismos para garantizar bloqueos de cuenta, proporcionar información al usuario, así como establecer medidas para garantizar un cambio seguro de las credenciales. Estás serán aplicadas de forma progresiva en función de la categoría de seguridad exigido.

1.1.1.7. OP. ACC. 7. ACCESO REMOTO

Las organizaciones deberán mantener las consideraciones de seguridad en cuanto al acceso remoto cuando éste se realice desde fuera de las propias instalaciones de la organización a través de redes de terceros.

Estas organizaciones deberán garantizar la seguridad, tanto en el propio acceso en sí, como en el canal del acceso remoto.

Nextcloud 15 y CentOS 7 Linux facultan el empleo de protocolos seguros para las comunicaciones y los procesos de autenticación. Sin embargo, no todos los protocolos empleados por defecto después de una instalación común se pueden considerar seguros. La presente guía tiene en consideración estos detalles y por lo tanto habilitará o deshabilitará en su defecto aquellos protocolos que son considerados seguros o no, incluido en ello los correspondientes a autenticaciones empleadas en redes locales o remotas.

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 aplicará la regla de mínima funcionalidad.

Nextcloud sobre un sistema operativo CentOS Linux pertenecen a la rama de software de código libre con licencias AGPL3 y GNU GPL respectivamente, por lo que se considera indispensable la comprobación de funcionalidades evitando en la medida de lo posible las provenientes de fuentes no confiables, manteniendo 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.

Para el cumplimiento de este sentido las diferentes plantillas de seguridad se dotarán de las funcionalidades necesarias para deshabilitar y configurar todos aquellos servicios que, no siendo necesarios para ningún entorno operativo, pudieran constituir un riesgo de seguridad. Adicionalmente se protegerán los más importantes de tal forma que quedarán configurados a través de las políticas que correspondieran por categorías. Se facilitarán consejos para conocer y gestionar los servicios implicados y cómo actuar ante riesgos de seguridad identificados en la red.

Adicionalmente la guía mostrará mecanismos de administración adicionales para configurar nuevos componentes con objeto de reducir la superficie de exposición, así como limitar la información remitida hacia Internet.

1.1.2.2. OP. EXP. 4. MANTENIMIENTO

Para mantener el equipamiento físico y lógico se deberán atender a las especificaciones de los fabricantes en lo relativo a la instalación y mantenimiento de los sistemas. Se realizará un seguimiento continuo para garantizar la seguridad de los sistemas. Para ello deberá existir un procedimiento que permita analizar, priorizar y determinar cuándo aplicar las actualizaciones de seguridad, parches, mejoras y nuevas versiones. La priorización tendrá en cuenta la variación del riesgo en función de la aplicación o no de la actualización.

En este sentido la presente guía sigue los patrones establecidos tanto por CentOS 7 Linux como por el propio Nextcloud. Debe tenerse en consideración que tanto el servidor de alojamiento se ficheros como el propio sistema operativo son elementos en constante evolución, donde ante la aparición de un riesgo de seguridad deberá dotar de los mecanismos necesarios para paliar el problema. Para ello ambos, hacen una constante difusión de actualizaciones de seguridad que deberá evaluar e implementar sobre los servidores, con objetos de mantener las garantías de seguridad necesarias.

Adicionalmente a las actualizaciones de seguridad, se debe tomar en consideración que Nextcloud ofrece versiones principales programadas generalmente una vez cada 4 meses, siendo las primeras 10 semanas la fase de desarrollo seguida de la fase de congelación con cuatro versiones beta, dos RC y una final cada una con un intervalo de 1 semana. No debe confundir no obstante dichas actualizaciones de funcionalidad con las actualizaciones tradicionales de seguridad, sin embargo, tanto CentOS 7 Linux, como Nextcloud seguirá recibiendo las actualizaciones de seguridad dentro del ciclo natural de publicación de las mismas.

Para ello deberá diferenciar los siguientes tipos de actualizaciones:

a) Actualizaciones de seguridad. Las actualizaciones de seguridad vienen a subsanar problemas más frecuentes del Sistema Operativo y muchos de sus servicios, en relación a los componentes más críticos del sistema.

b) Actualizaciones de seguridad: Los proveedores de sistemas operativos Linux proporcionan actualizaciones periódicas, que en su mayoría son parches de seguridad del sistema operativo. Debe asegurarse de que los sistemas operativos actualizados con los parches de seguridad más recientes.

Mediante el plugin yum-security es posible listar y restringir las actualizaciones únicamente a las que sean por criterios de seguridad. Los paquetes los clasifica según:

i. Enhancement. Una mejora que entra dentro de criterios de seguridad por algún motivo, por ejemplo, una mejora en el paquete chkrootkit.

ii. Bugfix. Solución de un bug, igualmente que cumple criterios de seguridad de forma secundaria.

iii. Security. Solución a un problema de seguridad propiamente dicho.

c) Actualizaciones de los repositorios: Un repositorio es un directorio o sitio web que contiene paquetes de software y archivos de índices. Las utilidades de administración de software como yum automáticamente ubican y obtienen los paquetes RPM correctos desde esos repositorios. Este método soluciona tener que buscar e instalar las nuevas aplicaciones o actualizaciones de forma manual. Se puede utilizar un único comando para actualizar todo el software del sistema o buscar por nuevo software según un criterio dado. Las utilidades de administración de paquetes en CentOS 7 están preconfiguradas para utilizar tres de estos repositorios:

i. Base. Los paquetes que conforman un lanzamiento de CentOS, tal y como están en el disco.

ii. Actualizaciones. Versiones actualizadas de los paquetes proporcionados en Base.

iii. Extras. Paquetes para una variada gama de software adicional.

Las actualizaciones de CentOS, por lo general, mantienen una compatibilidad binaria con versiones anteriores.

Recuerde por lo tanto que deberá atender no solo a las especificaciones del fabricante en cuanto a las actualizaciones de seguridad, sino también a las actualizaciones que incluyen las mejoras de funcionalidad.

Nota: No es un objetivo de esta guía especificar los mecanismos o procedimientos necesarios para mantener los sistemas actualizados. Las plantillas de seguridad configuran las directivas adecuadas para que los sistemas operativos puedan ser actualizados empleando para ello el servicio de actualizaciones tanto del sistema operativo CentOS 7 Linux como del servidor de alojamiento de ficheros Nextcloud y todos los servicios LAMP asociados necesarios para su correcto funcionamiento.

1.1.2.3. OP. EXP. 6. PROTECCIÓN FRENTE A CÓDIGO DAÑINO

La organización para puestos de trabajo deberá implementar una solución antimalware que proteja contra código dañino. Se considerarán como tal los virus, gusanos, troyanos, programas espías y en general cualquier tipo de aplicación considerada como malware.

Debe tomarse en consideración que, aunque CentOS 7 Linux venga provisto de un Firewall y la opción de implementar SELinux, estos no cubren todo el espectro de protección frente a código dañino. Por ejemplo, sin una solución de administración central no tendrá la visibilidad para hacer la gestión centralizada de la seguridad y gestión de incidencias demandadas por el Esquema Nacional de Seguridad.

Adicionalmente este producto en sí mismo no ofrece un mecanismo de protección con administración centralizada, objetivo fundamental de toda organización no solo para centralizar los procesos de despliegue y configuración de políticas de protección, sino de la centralización de los estados y reportes de detección y eliminación de malware.

Las organizaciones deberán por lo tanto proveer de otra solución frente a código dañino que ofrezca un alcance completo en la detección y eliminación de malware, así como atender a las recomendaciones del fabricante para su mantenimiento.

1.1.2.4. OP. EXP. 8. REGISTRO DE ACTIVIDAD DE LOS USUARIOS

Aplicable en las categorías básicas, media y alta de seguridad, se deberán implementar mecanismos para garantizar la trazabilidad de las acciones de los usuarios. Para ellos se deberá conocer:

a) Quién realiza la actividad, cuándo la realiza y sobre qué.

b) Se incluirá la actividad de los usuarios y especialmente la de los operadores y administradores del sistema en cuanto pueden acceder a la configuración y actuar en el mantenimiento del mismo.

c) Deben registrarse las actividades realizadas con éxito, así como los intentos infructuosos.

d) La determinación de las actividades y con qué nivel de detalles, se determinará en base al análisis de riesgos que se haya realizado sobre el sistema.

e) La categoría alta requiere un sistema automatizado de recolección, consolidación y análisis de los registros de actividad.

Nextcloud 15 sobre CentOS 7 Linux, implementa mecanismos para la auditoría de los sistemas e infraestructuras. El problema consiste en que de forma predeterminada los datos son almacenados localmente como la utilidad Audit.

Adicionalmente el Servidor de alojamiento de archivos dispone de mecanismo que permiten emitir informes sobre todo aquello que se almacena, modifica o elimina en él pudiendo realizar seguimientos y acciones correspondientes.

1.1.2.5. OP. EXP. 10. PROTECCIÓN DE LOS REGISTROS DE ACTIVIDAD

En las categorías medias y altas se deberán implementar mecanismos orientados a la protección de los registros de actividad. Estas medidas deberán:

a) Determinar el período de retención de los registros.

b) Asegurar la fecha y hora.

c) Permitir el mantenimiento de los registros sin que estos puedan ser alterados o eliminados por personal no autorizado.

d) Las copias de seguridad, si existen, se ajustarán a los mismos requisitos.

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 se incluye una gran variedad de las mismas que son aplicables desde las más puramente procedimentales, a las puramente físicas o a las de aplicación técnica.

Solo estas últimas se tendrán en consideración para su implementación en la presente guía y de ellas solo un número limitado son de aplicación sobre las funcionalidades del propio sistema operativo servidor. La mayor parte de ellas son de aplicación 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 dispuestos todos aquellos mecanismos de control físico necesarios, con objeto evitar el acceso a los equipos de escritorio existentes por parte de personal no autorizado.

1.2.1. PROTECCIÓN DE LOS EQUIPOS

Las medidas de protección de los equipos cubren todos aquellos mecanismos que son necesarios para garantizar tanto una configuración de seguridad válida para el sistema, así como para mantener la propia privacidad del trabajo desarrollado.

Dentro de las medidas se articulan la aplicación de mecanismos de índole tecnológica y otras de tipo física. Entre estas últimas, pueden localizarse las correspondientes a un puesto de trabajo despejado.

Aunque esta guía de seguridad se encuentra orientada a un sistema operativo tipo servidor, se tiene en consideración aquellas medidas que, siendo establecidas para un puesto de trabajo, le son de completa aplicación, por ejemplo, la necesidad de realizar un bloqueo del puesto de trabajo.

1.2.1.1. MP. EQ. 2. BLOQUEO DE PUESTO DE TRABAJO

Aplicable desde la categoría media se establece la necesidad de realizar un bloqueo de la cuenta toda vez que se haya producido una inactividad en el sistema tras un tiempo prudencial. Dicho tiempo prudencial deberá ser establecido por política de seguridad.

Adicionalmente a todos aquellos sistemas de categoría alta, deberán cancelarse las sesiones abiertas, cuando se supere un tiempo de actividad superior al anteriormente planteado.

Estos controles serán aplicables a Linux mediante la configuración de módulos PAM (Pluggable Authentication Modules), ficheros de configuración local del equipo y mecanismos internos del servidor de alojamiento de archivos Nextcloud.

1.2.2. PROTECCIÓN DE LAS COMUNICACIONES

Los conjuntos de medidas orientadas a la protección de las comunicaciones tienen como objetivo la protección de la información en tránsito, así como dotar a los mecanismos para la detección y bloqueo de intrusos en una red.

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

Se deberá asegurar la autenticidad del otro extremo en un canal de comunicaciones antes de proceder al intercambio de datos entre los mismos. Además, deberá prevenirse ataques activos, garantizando que los mismos serán al menos detectados, permitiendo activarse los procedimientos que se hubieran previsto en el tratamiento frente a incidentes.

En aquellos sistemas que les sea de aplicación la categoría media, además de los mecanismos anteriores aplicables a la categoría básica, les será de aplicación la necesidad de implementar redes virtuales privadas cuando su comunicación se realice por redes fuera de la organización. Para ello se deberá tener en consideración los algoritmos que han sido acreditados por el Centro Criptológico Nacional.

Para aquellos entornos con sistemas o información catalogados como de categoría alta, es recomendable el empleo de dispositivos hardware para el establecimiento y utilización de redes virtuales privadas, frente a soluciones de tipo software. Se deberá tener en consideración los productos que se encuentran certificados y acreditados.

A través de controles centralizados en plantillas de seguridad, se establecerán mecanismos que controlen el acceso y salida de información a los puestos de trabajo mediante el empleo del firewall en su modalidad avanzada. Aunque se tratará en extensión en un anexo de la presente guía, el operador podrá conocer todos los detalles de esta solución a través de la información que proporciona el fabricante. https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-using_firewalls

Nota: Aunque se proporciona una configuración base de firewalld de CentOS 7 con la presente guía, el administrador deberá aplicar y gestionar los perfiles y reglas del firewall acorde a las necesidades de su organización, prevaleciendo como regla primordial la mínima exposición hacia el exterior del equipo que se configura.

Además, se establecerán configuraciones relativas a la protección de la autenticación, habilitando solo aquellos protocolos que son válidos y seguros.

1.2.3. PROTECCIÓN DE LA INFORMACIÓN

Conjunto de procesos y medidas para un correcto uso y salvaguarda de los datos de carácter personal identificados en el sistema.

1.2.3.1. MP. INFO. 3. CIFRADO

Se debe asegurar la integridad de la información con una categoría alta de confidencialidad cifrada tanto durante su almacenamiento como durante su transmisión

Solo será visible en claro dicha información cuando se esté realizando uso de ella.

La presente guía establece mecanismos a través de Nextcloud para garantizar el cifrado de los datos existentes en el servidor de alojamiento de ficheros.

Las políticas y configuraciones en la presente guía establecen la implementación de los algoritmos más seguros posibles que garanticen la integridad y confidencialidad de los datos transmitidos dentro de la red de área local.

Deberá adicionalmente aplicar mecanismos que garanticen el cifrado de comunicaciones cuando acceda a servicios e información de la organización de forma remota cuando esté fuera de ella.

2. RESUMEN Y APLICACIÓN DE MEDIDAS EN NEXTCLOUD 15

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 aplicación de políticas de seguridad a nivel local o bien de la configuración de ficheros del sistema.

Control	Medida	Mecanismo de aplicación
OP. ACC. 1	Segregación de roles y tareas	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
OP. ACC. 1	Auditoría y supervisión de actividad	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.

Control	Medida	Mecanismo de aplicación
OP. ACC. 4	Gestión de derechos de acceso	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización
OP. ACC. 4	Control de cuentas de usuario	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización
OP. ACC. 5	Política de contraseñas	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización
OP. ACC. 5	Protocolos de autenticación local	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización
OP. ACC. 6	Bloqueo de cuentas	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización
OP. ACC. 7	Protocolos de autenticación en red	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización. Configuraciones adicionales de seguridad descritas a través de la presente guía.
OP. EXP. 2	Control de funcionalidad de servicios para garantizar el principio de mínima funcionalidad	Revisión de ficheros de configuración del sistema descritos en la presente guía.
OP. EXP. 2	Protección de aplicaciones de sistema para garantizar el principio de mínima funcionalidad.	Revisión de ficheros de configuración del sistema descritos en la presente guía.
OP. EXP. 4	Mantenimiento del Sistema Operativo, servidor de alojamiento de ficheros y servicios necesarios del mismo.	Configuraciones adicionales descritas a través de la presente guía. Deberá implementar mecanismos en su organización para garantizar la actualización de los sistemas y aplicaciones.
OP. EXP. 6	Protección frente a código dañino	La organización deberá emplear una solución adicional a las configuraciones que proporciona Nextcloud y CentOS 7 Linux por no cubrir este los mínimos exigidos por el ENS para la protección frente a código dañino.

Control	Medida	Mecanismo de aplicación
OP. EXP. 8	Registro de actividad de los usuarios	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde la categoría básica.
OP. EXP. 10	Protección de los registros de actividad	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización. Se debe tomar en consideración que el RD 951/2015 cambia la medida con respecto a lo establecido en RD 3/2010. En la actualidad el requisito del registro de actividad es requerido desde la categoría básica.
MP. EQ. 2	Bloqueo de los puestos de trabajo	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización
MP. COM. 3	Protección del sistema mediante implementación de firewall.	Configuraciones descritas a través de la presente guía. Implementación de configuración de firewall a nivel local.
MP. COM. 3	Protección de la autenticación.	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización.
MP. INFO. 3	Cifrado	Revisión e implementación de mecanismos articulados en la presente guía adaptándolos a la organización

ANEXO A.2. INSTALACIÓN DE LA APLICACIÓN Y REQUISITOS ESPECÍFICOS

1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE NEXTCLOUD 15

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 Nextcloud 15 independientemente de la categorización, 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 la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría básica, media o alta, 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.

Los pasos que se describen a continuación se realizarán en todos aquellos servidores Nextcloud sobre CentOS 7.4 Linux, independientes a un dominio, que se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

Este anexo ha sido diseñado para ayudar a los operadores a implementar las distintas configuraciones de seguridad. A continuación, se describe, paso a paso, como realizar la instalación y configuración de seguridad de un servidor de alojamiento de ficheros Nextcloud independiente de un dominio.

Antes de empezar deberán tenerse en cuenta las siguientes recomendaciones:

a) Todos los discos y particiones deberán encontrarse formateados utilizando el sistema de archivos XFS.

b) Se parte de un sistema operativo CentOS 7.4 Linux instalado según “ANEXO A.2. INSTALACIÓN DEL S.O. CONFIGURACIÓN SEGURA DEL GUI” de la guía codificada como “CCN-STIC-619”.

c) Es importante separar datos, aplicaciones y sistema operativo en distintos dispositivos de almacenamiento, tanto para mejorar el rendimiento como para evitar ataques que se realizan navegando entre directorios. Para la seguridad de un servidor con Nextcloud no se requiere la existencia de particiones más allá de las que vienen por defecto, pero se deberá tener en cuenta durante el proceso de instalación, ya que existen ciertas configuraciones y permisos para los cuales se requiere que existan estas particiones diferenciadas.

d) Si existen datos en el servidor antes del proceso de instalación, deberán eliminarse antes de comenzar el proceso.

e) No deberán realizarse actualizaciones desde versiones previas, ya que de lo contrario no podrá garantizarse que los valores por defecto de los parámetros de seguridad se hayan aplicado.

f) No utilizar discos o particiones que utilicen el sistema de archivos FAT.

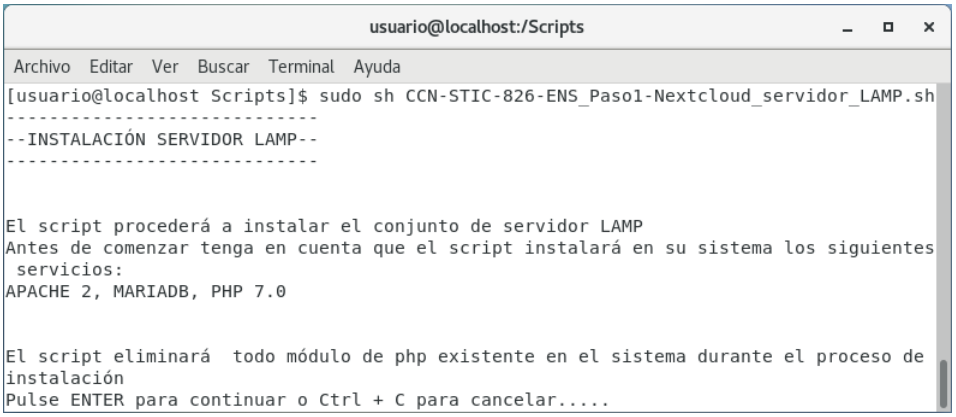
g) No instalar otros sistemas operativos en el equipo.

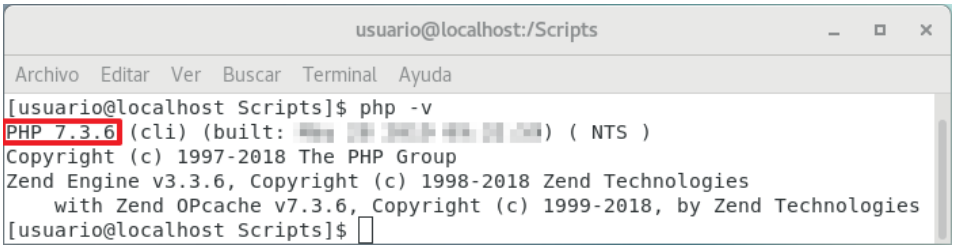
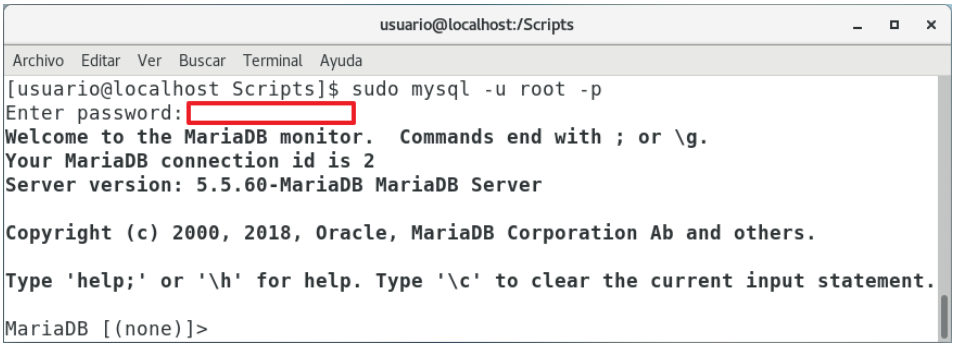
h) Asignar una contraseña compleja a la cuenta de usuario que se crea durante el proceso de instalación.

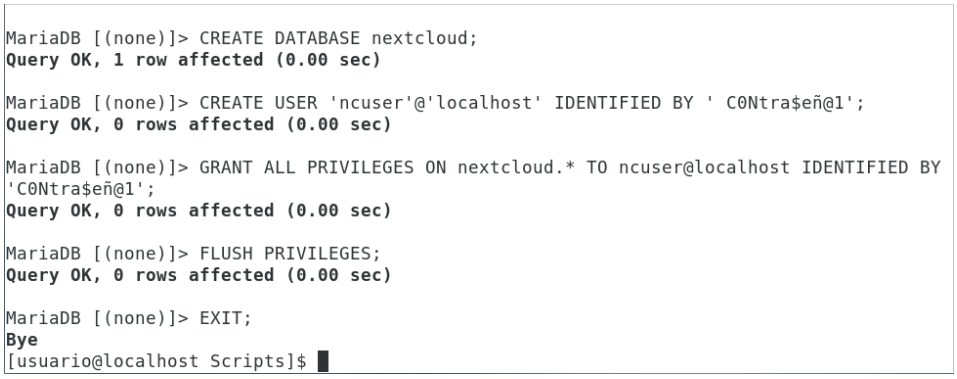
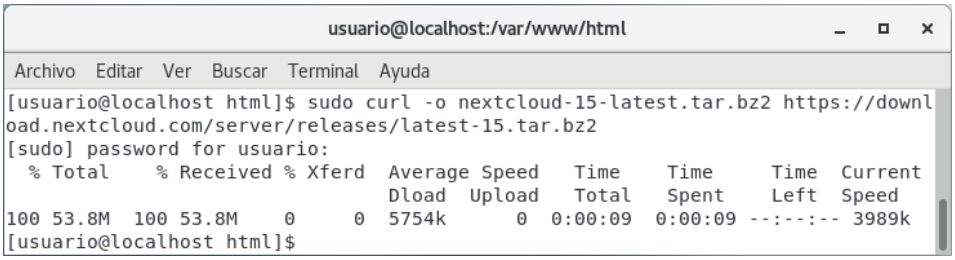
i) Una vez finalizada la instalación básica del sistema, asegurarse de que se instalan todas las actualizaciones de seguridad necesarias. Idealmente estas actualizaciones de seguridad se instalarán antes de conectar el equipo a la red o con el equipo conectado a una red segura.

El primer grupo de las acciones hace referencia a la instalación del sistema operativo sobre un equipo, eligiendo las opciones por defecto, tal y como se indica a continuación.

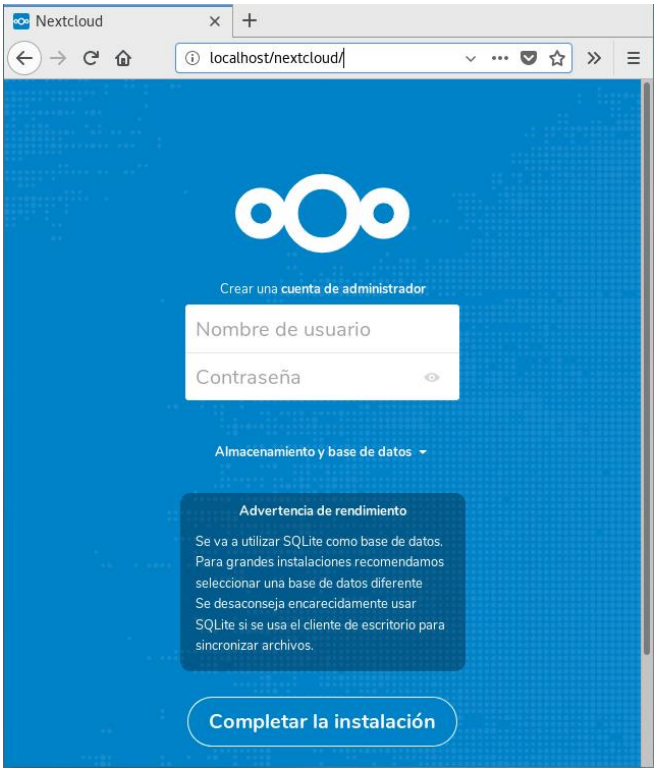
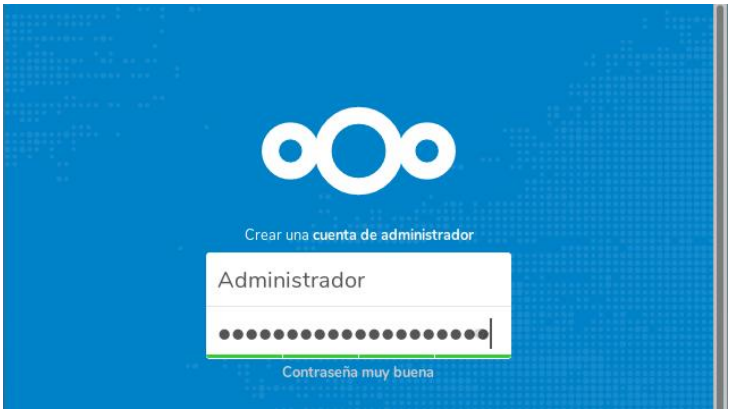
Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va a instalar Nextcloud según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o "Sudoers".
3.	Cree el directorio "**Scripts**" en "**/**" y copie aquí el contenido de la carpeta asociada a la categorización del equipo desde el medio de almacenamiento correspondiente. Deberá asignarles los permisos pertinentes para la ejecución de los mismos.
4.	Diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "Terminal". 

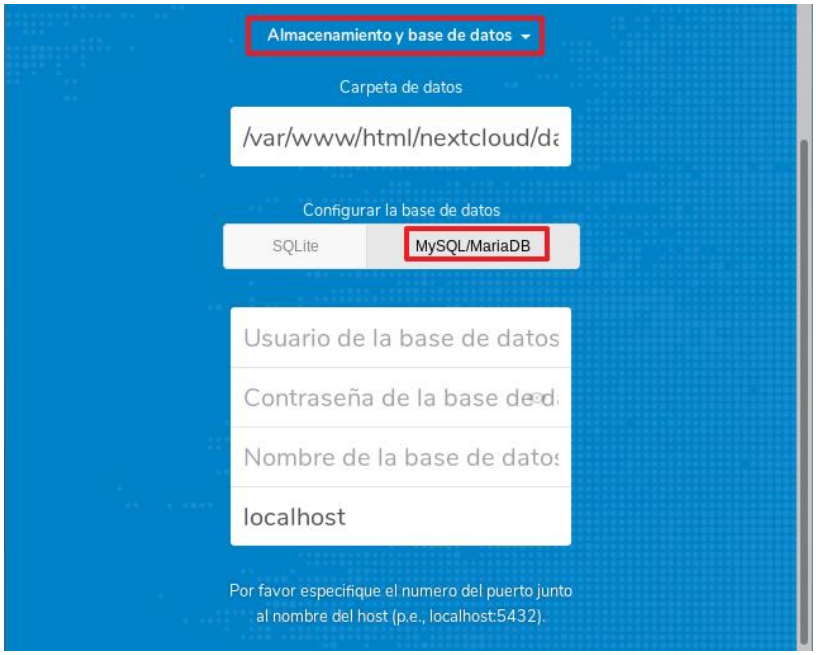
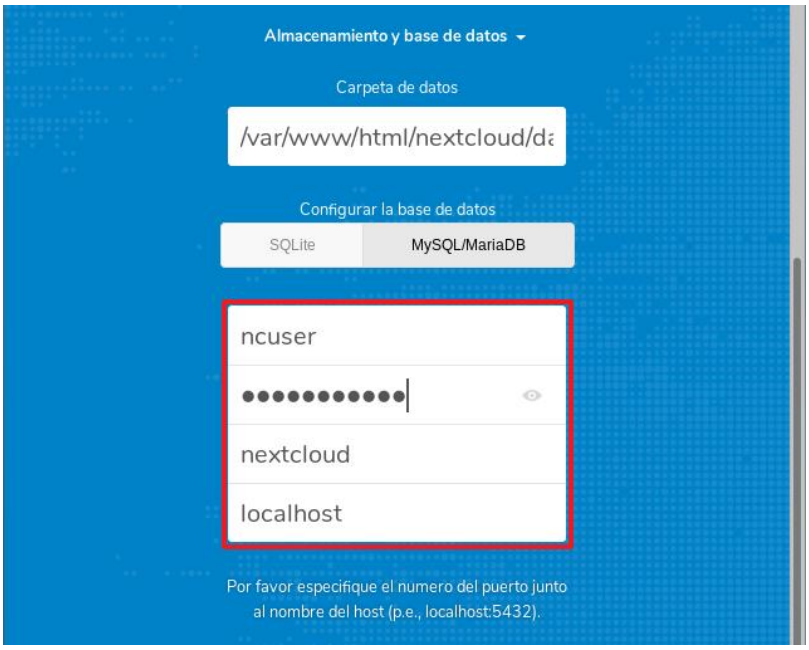
Paso	Descripción
5.	Se procederá a instalar los servicios previos para el funcionamiento del servidor de Nextcloud. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts** Ejecute el siguiente comando. **$ sudo sh CCN-STIC-826-ENS_Paso1-Nextcloud_servidor_LAMP.sh**  **Nota:** Realice un estudio para determinar aplicaciones o servicios que puedan ser incompatibles con la configuración actual de su servidor antes de proceder a la instalación.
6.	Pulse "Enter" cuando se lo indique para continuar. El proceso puede durar varios minutos.
7.	El script iniciará un proceso de instalación de servicios necesarios para el correcto funcionamiento de Nextcloud. Además, eliminará la totalidad de los módulos php instalados en el sistema. **Nota:** Tenga en cuenta que el script instala los siguientes servicios: - Apache2: Servidor Web - MariaDB: Servidor de Base de Datos - PHP 7.0: Lenguaje de código abierto interactuando entre ambos. Si por necesidades de su organización se necesita configurar distintos servidores como nginx o PostgreSQL, deberá adaptar el script para tal efecto. Por el contrario, si decide utilizar los servidores recomendados por esta guía ha de saber que es posible que, por decisiones de la comunidad ajenas a esta guía los repositorios pueden variar su ubicación, debiendo adaptar éstos con las nuevas direcciones disponibles.
8.	Para instalar la versión más actualizada de los servidores Apache, MariaDB y PHP el script instalará el repositorio Remi en el sistema. **Nota:** Remi provee versiones actualizadas de los componentes del stack LAMP en las siguientes distribuciones y versiones: - CentOS 6/7 - RHEL 6/7 - Fedora 23/24/25/26.

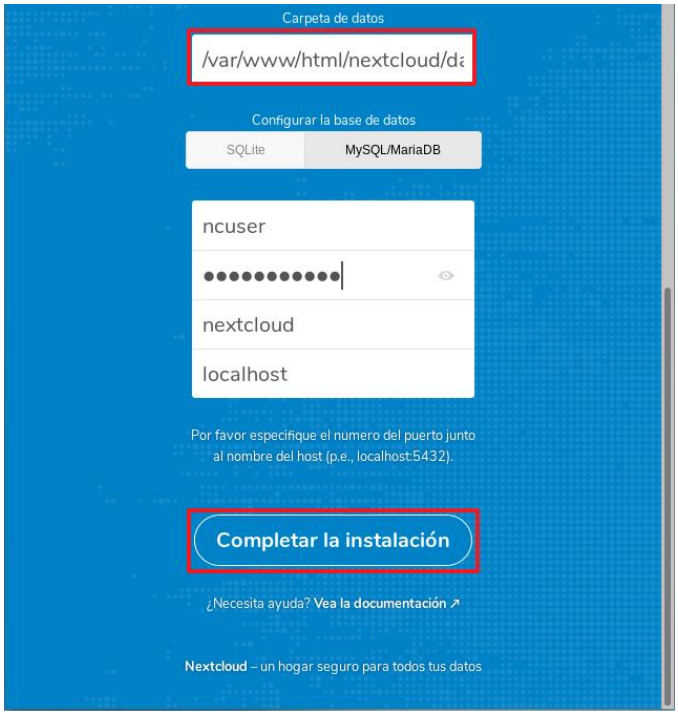
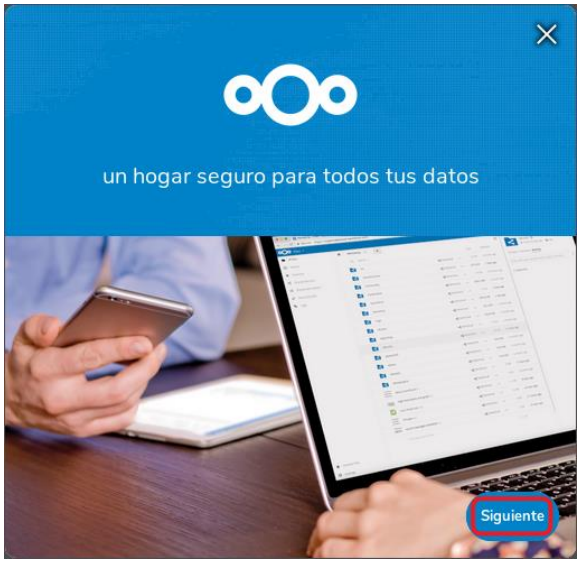
Paso	Descripción
9.	Es script finalizará mostrando la versión actual de php en el sistema. 
10.	Posteriormente se procederá a configurar la base de datos que utilizará Nextcloud. Para ello ejecute los siguientes comandos: **$ sudo systemctl start mariadb.service** **$ sudo systemctl enable mariadb.service**
11.	Una vez iniciado el servicio de base de datos MariaDB, ejecute el siguiente comando para acceder al servidor: **$ sudo mysql -u root -p**
12.	Cuando se le solicite contraseña, pulse “Enter” sin escribir ningún carácter, ya que la base de datos MariaDB por defecto no configura contraseña. 

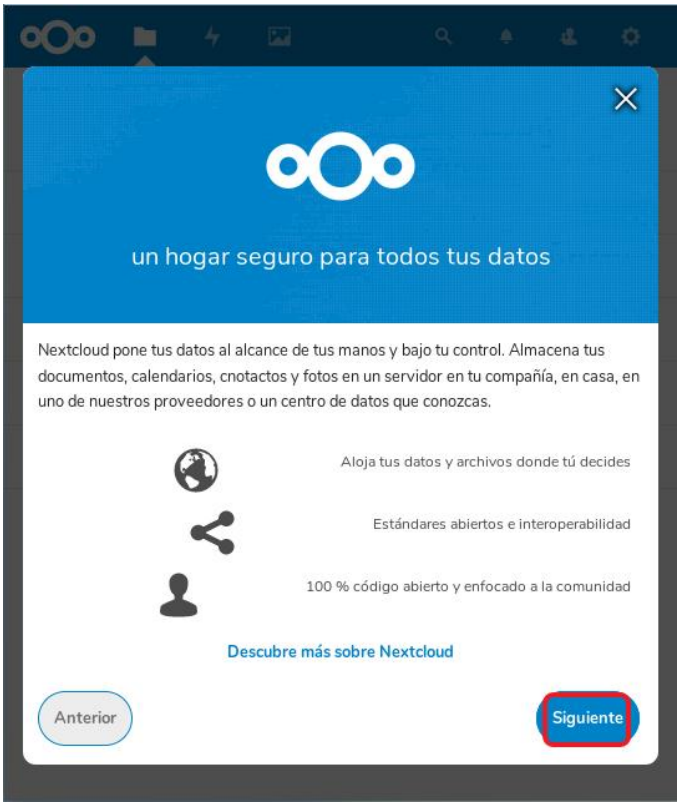
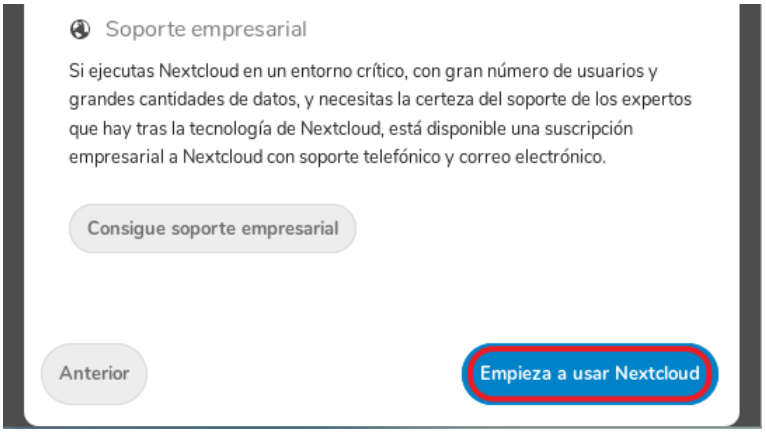
Paso	Descripción
13.	Una vez dentro del servidor, ejecute los siguientes parámetros modificando los aquellos en color rojo con las necesidades específicas de su organización: **mysql> CREATE DATABASE nextcloud;** **mysql> CREATE USER 'ncuser'@'localhost' IDENTIFIED BY ' C0Ntra$eñ@1';** **mysql> GRANT ALL PRIVILEGES ON nextcloud.* TO ncuser@localhost IDENTIFIED BY 'C0Ntra$eñ@1';** **mysql> FLUSH PRIVILEGES;** **mysql> EXIT;**  **Nota:** Los parámetros en color rojo se deben de modificar de manera que se eviten configuraciones por defecto y con los parámetros de seguridad necesarios. Si no tiene conocimientos sobre administración de MariaDB puede informarse en la siguiente URL: https://mariadb.org/
14.	Posteriormente diríjase a la dirección local donde vaya a instalar el servidor Nextcloud **$ cd /var/www/html**
15.	Si posee la herramienta **curl** ejecute el siguiente comando, ingrese la contraseña de superusuario si se la solicita: **$ sudo curl -o nextcloud-15-latest.tar.bz2 https://download.nextcloud.com/server/releases/latest-15.tar.bz2**  Si no posee la herramienta curl, inicie su navegador e ingrese la siguiente dirección para comenzar la descarga: https://download.nextcloud.com/server/releases/latest-15.tar.bz2 **Nota:** Tenga en cuenta que la descarga del archivo de instalación por medio del explorador deberá moverlo a la ubicación destinada para la instalación del servido.

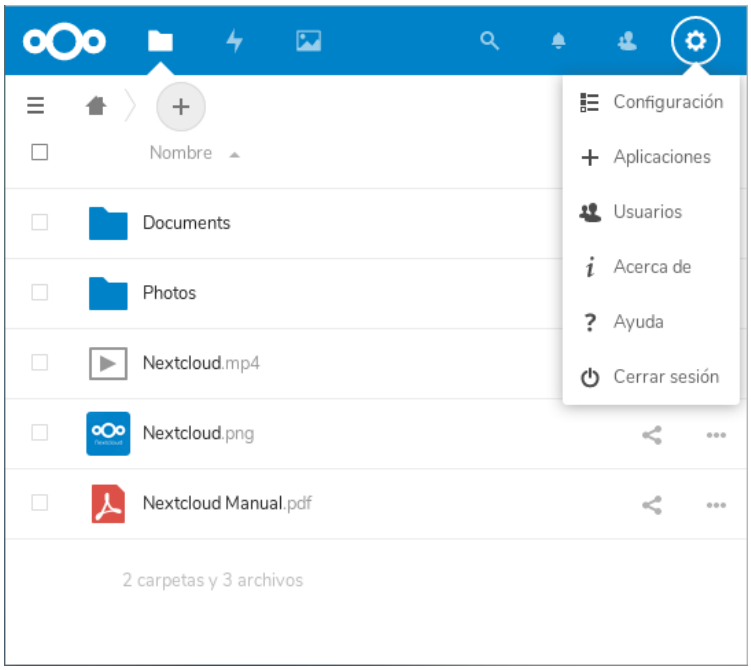
Paso	Descripción
16.	Descomprima el archivo que contiene la última versión de Nextcloud por medio del siguiente comando: **$ sudo tar -xvjf nextcloud-15-latest.tar.bz2** Compruebe que se ha descomprimido sin errores y elimine el fichero comprimido "**nextcloud-15-latest.tar.bz2**".
17.	Cree el directorio que contendrán los datos en el servidor de alojamiento de archivos Nextcloud por medio del siguiente comando: **$ sudo mkdir nextcloud/data** **Nota:** Antes de crear el directorio asegúrese que se encuentra en la ruta definida para la instalación del servidor, por defecto "/var/www/html".
18.	Cambie el propietario de la carpeta del servidor. Para ello ejecute el siguiente comando: **$ sudo chown -R apache:apache nextcloud** **Nota:** El propietario dependerá del servidor web que utilice en la instalación, si hubiera elegido uno distinto deberá sustituir "apache:apache" por el usuario creado por el servidor elegido.
19.	Ahora se procederá a configurar el servidor Apache con la configuración mínima que permita el visualizado y configuración del servidor Nextcloud. Para ello ejecute el siguiente comando: **$ sudo gnome-text-editor /etc/httpd/conf.d/nextcloud.conf &>/dev/null**
20.	Se abrirá un documento vacío con el editor de textos "gedit", introduzca las siguientes líneas dentro, tenga en cuenta que deberá modificar los caracteres en rojo con la dirección local que corresponda a la instalación de su servidor: **Alias /nextcloud "/var/www/html/nextcloud/"** **<Directory /var/www/html/nextcloud/>** **Options +FollowSymlinks** **AllowOverride All** **<IfModule mod_dav.c>** **Dav off** **</IfModule>** **SetEnv HOME /var/www/html/nextcloud** **SetEnv HTTP_HOME /var/www/html/nextcloud** **</Directory>** Al finalizar pulse "Guardar" y cierre el editor.
21.	Reinicie el servicio para que los cambios tengan efecto. Revise que se reinicia el servicio sin errores. **$ sudo systemctl restart httpd.service**

Paso	Descripción
22.	Diríjase a un navegador web e ingrese la siguiente URL: http://localhost/nextcloud  **Nota:** Si se deniega el acceso al servidor revise la configuración de SELinux o desactívelo momentáneamente con el siguiente comando: - $ sudo setenforce 0
23.	En el campo “Crear una cuenta de administrador” ingrese el nombre de usuario para el nuevo administrador del servidor y una contraseña que cumpla con los requisitos de seguridad exigidos. 

Paso	Descripción
24.	Posteriormente despliegue el campo “Almacenamiento y base de datos” pulsando sobre él y posteriormente seleccione MySQL/MariaDB. 
25.	Rellene estos campos con los parámetros definidos en el punto 13 de este mismo apartado. 

Paso	Descripción
26.	Por último, compruebe que la ruta del apartado “Carpeta de datos” coincide con la ruta local donde se ha creado la carpeta de /datos dentro del directorio de instalación de Nextcloud. Posteriormente pulse el botón “Completar la instalación” en la parte inferior de la pantalla. 
27.	El servidor procederá a la creación de datos del inicio y entradas en la base de datos, operación que puede demorarse unos minutos. Al finalizar se mostrará la pantalla de bienvenida, pulse en “Siguiente” para continuar. 

Paso	Descripción
28.	El servidor irá ofreciendo distintas pantallas de bienvenida con explicaciones sobre el funcionamiento del servidor y enlaces útiles. Si no está familiarizado con este tipo de servidores se recomienda leer la documentación. Pulse “Siguiente” para continuar o cierre la ventana pulsando en el icono “X” en la parte superior derecha para finalizar. 
29.	Si ha continuado con el asistente al llegar a la última pantalla pulse “Empieza a usar Nextcloud” para continuar. 

Paso	Descripción
30.	Finalmente se mostrará el entorno de navegación mediante Web del servidor de alojamiento Nextcloud con ejemplos de carpetas y archivos para probar su funcionamiento. 

ANEXO A.3. CATEGORÍA BÁSICA

ANEXO A.3.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES NEXTCLOUD 15 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS

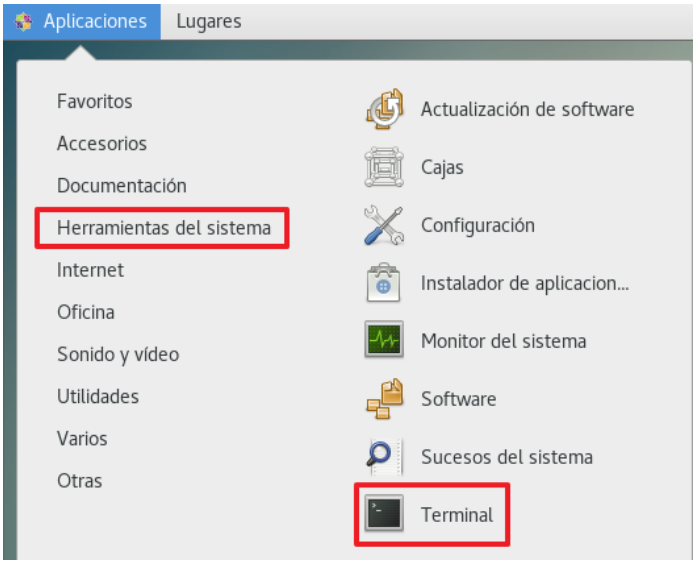
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de alojamiento de archivos Nextcloud 15 sobre Sistema Operativo CentOS 7.4 Linux con una categorización de seguridad básica según los criterios 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 la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. 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.

Los pasos que se describen a continuación se realizarán en todos aquellos servidores de alojamiento de archivos Nextcloud 15 sobre Sistema Operativo CentOS 7.4 Linux con categoría básica aplicada según guía CCN-STIC-619, independientes a un dominio, que implementen servicios o información de categoría básica y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

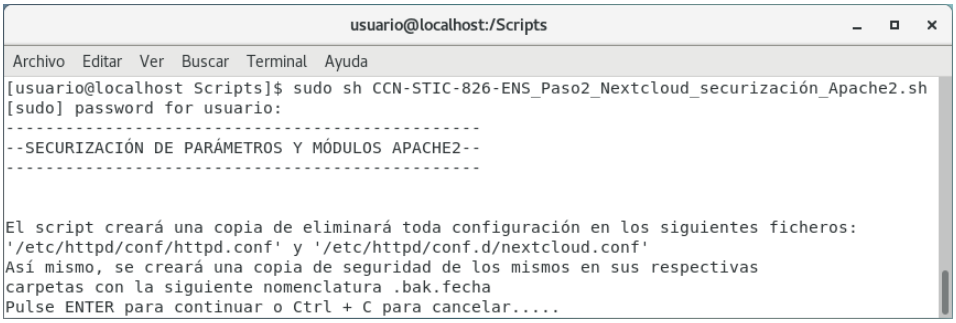
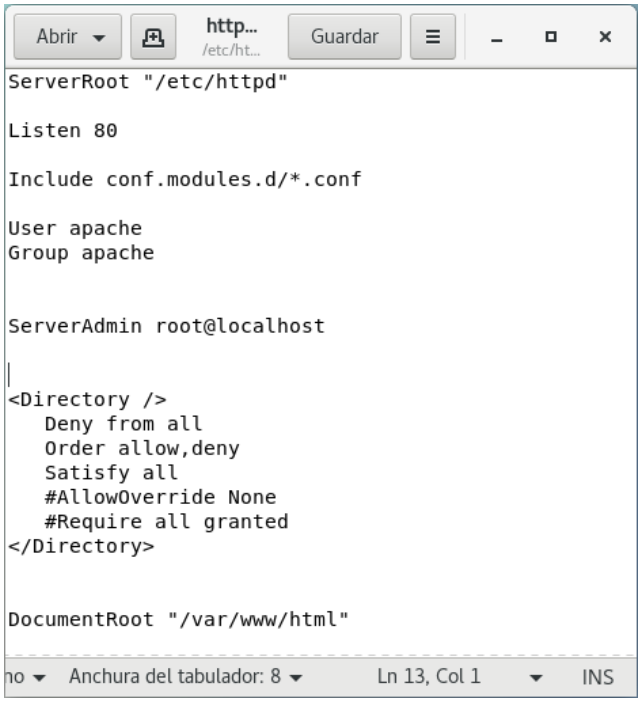
1. CONFIGURACIÓN SEGURA DE APACHE, PHP Y MARIADB PARA NEXTCLOUD

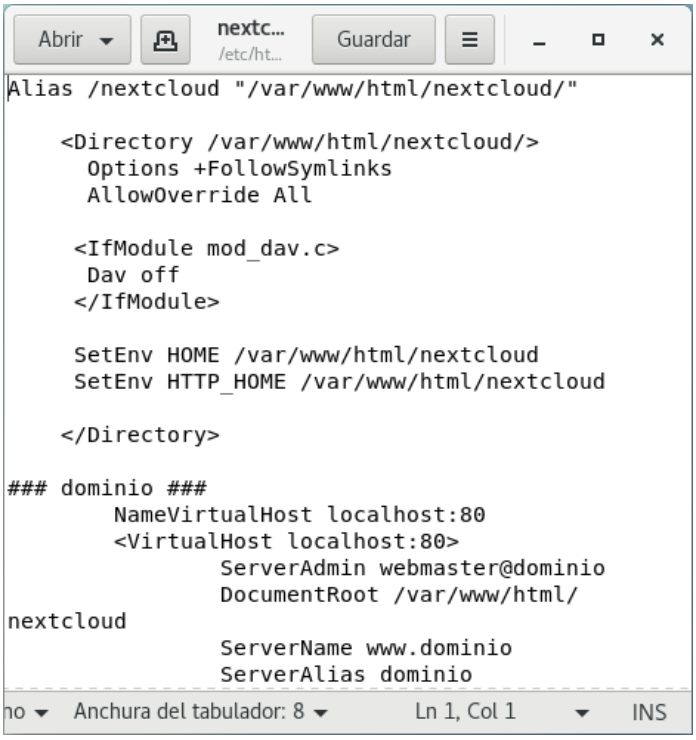
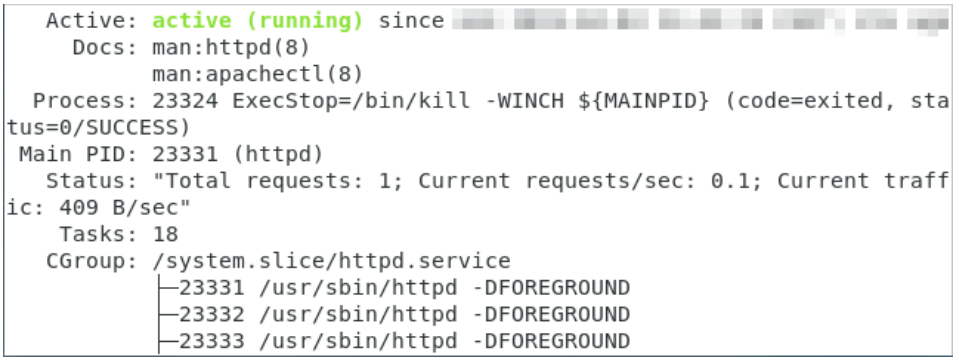
Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va a instalar Nextcloud según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o “Sudoers”.
3.	Cree el directorio **“Scripts”** en “/” y copie aquí el contenido de la carpeta asociada a la categorización del equipo desde el medio de almacenamiento correspondiente. Deberá asignarles los permisos pertinentes para la ejecución de los mismos.

Paso	Descripción
4.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
5.	Ejecute el comando “cd /Scripts/” y pulse la tecla “Enter”.
6.	Posteriormente ejecute “ls -l” y compruebe que están todos los scripts.

1.1. APACHE 2

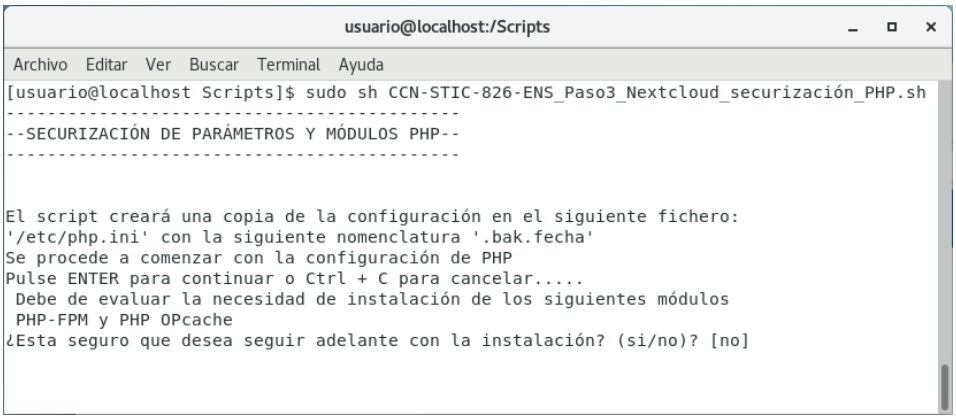
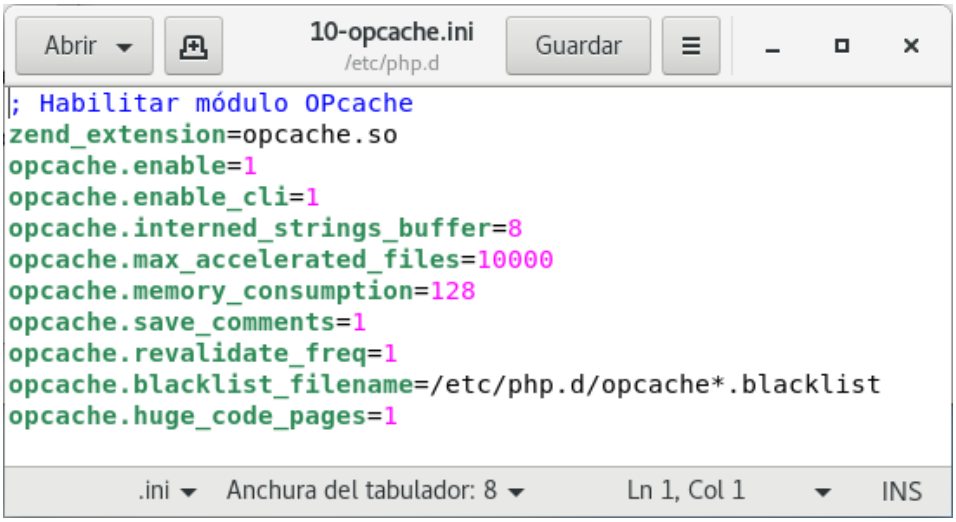
Paso	Descripción
7.	Si ha cerrado la “**Terminal** “en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “**Terminal**”. Ejecute el comando **“cd /”** y pulse la tecla “Enter”.
8.	Se procederá a securizar el servidor web Apache. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts**

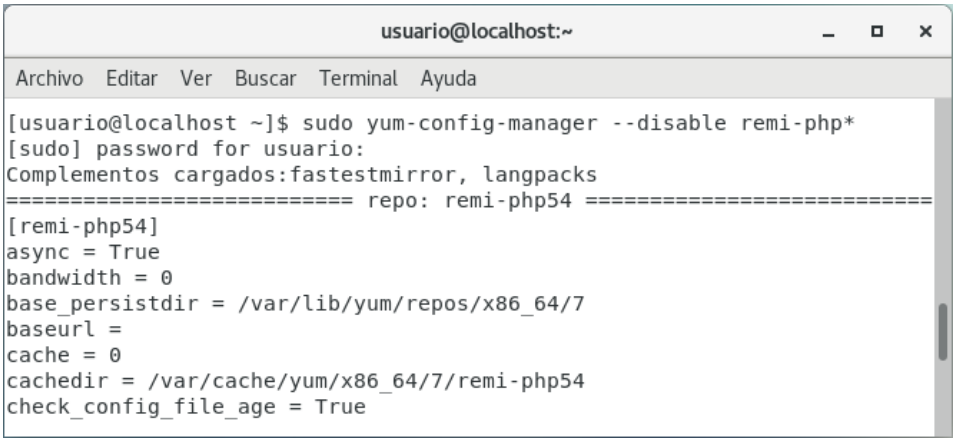
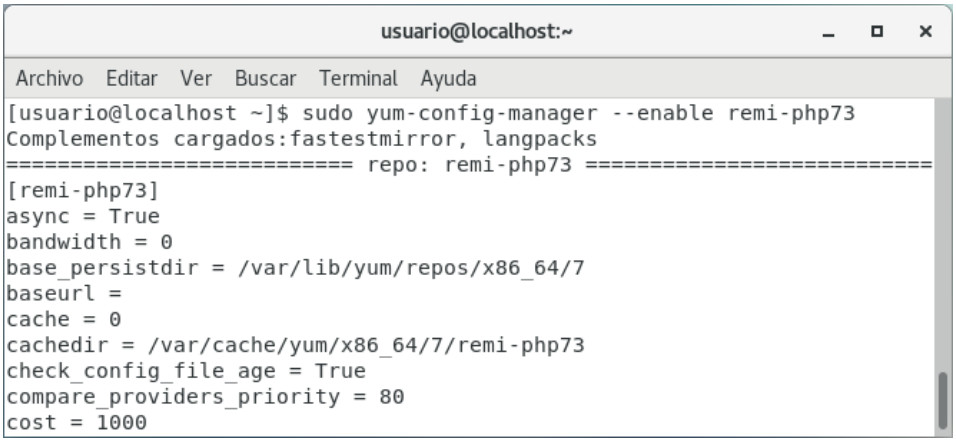
Paso	Descripción
9.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-826-ENS_Paso2_Nextcloud_securización_Apache2.sh** El script iniciará un proceso de instalación de los módulos “mod_security” y “mod_evasive” de Apache. Además, modificará los ficheros de configuración “/etc/httpd/conf/httpd.conf” y “/etc/httpd/conf.d/nextcloud.conf” eliminando toda configuración contenida en los mismos.  **Nota:** Tenga en cuenta que el script configura parámetros en rutas por defecto, si escoge un servidor web que no sea apache deberá adaptar el script a las necesidades específicas de su organización.
10.	El script mostrará el fichero “/etc/httpd/conf/httpd.conf” con una configuración aplicada con ejemplos y líneas comentadas (#) que deberá revisar y ajustar con los parámetros que más convengan a su organización. Cuando finalice pulse “Guardar” y cierre el editor de textos. 

Paso	Descripción
11.	Posteriormente el script mostrará el fichero "/etc/httpd/conf.d/nextcloud.conf" con una configuración aplicada con ejemplos y líneas comentadas (#) que, del mismo modo, deberá revisar y ajustar con los parámetros que más convengan a su organización. Cuando finalice pulse "Guardar" y cierre el editor de textos. 
12.	Finalmente compruebe que el servicio se ha reiniciado correctamente 

1.2. PHP

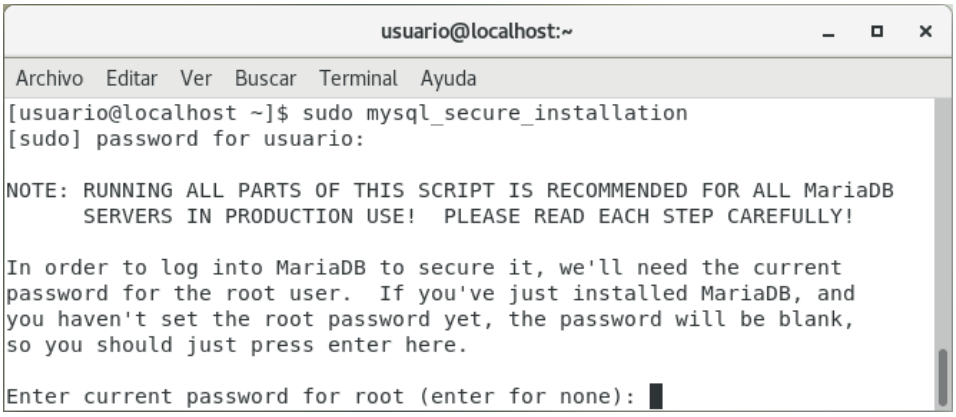
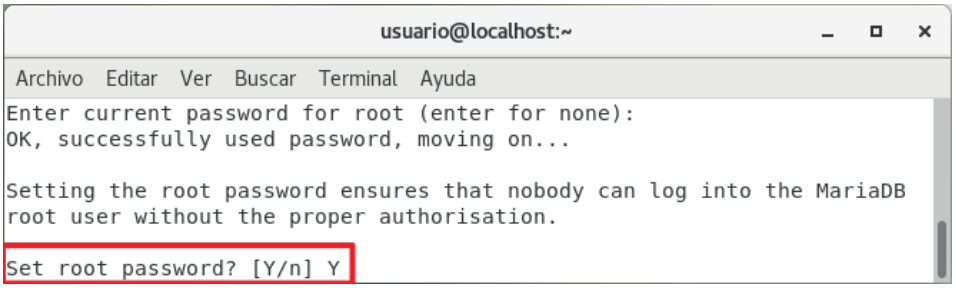
Paso	Descripción
13.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".

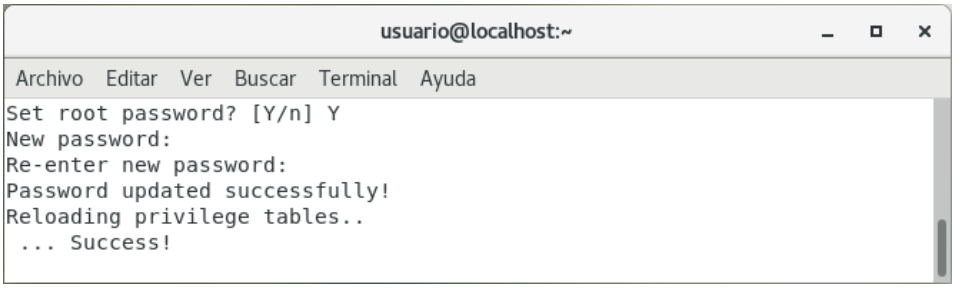
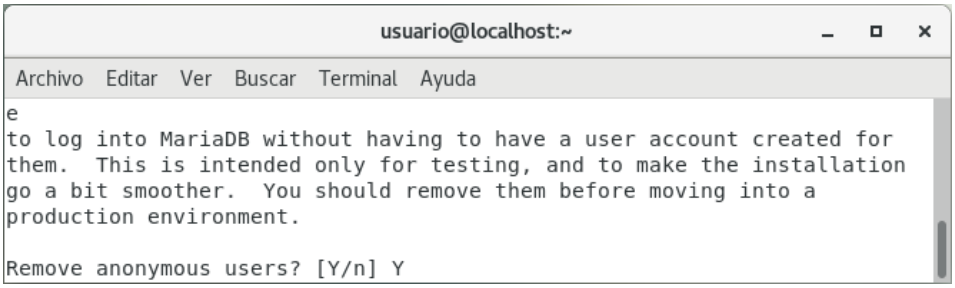
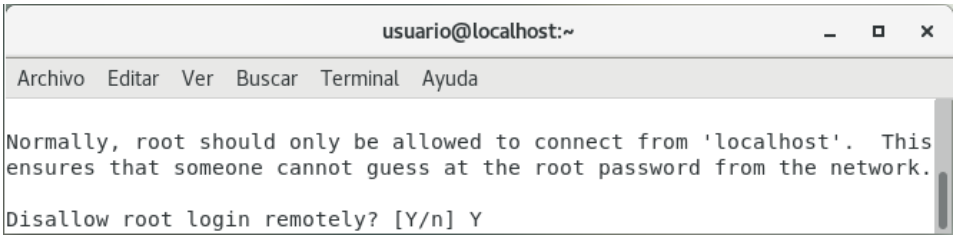
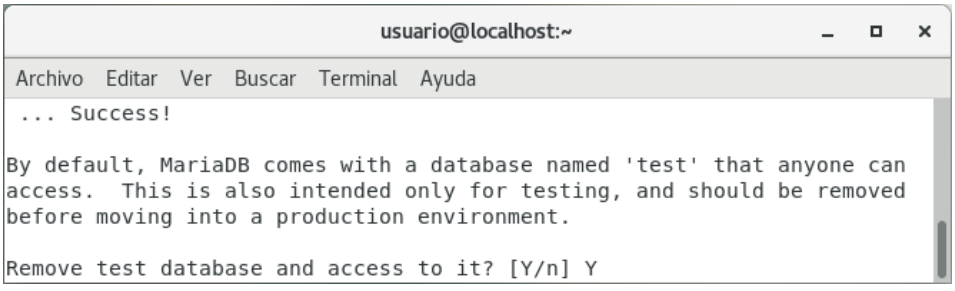
Paso	Descripción
14.	Se procederá a securizar el servicio PHP. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts**
15.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-826-ENS_Paso3_Nextcloud_securización_PHP.sh** Deberá evaluar la necesidad de los siguientes módulos “PHP-FPM” y “PHP OPcache” de PHP. El script le preguntará sobre las acciones al respecto, si los módulos son adecuados para su organización escriba “si” y pulse “Enter” para continuar con la instalación, si por el contrario no son necesarios escriba “no” y pulse “Enter” y el script finalizará.  usuario@localhost:/Scripts Archivo Editar Ver Buscar Terminal Ayuda [usuario@localhost Scripts]$ sudo sh CCN-STIC-826-ENS_Paso3_Nextcloud_securización_PHP.sh --SECURIZACIÓN DE PARÁMETROS Y MÓDULOS PHP-- El script creará una copia de la configuración en el siguiente fichero: '/etc/php.ini' con la siguiente nomenclatura '.bak.fecha' Se procede a comenzar con la configuración de PHP Pulse ENTER para continuar o Ctrl + C para cancelar..... Debe de evaluar la necesidad de instalación de los siguientes módulos PHP-FPM y PHP OPcache ¿Esta seguro que desea seguir adelante con la instalación? (si/no)? [no] **Nota:** El módulo PHP-FPM mejora notablemente la velocidad en servidores web de alto tráfico y OPcache mejora el rendimiento de PHP almacenando el código de bytes de un script precompilado en la memoria compartida, eliminando así la necesidad de que PHP cargue y analice los script en cada petición.
16.	Si ha escrito “si” el script proseguirá instalando los módulos y mostrando la configuración del fichero “/etc/php.d/10-opcache.ini” para su revisión. Se deben configurar los parámetros que más convengan a su organización.  Abrir 10-opcache.ini /etc/php.d Guardar ; Habilitar módulo OPcache zend_extension=opcache.so opcache.enable=1 opcache.enable_cli=1 opcache.interned_strings_buffer=8 opcache.max_accelerated_files=10000 opcache.memory_consumption=128 opcache.save_comments=1 opcache.revalidate_freq=1 opcache.blacklist_filename=/etc/php.d/opcache*.blacklist opcache.huge_code_pages=1 .ini Anchura del tabulador: 8 Ln 1, Col 1 INS Cuando finalice de configurar, pulse el botón “Guardar” y cierre el editor de texto.

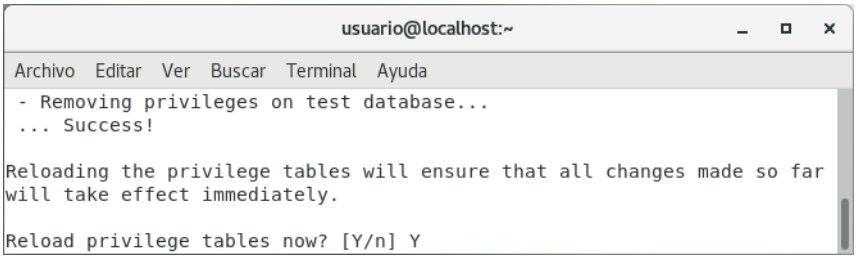
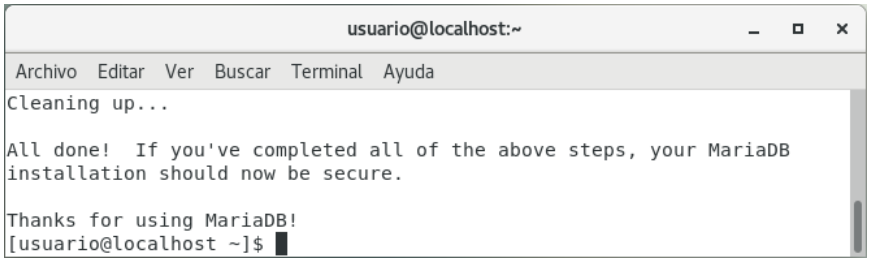
Paso	Descripción
17.	El servidor Apache se reiniciará, compruebe que se reinicia sin errores.
18.	Posteriormente se procederá a la actualización de php por medio del repositorio "remi". Para ello deshabilite los repositorios activos de php ejecutando el siguiente comando: **$ sudo yum-config-manager --disable remi-php*** 
19.	Ahora habilite el repositorio correspondiente a la versión de php más actualizada soportada por el sistema operativo y en versión estable. **$ sudo yum-config-manager --enable remi-phpXX[1]**  **Nota:** Si desea saber la versión que más se ajusta con las necesidades de su organización diríjase al siguiente enlace: https://www.php.net/
20.	Por último, ejecute el siguiente comando para actualizar el sistema por completo y que se aplique versión actualizada de php: **$ sudo yum -y update**

[1] Deberá adaptar la ejecución según la versión PHP a utilizar.

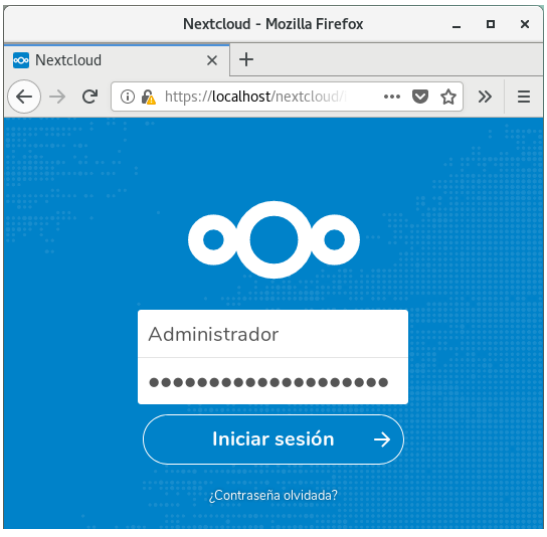
1.3. MARIADB

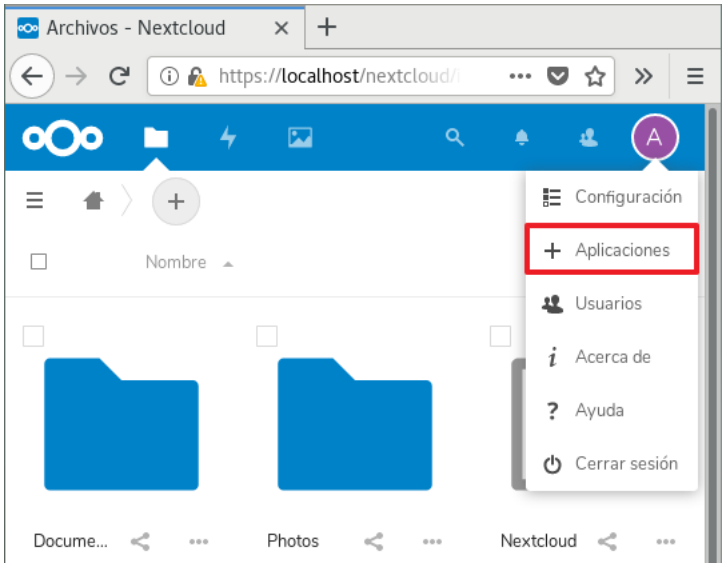
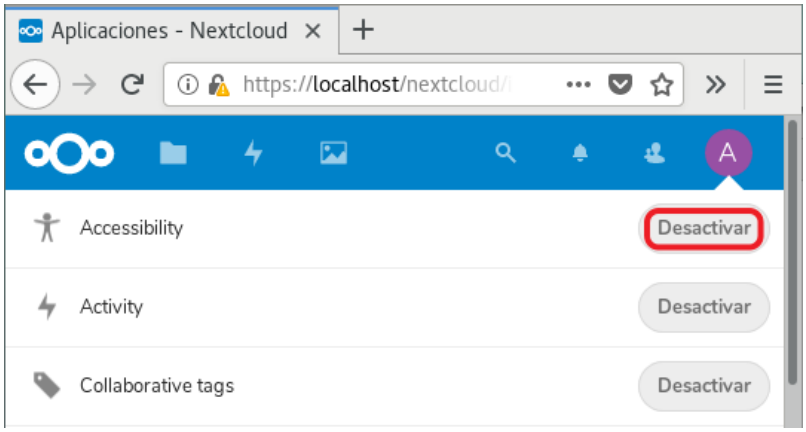
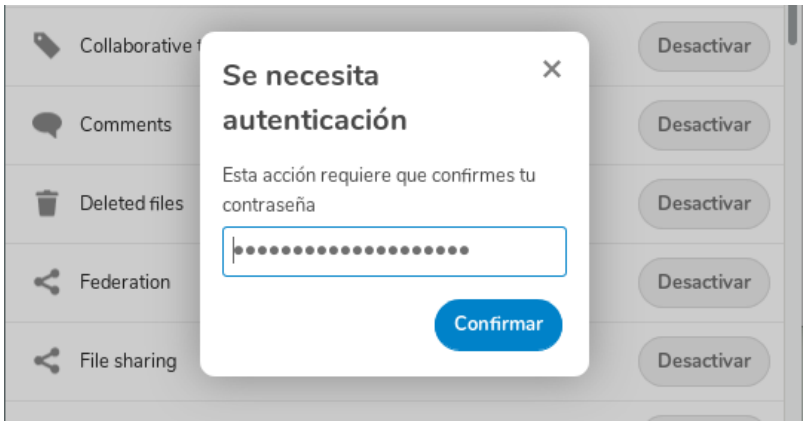
Paso	Descripción
21.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
22.	Se aplicarán medidas de seguridad en el servidor de Base de Datos MariaDB. Para ello ejecute el siguiente comando: **$ sudo mysql_secure_installation**
23.	En primer lugar, pedirá la contraseña del usuario "root", ingrese la contraseña y si no se ha configurado aún la misma deje el campo vacío y pulse "Enter" para continuar. 
24.	Posteriormente se preguntará si se quiere configurar una contraseña para "root", conteste con "Y" y pulse "Enter". 

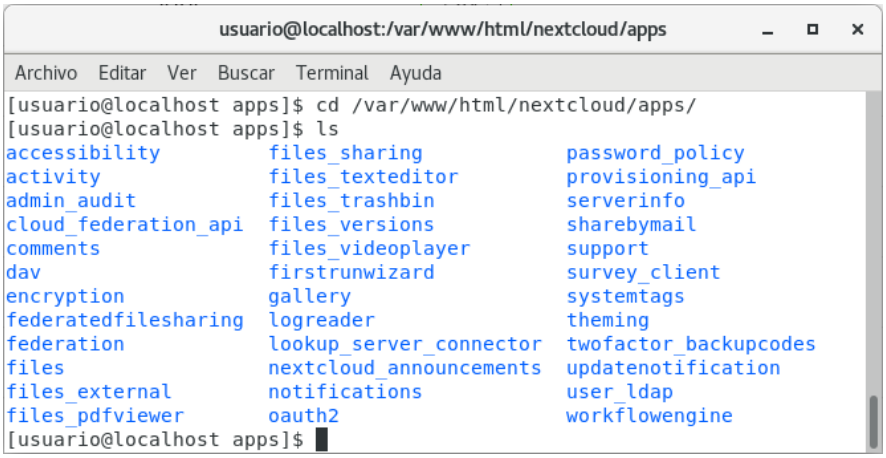
Paso	Descripción
25.	Escriba la nueva contraseña de “Root”, pulse “Enter” y vuelva a escribirla pulsando de nuevo “Enter” para continuar.  **Nota:** Tenga en cuenta, que el usuario “root” de la base de datos, es independiente al usuario “root” del sistema, por lo que las contraseñas difieren. Se deberá configurar la contraseña con los requisitos de seguridad exigidos.
26.	En el siguiente paso, preguntará si se eliminan usuarios anónimos, escriba “Y” y pulse “Enter” para continuar. 
27.	El siguiente punto pregunta si deshabilitar el inicio de sesión en la base de datos de forma remota con el usuario “root”. Escriba “Y” y pulse “Enter” para continuar. 
28.	Por defecto MariaDB contiene una base de datos de ‘test’, se pregunta si debe eliminarla. Escriba “Y” y pulse “Enter” para continuar. 

Paso	Descripción
29.	Se deberán recargar los privilegios de todas las tablas para que los cambios surtan efecto inmediatamente. Para ello escriba “Y” y pulse “Enter” para continuar. 
30.	Finalizará el proceso mostrando el mensaje “All done!” que garantiza que todos los campos configurados se han aplicado correctamente. 

2. LIMITACIÓN DE APLICACIONES Y MÓDULOS INSTALADOS

Paso	Descripción
31.	Se procede a deshabilitar aplicaciones y módulos instalados
32.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
33.	Debe iniciar sesión en la aplicación Nextcloud con una cuenta que pertenezca al grupo de Administradores. 

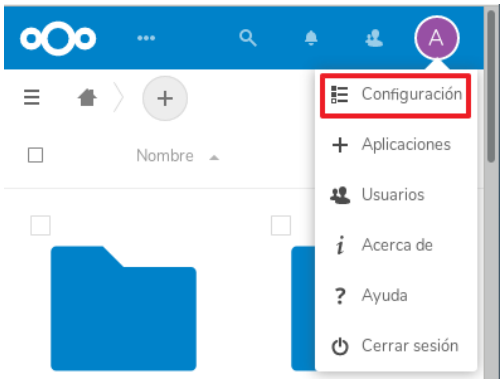
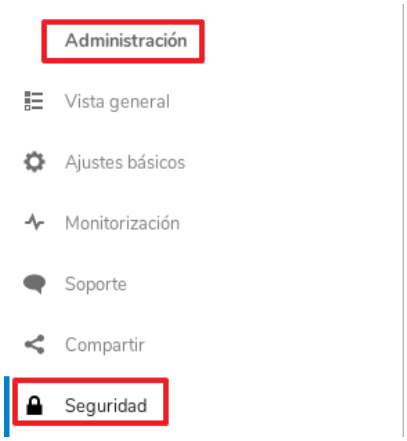
Paso	Descripción
34.	Diríjase al icono de su usuario y en el menú desplegable pulse “+ Aplicaciones “. 
35.	Revise las aplicaciones instaladas en su servidor y desactive las que no sean necesarias para su organización pulsando el botón “Desactivar”. 
36.	Si detecta alguna aplicación candidata para su desactivación y pulsa el botón “Desactivar”, le pedirá la contraseña del usuario Administrador para confirmar. 

Paso	Descripción
37.	Si quisiera eliminar la aplicación y toda su configuración por completo, diríjase a la ruta de su servidor y liste las aplicaciones allí contenidas por medio de los siguientes comandos: **$ cd /var/www/html/nextcloud/apps** **$ ls -la** 
38.	Revise las aplicaciones que más se ajusten con su organización y si se detecta una candidata para su eliminación ejecute el siguiente comando: **$ sudo rm -rf [Nombre_de_aplicacion]** **Nota:** En [Nombre_de_aplicacion] escriba el nombre de la aplicación que quiere eliminar respetando mayúsculas y minúsculas y sin corchetes "[]".

3. CONFIGURACIÓN DE USUARIOS Y POLÍTICAS DE CREDENCIALES

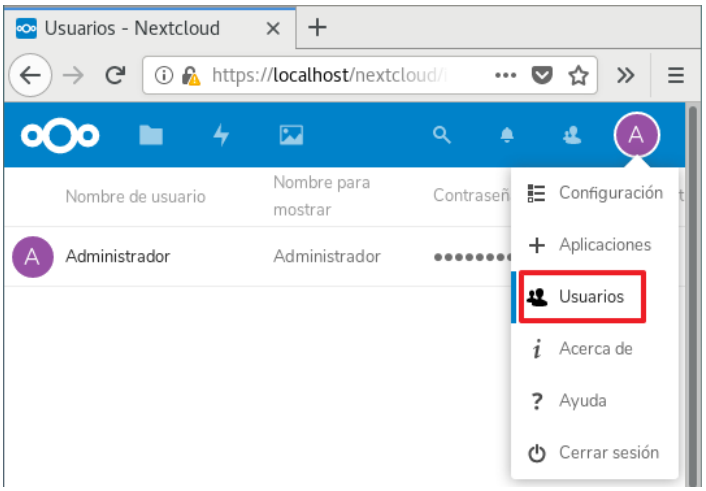
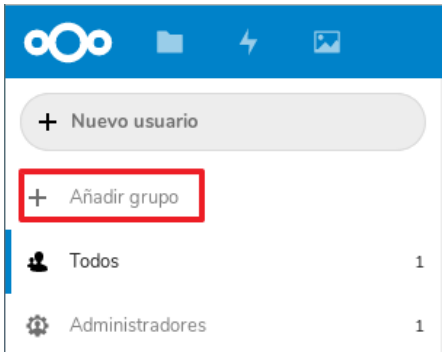
3.1. POLÍTICA DE CREDENCIALES

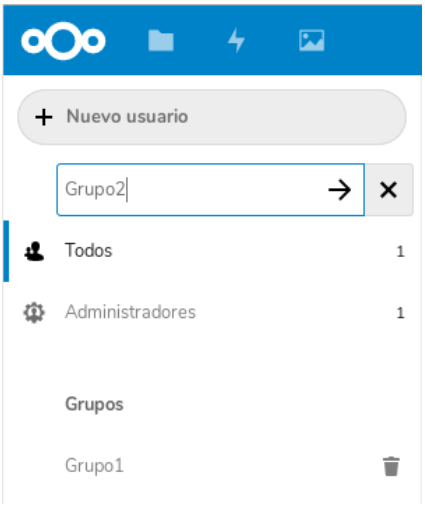
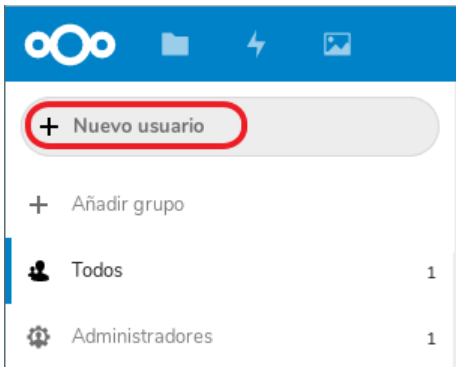
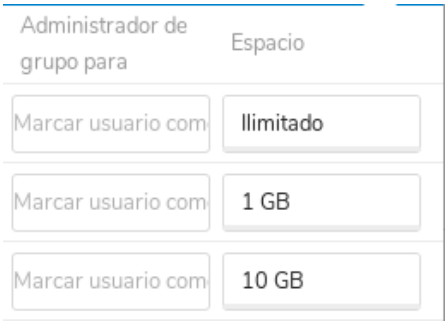
Paso	Descripción
39.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Internet" seleccione "Firefox" o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
40.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
41.	Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de admin.

Paso	Descripción
42.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
43.	En la barra lateral izquierda en el apartado “Administración”, seleccione “Seguridad”. 
44.	Diríjase hasta el final de la página deténgase en el punto “Política de contraseñas” y establezca los siguientes parámetros: – Longitud mínima: 8 caracteres – Imponer caracteres en mayúsculas y minúsculas: seleccionado – Imponer caracteres numéricos: seleccionado – Imponer caracteres especiales: seleccionado 

Paso	Descripción
45.	Para mayor seguridad y cumplimiento, se recomienda autenticación mediante LDAP. Si desea realizar la integración de usuarios por medio de LDAP, vaya al punto “ANEXO A.6.3 INTEGRACIÓN DE USUARIOS CON LDAP” de esta guía.

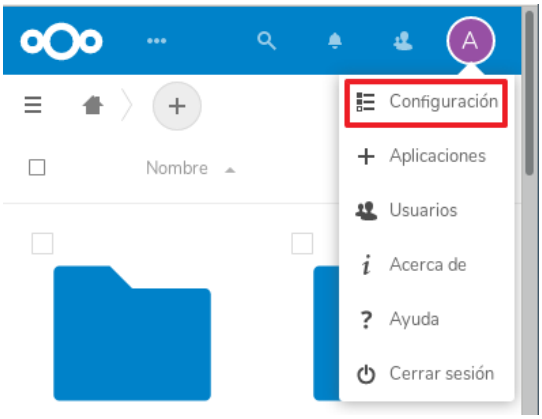
3.2. PERMISOS DE USUARIOS Y ESTRUCTURA DE GRUPOS

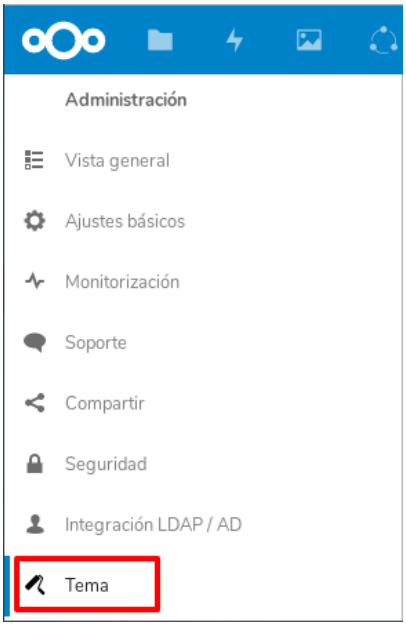
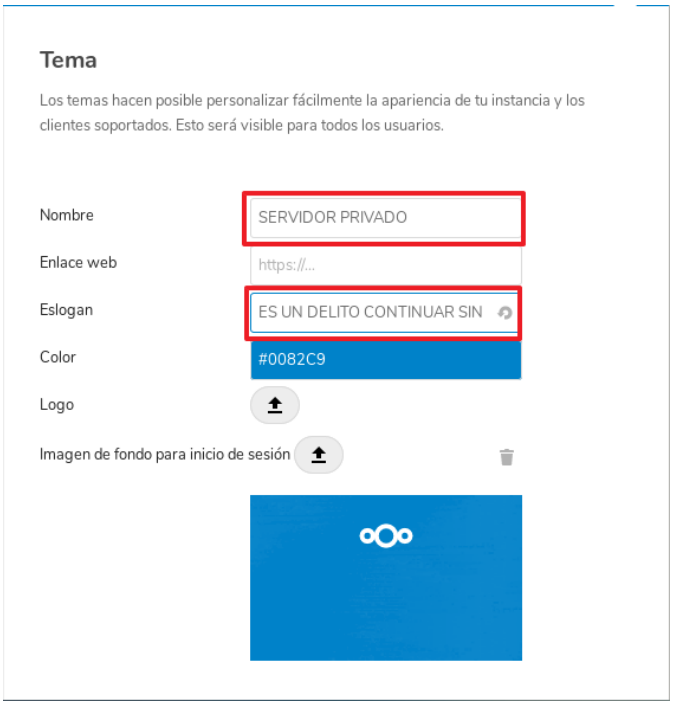
Paso	Descripción
46.	Se procede a configurar usuarios y grupos.
47.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “Firefox” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
48.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
49.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de admin.
50.	Diríjase al icono de su usuario y en el menú desplegable pulse “Usuarios”. 
51.	En el menú de usuarios, se recomienda empezar con la creación de grupos si no se encuentran creados aún, para ello pulse sobre “+ Añadir grupo” en la parte izquierda de la pantalla. 

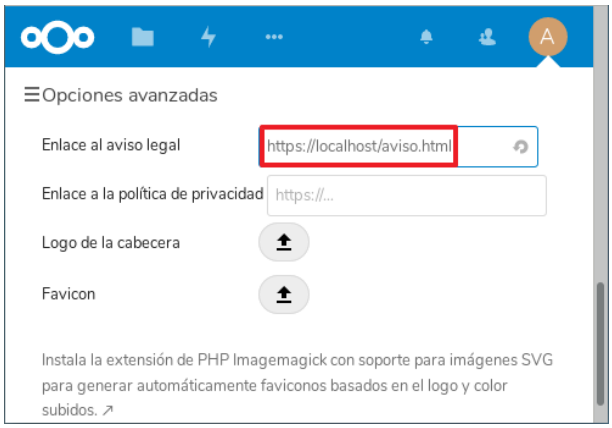
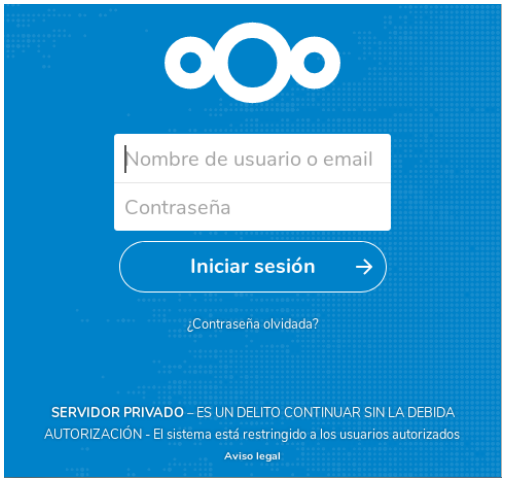
Paso	Descripción
52.	Se recomienda crear diferentes grupos identificando posteriormente usuarios comunes de usuarios administradores pertenecientes a cada grupo y teniendo en cuenta las preferencias y necesidades de su organización. 
53.	Una vez creados los grupos necesarios para su organización, se deberán crear los usuarios y asignarles un grupo y un rol dentro de ese grupo. El rol puede ser usuario común del grupo o usuario administrador de ese grupo. Comience creando los usuarios comunes teniendo en cuenta las preferencias y necesidades de su organización. Para ello pulse en el botón nuevo usuario: 
54.	Rellene todos los campos, dejando vacío el apartado “Administrador de grupo para”. Si quisiera configurar cuotas defina éstas en el apartado “Espacio”. 

Paso	Descripción
55.	Cuando finalice de rellenar todos los campos con las preferencias deseadas, diríjase al final de la línea y pulse sobre el icono de verificación para añadir y finalizar. 
56.	Se muestra una captura de ejemplo donde el "usuario_comun1" pertenece al grupo "Grupo1" con 1GB de límite de espacio en disco. En cambio, usuario_común2 pertenece al grupo "Grupo2" con 10GB de límite de espacio en disco. 

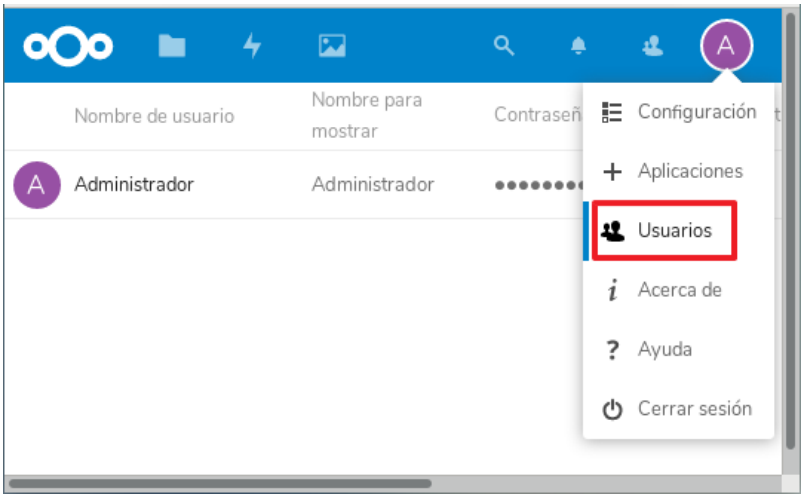
3.3. CONFIGURACIÓN MENSAJE DISUASORIO

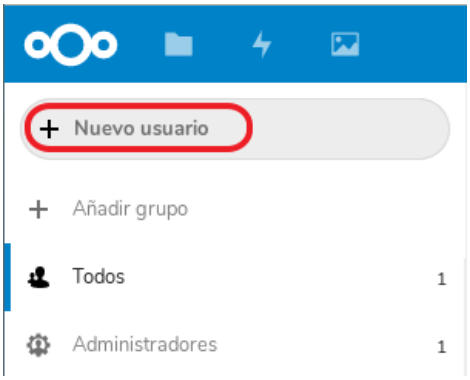
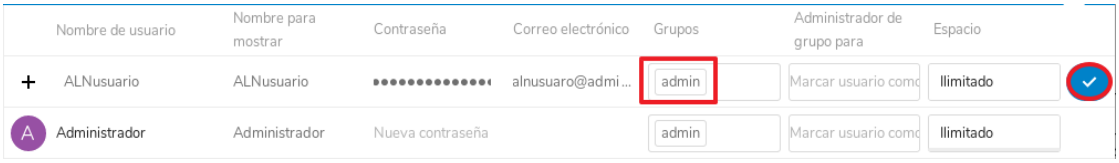
Paso	Descripción
57.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Internet" seleccione "Firefox" o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
58.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
59.	Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de admin.
60.	Diríjase al icono de su usuario y en el menú desplegable pulse "Configuración". 

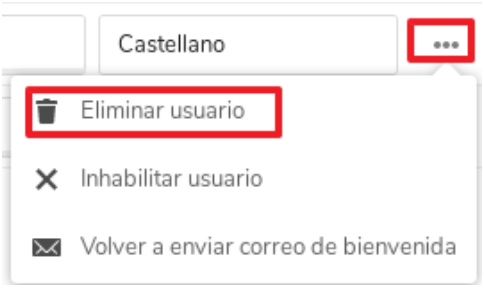
Paso	Descripción
61.	En la barra lateral izquierda en el apartado “Administración”, seleccione “Tema”. 
62.	En el apartado “Nombre”, seleccione el nombre que más convenga a su organización, posteriormente en el apartado “Eslogan” configure el mensaje disuasorio que más se ajuste a las necesidades específicas de su organización.  **Nota:** Nextcloud 15 presenta mecanismos para implementar mensajes que son advertidos al usuario cuando va a realizar el inicio de la sesión. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.

Paso	Descripción
63.	En el apartado “Opciones avanzadas”, si su organización lo posee, se puede añadir un enlace hacia el aviso legal de su organización. Para ello ingrese la URL correspondiente al aviso legal en el apartado “Enlace al aviso legal”. 
64.	Compruebe que se muestra correctamente el mensaje en la pantalla de inicio de sesión. 
65.	Compruebe que se muestra correctamente el mensaje en el primer inicio de sesión. 

4. POLÍTICA DE SEGURIDAD DE ACCESO PARA ADMINISTRADORES LOCALES

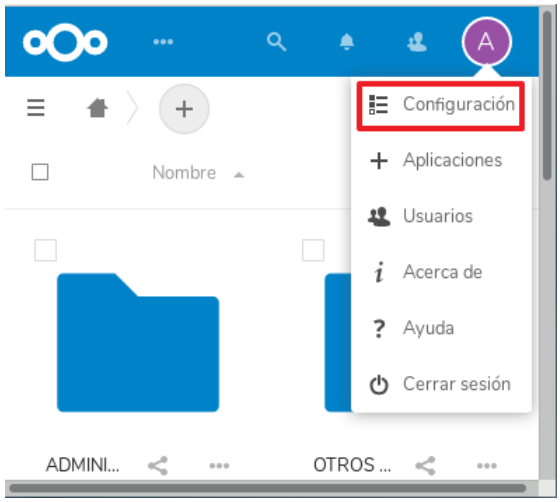
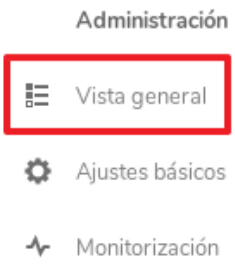
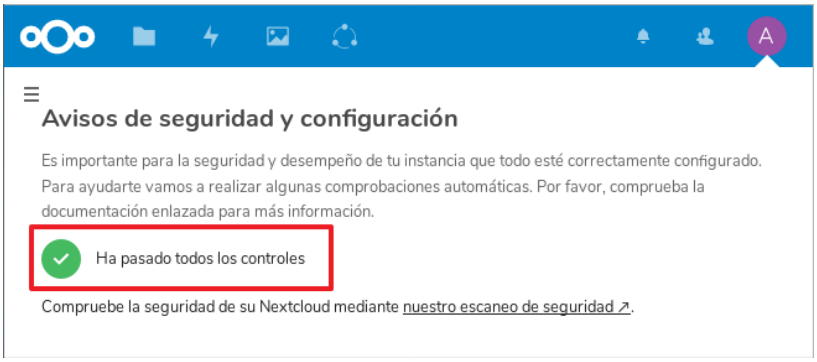
Paso	Descripción
66.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “Firefox” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
67.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
68.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
69.	Se va a proceder a modificar el usuario Administrador global del servidor de alojamiento de archivos Nextcloud. Para ello diríjase al icono de su usuario y en el menú desplegable pulse sobre el icono “Usuarios”. 
70.	Como se puede observar en la siguiente imagen, el usuario que se crea en la instalación (en este caso “Administrador”) se añade al grupo “admin”. El usuario que pertenezca al grupo “admin” el sistema lo considerará Administrador global. 

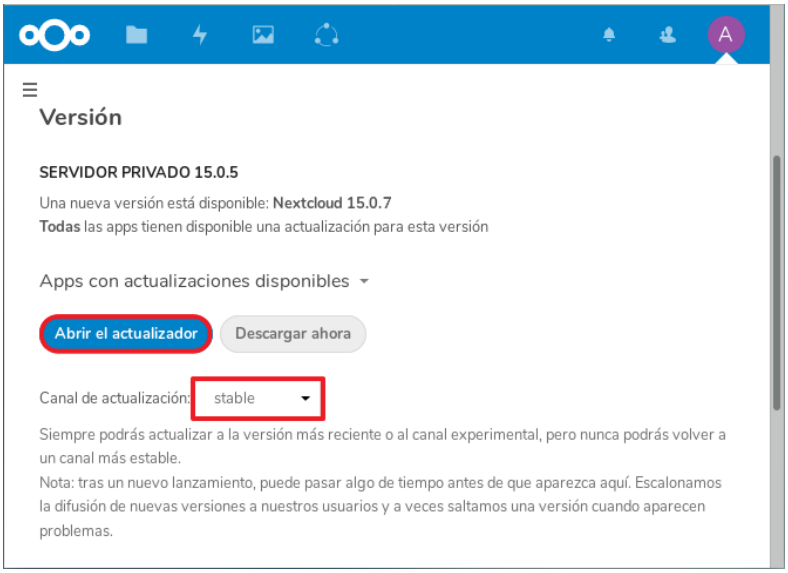
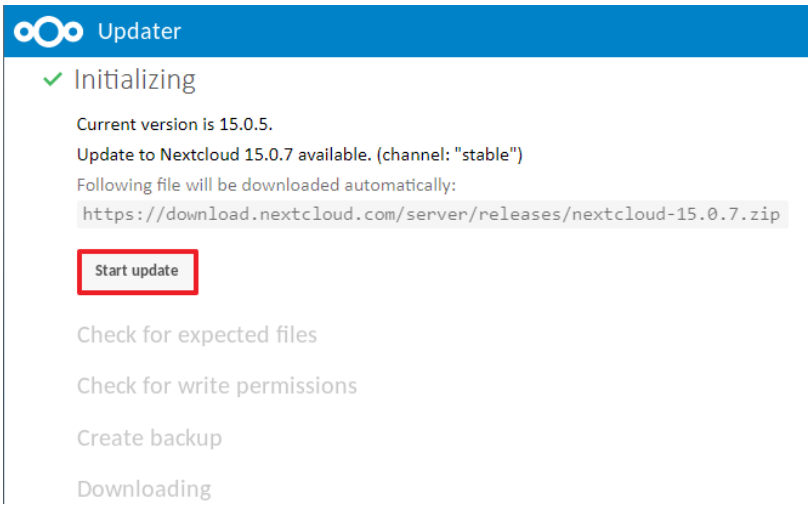
Paso	Descripción
71.	Para modificar el usuario que se creó en la instalación, se debe añadir primero un usuario nuevo y agregarlo al grupo “admin”. En este caso se pondrá un ejemplo con el usuario “ALNusuario”. 
72.	Agregue al usuario “ALNusuario” al grupo “admin”, configure los demás campos con los parámetros que más convengan a su organización y pulse el icono azul de confirmación. 
73.	Pulse sobre el icono de su usuario en el menú desplegable seleccione “Cerrar sesión”. 

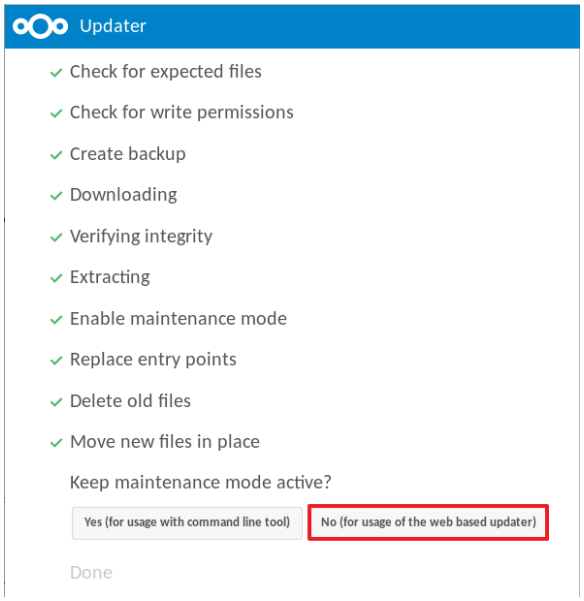
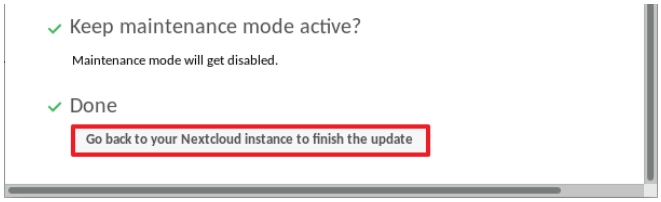
Paso	Descripción
74.	Inicie sesión con el usuario recién creado “ALNusuario” y en el icono de usuario en el menú desplegable seleccione “Usuarios”. Una vez en el menú de usuarios, elimine el usuario “Administrador” que se creó por defecto en la instalación. Para ello pulse en el icono “**…**” y seleccione “Eliminar usuario”. 
75.	Posteriormente se creará un usuario administrador de grupos. Para ello se creará el usuario “ALGusuario” y se le asignarán los grupos anteriormente creados. Modifique estos valores con los requerimientos específicos de su organización.  **Nota:** Si necesita revisar el modo de creación de usuarios y grupos, diríjase al punto 53 del apartado 3.2 PERMISOS DE USUARIOS Y ESTRUCTURA DE GRUPOS.
76.	Para finalizar diríjase al final de la línea y pulse sobre el icono de verificación para añadir y finalizar. 

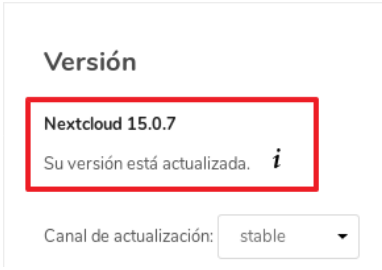
5. APLICACIÓN DE ACTUALIZACIONES

Paso	Descripción
77.	Se procede a configurar usuarios y grupos.
78.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
79.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.

Paso	Descripción
80.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
81.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
82.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Vista general”. 
83.	Antes de comprobar y comenzar a instalar las actualizaciones, diríjase al apartado inicial “Avisos de seguridad y configuración”. Se recomienda que solvente los problemas que pudiera notificar el servidor Nextcloud antes de comenzar a aplicar actualizaciones. Una vez solventadas las posibles cuestiones a resolver, se le notificará en el mismo apartado mediante un icono de confirmación verde y el siguiente texto “Ha pasado todos los controles”. 

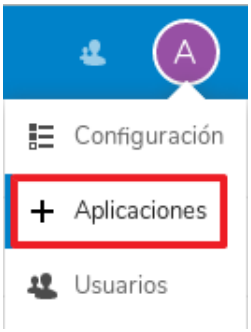
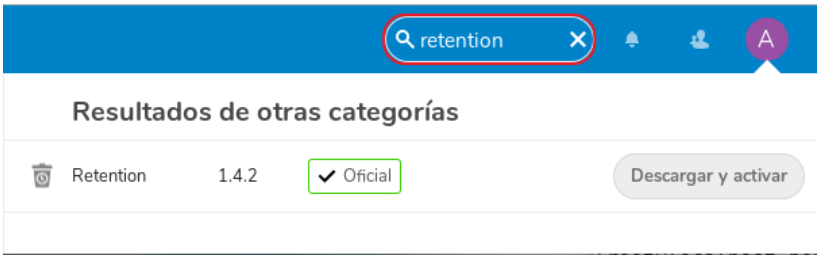
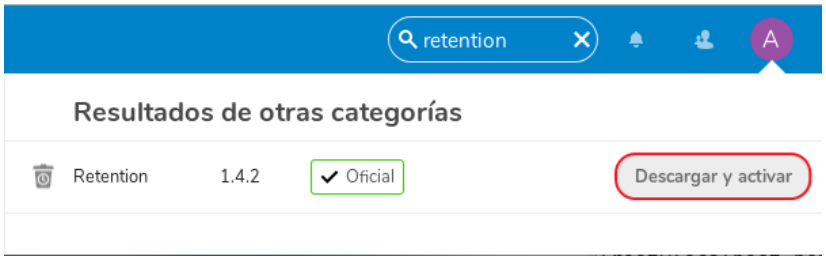
Paso	Descripción
84.	Posteriormente en el siguiente apartado “Versión” se notificarán las actualizaciones disponibles para su servidor. Para comenzar compruebe que en el menú desplegable “Canal de actualización” se encuentra seleccionada la opción “stable”. Posteriormente pulse “Abrir el actualizador”.  **Nota:** Los canales de actualización disponibles son los siguientes. - **production** siempre proporcionará el último nivel de parches, pero no se actualizará a la próxima versión principal de inmediato. Esa actualización generalmente ocurre con la segunda versión menor (x.0.2). - **stable** es la versión estable más reciente. Es adecuada para uso en producción y siempre se actualizará a la última versión principal. - **beta** es una versión preliminar solo para probar nuevas características, no para entornos de producción.
85.	El actualizador realizará varios pasos necesarios para una correcta actualización. Para comenzar pulse “Start update”. 

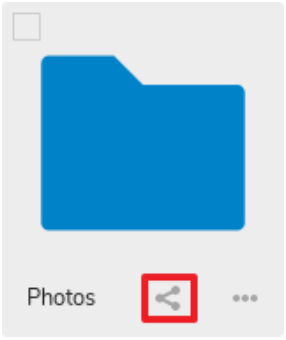
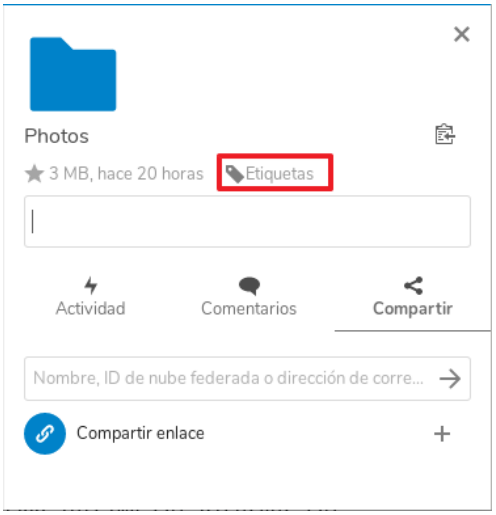
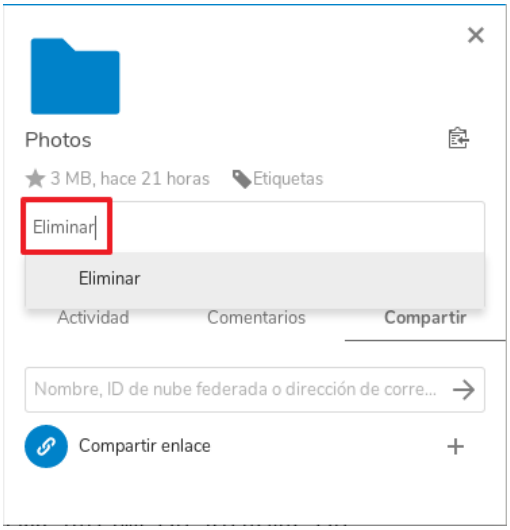
Paso	Descripción
86.	Cuando finalice de realizar todos los pasos necesarios preguntará si desea mantener activo el modo de mantenimiento, pulse en “No (for usage of the web based updater)”. 
87.	Al realizarlo de este modo, el servidor redireccionará hacia el updater basado en WEB. Para ello pulse en “Go back to your Nextcloud instance to finish the update”. 

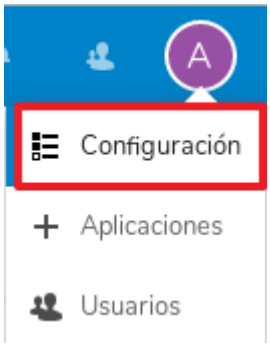
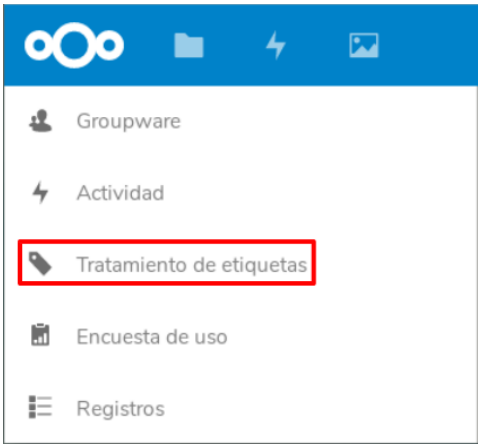
Paso	Descripción
88.	Se mostrará el asistente de actualización de Nextcloud (Updater). Lea detenidamente las advertencias y cuando esté listo pulse el botón “Iniciar actualización”. 
89.	El servidor comenzará la actualización y comprobará la integridad del código una vez finalice, al finalizar le redireccionará al servidor si el proceso ha sido satisfactorio. 
90.	Compruebe que no existen nuevas actualizaciones cuando finalice. 

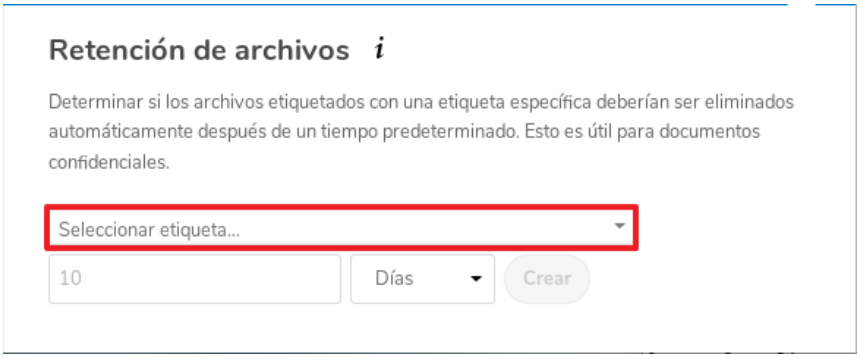
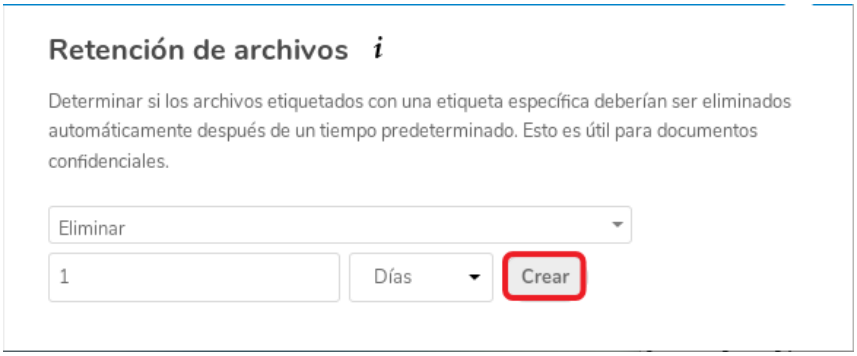
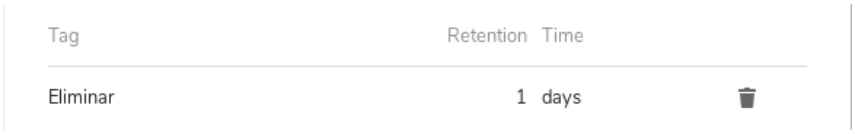
6. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

6.1. ELIMINACIÓN AUTOMÁTICA DE ARCHIVOS

Paso	Descripción
91.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
92.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
93.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
94.	Diríjase al icono de su usuario y en el menú desplegable pulse “Aplicaciones”. 
95.	En el panel de navegación superior elija el icono de la lupa para buscar y escriba el siguiente texto: “retention”. 
96.	Pulse el botón “Descargar y activar” para obtener la aplicación y que se encuentre activa en el servidor.  **Nota:** Fíjese siempre que las aplicaciones lleven el recuadro verde que garantice que son aplicaciones **oficiales** y por tanto están aprobadas por los desarrolladores de Nextcloud.

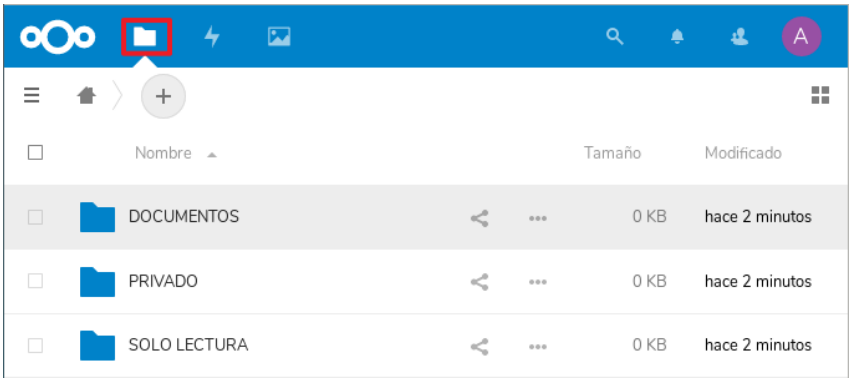
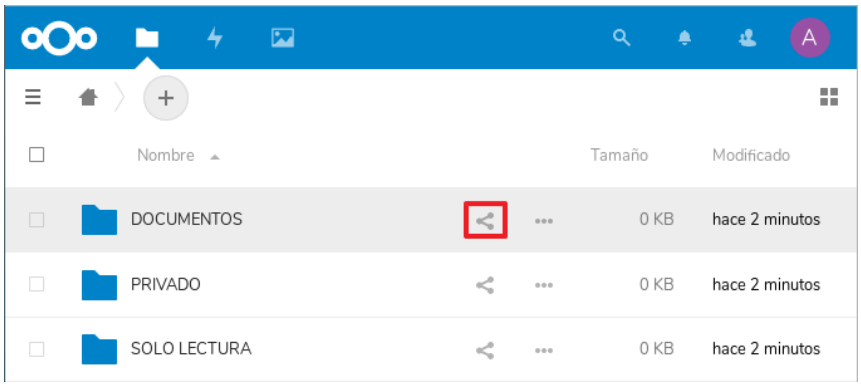
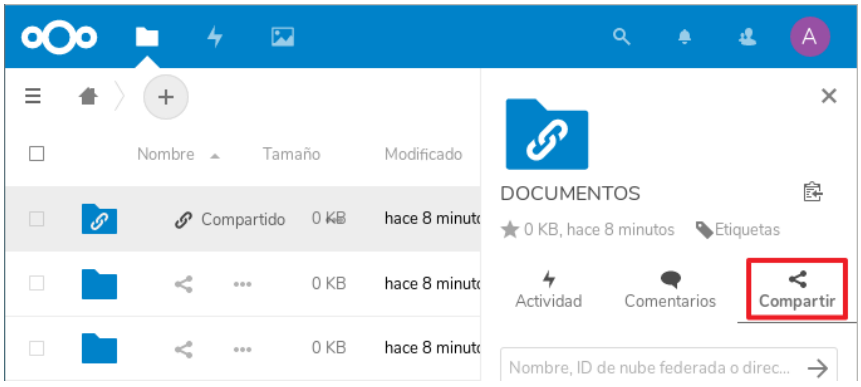
Paso	Descripción
97.	Para programar la eliminación automática de archivos se deben asignar etiquetas anteriormente. Se muestra un ejemplo a continuación de asignación de etiquetas a un archivo alojado en el servidor. Diríjase a los archivos del servidor elija el fichero que quiere programar su eliminación y pulse el icono compartir. 
98.	Se desplegará automáticamente un menú a la derecha de la pantalla. Pulse en "Etiquetas" para añadir una etiqueta. 
99.	Escriba una etiqueta característica para marcar ese fichero o directorio y pulse "Enter". 

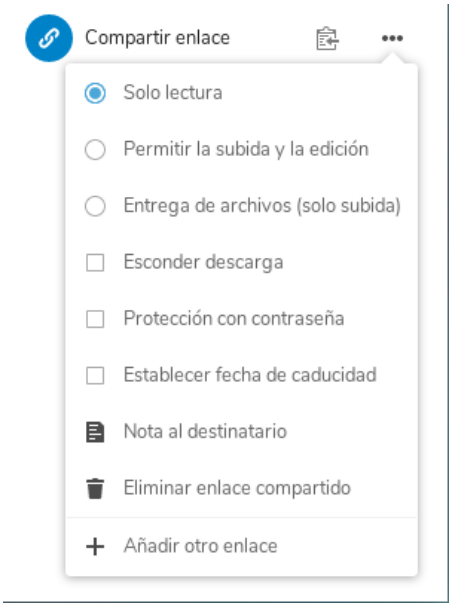
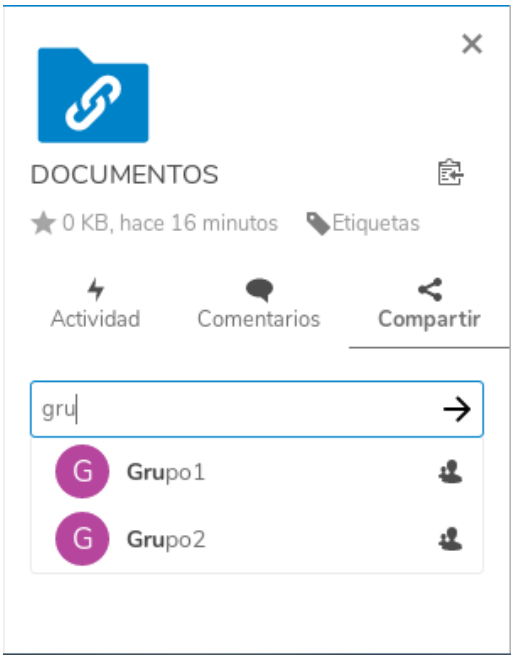
Paso	Descripción
100.	Compruebe que se añade la etiqueta correctamente al fichero o directorio. 
101.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
102.	En la columna de la izquierda seleccione “Flujo de trabajo”.  **Nota:** Debido a las constantes actualizaciones que se producen el producto “**Nextcloud**”, los títulos de las opciones o apartados, podrían sufrir alguna discrepancia con respecto al momento de la elaboración de esta guía. Por ejemplo, en versiones anteriores de la 15.0.7, la aplicación “retention”, en su opción de “Flujo de datos” cambia el nombre a “tratamiento de etiquetas”, manteniendo el mismo icono.

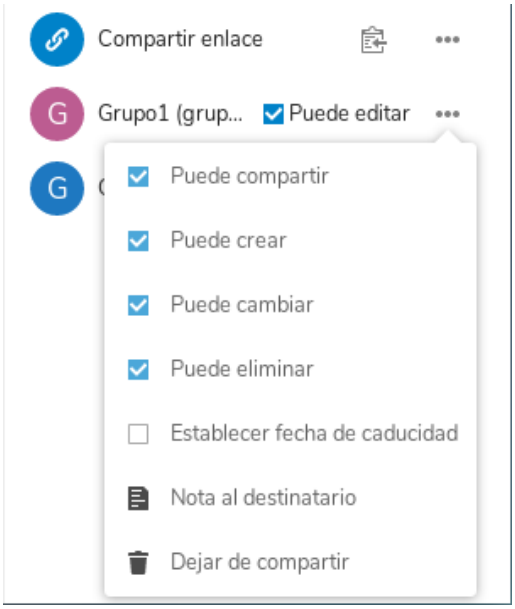
Paso	Descripción
103.	Diríjase al título “Retención de archivos” y en la pestaña “Seleccionar etiqueta…” elija la etiqueta creada anteriormente. En este ejemplo será la etiqueta “Eliminar”. 
104.	Configure la franja de tiempo en la que el fichero o directorio se eliminará y pulse el botón “Crear” para finalizar. 
105.	Se creará la regla en el servidor.  **Nota:** Tenga en cuenta que todo archivo que contenga esta etiqueta se eliminará en la franja de tiempo configurada en la regla.

6.2. COMPARTICIÓN DE CARPETAS Y DOCUMENTOS

Paso	Descripción
106.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “**Firefox**” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
107.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
108.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.

Paso	Descripción
109.	Diríjase al icono “Archivos” para que se muestren todos los documentos de su usuario. 
110.	Seleccione el icono compartir para desplegar las opciones de compartición. 
111.	Se mostrará el menú de propiedades del directorio, seleccionando el apartado “Compartir”. 

Paso	Descripción
112.	Se crea automáticamente el apartado “Compartir enlace”, pulse sobre “…” y seleccione los permisos que más convengan a su organización. 
113.	Posteriormente diríjase a la barra de búsqueda de usuarios y grupos ubicada justo encima y seleccione los usuarios y grupos a los que se le compartirá la carpeta. 

Paso	Descripción
114.	Una vez seleccionado el Grupo o el usuario, pude permitir o denegar los permisos del mismo en el interior de la carpeta. Además, puede seleccionar una fecha de caducidad para la compartición de la carpeta. 

ANEXO A.3.2. LISTA DE COMPROBACIÓN DEL SERVIDOR NEXTCLOUD 15 PARA LA CATEGORÍA BÁSICA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.3.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES NEXTCLOUD 15 QUE LES SEA DE APLICACIÓN LA CATEGORÍA BÁSICA DEL ENS".

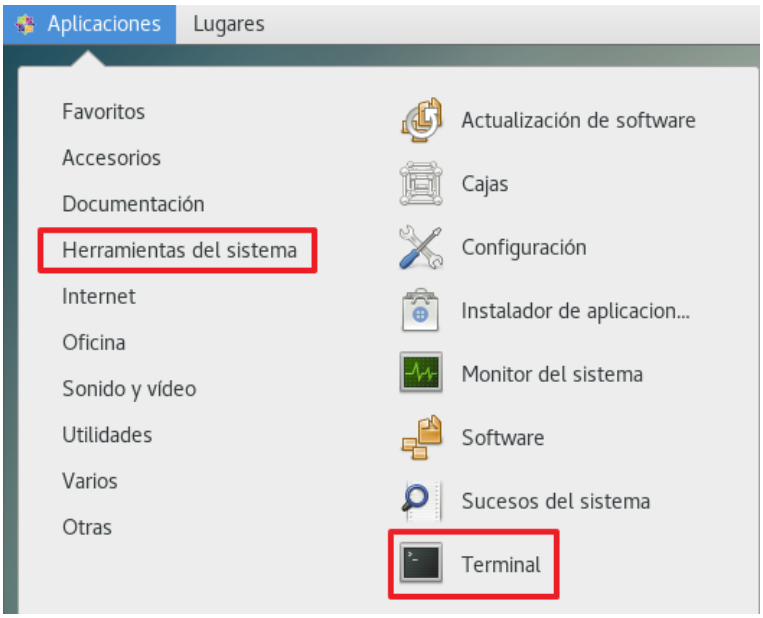
Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores de alojamiento de archivos Nextcloud 15 independientes con implementación de seguridad de categoría básica del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas con permisos "root" y usuarios de Nextcloud pertenecientes al grupo "admin". Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario perteneciente al grupo de "sudoers". Las consolas y herramientas que se utilizarán son las siguientes:

a) Terminal de Linux

b) Entorno Web Nextcloud 15

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En el cliente, inicie sesión con una cuenta con privilegios de root.
2. Inicie la Terminal de Linux		Ejecute la "Terminal". Para ello Diríjase a la barra de tareas, pulse en Aplicaciones y en el apartado "Herramientas del sistema" seleccione "Terminal". 

Comprobación	OK/NOK	Cómo hacerlo

3. Verifique versiones del conjunto de servidores LAMP.		En la "Terminal" ejecute los siguientes comandos y verifique las versiones instaladas.
		$ sudo yum info mariadb
		$ sudo yum info httpd
		$ sudo php -v
		`Paquetes instalados`
		`Nombre : httpd`
		`Arquitectura : x86_64`
		`Versión : 2.4.6`
		`Lanzamiento : 88.el7.centos`
		`Tamaño : 9.4 M`
		`Repositorio : installed`
		`Desde el repositorio : base`
		`Resumen : Apache HTTP Server`
		`URL : http://httpd.apache.org/`
		`Licencia : ASL 2.0`
		`Descripción :The Apache HTTP Server is a powerful,`
		`: web server.`
		Nota: Debe adecuar las versiones a las necesidades y compatibilidad de los diferentes elementos de su organización, teniendo en cuenta que las versiones deben ser las últimas con soporte y recomendadas por el desarrollador.

4. Comprobación de repositorios remi activos.		Abra la Terminal y ejecute el siguiente comando.
		$ sudo ls /etc/yum.repos.d/remi*
		usuario@localhost:~
		Archivo Editar Ver Buscar Terminal Ayuda
		`[usuario@localhost ~]$ sudo ls /etc/yum.repos.d/remi*`
		`/etc/yum.repos.d/remi-glpi91.repo`
		`/etc/yum.repos.d/remi-glpi92.repo`
		`/etc/yum.repos.d/remi-glpi93.repo`
		`/etc/yum.repos.d/remi-glpi94.repo`
		`/etc/yum.repos.d/remi-modular.repo`
		`/etc/yum.repos.d/remi-php54.repo`
		`/etc/yum.repos.d/remi-php70.repo`
		`/etc/yum.repos.d/remi-php71.repo`
		`/etc/yum.repos.d/remi-php72.repo`
		`/etc/yum.repos.d/remi-php73.repo`
		`/etc/yum.repos.d/remi.repo`
		`/etc/yum.repos.d/remi-safe.repo`
		`[usuario@localhost ~]$`
		Nota: Tenga en consideración que a medida que aparezcan nuevas versiones, los repositorios pueden variar.

Comprobación	OK/NOK	Cómo hacerlo

Configuración	OK/NOK
/etc/yum.repos.d/remi-glpi91.repo	
/etc/yum.repos.d/remi-glpi92.repo	
/etc/yum.repos.d/remi-glpi93.repo	
/etc/yum.repos.d/remi-glpi94.repo	
/etc/yum.repos.d/remi-modular.repo	
/etc/yum.repos.d/remi-php54.repo	
/etc/yum.repos.d/remi-php70.repo	
/etc/yum.repos.d/remi-php71.repo	
/etc/yum.repos.d/remi-php72.repo	
/etc/yum.repos.d/remi-php73.repo	
/etc/yum.repos.d/remi.repo	

5. Ficheros de configuración Apache.

Ejecute los siguientes comandos y compruebe que es correcta la configuración según las necesidades específicas de su organización.

$ sudo gnome-text-editor/etc/httpd/conf/httpd.conf &>/dev/null

$ sudo gnome-text-editor/etc/httpd/conf.d/nextcloud.conf &>/dev/null

6. Ficheros de configuración PHP.

Ejecute los siguientes comandos y compruebe que es correcta la configuración según las necesidades específicas de su organización.

$ sudo gnome-text-editor /etc/php.ini &>/dev/null

$ sudo gnome-text-editor /etc/php.d/10-opcache.ini &>/dev/null

7. Comprobación de cifrado seguro.

Inicie sesión en la base de datos MariaDB y compruebe los parámetros requeridos, para ello ejecute los siguientes comandos.

$ sudo mysql -u root -p

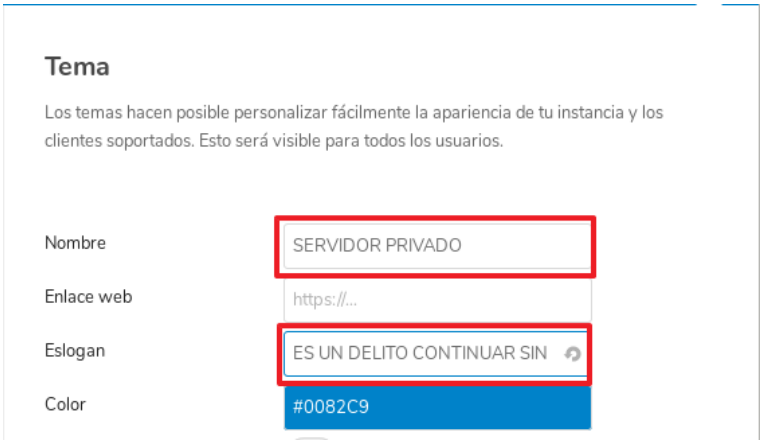
MariaDB [(none)]> use nextcloud;

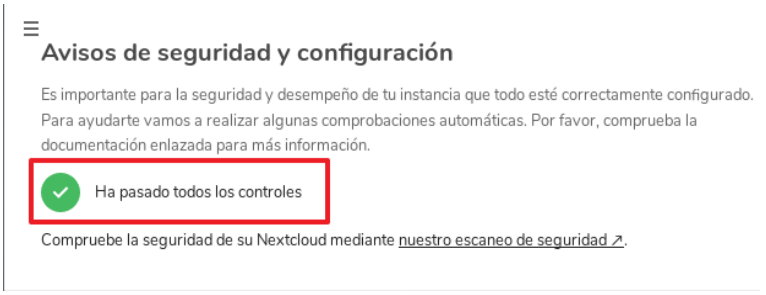
MariaDB [nextcloud]>select * from oc_users;

MariaDB [nextcloud]>exit;

```
+--------------------------------------------------------------+
| password                                                     |
+--------------------------------------------------------------+
| 2|$argon2i$v=19$m=1024,t=2,p=[redacted]                      |
| 2|$argon2i$v=19$m=1024,t=2,p=[redacted]                      |
| 2|$argon2i$v=19$m=1024,t=2,p=[redacted]                      |
+--------------------------------------------------------------+
```

Configuración	Valor	OK/NOK
Usuario Administrador	2|$argon2i$v=19$m=1024,t=2,	
Resto de usuarios	2|$argon2i$v=19$m=1024,t=2,	

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>8. Aplicaciones instaladas</td><td></td><td>Compruebe que las aplicaciones existentes en el servidor Nextcloud son las mínimas necesarias para su organización. Para ello ejecute el siguiente comando.
$ sudo ls /var/www/html/nextcloud/apps</td></tr>
<tr><td>9. Inicie sesión en el servidor Nextcloud</td><td></td><td>Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “Firefox” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud. Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de “admin”.</td></tr>
<tr><td rowspan="5">10. Política de contraseñas</td><td></td><td>Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración” → “Administración” → “Seguridad” →“Política de contraseñas”.</td></tr>
<tr><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Longitud mínima</td><td>8</td><td></td></tr>
<tr><td>Imponer caracteres en mayúsculas y minúsculas</td><td>☑</td><td></td></tr>
<tr><td>Imponer caracteres numéricos</td><td>☑</td><td></td></tr>
<tr><td>Imponer caracteres especiales</td><td>☑</td><td></td></tr>
</table></td></tr>
<tr><td>11. Mensaje disuasorio</td><td></td><td>Vaya al icono de su usuario y en el menú desplegable pulse “Configuración” → “Administración” → “Tema” y compruebe que se encuentran configurados los apartados remarcados en la siguiente imagen.
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
12. Avisos de seguridad.		Vaya al icono de su usuario y en el menú desplegable pulse **"Configuración" → "Administración" → "Vista general"** y compruebe que se no existen avisos de seguridad y se muestra el mensaje "Ha pasado todos los controles". 
13. Retención de archivos		Vaya al icono de su usuario y en el menú desplegable pulse **"Aplicaciones" → "Apps activas"** y compruebe que se encuentra instalada y activada la aplicación "Retention".

ANEXO A.4. CATEGORÍA MEDIA

ANEXO A.4.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES NEXTCLOUD 15 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS

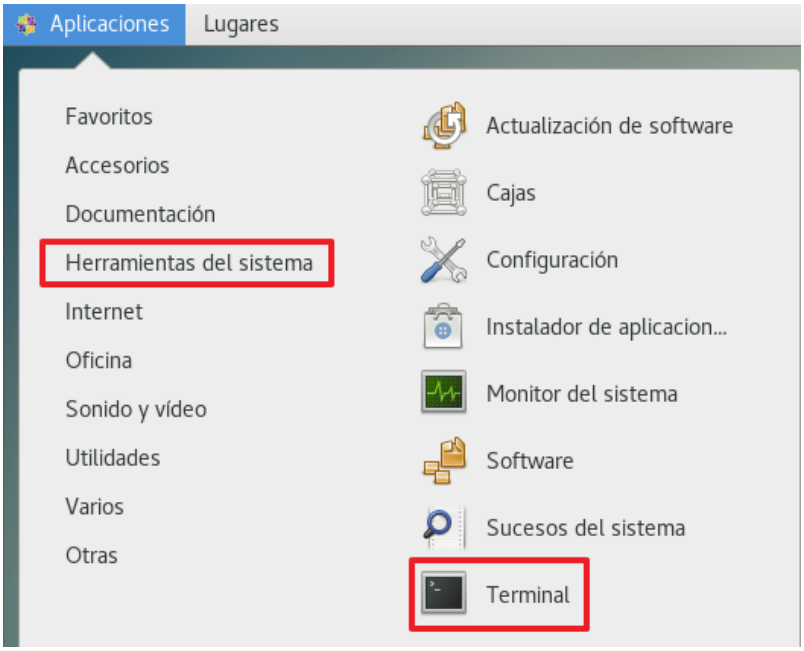
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de alojamiento de archivos Nextcloud 15 sobre Sistema Operativo CentOS 7.4 Linux con una categorización de seguridad media según los criterios 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 la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría media, 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.

Los pasos que se describen a continuación se realizarán en todos aquellos servidores de alojamiento de archivos Nextcloud 15 sobre Sistema Operativo CentOS 7.4 Linux con categoría media aplicada según guía CCN-STIC-619 independientes a un dominio, que implementen servicios o información de categoría media y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

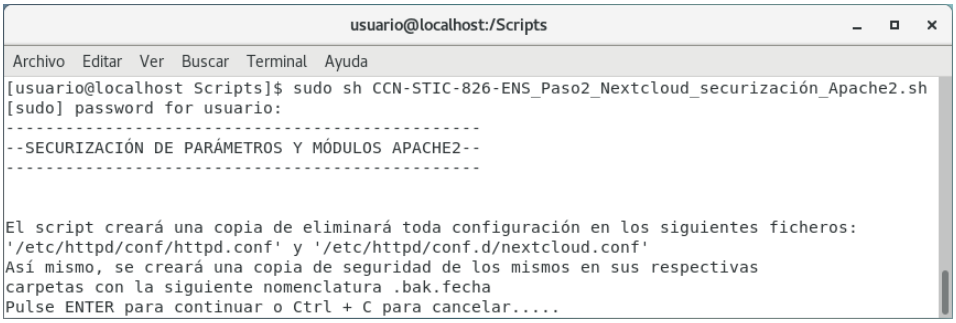
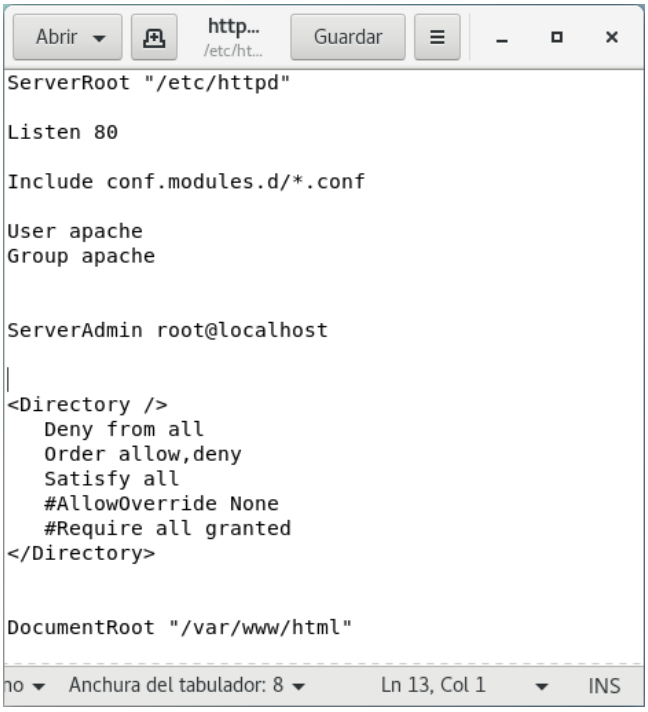
1. CONFIGURACIÓN SEGURA DE APACHE, PHP Y MARIADB PARA NEXTCLOUD

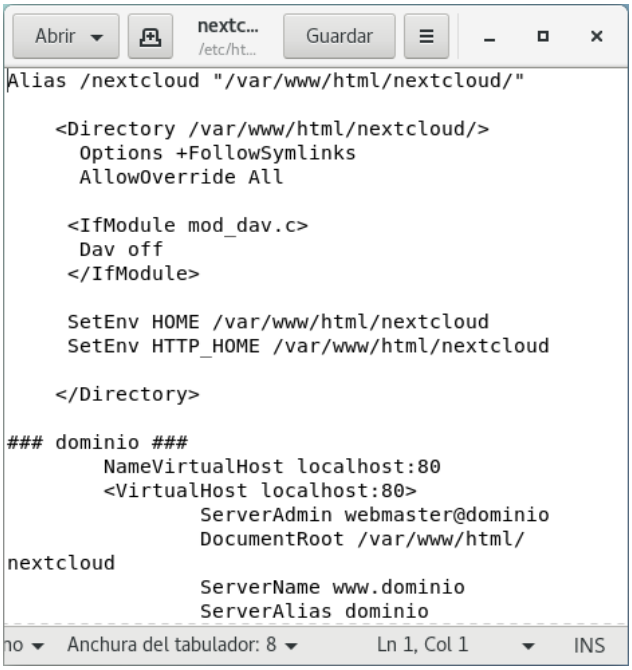
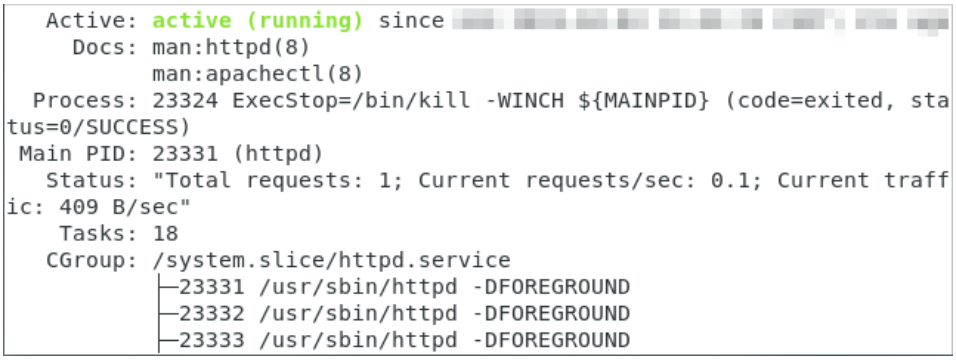
Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va a instalar Nextcloud según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o “Sudoers”.
3.	Cree el directorio **“Scripts”** en **“/”** y copie aquí el contenido de la carpeta asociada a la categorización del equipo desde el medio de almacenamiento correspondiente. Deberá asignarles los permisos pertinentes para la ejecución de los mismos.

Paso	Descripción
4.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
5.	Ejecute el comando “cd /Scripts/” y pulse la tecla “Enter”.
6.	Posteriormente ejecute “ls -l” y compruebe que están todos los scripts.

1.1. APACHE 2

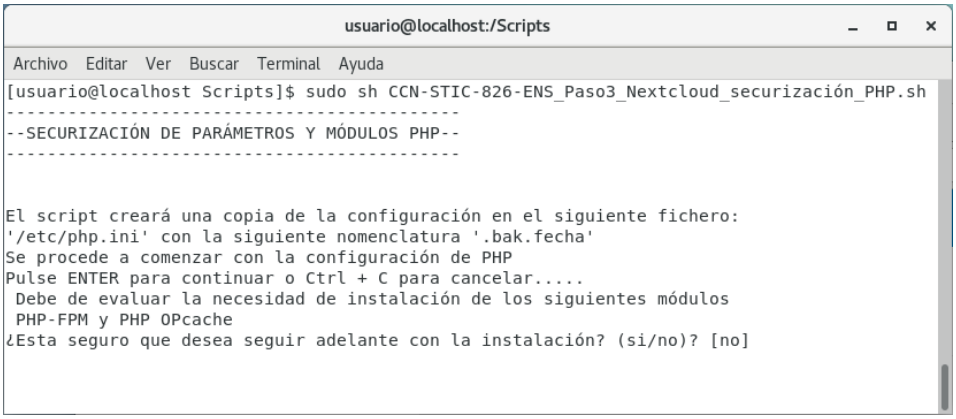
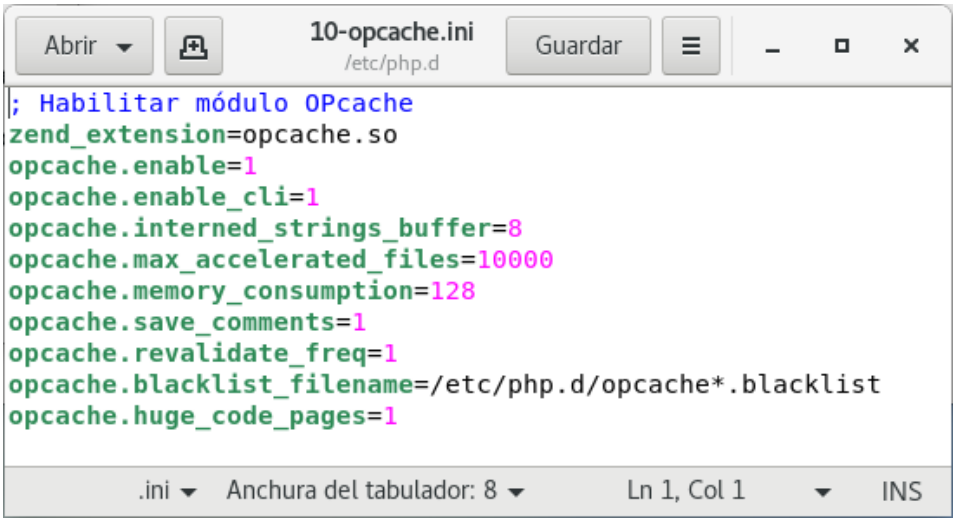
Paso	Descripción
7.	Si ha cerrado la **“Terminal“** en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione **“Terminal”**. Ejecute el comando **“cd /”** y pulse la tecla “Enter”.
8.	Se procederá a securizar el servidor web Apache. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts**

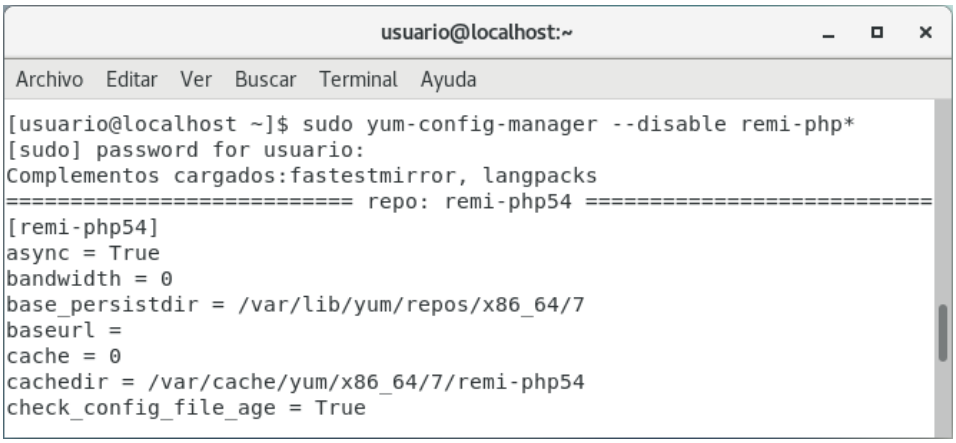
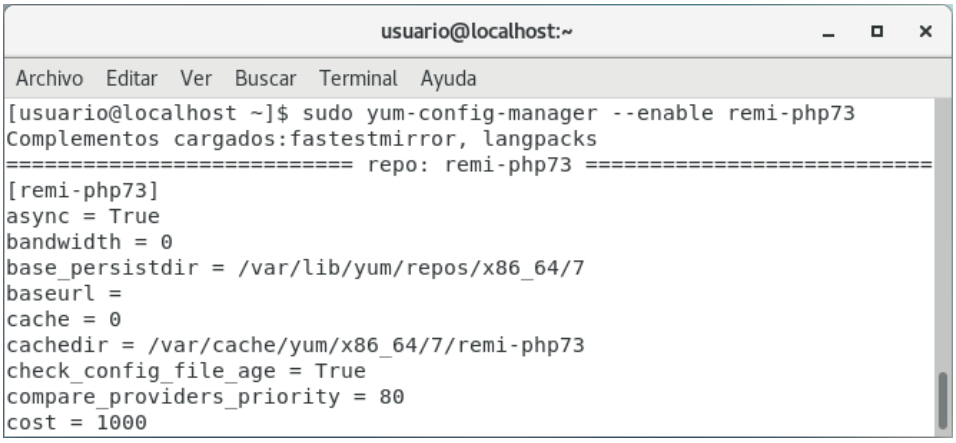
Paso	Descripción
9.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-826-ENS_Paso2_Nextcloud_securización_Apache2.sh** El script iniciará un proceso de instalación de los módulos “mod_security” y “mod_evasive” de Apache. Además, modificará los ficheros de configuración “/etc/httpd/conf/httpd.conf” y “/etc/httpd/conf.d/nextcloud.conf” eliminando toda configuración contenida en los mismos.  **Nota:** Tenga en cuenta que el script configura parámetros en rutas por defecto, si escoge un servidor web que no sea apache deberá adaptar el script a las necesidades específicas de su organización.
10.	El script mostrará el fichero “/etc/httpd/conf/httpd.conf” con una configuración aplicada con ejemplos y líneas comentadas (#) que deberá revisar y ajustar con los parámetros que más convengan a su organización. Cuando finalice pulse “Guardar” y cierre el editor de textos. 

Paso	Descripción
11.	Posteriormente el script mostrará el fichero "/etc/httpd/conf.d/nextcloud.conf" con una configuración aplicada con ejemplos y líneas comentadas (#) que, del mismo modo, deberá revisar y ajustar con los parámetros que más convengan a su organización. Cuando finalice pulse "Guardar" y cierre el editor de textos. 
12.	Finalmente compruebe que el servicio se ha reiniciado correctamente 

1.2. PHP

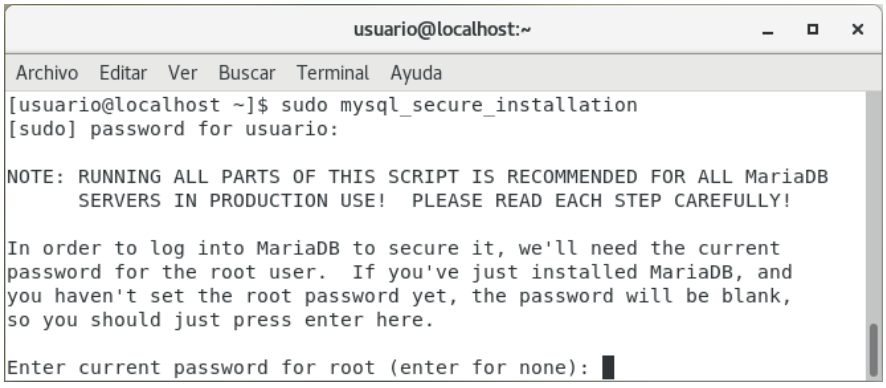
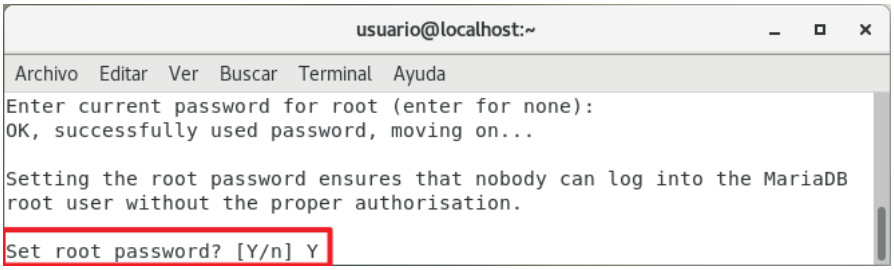
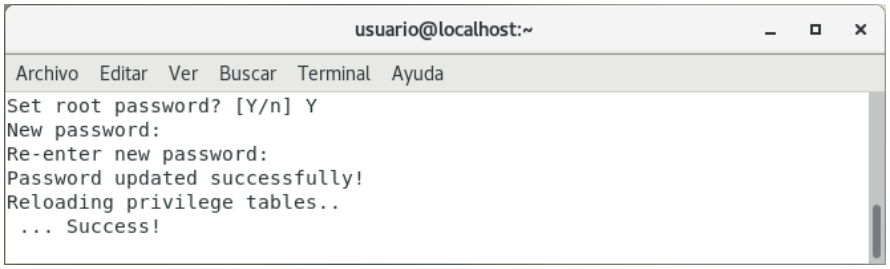
Paso	Descripción
13.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
14.	Se procederá a securizar el servicio PHP. Para ello diríjase a la carpeta "Scripts". **$ cd /Scripts**

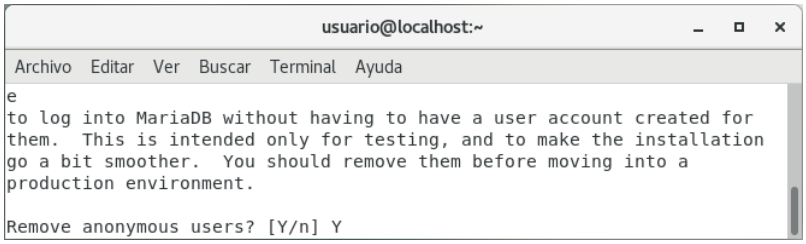
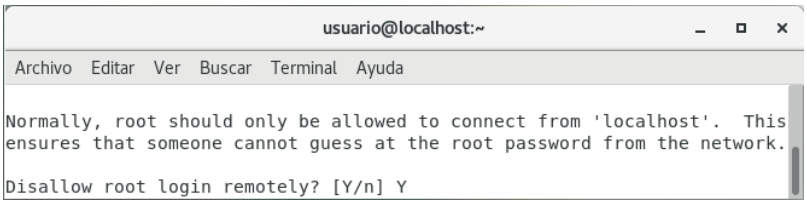
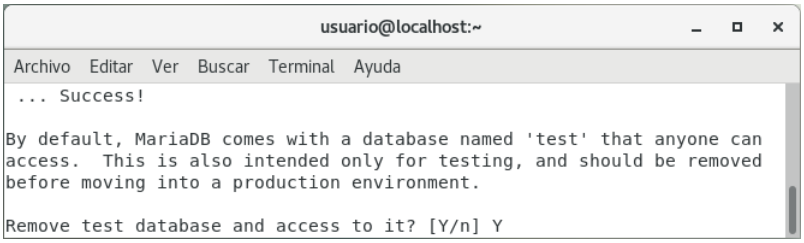
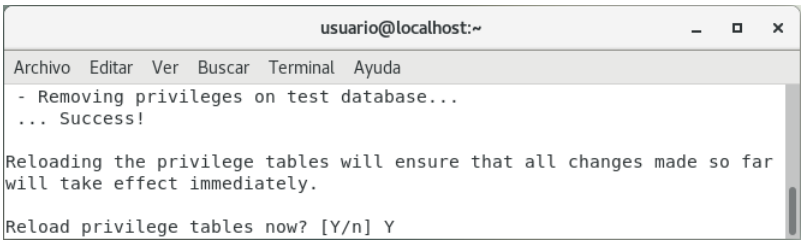
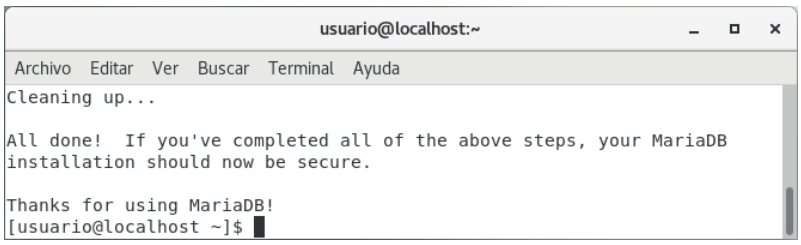
Paso	Descripción
15.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-826-ENS_Paso3_Nextcloud_securización_PHP.sh** Deberá evaluar la necesidad de los siguientes módulos “PHP-FPM” y “PHP OPcache” de PHP. El script le preguntará sobre las acciones al respecto, si los módulos son adecuados para su organización escriba “si” y pulse “Enter” para continuar con la instalación, si por el contrario no son necesarios escriba “no” y pulse “Enter” y el script finalizará.  **Nota:** El módulo PHP-FPM mejora notablemente la velocidad en servidores web de alto tráfico y OPcache mejora el rendimiento de PHP almacenando el código de bytes de un script precompilado en la memoria compartida, eliminando así la necesidad de que PHP cargue y analice los scripts en cada petición.
16.	Si ha escrito “si” el script proseguirá instalando los módulos y mostrando la configuración del fichero “/etc/php.d/10-opcache.ini” para su revisión. Se deben configurar los parámetros que más convengan a su organización.  Cuando finalice de configurar, pulse el botón “Guardar” y cierre el editor de texto.
17.	El servidor Apache se reiniciará, compruebe que se reinicia sin errores.

Paso	Descripción
18.	Posteriormente se procederá a la actualización de php por medio del repositorio "remi". Para ello deshabilite los repositorios activos de php ejecutando el siguiente comando: **$ sudo yum-config-manager --disable remi-php*** 
19.	Ahora habilite el repositorio correspondiente a la versión de php más actualizada soportada por el sistema operativo y en versión estable. **$ sudo yum-config-manager --enable remi-phpXX[2]**  **Nota:** Si desea saber la versión que más se ajusta con las necesidades de su organización diríjase al siguiente enlace: https://www.php.net/
20.	Por último, ejecute el siguiente comando para actualizar el sistema por completo y que se aplique versión actualizada de php: **$ sudo yum -y update**

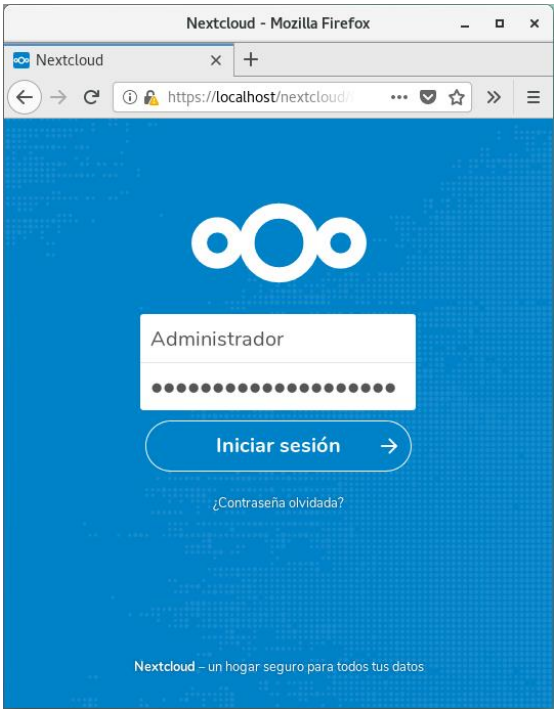
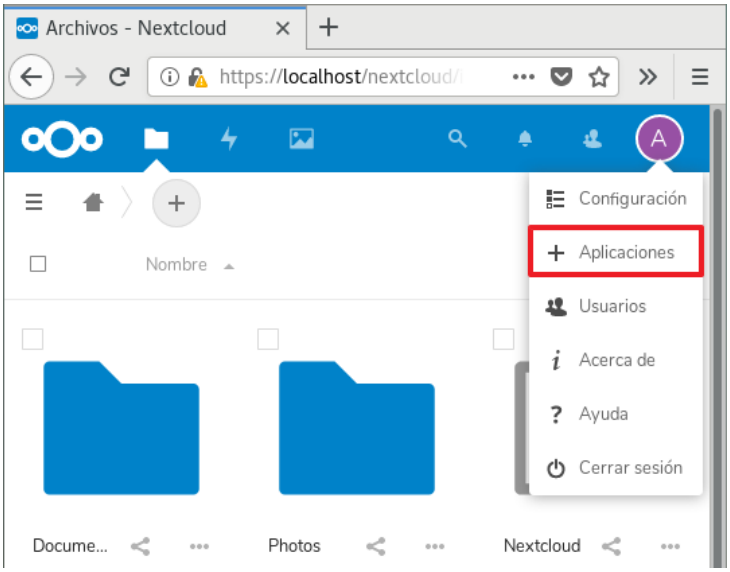
[2] Deberá adaptar la ejecución según la versión PHP a utilizar.

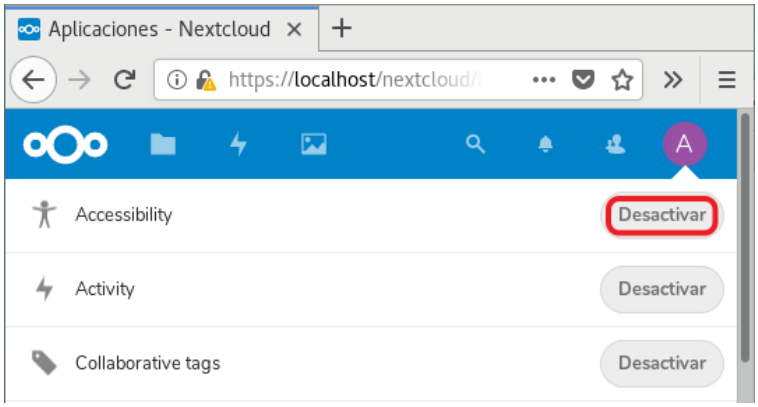
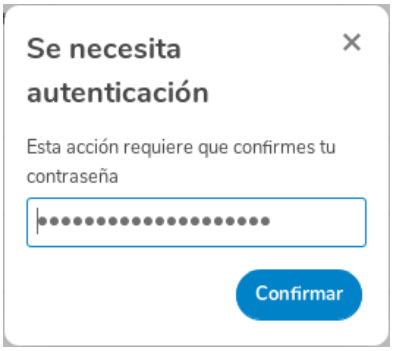
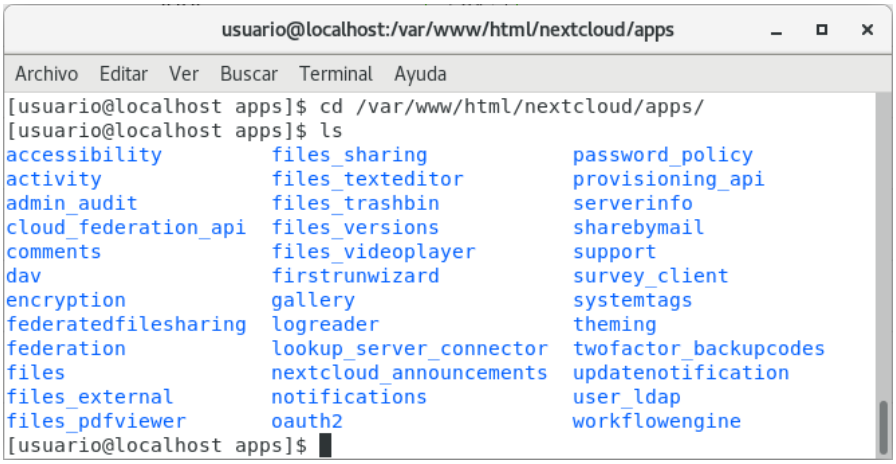
1.3. MARIADB

Paso	Descripción
21.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
22.	Se aplicarán medidas de seguridad en el servidor de Base de Datos MariaDB. Para ello ejecute el siguiente comando: **$ sudo mysql_secure_installation**
23.	En primer lugar, pedirá la contraseña del usuario "root", ingrese la contraseña y si no se ha configurado aún la misma deje el campo vacío y pulse "Enter" para continuar. 
24.	Posteriormente se preguntará si se quiere configurar una contraseña para "root", conteste con "Y" y pulse "Enter". 
25.	Escriba la nueva contraseña de "Root", pulse "Enter" y vuelva a escribirla pulsando de nuevo "Enter" para continuar.  **Nota:** Tenga en cuenta, que el usuario "root" de la base de datos, es independiente al usuario "root" del sistema, por lo que las contraseñas difieren. Se deberá configurar la contraseña con los requisitos de seguridad exigidos.

Paso	Descripción
26.	En el siguiente paso, preguntará si se eliminan usuarios anónimos, escriba “Y” y pulse “Enter” para continuar. 
27.	El siguiente punto pregunta si deshabilitar el inicio de sesión en la base de datos de forma remota con el usuario “root”. Escriba “Y” y pulse “Enter” para continuar. 
28.	Por defecto MariaDB contiene una base de datos de ‘test’, se pregunta si debe eliminarla. Escriba “Y” y pulse “Enter” para continuar. 
29.	Se deberán recargar los privilegios de todas las tablas para que los cambios surtan efecto inmediatamente. Para ello escriba “Y” y pulse “Enter” para continuar. 
30.	Finalizará el proceso mostrando el mensaje “All done!” que garantiza que todos los campos configurados se han aplicado correctamente. 

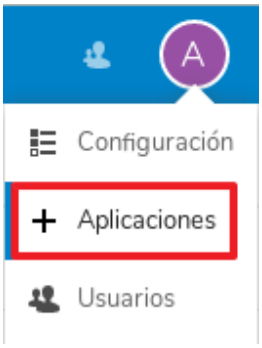
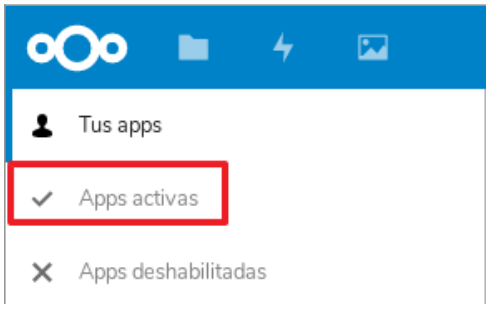
2. LIMITACIÓN DE APLICACIONES Y MÓDULOS INSTALADOS

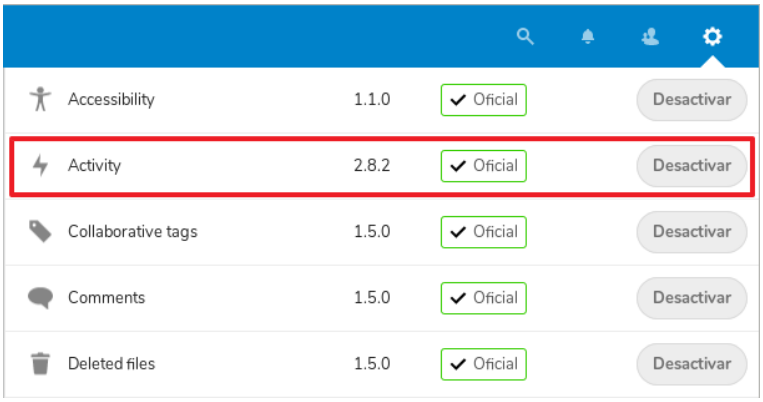
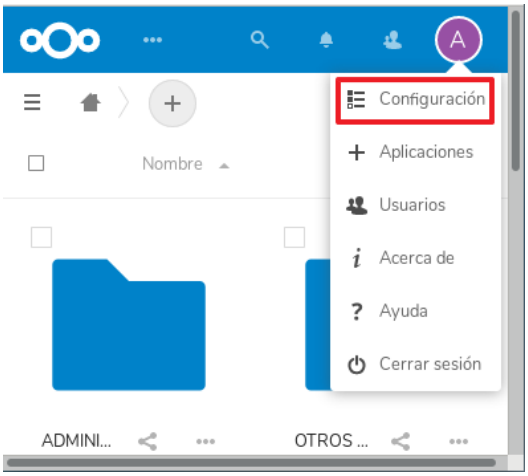
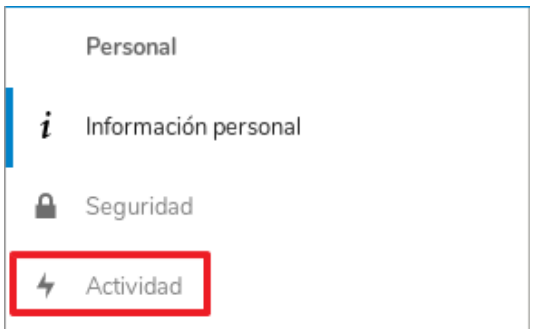
Paso	Descripción
31.	Se procede a deshabilitar aplicaciones y módulos instalados
32.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
33.	Debe iniciar sesión en la aplicación Nextcloud con una cuenta que pertenezca al grupo de Administradores. 
34.	Diríjase al icono de su usuario y en el menú desplegable pulse “+ Aplicaciones”. 

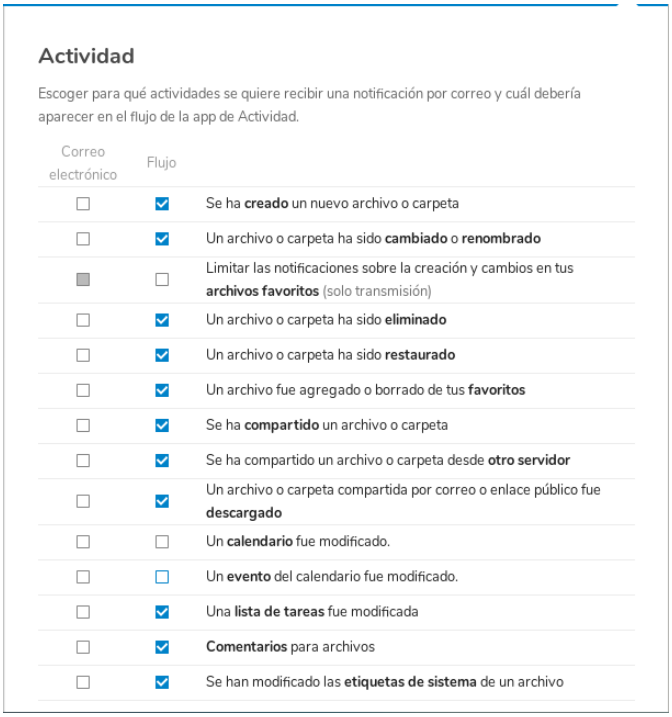
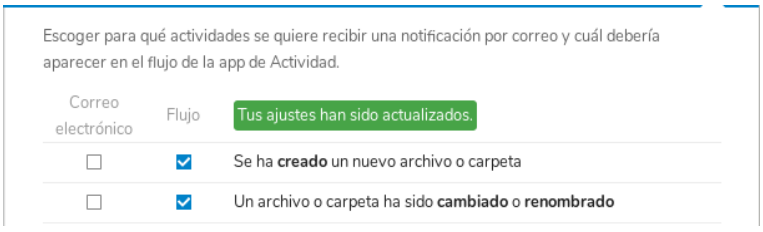
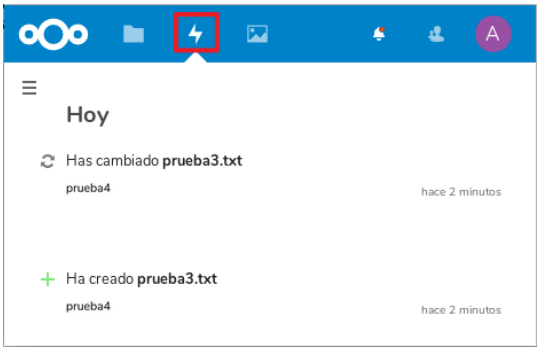
Paso	Descripción
35.	Revise las aplicaciones instaladas en su servidor y desactive las que no sean necesarias para su organización pulsando el botón “Desactivar”. 
36.	Si detecta alguna aplicación candidata para su desactivación y pulsa el botón “Desactivar”, le pedirá la contraseña del usuario Administrador para confirmar. 
37.	Si quisiera eliminar la aplicación y toda su configuración por completo, diríjase a la ruta de su servidor y liste las aplicaciones allí contenidas por medio de los siguientes comandos: **$ cd /var/www/html/nextcloud/apps** **$ ls -la** 

Paso	Descripción
38.	Revise las aplicaciones que más se ajusten con su organización y si se detecta una candidata para su eliminación ejecute el siguiente comando: **$ sudo rm -rf [Nombre_de_aplicacion]** **Nota:** En [Nombre_de_aplicacion] escriba el nombre de la aplicación que quiere eliminar respetando mayúsculas y minúsculas y sin corchetes "[]".

3. CONFIGURACIÓN DE REGISTROS DE ACTIVIDAD

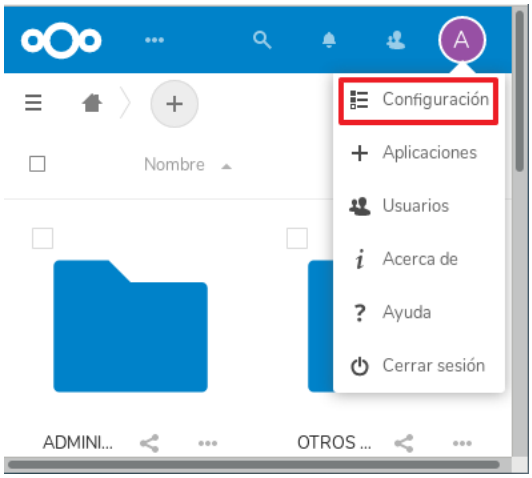
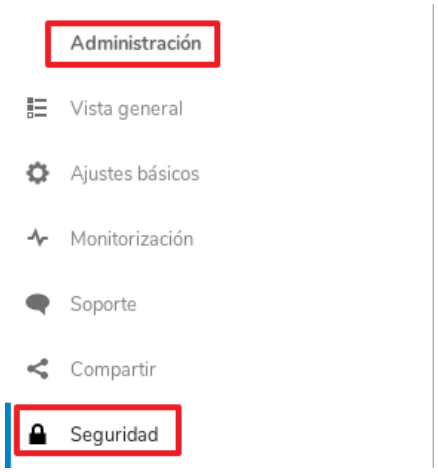
Paso	Descripción
39.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Internet" seleccione "Firefox" o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
40.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
41.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de "admin".
42.	Diríjase al icono de su usuario y en el menú desplegable pulse "Aplicaciones". 
43.	En la columna de la izquierda, en el apartado "Tus apps", seleccione "Apps activas". 

Paso	Descripción
44.	Compruebe que se encuentra activa, si no es así actívela.  **Nota:** Si por cualquier motivo la aplicación no se hubiera descargado, vaya al panel superior de navegación, elija el icono de la lupa para buscar y escriba “activity”. Posteriormente pulse “Descargar y activar”.
45.	Pulse sobre el icono de su usuario y en el menú desplegable pulse “Configuración”. 
46.	En la barra lateral izquierda en el apartado “Personal”, seleccione el icono “Actividad”. 

Paso	Descripción
47.	Seleccione y deseleccione con los registros que desee que la aplicación guarde y los registros que desee que se envíen por correo.  **Nota:** Modificando las configuraciones en el apartado “Personal”, se le notificará al correo configurado en su usuario, si quisiera modificar las configuraciones para todos los administradores, debe dirigirse al título “Administración” y seleccionar “Actividad” para modificar las notificaciones desde ahí.
48.	Cuando los ajustes se actualicen lo notificará por pantalla. 
49.	Diríjase a la barra superior de navegación y pulse sobre el icono de “actividad” para revisar los registros generados por el servidor. 

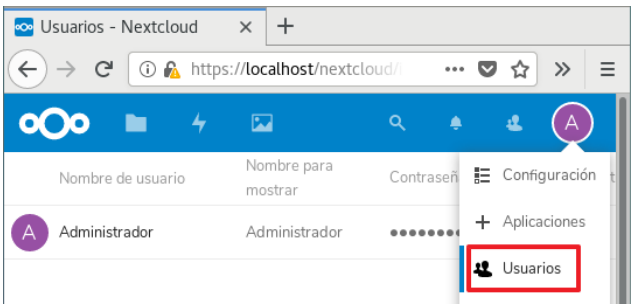
4. CONFIGURACIÓN DE USUARIOS Y POLÍTICAS DE CREDENCIALES

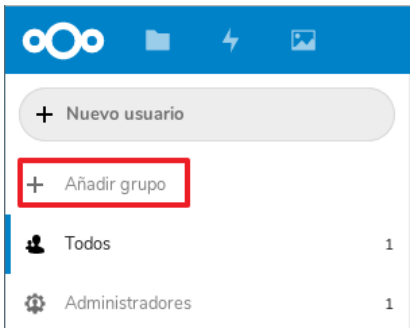
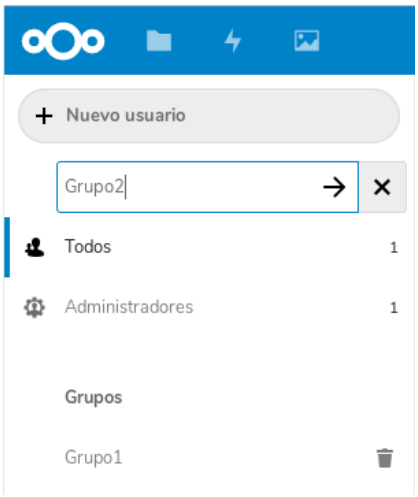
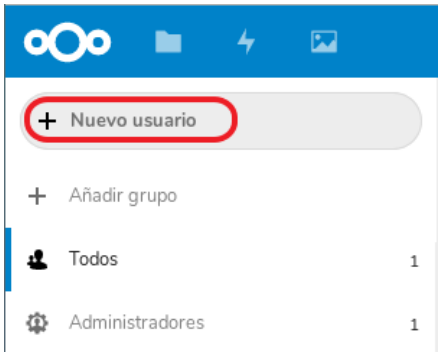
4.1. POLÍTICA DE CREDENCIALES

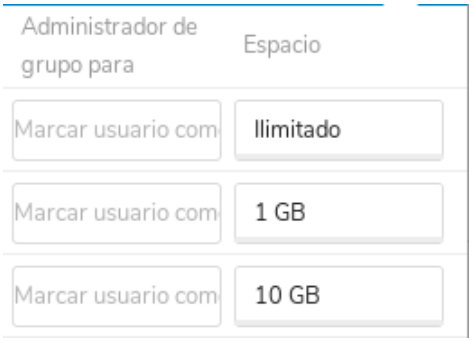
Paso	Descripción
50.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
51.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios del ENS.
52.	Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de “admin”.
53.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
54.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Seguridad”. 

Paso	Descripción
55.	Diríjase hasta el final de la página deténgase en el punto “Política de contraseñas” y establezca los siguientes parámetros: – Longitud mínima: 10 caracteres – Imponer caracteres en mayúsculas y minúsculas: seleccionado – Imponer caracteres numéricos: seleccionado – Imponer caracteres especiales: seleccionado 
56.	Para mayor seguridad y cumplimiento, se recomienda autenticación mediante LDAP. Si desea realizar la integración de usuarios por medio de LDAP, vaya al punto “ANEXO A.6.3 INTEGRACIÓN DE USUARIOS CON LDAP” de esta guía.

4.2. PERMISOS DE USUARIOS Y ESTRUCTURA DE GRUPOS

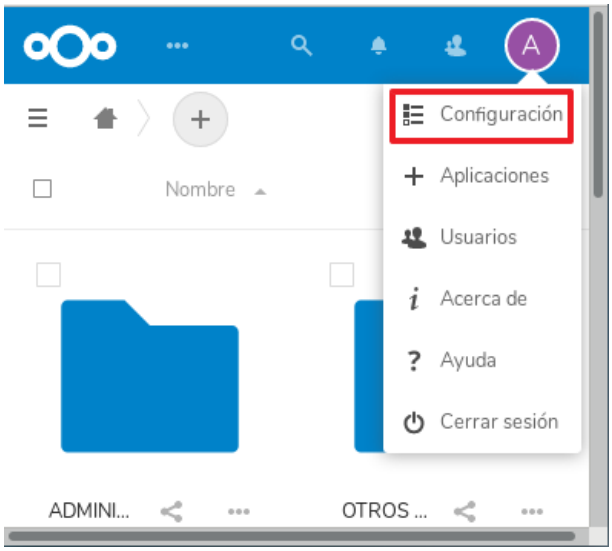
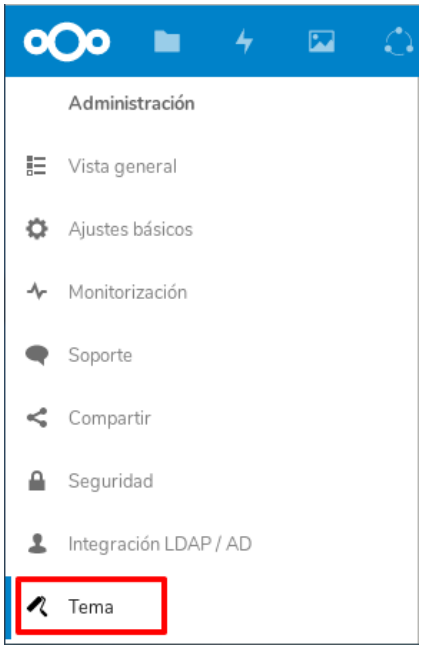
Paso	Descripción
57.	Se procede a configurar usuarios y grupos.
58.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “**Firefox**” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
59.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
60.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
61.	Diríjase al icono de su usuario y en el menú desplegable pulse “Usuarios”. 

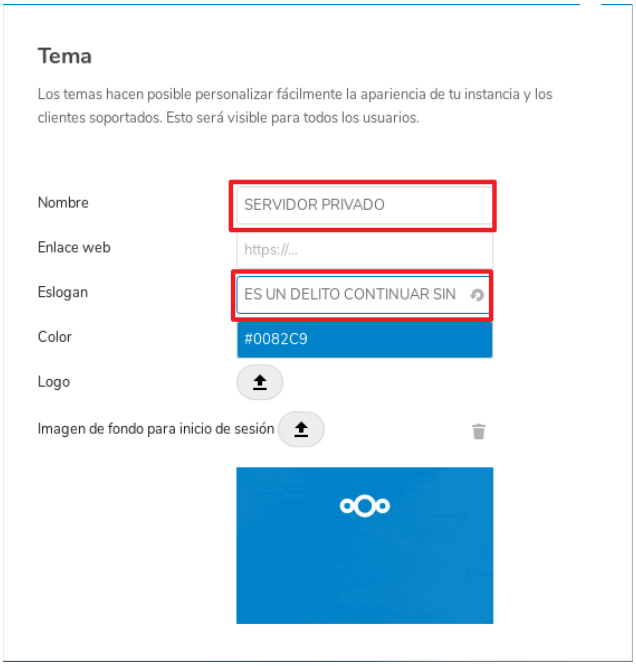
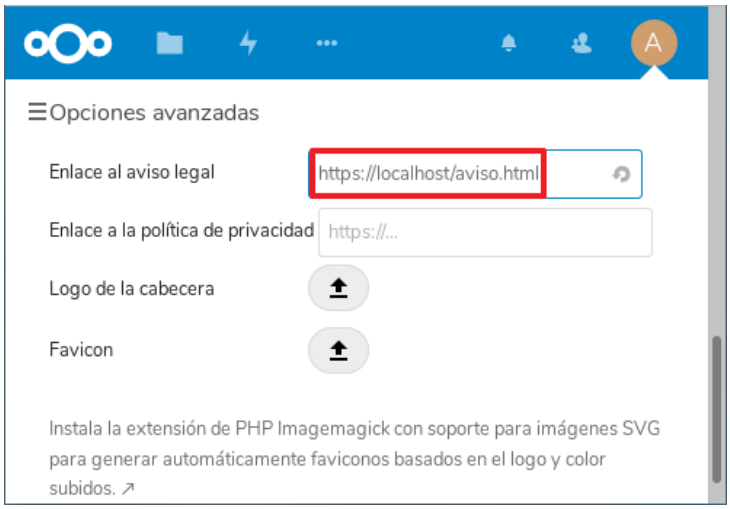
Paso	Descripción
62.	En el menú de usuarios, se recomienda empezar con la creación de grupos si no se encuentran creados aún, para ello pulse sobre "+ Añadir grupo" en la parte izquierda de la pantalla. 
63.	Se recomienda crear diferentes grupos identificando posteriormente usuarios comunes de usuarios administradores pertenecientes a cada grupo y teniendo en cuenta las preferencias y necesidades de su organización. 
64.	Una vez creados los grupos necesarios para su organización, se deberán crear los usuarios y asignarles un grupo y un rol dentro de ese grupo. El rol puede ser usuario común del grupo o usuario administrador de ese grupo. Comience creando los usuarios comunes teniendo en cuenta las preferencias y necesidades de su organización. Para ello pulse en el botón nuevo usuario. 

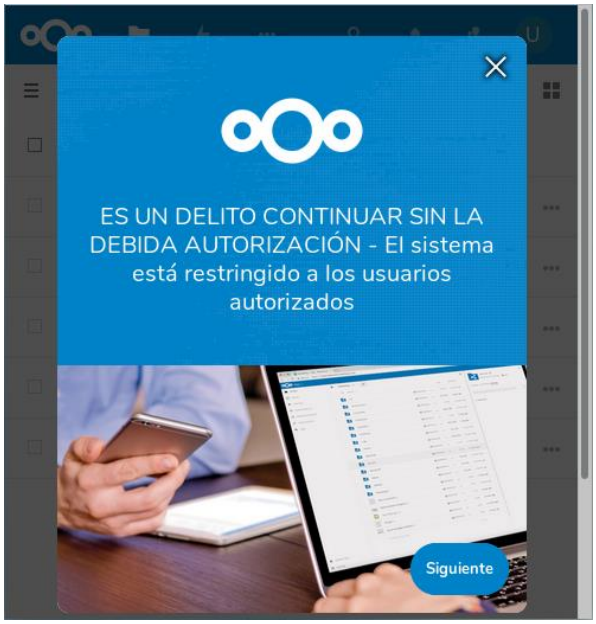
Paso	Descripción
65.	Rellene todos los campos, dejando vacío el apartado “Administrador de grupo para”. Si quisiera configurar cuotas defina éstas en el apartado “Espacio”. 
66.	Cuando finalice de rellenar todos los campos con las preferencias deseadas, diríjase al final de la línea y pulse sobre el icono de verificación para añadir y finalizar. 
67.	Se muestra una captura de ejemplo donde el “usuario_comun1” pertenece al grupo “Grupo1” con 1GB de límite de espacio en disco. En cambio, usuario_común2 pertenece al grupo “Grupo2” con 10GB de límite de espacio en disco. 

4.3. CONFIGURACIÓN MENSAJE DISUASORIO

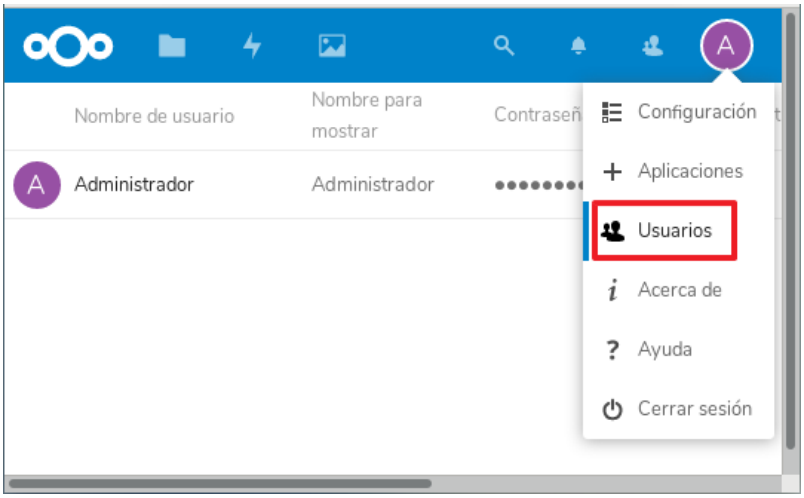
Paso	Descripción
68.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “**Firefox**” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
69.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
70.	Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de “admin”.

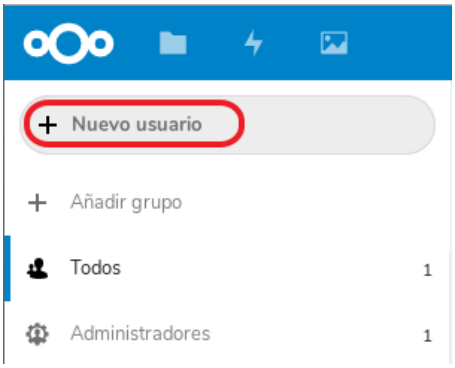
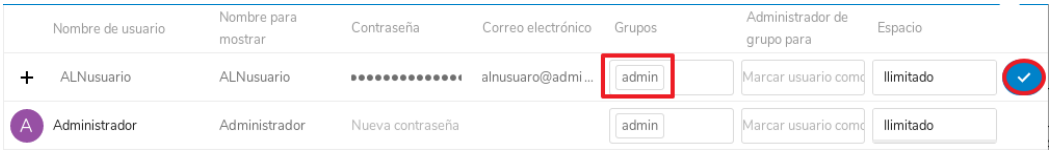
Paso	Descripción
71.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
72.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Tema”. 

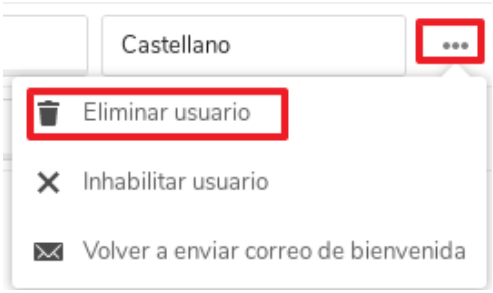
Paso	Descripción
73.	En el apartado “Nombre”, seleccione el nombre que más convenga a su organización, posteriormente en el apartado “Eslogan” configure el mensaje disuasorio que más se ajuste a las necesidades específicas de su organización.  **Nota:** Nextcloud 15 presenta mecanismos para implementar mensajes que son advertidos al usuario cuando va a realizar el inicio de la sesión. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.
74.	En el apartado “Opciones avanzadas”, si su organización lo posee, se puede añadir un enlace hacia el aviso legal de su organización. Para ello ingrese la URL correspondiente al aviso legal en el apartado “Enlace al aviso legal”. 

Paso	Descripción
75.	Compruebe que se muestra correctamente el mensaje en la pantalla de inicio de sesión. 
76.	Compruebe que se muestra correctamente el mensaje en el primer inicio de un nuevo usuario. 

5. POLÍTICA DE SEGURIDAD DE ACCESO PARA ADMINISTRADORES LOCALES

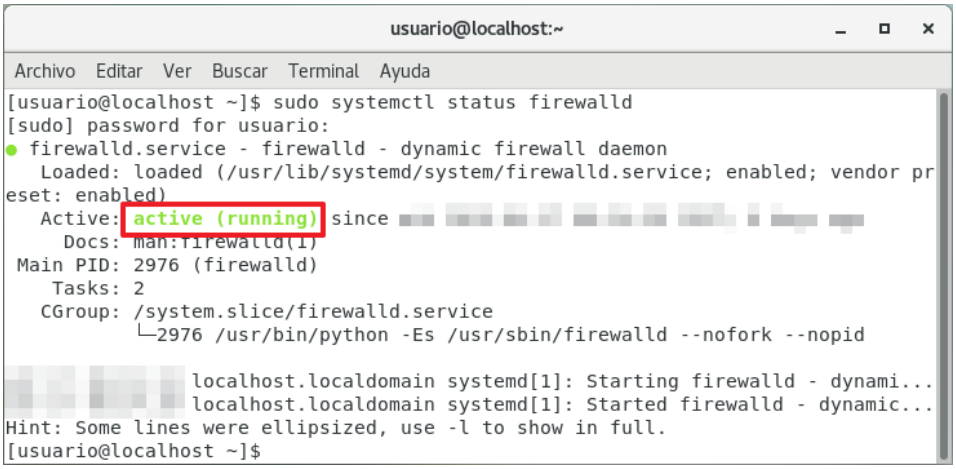
Paso	Descripción
77.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “**Firefox**” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
78.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios del ENS.
79.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
80.	Se va a proceder a modificar el usuario Administrador global del servidor de alojamiento de archivos Nextcloud. Para ello diríjase al icono de su usuario y en el menú desplegable pulse sobre el icono “Usuarios”. 
81.	Como se puede observar en la siguiente imagen, el usuario que se crea en la instalación (en este caso “Administrador”) se añade al grupo “admin”. El usuario que pertenezca al grupo “admin” el sistema lo considerará Administrador global. 

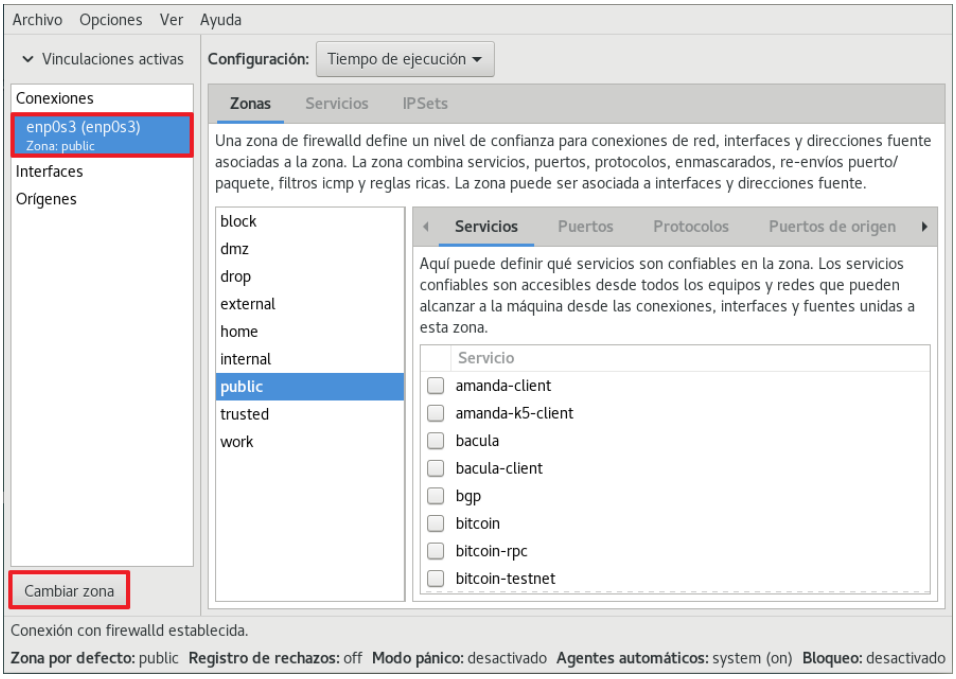
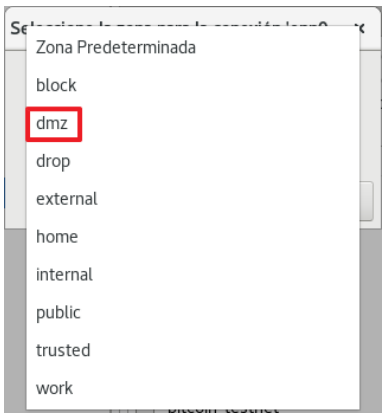
Paso	Descripción
82.	Para modificar el usuario que se creó en la instalación, se debe añadir primero un usuario nuevo y agregarlo al grupo “admin”. En este caso se pondrá un ejemplo con el usuario “ALNusuario”. 
83.	Agregue al usuario “ALNusuario” al grupo “admin”, configure los demás campos con los parámetros que más convengan a su organización y pulse el icono azul de confirmación. 
84.	Pulse sobre el icono de su usuario en el menú desplegable seleccione “Cerrar sesión”. 

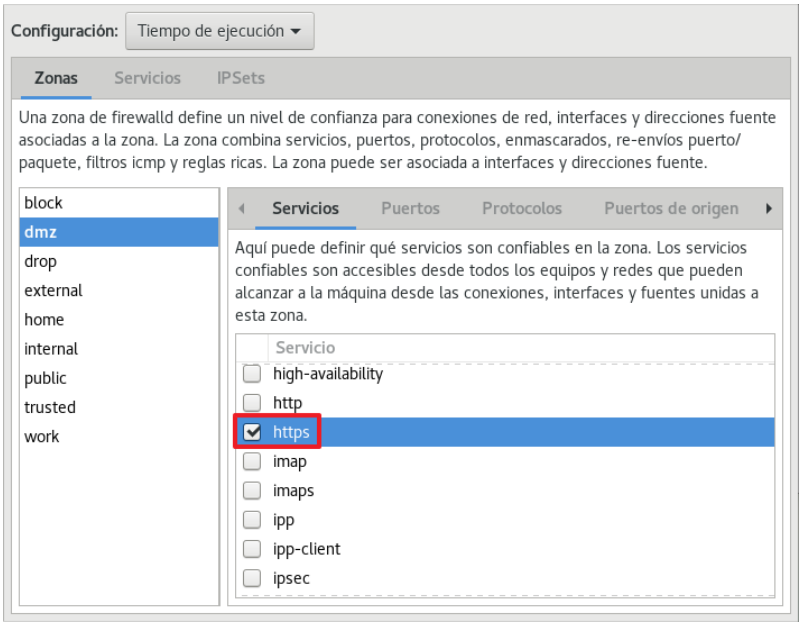
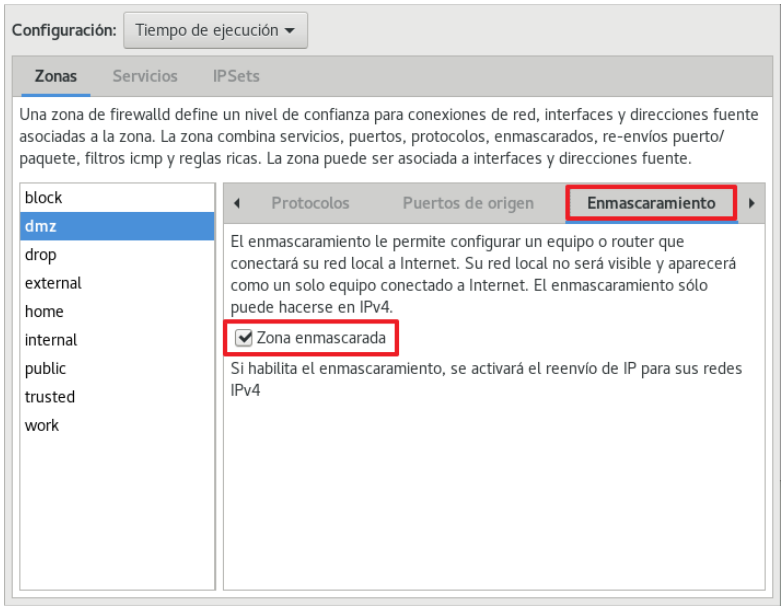
Paso	Descripción
85.	Inicie sesión con el usuario recién creado “ALNusuario” y en el icono de usuario en el menú desplegable seleccione “Usuarios”. Una vez en el menú de usuarios, elimine el usuario “Administrador” que se creó por defecto en la instalación. Para ello pulse en el icono “…” y seleccione “Eliminar usuario”. 
86.	Posteriormente se creará un usuario administrador de grupos. Para ello se creará el usuario “ALGusuario” y se le asignarán los grupos anteriormente creados. Modifique estos valores con los requerimientos específicos de su organización.  **Nota:** Si necesita revisar el modo de creación de usuarios y grupos, diríjase al punto 53 del apartado 3.2 PERMISOS DE USUARIOS Y ESTRUCTURA DE GRUPOS.
87.	Para finalizar diríjase al final de la línea y pulse sobre el icono de verificación para añadir y finalizar. 

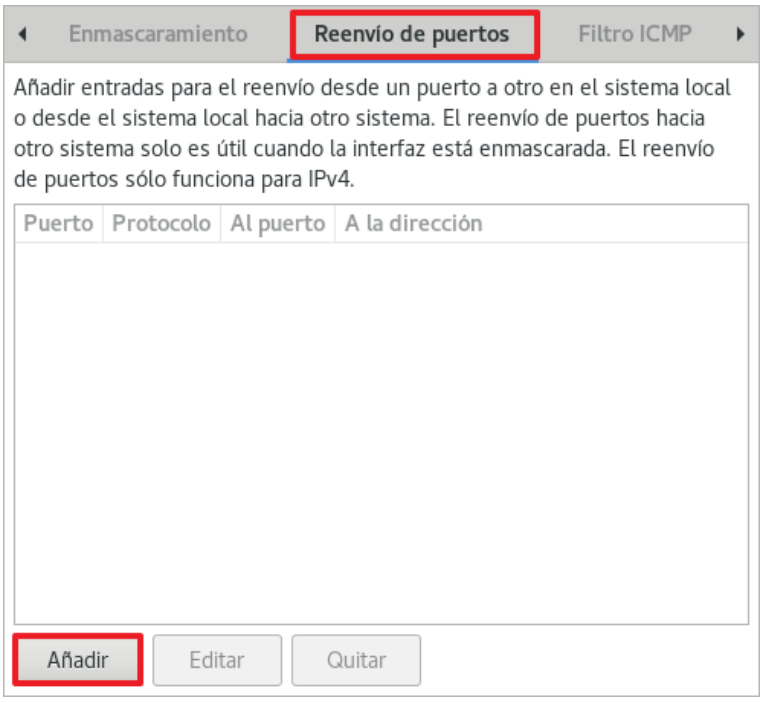
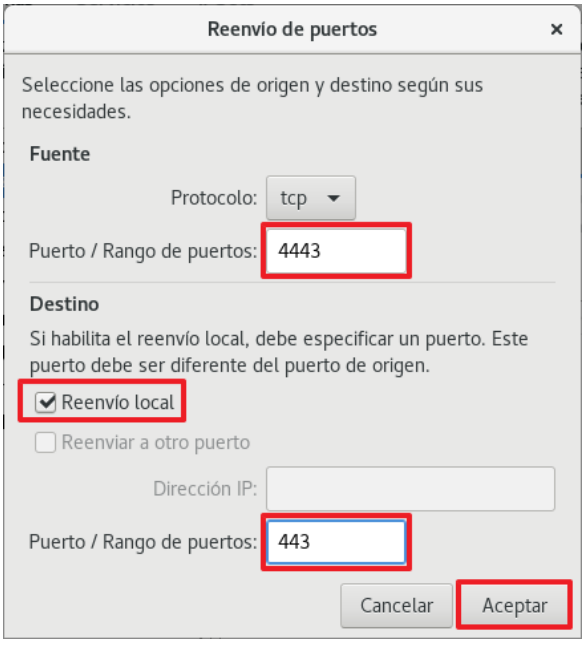
6. CONFIGURACIÓN DE FIREWALLD PARA SERVICIOS NEXTCLOUD

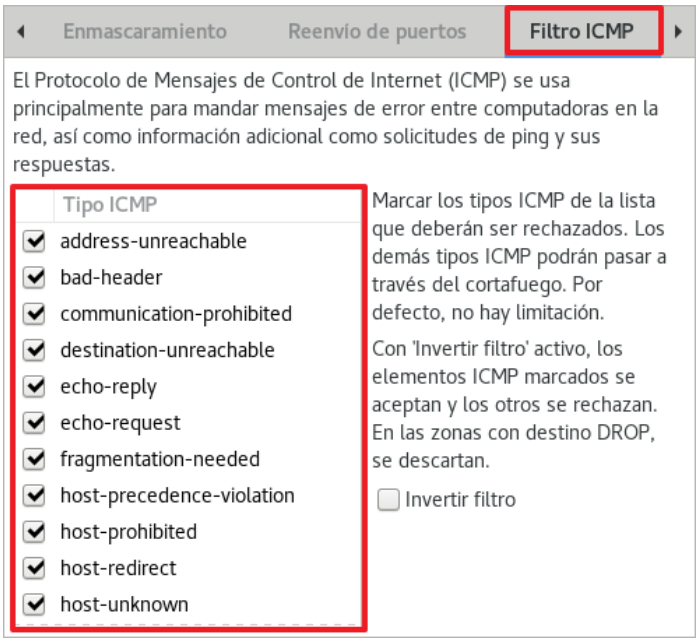
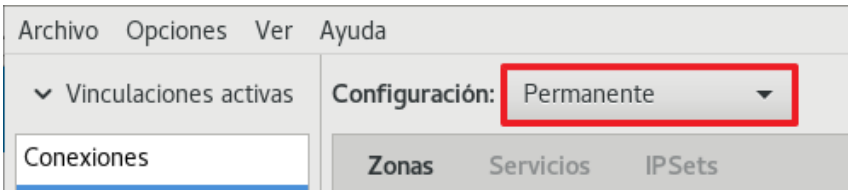
Paso	Descripción
88.	Si ha cerrado la “**Terminal** “en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “**Terminal**”. Ejecute el comando **“cd /”** y pulse la tecla “Enter”.

Paso	Descripción
89.	El primer paso es comprobar el estado del servicio firewalld, además se debe reiniciar y configurar para que arranque al inicio. Para todo ello ejecute los siguientes comandos. **$ sudo systemctl restart firewalld** **$ sudo systemctl enable firewalld** **$ sudo systemctl status firewalld** 
90.	Para iniciar el asistente gráfico diríjase a la barra de tareas, pulse en **"Aplicaciones"** → **"Varios"** → **"Cortafuegos"**. Introduzca la contraseña si se la solicita. 

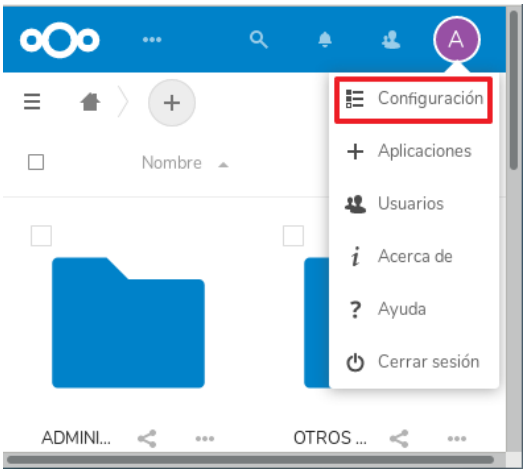
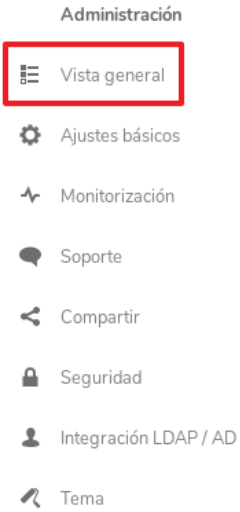
Paso	Descripción
91.	Seleccione su interfaz y pulse en el botón “Cambiar zona”. 
92.	En el menú desplegable podrá seleccionar la zona que más convenga a su organización, en este ejemplo se seleccionará la zona “DMZ”. 

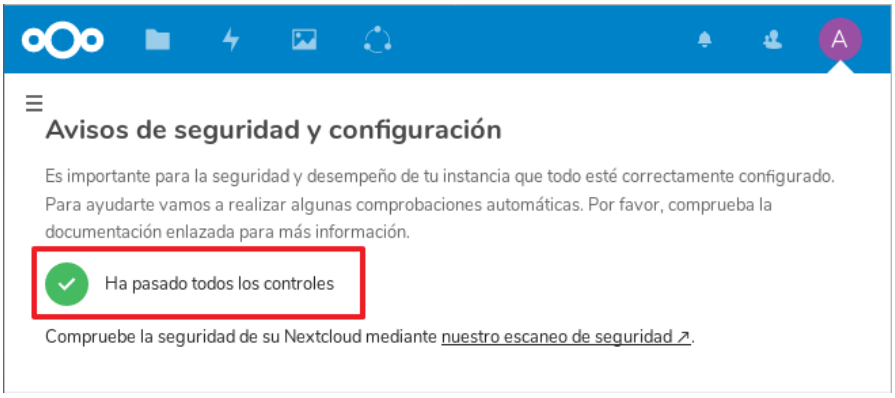
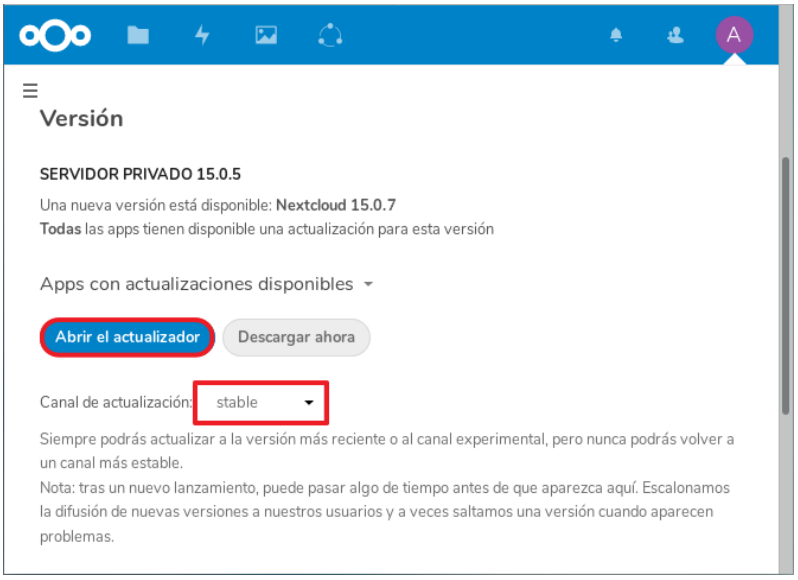
Paso	Descripción
93.	Una vez seleccione la zona deseada, deberá habilitar los servicios y puertos que le sean de aplicación en su entorno, para ello comience dirigiéndose a **"Zonas" → "Servicios"** y habilite los servicios necesarios en su organización, el servicio por **http** deberá encontrarse **desactivado**.  **Nota:** Deberá evaluar la necesidad de servicios, puertos y protocolos activos en el servidor, reduciendo a los mínimos necesarios cumpliendo con el principio de mínima exposición.
94.	Otro punto de revisión es el de Enmascaramiento. Si le es de aplicación en su organización diríjase al apartado "Enmascaramiento" y seleccione "Zona enmascarada". De esta manera la red local no será visible y se publicará solo un equipo hacia redes externas.  **Nota:** Hay que tener en cuenta que el enmascaramiento solo funcionará en redes IPv4.

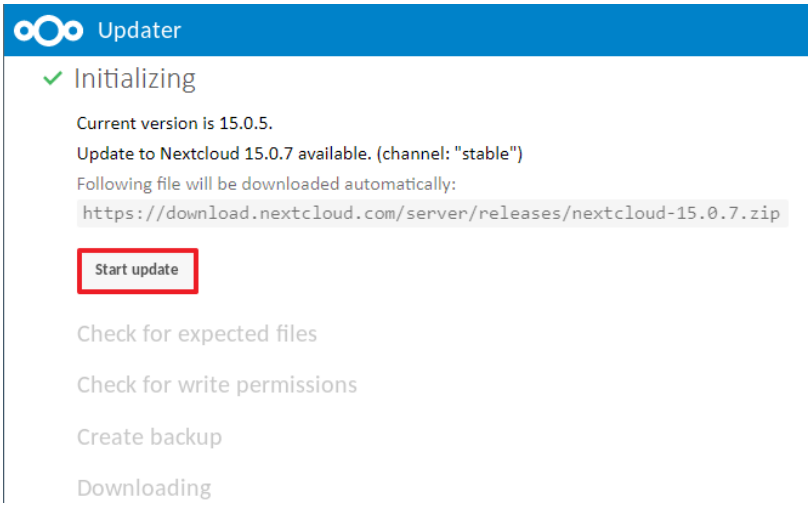
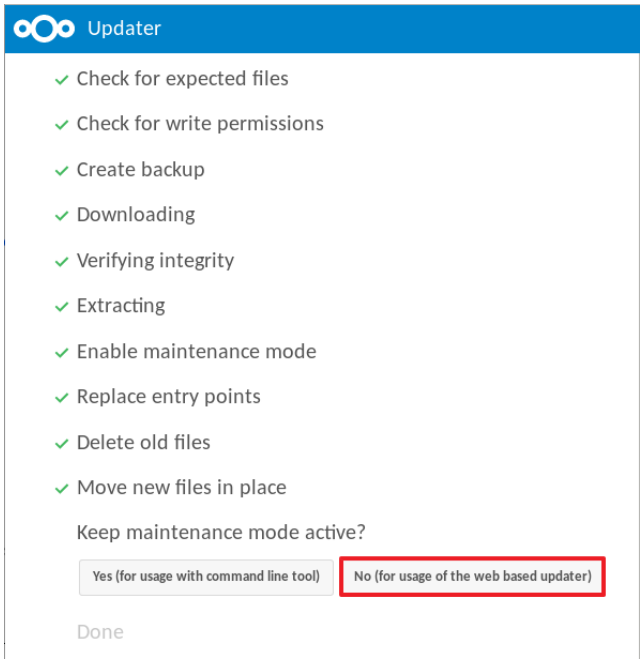
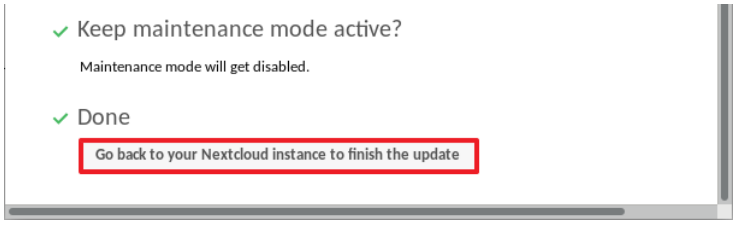
Paso	Descripción
95.	Se recomienda modificar los puertos por defecto (443,80…etc.) en los que el servidor acepta solicitudes. Si su servidor Nextcloud acepta solicitudes en un puerto distinto al habitual, diríjase al punto “Reenvío de puertos” para ajustar esta característica en el firewall de CentOS 7. Se va a configurar un ejemplo que fuerza el reenvió al puerto 443 si se realizan peticiones desde el puerto 4443. Para ello pulse en “Añadir”. 
96.	Como se puede observar en la imagen adjunta, se selecciona el puerto tcp 4443 como “Fuente” y en “Destino” se selecciona “Reenvío local” y en “Puerto / Rango de puertos:” el puerto 443 correspondiente al servicio https. Cuando finalice de configurar pulse “Aceptar”. 

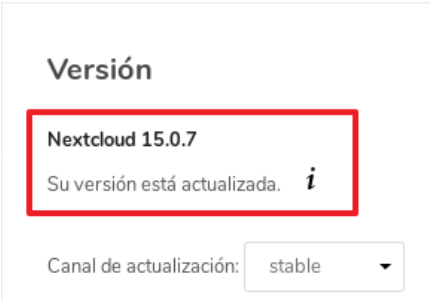
Paso	Descripción
97.	Posteriormente se debe revisar el apartado Filtro ICMP. Deberá de realizar un análisis para bloquear o permitir los distintos mensajes de control que sean de aplicación en su organización.  **Nota:** Al seleccionar los diferentes tipos de mensajes de control, se aplicarán automáticamente los bloqueos. Esto se debe a que la configuración del firewall es en "Tiempo de ejecución".
98.	Una vez comprobada la funcionalidad de la configuración realizada anteriormente, deberá de realizarla de nuevo de forma permanente. Para ello vaya al inicio de la pantalla de "Configuración del cortafuegos" y en el desplegable de "Configuración" seleccione "Permanente".  **Nota:** Deberá realizar la configuración desde el paso 91 del punto 6 CONFIGURACIÓN DE FIREWALLD PARA SERVICIOS NEXTCLOUD fijándose que el apartado "Configuración" mantiene seleccionada la opción "Permanente".
99.	Cuando finalice, cierre la ventana de "Configuración del cortafuegos".

7. APLICACIÓN DE ACTUALIZACIONES

Paso	Descripción
100.	Se procede a configurar usuarios y grupos.
101.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
102.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
103.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
104.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
105.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Vista general”. 

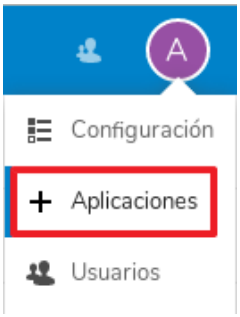
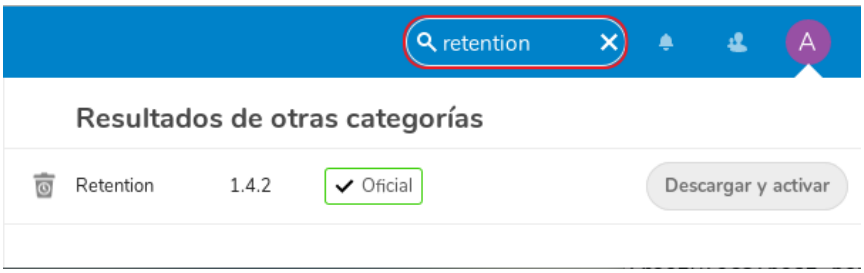
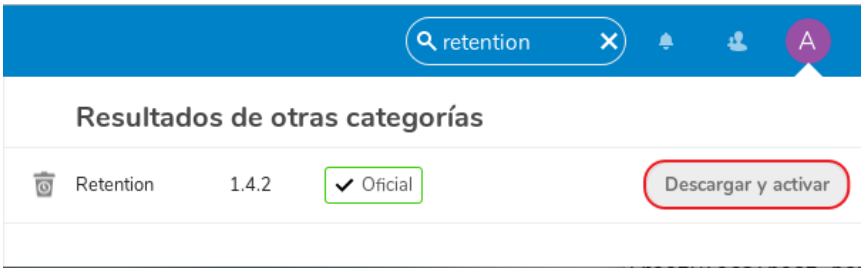
Paso	Descripción
106.	Antes de comprobar y comenzar a instalar las actualizaciones, diríjase al apartado inicial “Avisos de seguridad y configuración”. Se recomienda que solvente los problemas que pudiera notificar el servidor Nextcloud antes de comenzar a aplicar actualizaciones. Una vez solventadas las posibles cuestiones a resolver, se le notificará en el mismo apartado mediante un icono de confirmación verde y el siguiente texto “Ha pasado todos los controles”. 
107.	Posteriormente en el siguiente apartado “Versión” se notificarán las actualizaciones disponibles para su servidor. Para comenzar compruebe que en el menú desplegable “Canal de actualización” se encuentra seleccionada la opción “stable”. Posteriormente pulse “Abrir el actualizador”.  **Nota:** Los canales de actualización disponibles son los siguientes. - **production** siempre proporcionará el último nivel de parches, pero no se actualizará a la próxima versión principal de inmediato. Esa actualización generalmente ocurre con la segunda versión menor (x.0.2). - **stable** es la versión estable más reciente. Es adecuada para uso en producción y siempre se actualizará a la última versión principal. - **beta** es una versión preliminar solo para probar nuevas características, no para entornos de producción.

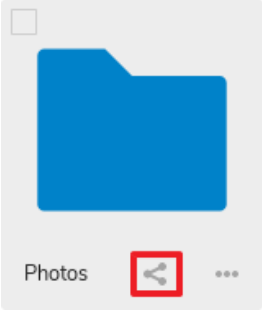
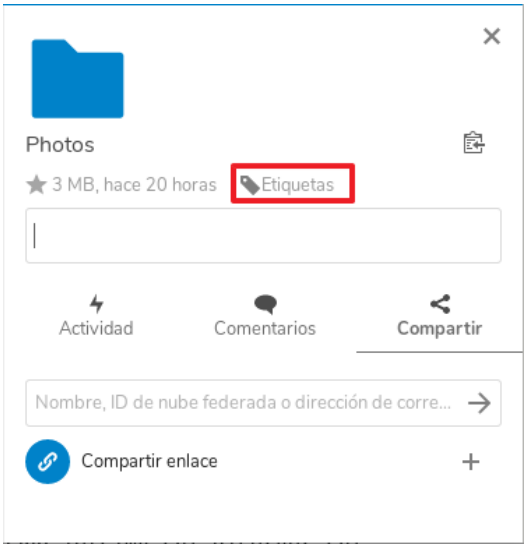
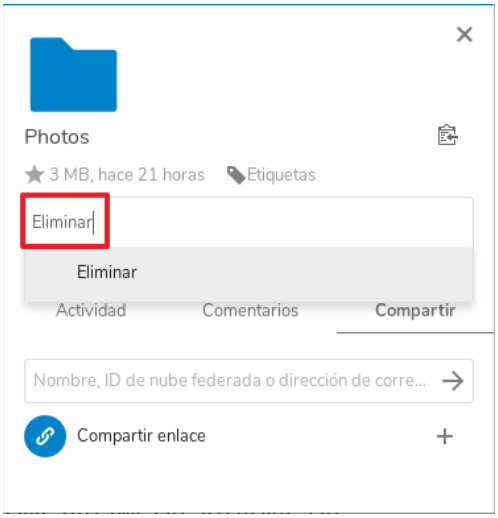
Paso	Descripción
108.	El actualizador realizará varios pasos necesarios para una correcta actualización. Para comenzar pulse “Start update”. 
109.	Cuando finalice de realizar todos los pasos necesarios preguntará si desea mantener activo el modo de mantenimiento, pulse en “No (for usage of the web based updater)”. 
110.	Al realizarlo de este modo, el servidor redireccionará hacia el updater basado en WEB. Para ello pulse en “Go back to your Nextcloud instance to finish the update”. 

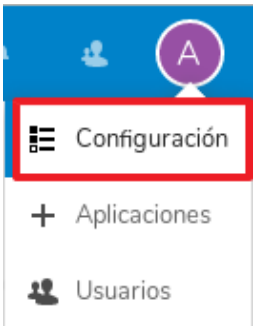
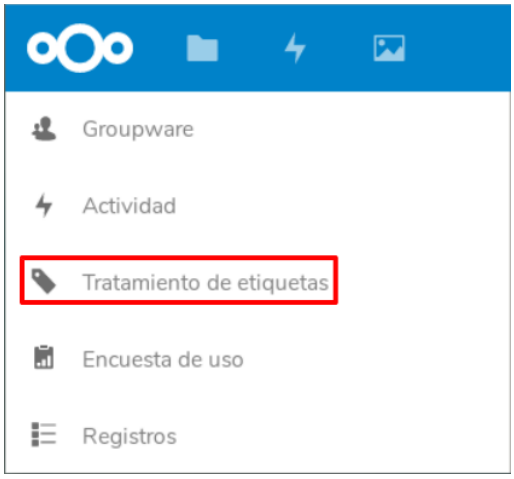
Paso	Descripción
111.	Se mostrará el asistente de actualización de Nextcloud (Updater). Lea detenidamente las advertencias y cuando esté listo pulse el botón “Iniciar actualización”. 
112.	El servidor comenzará la actualización y comprobará la integridad del código una vez finalice, al finalizar le redireccionará al servidor si el proceso ha sido satisfactorio. 
113.	Compruebe que no existen nuevas actualizaciones cuando finalice. 

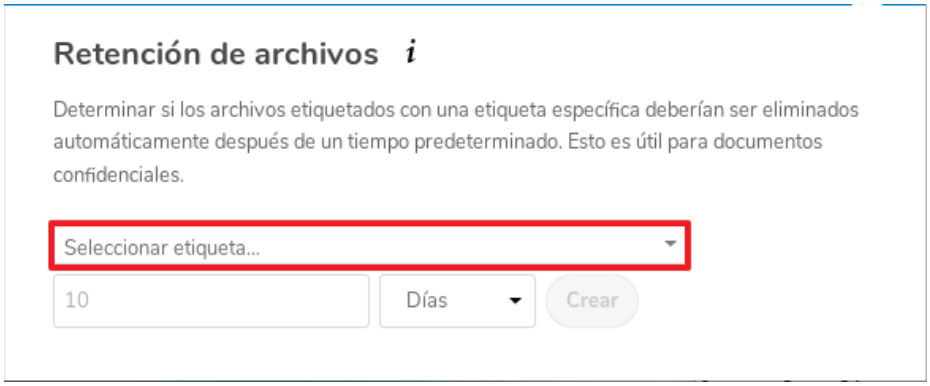
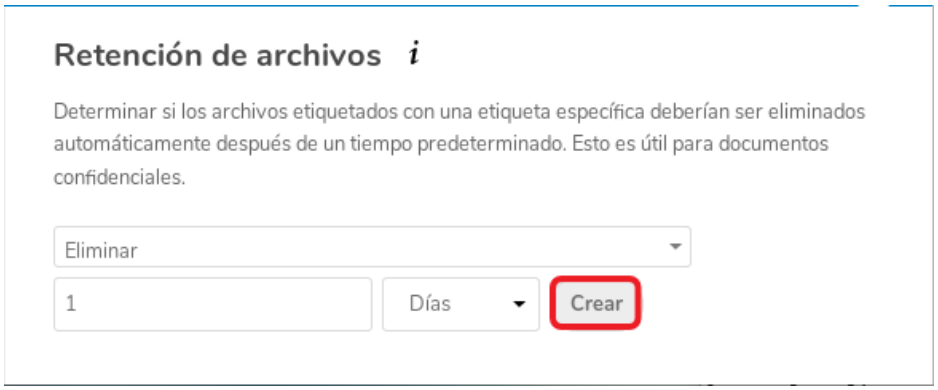
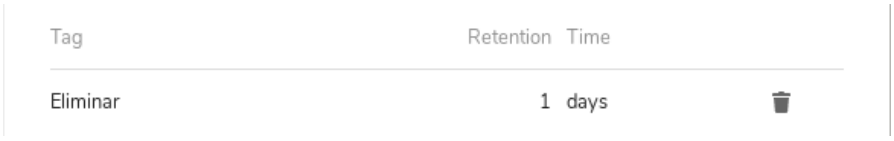
8. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

8.1. ELIMINACIÓN AUTOMÁTICA DE ARCHIVOS

Paso	Descripción
114.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
115.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
116.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
117.	Diríjase al icono de su usuario y en el menú desplegable pulse “Aplicaciones”. 
118.	En el panel de navegación superior elija el icono de la lupa para buscar y escriba el siguiente texto: “retention”. 
119.	Pulse el botón “Descargar y activar” para obtener la aplicación y que se encuentre activa en el servidor.  **Nota:** Fíjese siempre que las aplicaciones lleven el recuadro verde que garantice que son aplicaciones **oficiales** y por tanto están aprobadas por los desarrolladores de Nextcloud.

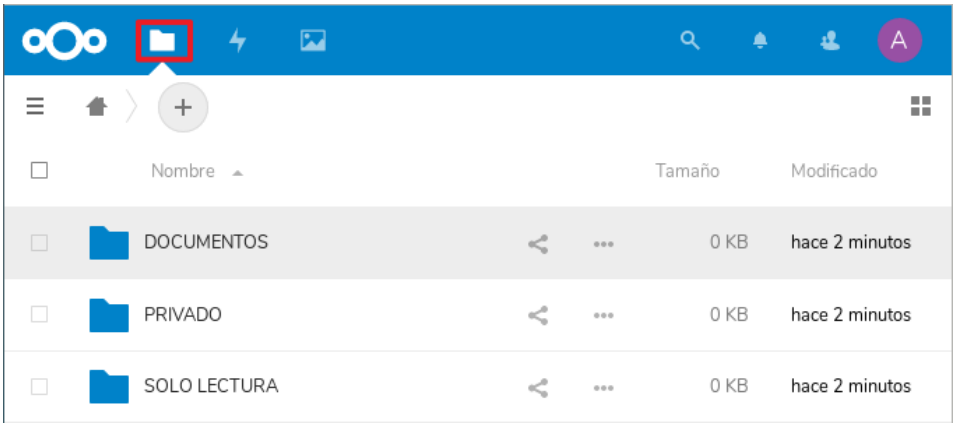
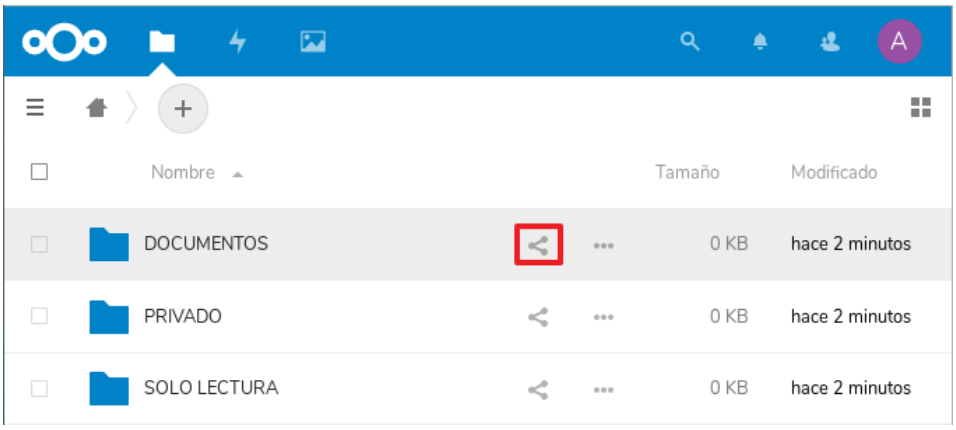
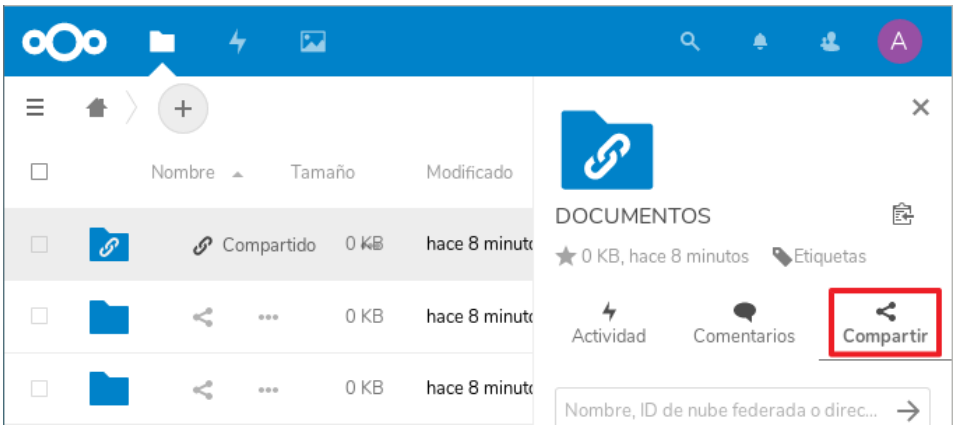
Paso	Descripción
120.	Para programar la eliminación automática de archivos se deben asignar etiquetas anteriormente. Se muestra un ejemplo a continuación de asignación de etiquetas a un archivo alojado en el servidor. Diríjase a los archivos del servidor elija el fichero que quiere programar su eliminación y pulse el icono compartir. 
121.	Se desplegará automáticamente un menú a la derecha de la pantalla. Pulse en "Etiquetas" para añadir una etiqueta. 
122.	Escriba una etiqueta característica para marcar ese fichero o directorio y pulse "Enter". 

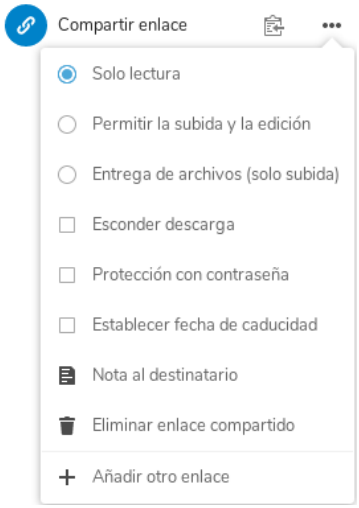
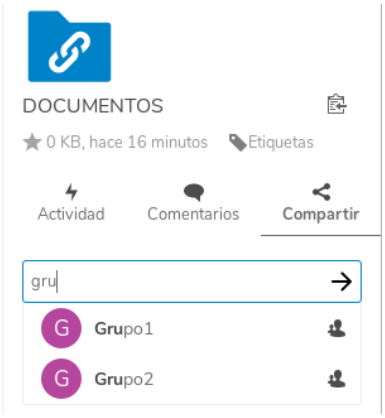
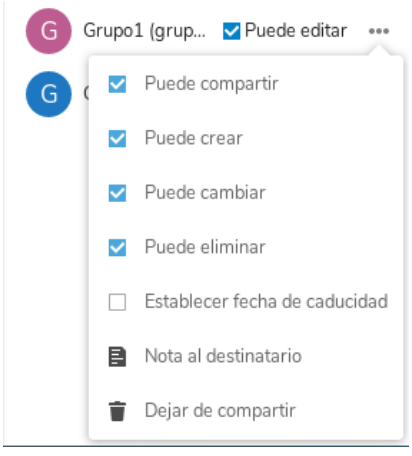
Paso	Descripción
123.	Compruebe que se añade la etiqueta correctamente al fichero o directorio. 
124.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
125.	En la columna de la izquierda seleccione “Flujo de trabajo”.  **Nota:** Debido a las constantes actualizaciones que se producen el producto “**Nextcloud**”, los títulos de las opciones o apartados, podrían sufrir alguna discrepancia con respecto al momento de la elaboración de esta guía. Por ejemplo, en versiones anteriores de la 15.0.7, la aplicación “retention”, en su opción de “Flujo de trabajo” cambia el nombre a “Tratamiento de etiquetas”, manteniendo el mismo icono.

Paso	Descripción
126.	Diríjase al título “Retención de archivos” y en la pestaña “Seleccionar etiqueta…” elija la etiqueta creada anteriormente. En este ejemplo será la etiqueta “Eliminar”. 
127.	Configure la franja de tiempo en la que el fichero o directorio se eliminará y pulse el botón “Crear” para finalizar. 
128.	Se creará la regla en el servidor.  **Nota:** Tenga en cuenta que todo archivo que contenga esta etiqueta se eliminará en la franja de tiempo configurada en la regla.

8.2. COMPARTICIÓN DE CARPETAS Y DOCUMENTOS

Paso	Descripción
129.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “**Firefox**” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
130.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.

Paso	Descripción
131.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
132.	Diríjase al icono “Archivos” para que se muestren todos los documentos de su usuario. 
133.	Seleccione el icono compartir para desplegar las opciones de compartición. 
134.	Se mostrará el menú de propiedades del directorio, seleccionando el apartado “Compartir”. 

Paso	Descripción
135.	Se crea automáticamente el apartado “Compartir enlace”, pulse sobre “…” y seleccione los permisos que más convengan a su organización. 
136.	Posteriormente diríjase a la barra de búsqueda de usuarios y grupos ubicada justo encima y seleccione los usuarios y grupos a los que se le compartirá la carpeta. 
137.	Una vez seleccionado el Grupo o el usuario, pude permitir o denegar los permisos del mismo en el interior de la carpeta. Además, puede seleccionar una fecha de caducidad para la compartición de la carpeta. 

ANEXO A.4.2. LISTA DE COMPROBACIÓN DEL SERVIDOR NEXTCLOUD 15 PARA LA CATEGORÍA MEDIA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.4.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES NEXTCLOUD 15 QUE LES SEA DE APLICACIÓN LA CATEGORÍA MEDIA DEL ENS".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores de alojamiento de archivos Nextcloud 15 independientes con implementación de seguridad de categoría media del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas con permisos "root" e iniciar sesión con usuarios de Nextcloud pertenecientes al grupo "admin". Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario perteneciente al grupo de "sudoers". Las consolas y herramientas que se utilizarán son las siguientes:

a) Terminal de Linux

b) Entorno Web Nextcloud 15

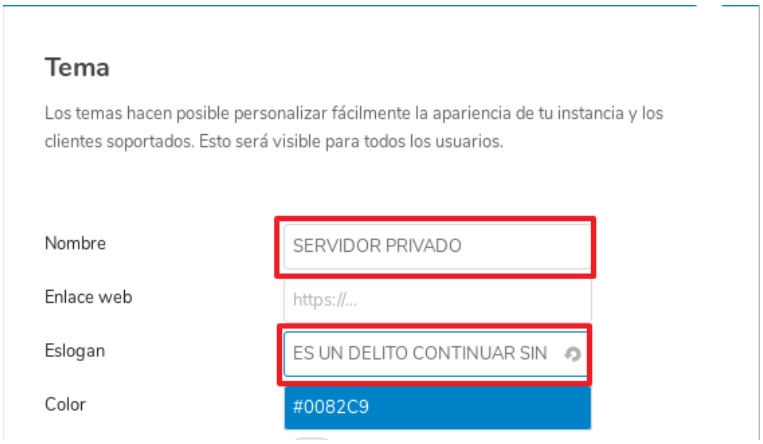
Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En el cliente, inicie sesión con una cuenta con privilegios de root.
2. Inicie la Terminal de Linux		Ejecute la "Terminal". Para ello Diríjase a la barra de tareas, pulse en Aplicaciones y en el apartado "Herramientas del sistema" seleccione "Terminal". 

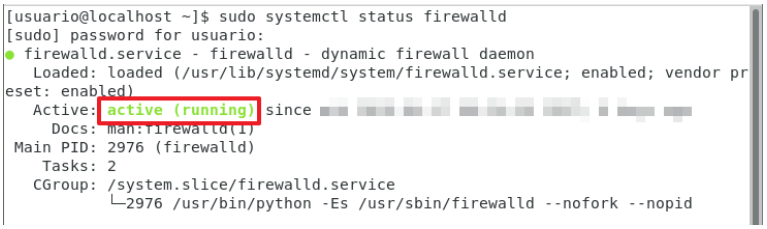
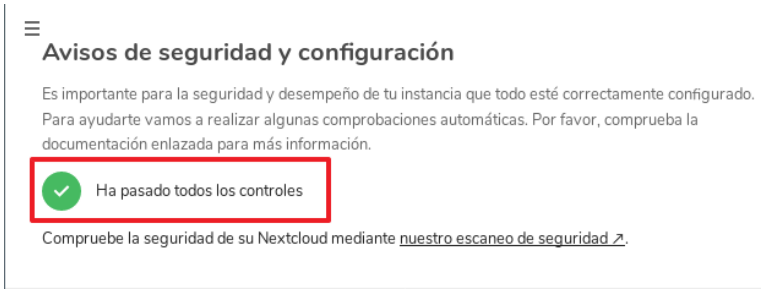
Comprobación	OK/NOK	Cómo hacerlo

3. Verifique versiones del conjunto de servidores LAMP.		En la "Terminal" ejecute los siguientes comandos y verifique las versiones instaladas.
		$ sudo yum info mariadb
		$ sudo yum info httpd
		$ sudo php -v
		`Paquetes instalados`
		`Nombre : httpd`
		`Arquitectura : x86_64`
		`Versión : 2.4.6`
		`Lanzamiento : 88.el7.centos`
		`Tamaño : 9.4 M`
		`Repositorio : installed`
		`Desde el repositorio : base`
		`Resumen : Apache HTTP Server`
		`URL : http://httpd.apache.org/`
		`Licencia : ASL 2.0`
		`Descripción :The Apache HTTP Server is a powerful,`
		`: web server.`
		Nota: Debe adecuar las versiones a las necesidades y compatibilidad de los diferentes elementos de su organización, teniendo en cuenta que las versiones deben ser las últimas con soporte y recomendadas por el desarrollador.

4. Comprobación de repositorios remi activos.		Abra la Terminal y ejecute el siguiente comando.
		$ sudo ls /etc/yum.repos.d/remi*
		usuario@localhost:~
		Archivo Editar Ver Buscar Terminal Ayuda
		`[usuario@localhost ~]$ sudo ls /etc/yum.repos.d/remi*`
		`/etc/yum.repos.d/remi-glpi91.repo`
		`/etc/yum.repos.d/remi-glpi92.repo`
		`/etc/yum.repos.d/remi-glpi93.repo`
		`/etc/yum.repos.d/remi-glpi94.repo`
		`/etc/yum.repos.d/remi-modular.repo`
		`/etc/yum.repos.d/remi-php54.repo`
		`/etc/yum.repos.d/remi-php70.repo`
		`/etc/yum.repos.d/remi-php71.repo`
		`/etc/yum.repos.d/remi-php72.repo`
		`/etc/yum.repos.d/remi-php73.repo`
		`/etc/yum.repos.d/remi.repo`
		`/etc/yum.repos.d/remi-safe.repo`
		`[usuario@localhost ~]$`
		Nota: Tenga en consideración que a medida que aparezcan nuevas versiones, los repositorios pueden variar.

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th colspan="3">Cómo hacerlo</th></tr>
<tr><td></td><td colspan="4"><table>
<tr><th>Configuración</th><th>OK/NOK</th></tr>
<tr><td>/etc/yum.repos.d/remi-glpi91.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-glpi92.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-glpi93.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-glpi94.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-modular.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-php54.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-php70.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-php71.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-php72.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi-php73.repo</td><td></td></tr>
<tr><td>/etc/yum.repos.d/remi.repo</td><td></td></tr>
</table></td></tr>
<tr><td>5. Ficheros de configuración Apache.</td><td></td><td colspan="3">Ejecute los siguientes comandos y compruebe que es correcta la configuración según las necesidades específicas de su organización.
$ sudo gnome-text-editor /etc/httpd/conf/httpd.conf &>/dev/null
$ sudo gnome-text-editor /etc/httpd/conf.d/nextcloud.conf &>/dev/null</td></tr>
<tr><td>6. Ficheros de configuración PHP.</td><td></td><td colspan="3">Ejecute los siguientes comandos y compruebe que es correcta la configuración según las necesidades específicas de su organización.
$ sudo gnome-text-editor /etc/php.ini &>/dev/null
$ sudo gnome-text-editor /etc/php.d/10-opcache.ini &>/dev/null</td></tr>
<tr><td>7. Comprobación de cifrado seguro.</td><td></td><td colspan="3">Inicie sesión en la base de datos MariaDB y compruebe los parámetros requeridos, para ello ejecute los siguientes comandos.
$ sudo mysql -u root -p
MariaDB [(none)]> use nextcloud;
MariaDB [nextcloud]>select * from oc_users;
MariaDB [nextcloud]>exit;
+----------+
| password |
+----------+
| 2|$argon2i$v=19$m=1024,t=2, p=[redacted] |
| 2|$argon2i$v=19$m=1024,t=2, p=[redacted] |
| 2|$argon2i$v=19$m=1024,t=2, p=[redacted] |
+----------+
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Usuario Administrador</td><td>2|$argon2i$v=19$m=1024,t=2,</td><td></td></tr>
<tr><td>Resto de usuarios</td><td>2|$argon2i$v=19$m=1024,t=2,</td><td></td></tr>
</table></td></tr>
</table>

<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>8. Aplicaciones instaladas</td><td></td><td>Compruebe que las aplicaciones existentes en el servidor Nextcloud son las mínimas necesarias para su organización. Para ello ejecute el siguiente comando.
$ sudo ls /var/www/html/nextcloud/apps</td></tr>
<tr><td>9. Inicie sesión en el servidor Nextcloud</td><td></td><td>Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “Firefox” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud. Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de “admin”.</td></tr>
<tr><td>10. Registros de actividad</td><td></td><td>Vaya al icono de su usuario y en el menú desplegable pulse “Aplicaciones” → “Apps activas” y compruebe que se encuentra instalada y activada la aplicación “Activity”.</td></tr>
<tr><td rowspan="6">11. Política de contraseñas</td><td></td><td>Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración” → “Administración” → “Seguridad” → “Política de contraseñas”.</td></tr>
<tr><td colspan="2"><table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Longitud mínima</td><td>10</td><td></td></tr>
<tr><td>Imponer caracteres en mayúsculas y minúsculas</td><td>☑</td><td></td></tr>
<tr><td>Imponer caracteres numéricos</td><td>☑</td><td></td></tr>
<tr><td>Imponer caracteres especiales</td><td>☑</td><td></td></tr>
</table></td></tr>
<tr><td>12. Mensaje disuasorio</td><td></td><td>Vaya al icono de su usuario y en el menú desplegable pulse “Configuración” → “Administración” → “Tema” y compruebe que se encuentran configurados los apartados remarcados en la siguiente imagen.
 
</td></tr>
</table>

Comprobación	OK/NOK	Cómo hacerlo
13. Demonio Firewalld		Ejecute el siguiente comando y compruebe que el firewall de CentOS 7 Linux se encuentra activo. **$ sudo systemctl status firewalld** 
14. Firewall CentOS 7 Linux		Vaya a la barra de tareas, pulse en **"Aplicaciones" → "Varios" → "Cortafuegos"**. En el apartado "Configuración:" seleccione en el menú desplegable la opción "Permanente" y revise su configuración.
15. Avisos de seguridad.		Vaya al icono de su usuario y en el menú desplegable pulse **"Configuración" → "Administración" → "Vista general"** y compruebe que se no existen avisos de seguridad y se muestra el mensaje "Ha pasado todos los controles". 
16. Retención de archivos		Vaya al icono de su usuario y en el menú desplegable pulse **"Aplicaciones" → "Apps activas"** y compruebe que se encuentra instalada y activada la aplicación "Retention".

ANEXO A.5. CATEGORÍA ALTA

ANEXO A.5.1. PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES NEXTCLOUD 15 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS

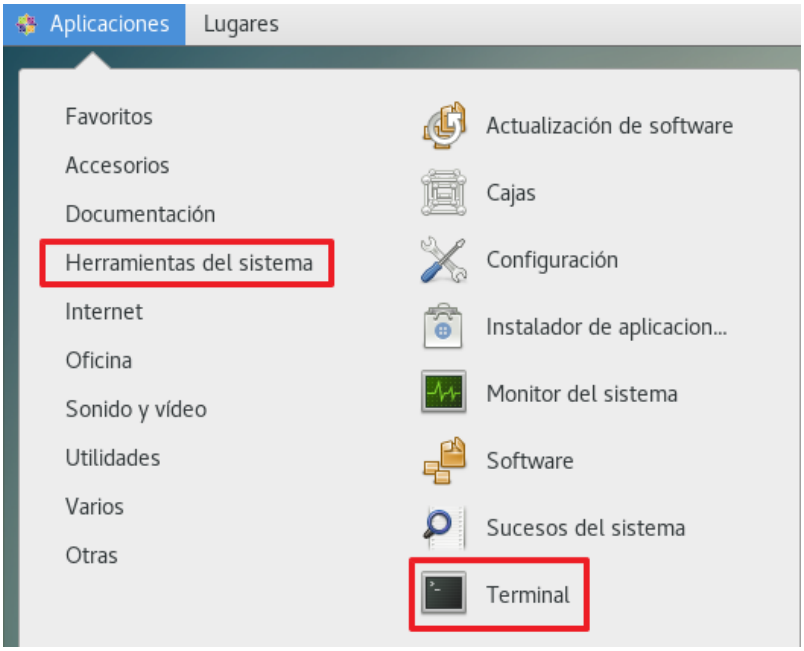
El presente anexo ha sido diseñado para ayudar a los operadores de sistemas a realizar una implementación de seguridad en escenarios donde se empleen servidores de alojamiento de archivos Nextcloud 15 sobre Sistema Operativo CentOS 7.4 Linux con una categorización de seguridad alta según los criterios 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 la categoría de cada una de las dimensiones de seguridad según se establece en el Anexo I del RD 3/2010. Si el conjunto resultante para todos los servicios e información manejada por la organización correspondieran a la categoría alta, 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.

Los pasos que se describen a continuación se realizarán en todos aquellos servidores de alojamiento de archivos Nextcloud 15 sobre Sistema Operativo CentOS 7.4 Linux con categoría alta aplicada según guía CCN-STIC-619 independientes a un dominio, que implementen servicios o información de categoría alta y se encuentren supeditados al cumplimiento del Esquema Nacional de Seguridad.

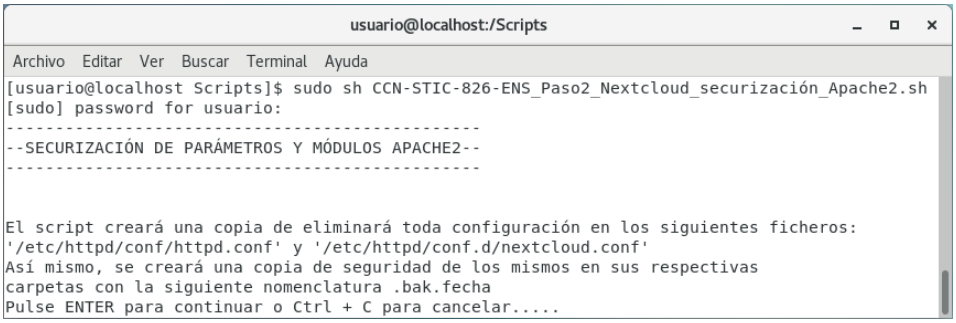
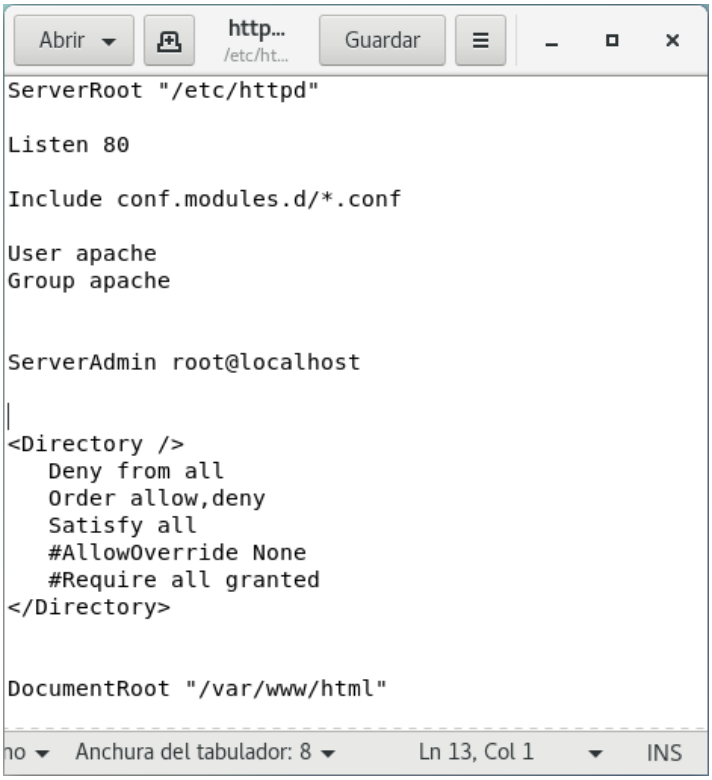
1. CONFIGURACIÓN SEGURA DE APACHE, PHP Y MARIADB PARA NEXTCLOUD

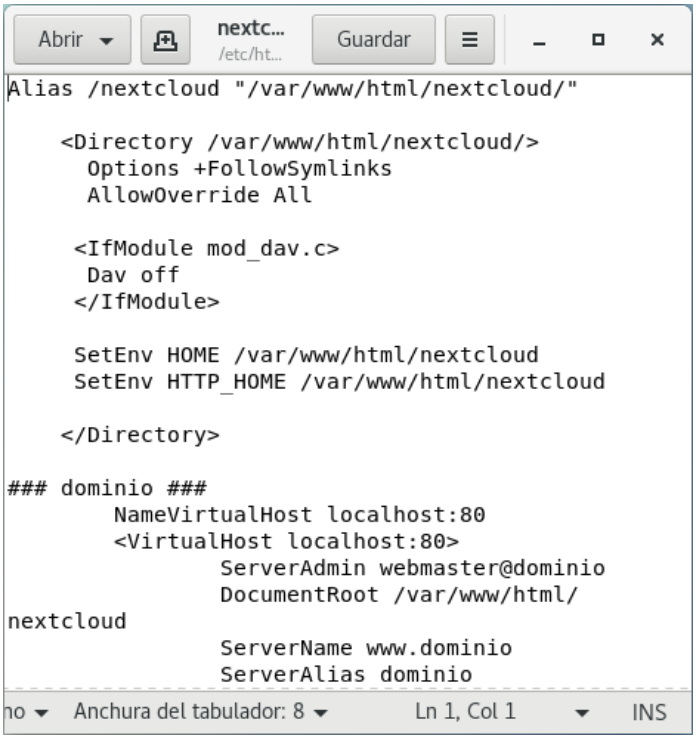
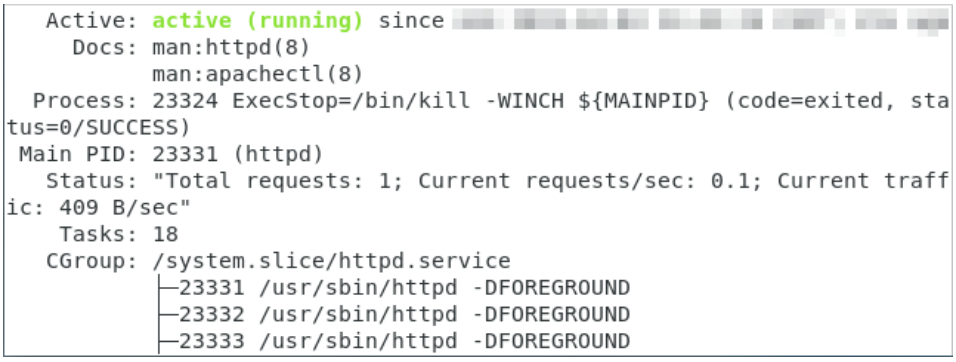
Paso	Descripción
1.	Inicie sesión en el servidor independiente donde se va a instalar Nextcloud según criterios de ENS.
2.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o “Sudoers”.
3.	Cree el directorio **“Scripts”** en **“/”** y copie aquí el contenido de la carpeta asociada a la categorización del equipo desde el medio de almacenamiento correspondiente. Deberá asignarles los permisos pertinentes para la ejecución de los mismos.

Paso	Descripción
4.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
5.	Ejecute el comando **“cd /Scripts/”** y pulse la tecla “Enter”.
6.	Posteriormente ejecute “**ls -l**” y compruebe que están todos los scripts.

1.1. APACHE 2

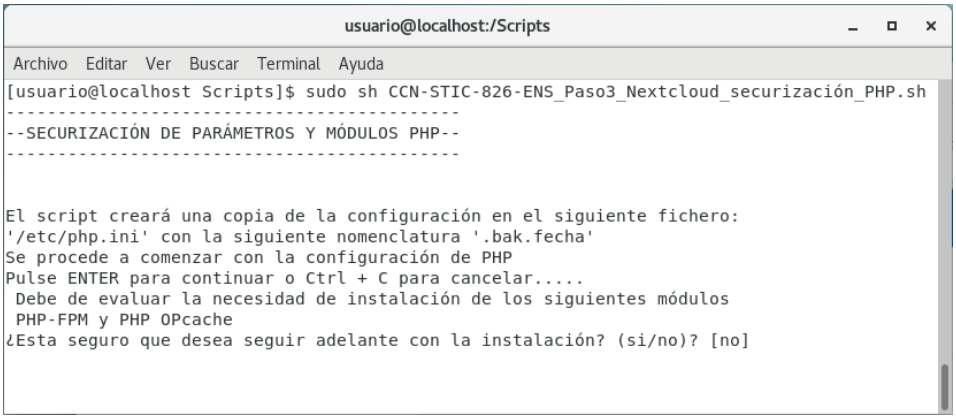
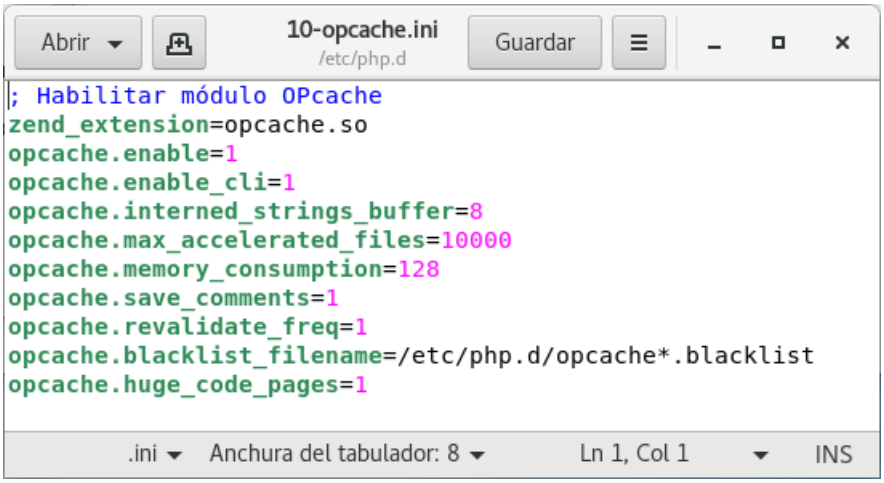
Paso	Descripción
7.	Si ha cerrado la “**Terminal** “en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “**Terminal**”. Ejecute el comando **“cd /”** y pulse la tecla “Enter”.
8.	Se procederá a securizar el servidor web Apache. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts**

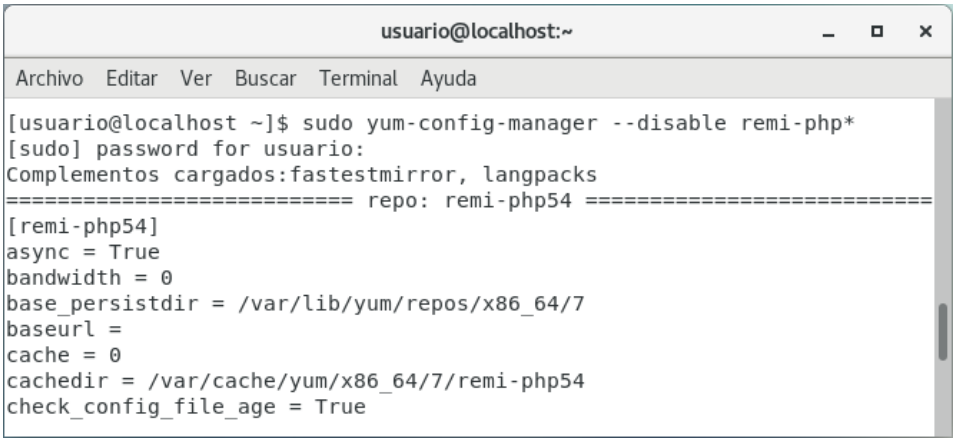
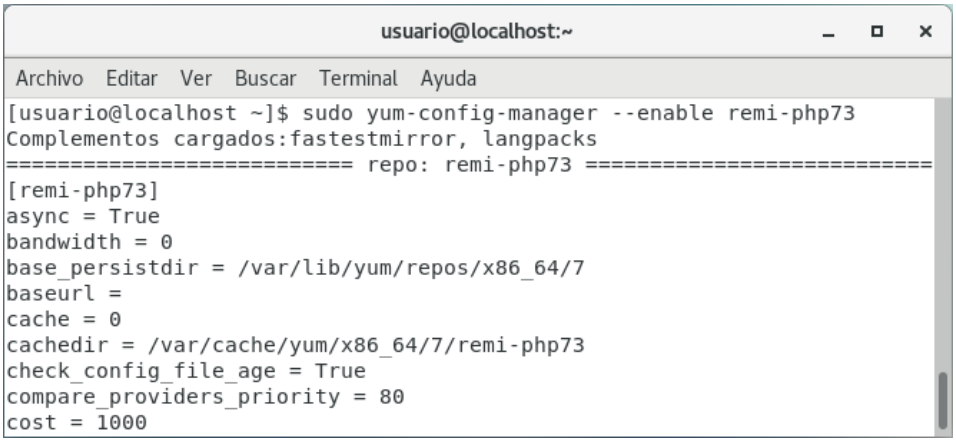
Paso	Descripción
9.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-826-ENS_Paso2_Nextcloud_securización_Apache2.sh** El script iniciará un proceso de instalación de los módulos “mod_security” y “mod_evasive” de Apache. Además, modificará los ficheros de configuración “/etc/httpd/conf/httpd.conf” y “/etc/httpd/conf.d/nextcloud.conf” eliminando toda configuración contenida en los mismos.  **Nota:** Tenga en cuenta que el script configura parámetros en rutas por defecto, si escoge un servidor web que no sea apache deberá adaptar el script a las necesidades específicas de su organización.
10.	El script mostrará el fichero “/etc/httpd/conf/httpd.conf” con una configuración aplicada con ejemplos y líneas comentadas (#) que deberá revisar y ajustar con los parámetros que más convengan a su organización. Cuando finalice pulse “Guardar” y cierre el editor de textos. 

Paso	Descripción
11.	Posteriormente el script mostrará el fichero "/etc/httpd/conf.d/nextcloud.conf" con una configuración aplicada con ejemplos y líneas comentadas (#) que, del mismo modo, deberá revisar y ajustar con los parámetros que más convengan a su organización. Cuando finalice pulse "Guardar" y cierre el editor de textos. 
12.	Finalmente compruebe que el servicio se ha reiniciado correctamente. 

1.2. PHP

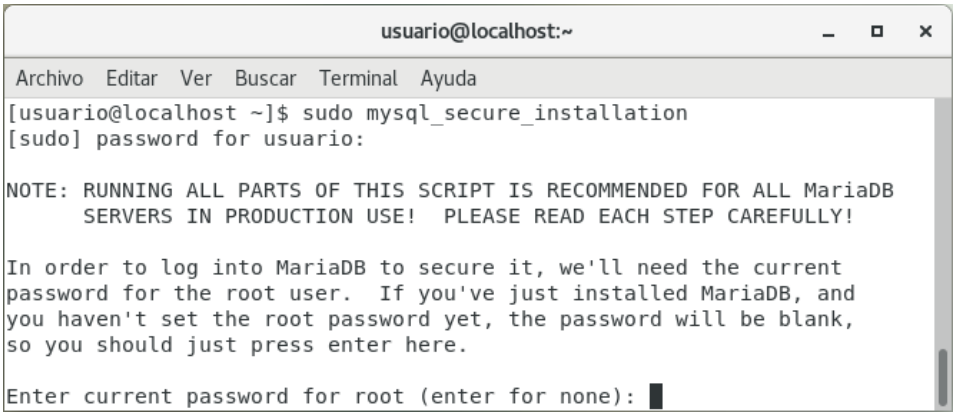
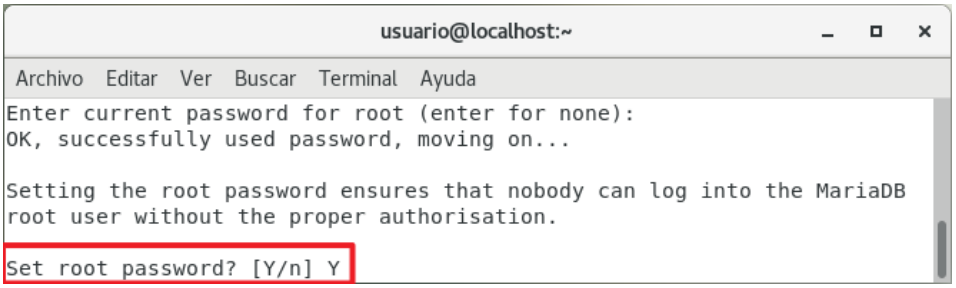
Paso	Descripción
13.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".

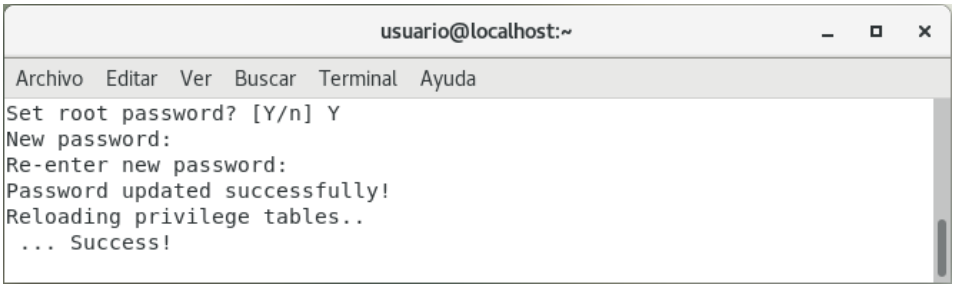
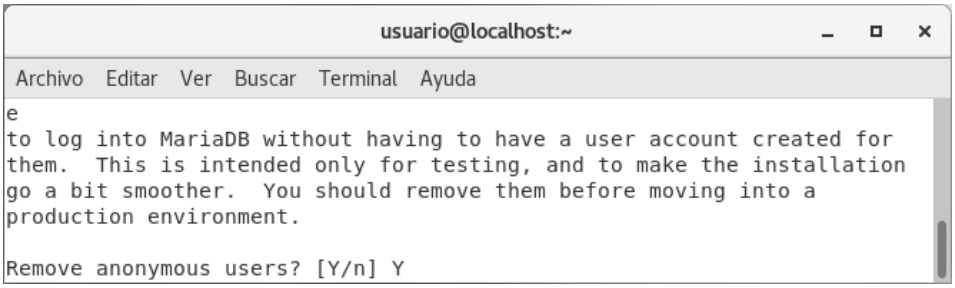
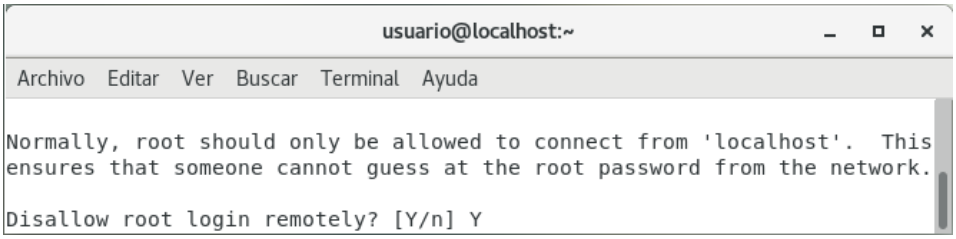
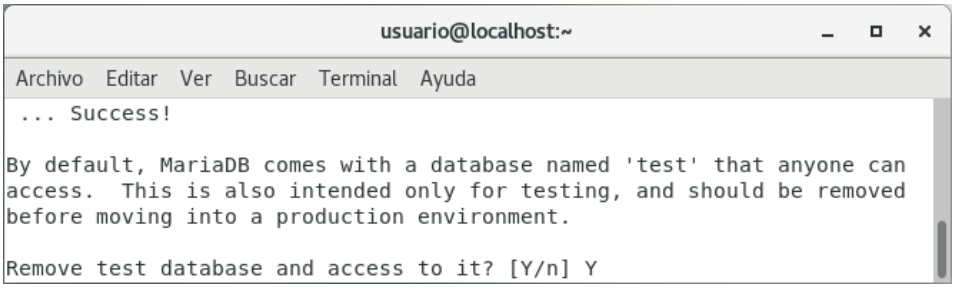
Paso	Descripción
14.	Se procederá a securizar el servicio PHP. Para ello diríjase a la carpeta “Scripts”. **$ cd /Scripts**
15.	Ejecute el siguiente comando. **$ sudo sh CCN-STIC-826-ENS_Paso3_Nextcloud_securización_PHP.sh** Deberá evaluar la necesidad de los siguientes módulos “PHP-FPM” y “PHP OPcache” de PHP. El script le preguntará sobre las acciones al respecto, si los módulos son adecuados para su organización escriba “si” y pulse “Enter” para continuar con la instalación, si por el contrario no son necesarios escriba “no” y pulse “Enter” y el script finalizará.  usuario@localhost:/Scripts Archivo Editar Ver Buscar Terminal Ayuda [usuario@localhost Scripts]$ sudo sh CCN-STIC-826-ENS_Paso3_Nextcloud_securización_PHP.sh --SECURIZACIÓN DE PARÁMETROS Y MÓDULOS PHP-- El script creará una copia de la configuración en el siguiente fichero: '/etc/php.ini' con la siguiente nomenclatura '.bak.fecha' Se procede a comenzar con la configuración de PHP Pulse ENTER para continuar o Ctrl + C para cancelar..... Debe de evaluar la necesidad de instalación de los siguientes módulos PHP-FPM y PHP OPcache ¿Esta seguro que desea seguir adelante con la instalación? (si/no)? [no] **Nota:** El módulo PHP-FPM mejora notablemente la velocidad en servidores web de alto tráfico y OPcache mejora el rendimiento de PHP almacenando el código de bytes de un script precompilado en la memoria compartida, eliminando así la necesidad de que PHP cargue y analice los script en cada petición.
16.	Si ha escrito “si” el script proseguirá instalando los módulos y mostrando la configuración del fichero “/etc/php.d/10-opcache.ini” para su revisión. Se deben configurar los parámetros que más convengan a su organización.  Abrir 10-opcache.ini /etc/php.d Guardar ; Habilitar módulo OPcache zend_extension=opcache.so opcache.enable=1 opcache.enable_cli=1 opcache.interned_strings_buffer=8 opcache.max_accelerated_files=10000 opcache.memory_consumption=128 opcache.save_comments=1 opcache.revalidate_freq=1 opcache.blacklist_filename=/etc/php.d/opcache*.blacklist opcache.huge_code_pages=1 .ini Anchura del tabulador: 8 Ln 1, Col 1 INS Cuando finalice de configurar, pulse el botón “Guardar” y cierre el editor de texto.

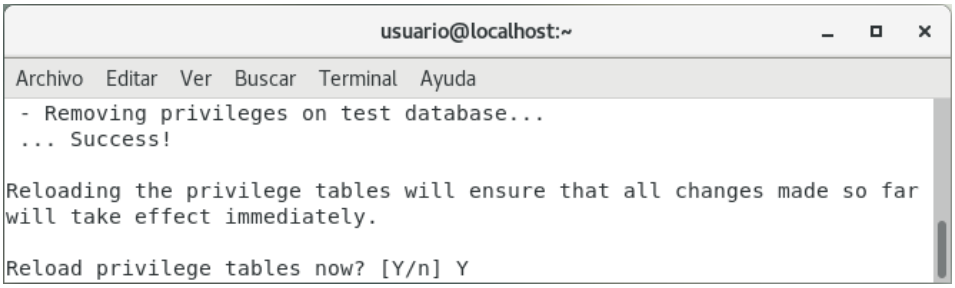
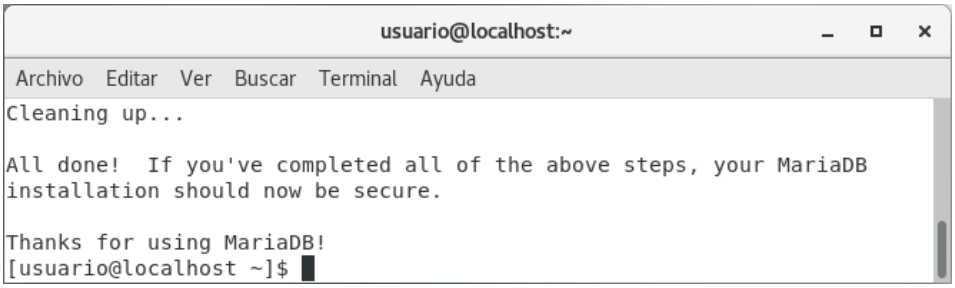
Paso	Descripción
17.	El servidor Apache se reiniciará, compruebe que se reinicia sin errores.
18.	Posteriormente se procederá a la actualización de php por medio del repositorio "remi". Para ello deshabilite los repositorios activos de php ejecutando el siguiente comando: **$ sudo yum-config-manager --disable remi-php*** 
19.	Ahora habilite el repositorio correspondiente a la versión de php más actualizada soportada por el sistema operativo y en versión estable. **$ sudo yum-config-manager --enable remi-php[XX][3]**  **Nota:** Si desea saber la versión que más se ajusta con las necesidades de su organización diríjase al siguiente enlace: https://www.php.net/.
20.	Por último, ejecute el siguiente comando para actualizar el sistema por completo y que se aplique versión actualizada de php: **$ sudo yum -y update**

[3] Deberá adaptar la ejecución según la versión PHP a utilizar.

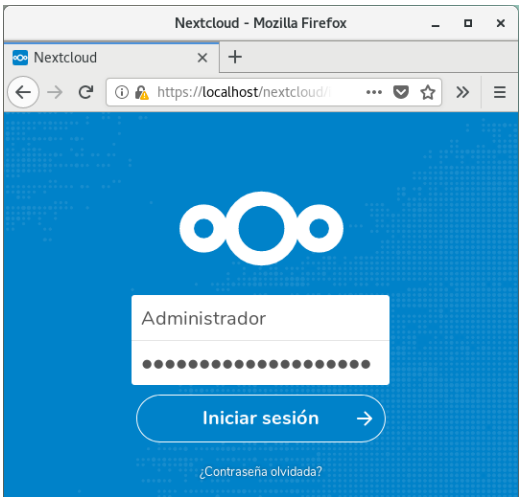
1.3. MARIADB

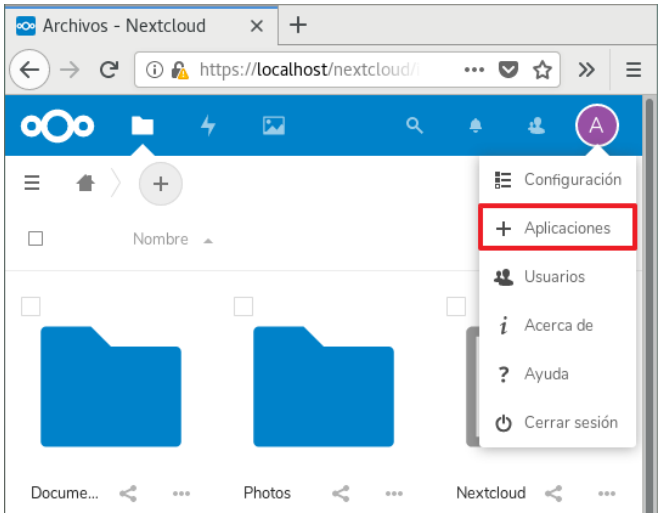
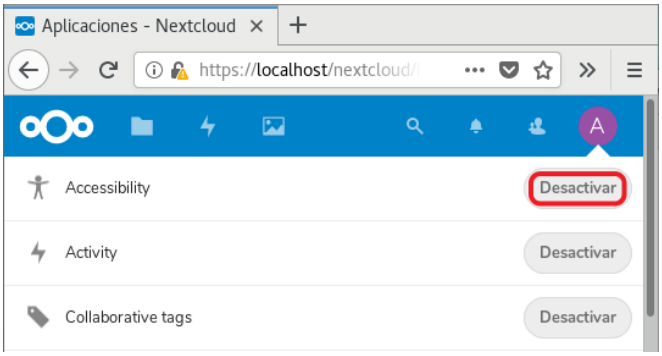
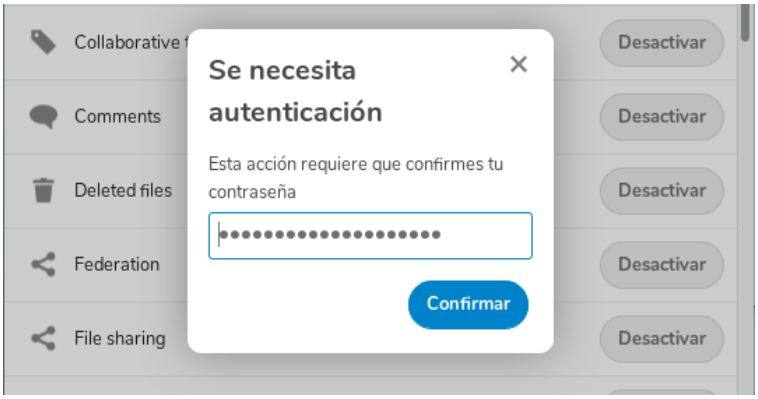
Paso	Descripción
21.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
22.	Se aplicarán medidas de seguridad en el servidor de Base de Datos MariaDB. Para ello ejecute el siguiente comando: **$ sudo mysql_secure_installation**
23.	En primer lugar, pedirá la contraseña del usuario "root", ingrese la contraseña y si no se ha configurado aún la misma deje el campo vacío y pulse "Enter" para continuar. 
24.	Posteriormente se preguntará si se quiere configurar una contraseña para "root", conteste con "Y" y pulse "Enter". 

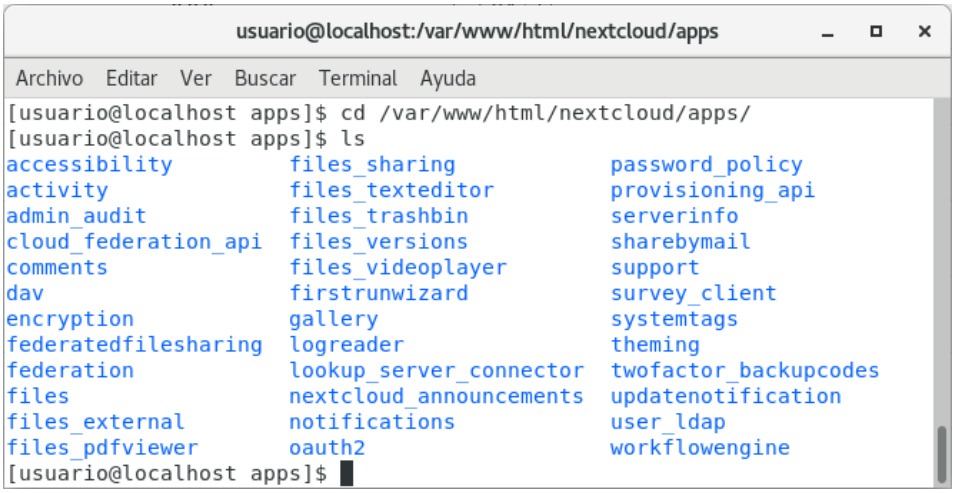
Paso	Descripción
25.	Escriba la nueva contraseña de “Root”, pulse “Enter” y vuelva a escribirla pulsando de nuevo “Enter” para continuar.  **Nota:** Tenga en cuenta, que el usuario “root” de la base de datos, es independiente al usuario “root” del sistema, por lo que las contraseñas difieren. Se deberá configurar la contraseña con los requisitos de seguridad exigidos.
26.	En el siguiente paso, preguntará si se eliminan usuarios anónimos, escriba “Y” y pulse “Enter” para continuar. 
27.	El siguiente punto pregunta si deshabilitar el inicio de sesión en la base de datos de forma remota con el usuario “root”. Escriba “Y” y pulse “Enter” para continuar. 
28.	Por defecto MariaDB contiene una base de datos de ‘test’, se pregunta si debe eliminarla. Escriba “Y” y pulse “Enter” para continuar. 

Paso	Descripción
29.	Se deberán recargar los privilegios de todas las tablas para que los cambios surtan efecto inmediatamente. Para ello escriba “Y” y pulse “Enter” para continuar. 
30.	Finalizará el proceso mostrando el mensaje “All done!” que garantiza que todos los campos configurados se han aplicado correctamente. 

2. LIMITACIÓN DE APLICACIONES Y MÓDULOS INSTALADOS

Paso	Descripción
31.	Se procede a deshabilitar aplicaciones y módulos instalados.
32.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
33.	Debe iniciar sesión en la aplicación Nextcloud con una cuenta que pertenezca al grupo de Administradores. 

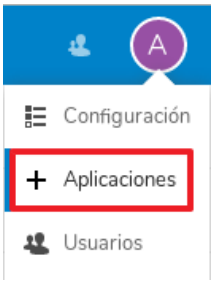
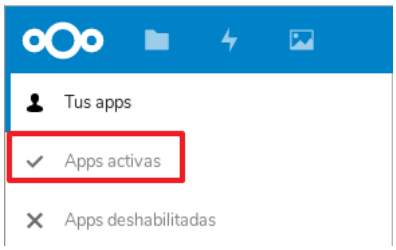
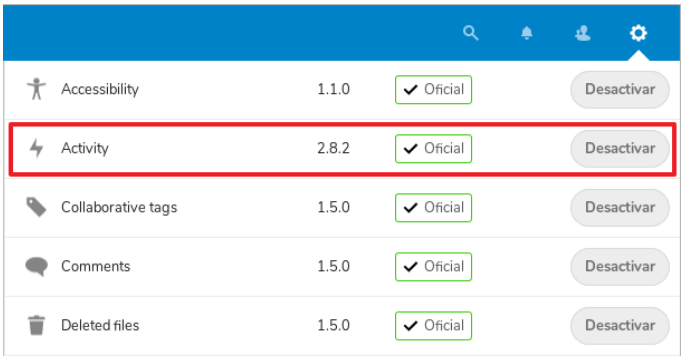
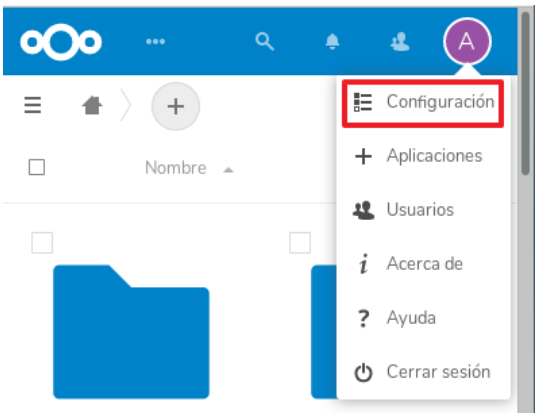
Paso	Descripción
34.	Diríjase al icono de su usuario y en el menú desplegable pulse “+ Aplicaciones”. 
35.	Revise las aplicaciones instaladas en su servidor y desactive las que no sean necesarias para su organización pulsando el botón “Desactivar”. 
36.	Si detecta alguna aplicación candidata para su desactivación y pulsa el botón “Desactivar”, le pedirá la contraseña del usuario Administrador para confirmar. 

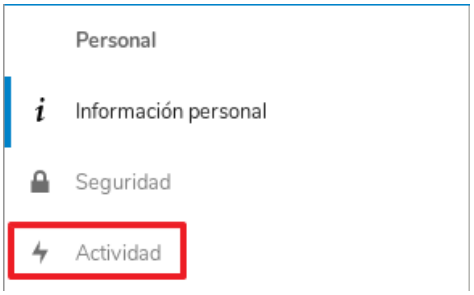
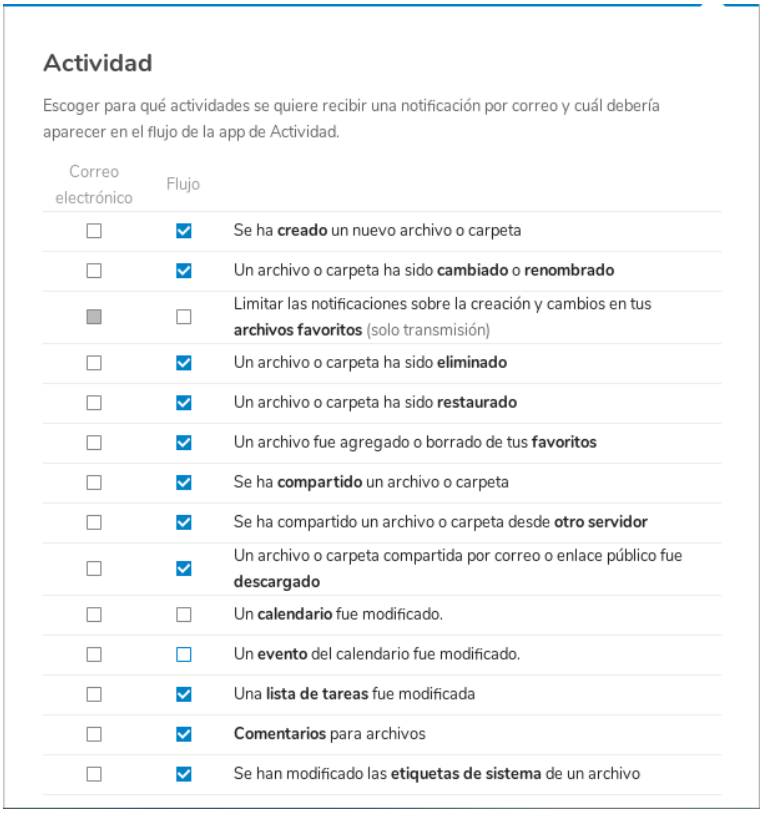
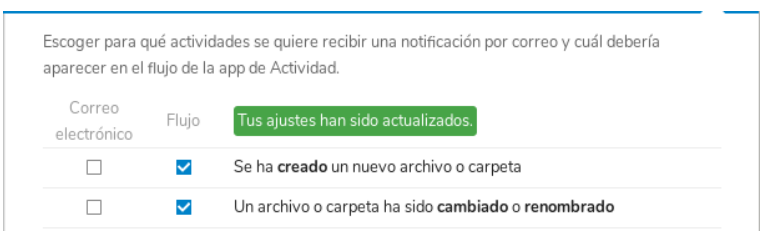
Paso	Descripción
37.	Si quisiera eliminar la aplicación y toda su configuración por completo, diríjase a la ruta de su servidor y liste las aplicaciones allí contenidas por medio de los siguientes comandos: **$ cd /var/www/html/nextcloud/apps** **$ ls -la** 
38.	Revise las aplicaciones que más se ajusten con su organización y si se detecta una candidata para su eliminación ejecute el siguiente comando: **$ sudo rm -rf [Nombre_de_aplicacion]** **Nota:** En [Nombre_de_aplicacion] escriba el nombre de la aplicación que quiere eliminar respetando mayúsculas y minúsculas y sin corchetes "[]".

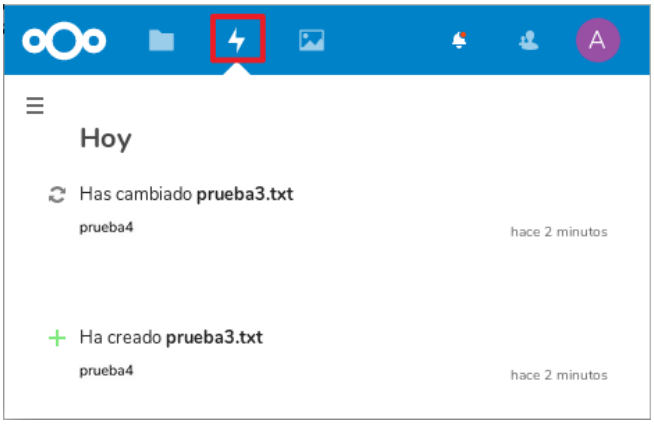
3. CONFIGURACIÓN DE REGISTROS DE ACTIVIDAD Y TRAZABILIDAD

3.1. REGISTROS DE ACTIVIDAD

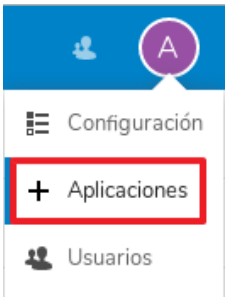
Paso	Descripción
39.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Internet" seleccione **"Firefox"** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
40.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
41.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de "admin".

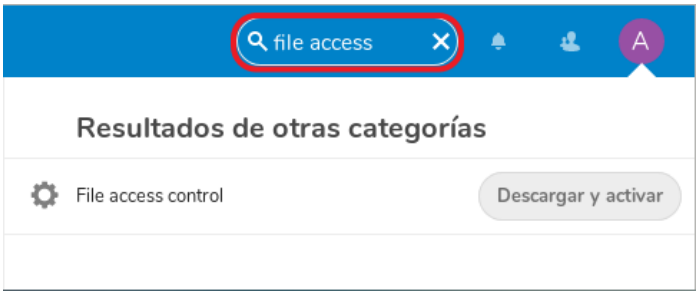
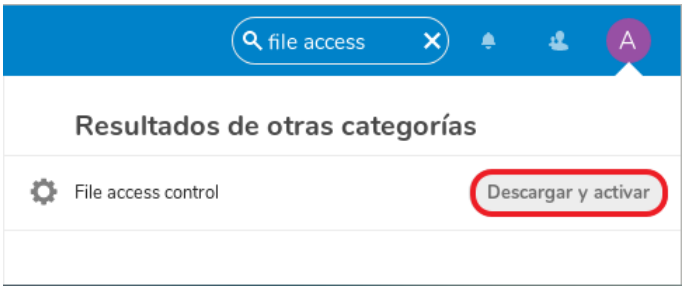
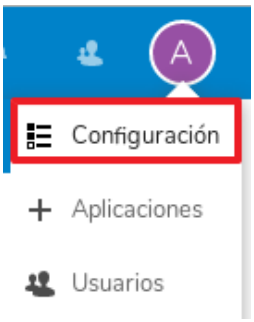
Paso	Descripción
42.	Diríjase al icono de su usuario y en el menú desplegable pulse “Aplicaciones”. 
43.	En la columna de la izquierda, en el apartado “Tus apps”, seleccione “Apps activas”. 
44.	Compruebe que se encuentra activa, si no es así actívela.  **Nota:** Si por cualquier motivo la aplicación no se hubiera descargado, vaya al panel superior de navegación, elija el icono de la lupa para buscar y escriba “activity”. Posteriormente pulse “Descargar y activar”.
45.	Pulse sobre el icono de su usuario y en el menú desplegable pulse “Configuración”. 

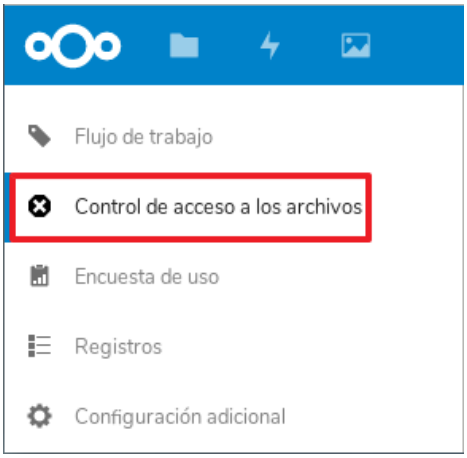
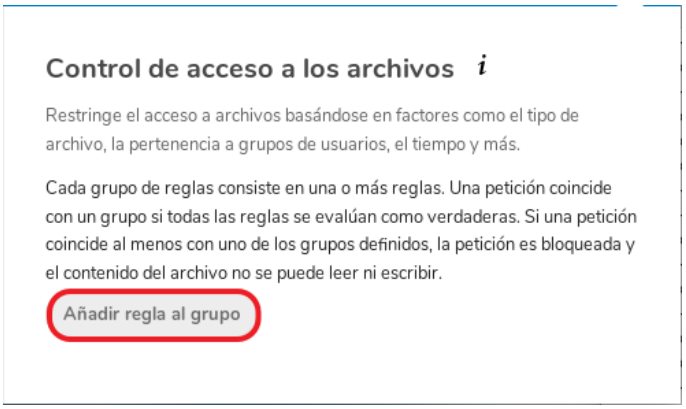
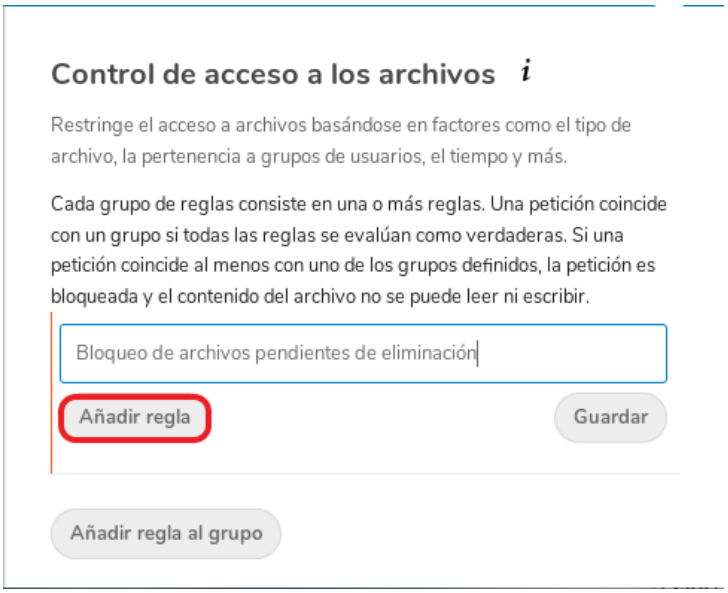
Paso	Descripción
46.	En la barra lateral izquierda en el apartado “Personal”, seleccione el icono “Actividad”. 
47.	Seleccione y deseleccione con los registros que desee que la aplicación guarde y los registros que desee que se envíen por correo.  **Nota:** Modificando las configuraciones en el apartado “Personal”, se le notificará al correo configurado en su usuario, si quisiera modificar las configuraciones para todos los administradores, debe dirigirse al título “Administración” y seleccionar “Actividad” para modificar las notificaciones desde ahí.
48.	Cuando los ajustes se actualicen lo notificará por pantalla. 

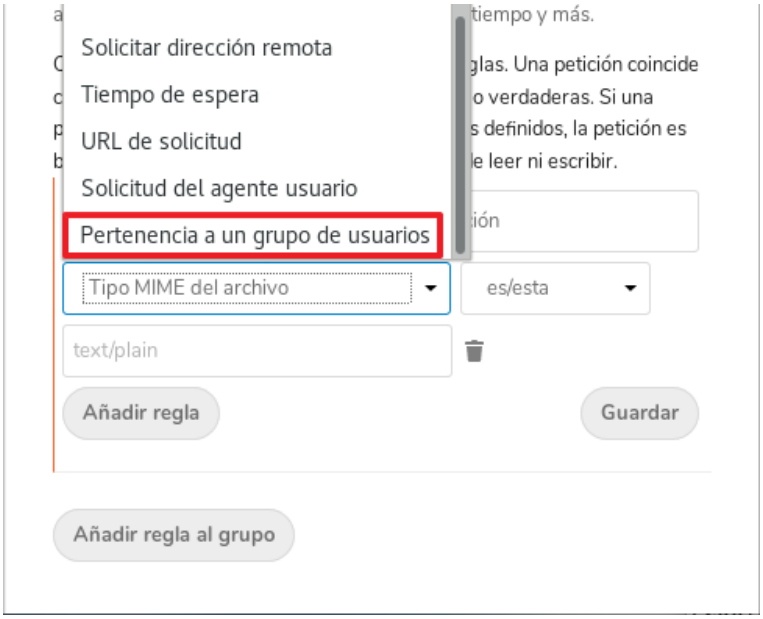
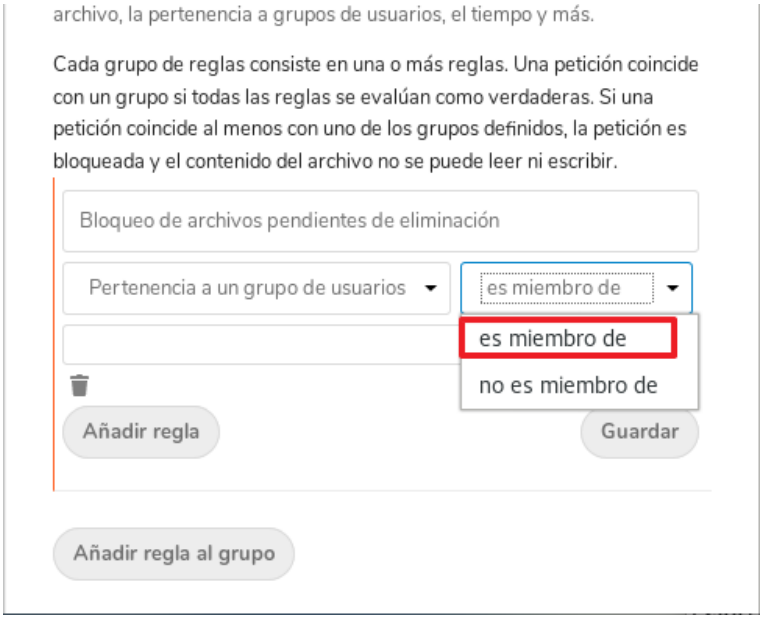
Paso	Descripción
49.	Diríjase a la barra superior de navegación y pulse sobre el icono de “actividad” para revisar los registros generados por el servidor. 

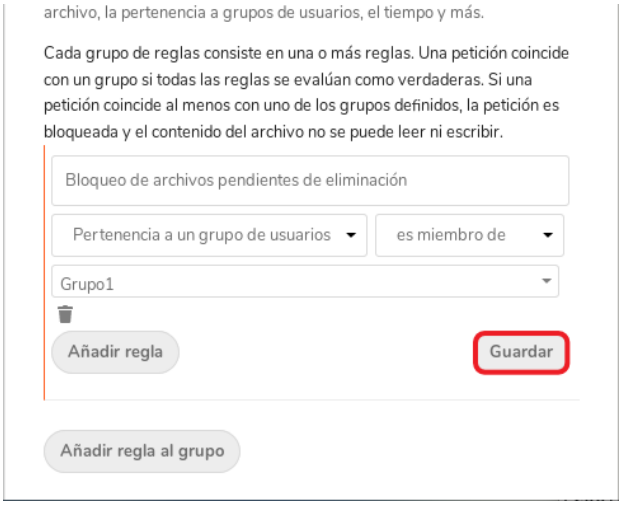
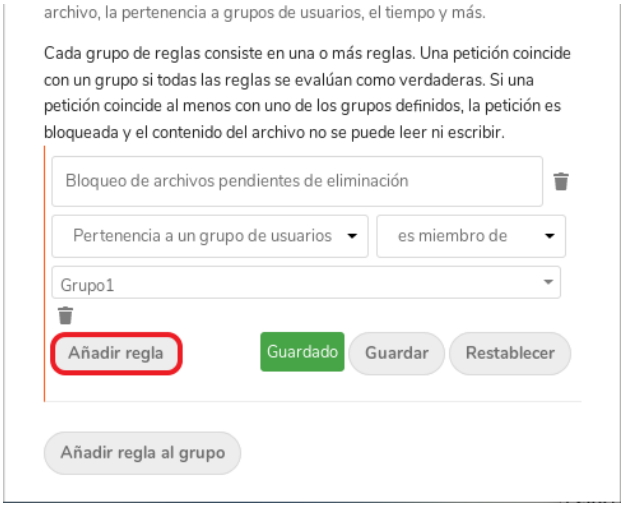
3.2. CONTROL DE ACCESO A FICHEROS NEXTCLOUD

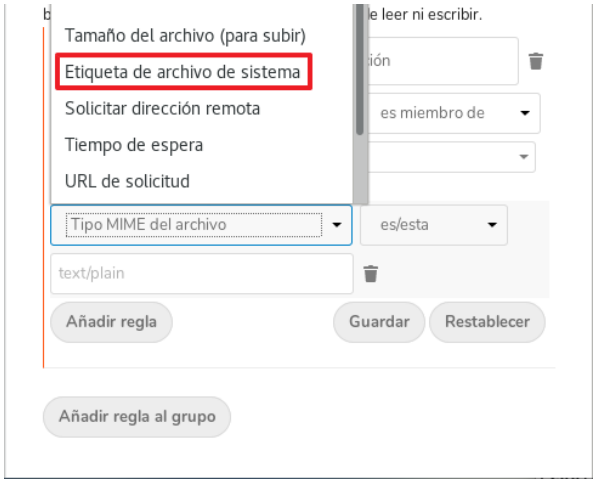
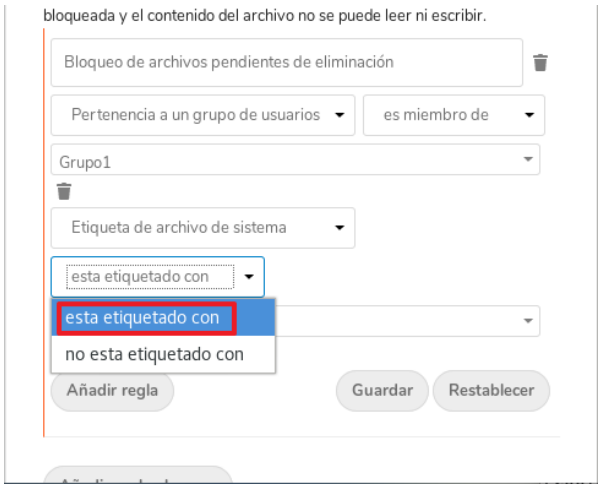
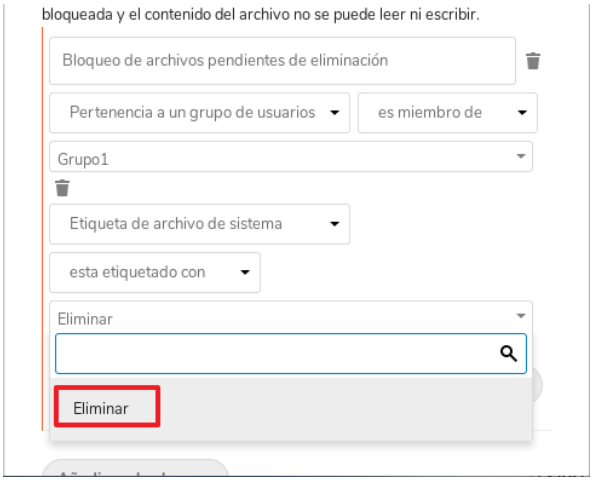
Paso	Descripción
50.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “**Firefox**” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
51.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
52.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
53.	Diríjase al icono de su usuario y en el menú desplegable pulse “Aplicaciones”. 

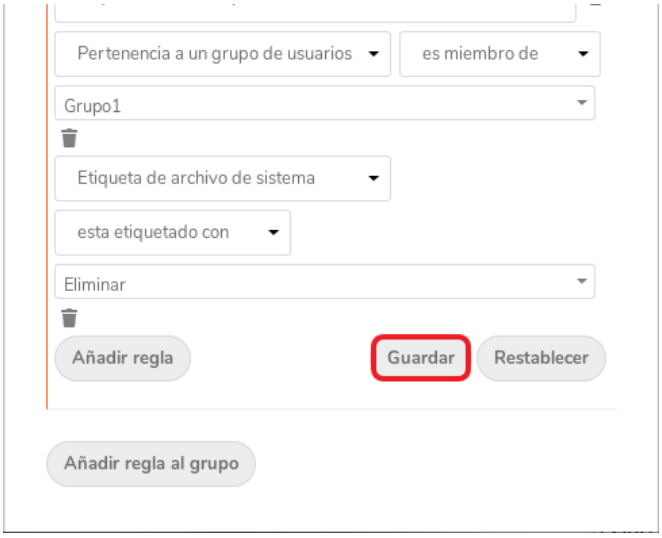
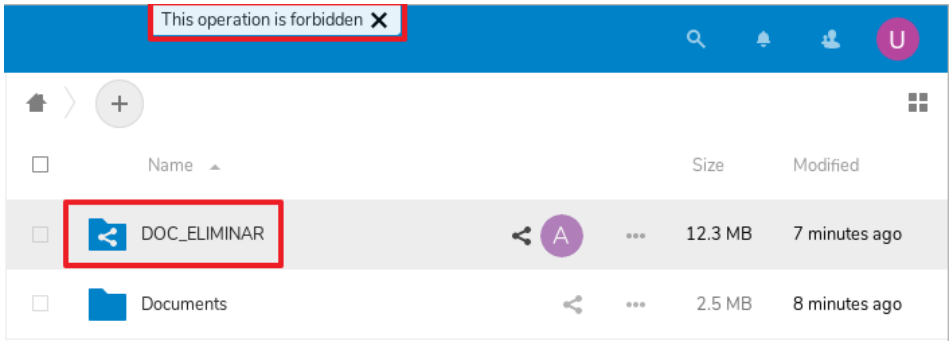
Paso	Descripción
54.	En el panel de navegación superior elija el icono de la lupa para buscar y escriba el siguiente texto: “file access” 
55.	Pulse el botón “Descargar y activar” para obtener la aplicación y que se encuentre activa en el servidor.  **Nota:** Fíjese siempre que las aplicaciones lleven el recuadro verde que garantice que son aplicaciones **oficiales** y por tanto están aprobadas por los desarrolladores de Nextcloud.
56.	Posteriormente diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 

Paso	Descripción
57.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Control de acceso a los archivos”. 
58.	Lea detenidamente la descripción de la aplicación y posteriormente pulse en “Añadir regla al grupo”. 
59.	Defina una descripción que se ajuste al motivo de la regla y pulse “Añadir regla”. 

Paso	Descripción
60.	En el siguiente ejemplo se bloquean los archivos que coincidan con la etiqueta “Eliminar” para los usuarios pertenecientes al grupo “Grupo1”. Para ello en el primer menú desplegable seleccione “Pertenencia a un grupo de usuarios”. 
61.	En el segundo menú desplegable seleccione “es miembro de”. 

Paso	Descripción
62.	En el menú desplegable de la parte inferior seleccione “Grupo1”. 
63.	Para añadir esta regla al grupo pulse “Guardar”. 
64.	Vuelva a pulsar el botón “Añadir regla”. 

Paso	Descripción
65.	Del mismo modo que en la anterior regla comience con el primer menú desplegable seleccionando esta vez “Etiqueta de archivo de sistema”. 
66.	En el menú desplegable inferior seleccione “está etiquetado con”. 
67.	En el segundo menú desplegable de la parte inferior seleccione la etiqueta creada en pasos anteriores, en este ejemplo será la etiqueta “Eliminar”. 

Paso	Descripción
68.	Para añadir este grupo de reglas pulse “Guardar”. 
69.	Se muestra un ejemplo con una carpeta llamada “DOC_ELIMINAR”, que contiene la etiqueta “Eliminar” y se encuentra compartido con el grupo “Grupo1”. Se inicia sesión con el usuario “usuario_común1” que pertenece al grupo “Grupo1” y se intenta acceder a la carpeta. Al cumplir las dos reglas creadas, se deniega el acceso a la misma mostrando el siguiente mensaje “This operation is forbidden”.  **Nota:** Para que se cumpla la denegación de acceso por grupo de reglas, todas y cada una de las reglas contenidas en el grupo de reglas deben de ser afirmativas.

4. REENVIO DE LOGS A SYSLOG

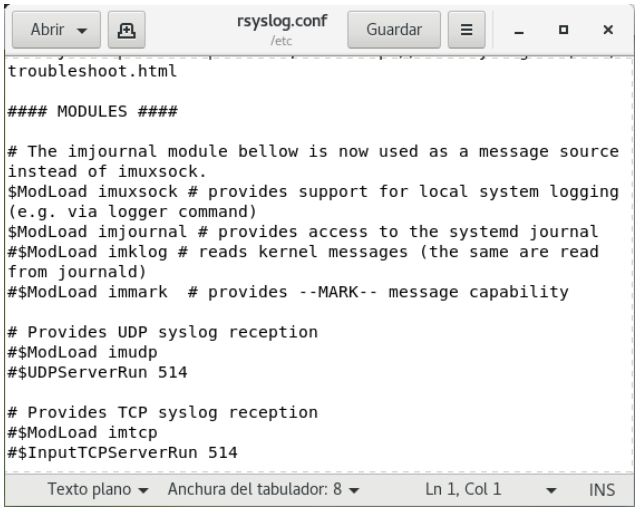
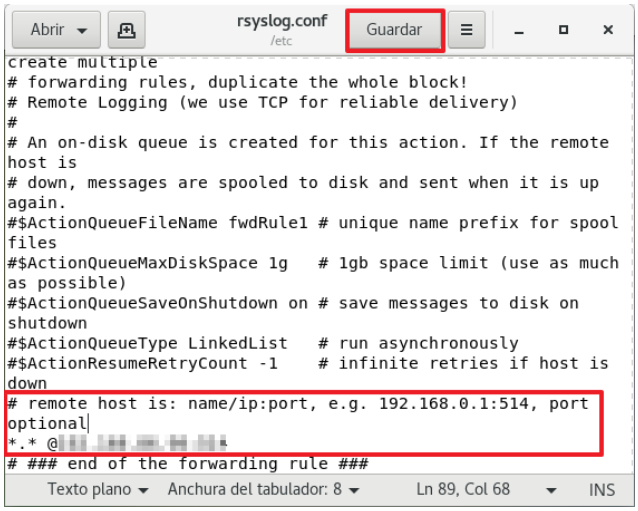
Paso	Descripción
70.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “**Terminal**”. Ejecute el comando **“cd /”** y pulse la tecla “Enter”.

Paso	Descripción

71.	Se va a comprobar que el servicio “rsyslog” se encuentra activo. Para ello ejecute el siguiente comando.
	$ sudo systemctl status rsyslog.service
	`[usuario@localhost ~]$ sudo systemctl status rsyslog.service`
	`[sudo] password for usuario:`
	`● rsyslog.service - System Logging Service`
	`Loaded: loaded (/usr/lib/systemd/system/rsyslog.service; enabled; vendor preset: enabled)`
	`Active: active (running) since [redacted]`
	`Docs: man:rsyslogd(8)`
	`http://www.rsyslog.com/doc/`
	`Main PID: 8647 (rsyslogd)`
	`Tasks: 3`
	`CGroup: /system.slice/rsyslog.service`
	`└─8647 /usr/sbin/rsyslogd -n`

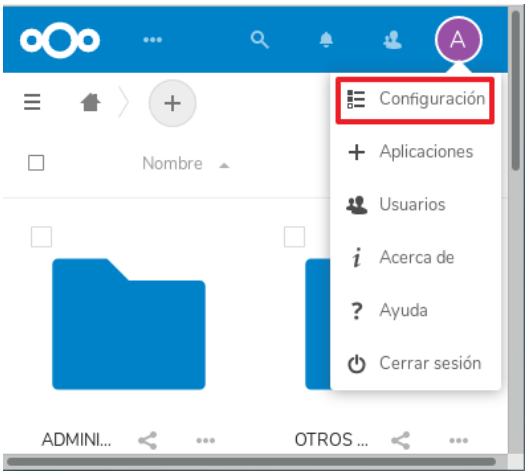
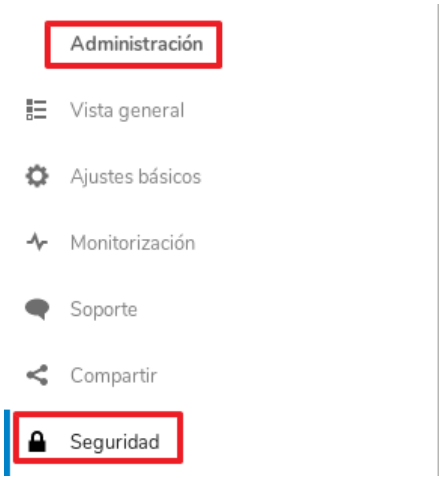
72.	Diríjase al directorio de su servidor de alojamiento de archivos Nextcloud, la ruta por defecto en esta guía es “/var/www/html/nextcloud”. Para ello escriba el siguiente comando, modificando la ruta si fuera necesario. **$ cd /var/www/html/nextcloud**
73.	Edite el fichero de configuración de PHP perteneciente al servidor Nextcloud, para ello ejecute el siguiente comando. **$ sudo gnome-text-editor config/config.php &>/dev/null**
74.	Deberá efectuar un estudio para determinar los campos que son de aplicación en su organización. – **LOGLEVEL**= Los valores válidos son 0=Depurar, 1=Información, 2=Advertencia, 3=Error, y 4=Fatal. El valor predeterminado es 2. – **SYSLOG_TAG**= Etiqueta del log. – **LOG.CONDITION**= Se configuran las condiciones para el aumento del nivel de registro. Una vez que se cumple una de estas condiciones, el nivel de registro requerido se configura en modo depuración. Esto permite depurar solicitudes específicas, usuarios o aplicaciones. Admite las siguientes configuraciones “shared_secret”, “users”, apps”. – **LOGTIMEZONE**= Se configura la zona horaria. – **LOG_ROTATE_SIZE**= Habilita la rotación de registros y limita el tamaño total de los archivos de registro por ejemplo 100 megabytes = 100 * 1024 * 1024 bytes.

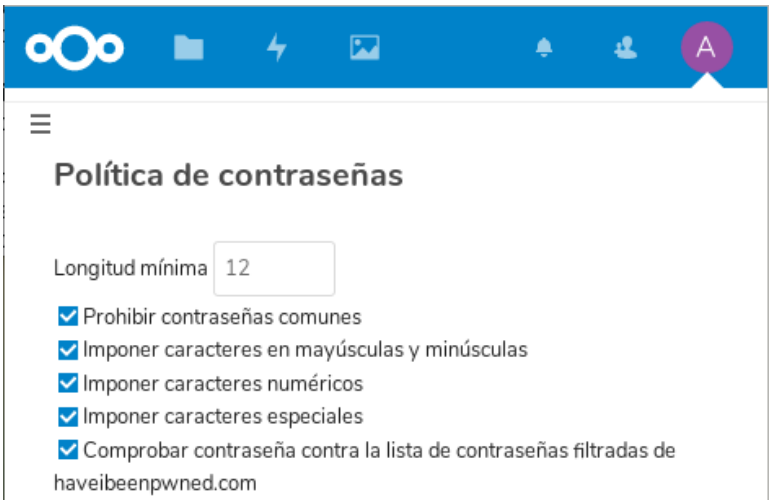
Paso	Descripción
75.	Añada las siguientes líneas al fichero de configuración y modifique acorde a las necesidades de su organización los datos que se remarcan en color rojo. Pulse "Guardar" cuando finalice. **'log_type' => 'syslog',** **'logfile' => '',** **'logfilemode' => 0640,** **'loglevel' => 2,** **'syslog_tag' => 'NEXTCLOUD',** **'log.condition' => [** **'shared_secret' => '97b53edb637fe3059b3595cfcc41b9',** **'users' => ['usuario-ejemplo'],** **'apps' => ['files'],** **],** **'logdateformat' => 'F d, Y H:i:s',** **'logtimezone' => 'Europe/Madrid',** **'log_query' => false,** **'log_rotate_size' => 100 * 1024 * 1024,** 
76.	Para que los cambios tengan efecto reinicie el servicio Apache, para ello ejecute el siguiente comando. Fíjese que reinicia sin errores. **$ sudo systemctl restart httpd.service**

Paso	Descripción
77.	Edite el fichero de configuración de rsyslog para reenviar logs a un servidor externo. Para editarlo ejecute el siguiente comando. **$ sudo gnome-text-editor /etc/rsyslog.conf &>/dev/null** 
78.	Diríjase al final del fichero y edite debajo del título “#remote host”, de la siguiente forma: host/ip:puerto, (ejemplo. 192.168.0.1:514, puerto opcional). Pulse “Guardar” para finalizar. 
79.	Para que los cambios tengan efecto reinicie el servicio rsyslog, para ello ejecute el siguiente comando. Fíjese que reinicia sin errores. **$ sudo systemctl restart rsyslog.service**

5. CONFIGURACIÓN DE USUARIOS Y POLÍTICAS DE CREDENCIALES

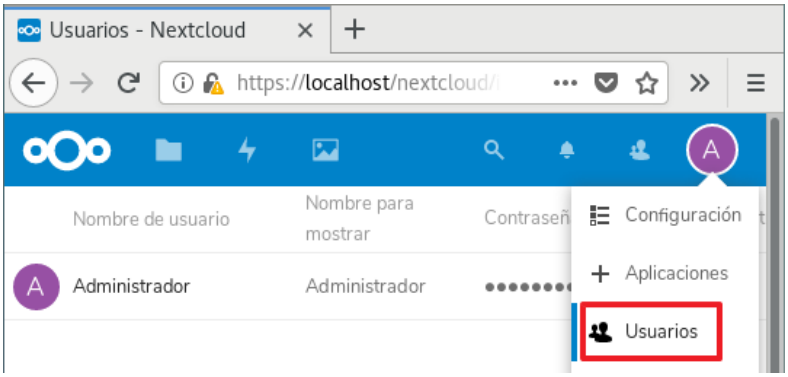
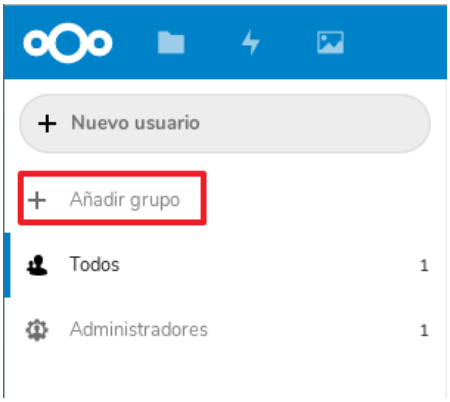
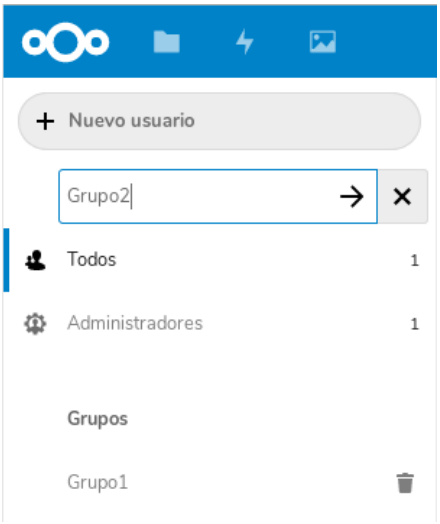
5.1. POLÍTICA DE CREDENCIALES

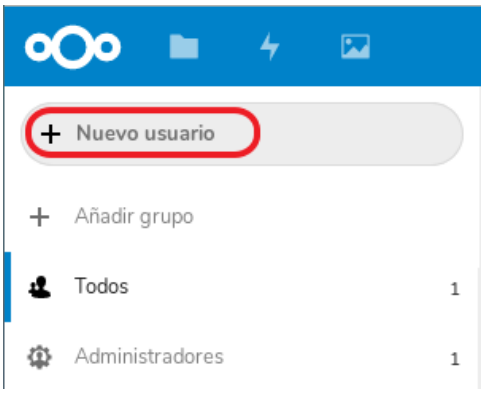
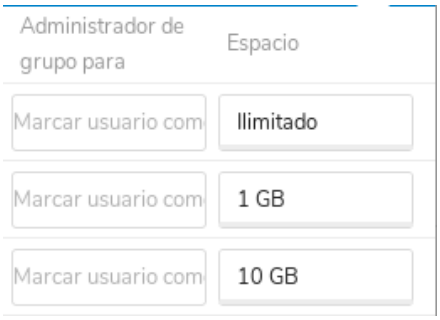
Paso	Descripción
80.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
81.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
82.	Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de “admin”.
83.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
84.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Seguridad”. 

Paso	Descripción
85.	Diríjase hasta el final de la página deténgase en el punto “Política de contraseñas” y establezca los siguientes parámetros: – Longitud mínima: 12 caracteres – Imponer caracteres en mayúsculas y minúsculas: seleccionado – Imponer caracteres numéricos: seleccionado – Imponer caracteres especiales: seleccionado – Comprobar contraseña contra la lista de contraseñas filtradas de haveibeenpwned.com 
86.	Para mayor seguridad y cumplimiento, se recomienda autenticación mediante LDAP. Si desea realizar la integración de usuarios por medio de LDAP, vaya al punto ANEXO A.6.3 INTEGRACIÓN DE USUARIOS CON LDAP de esta guía.

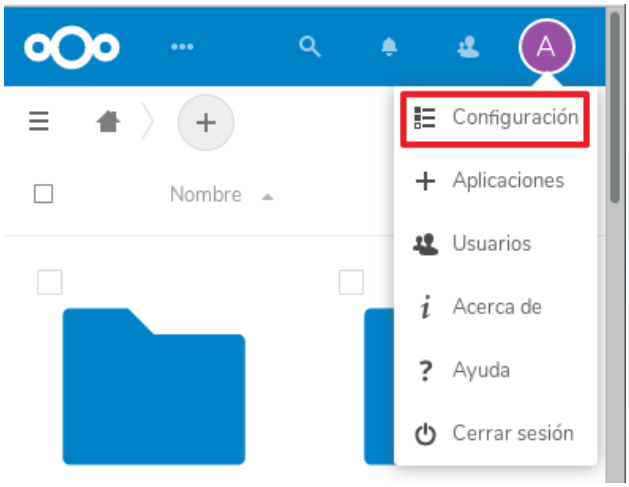
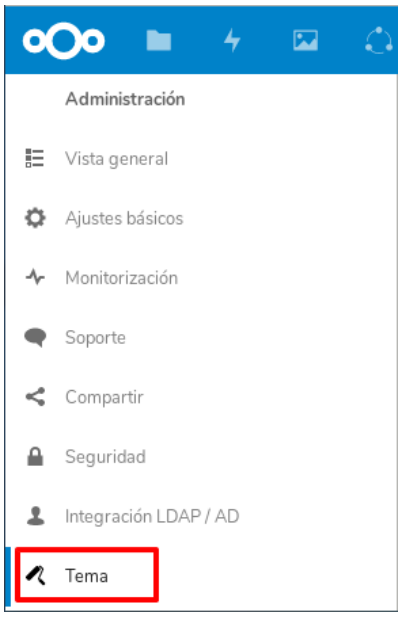
5.2. PERMISOS DE USUARIOS Y ESTRUCTURA DE GRUPOS

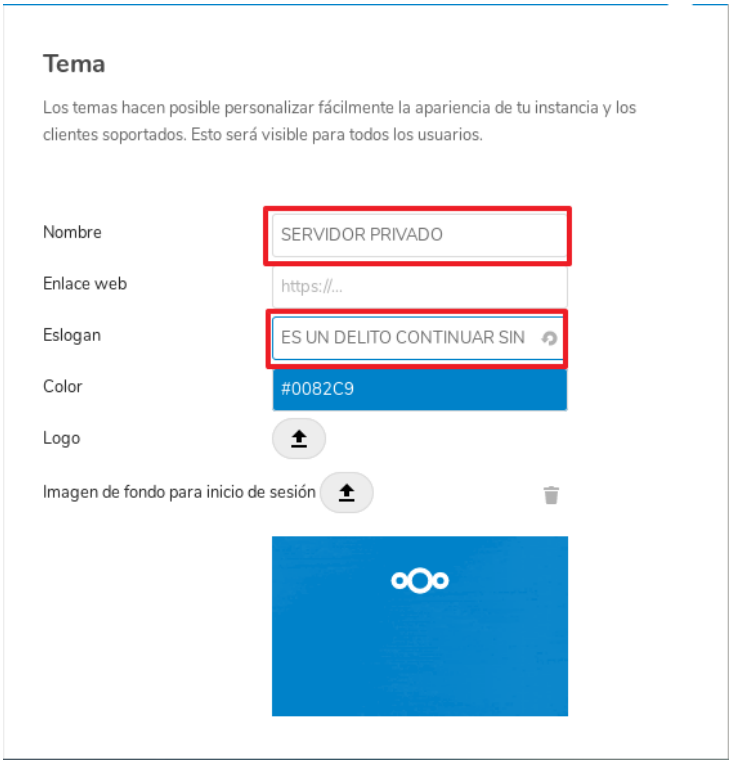
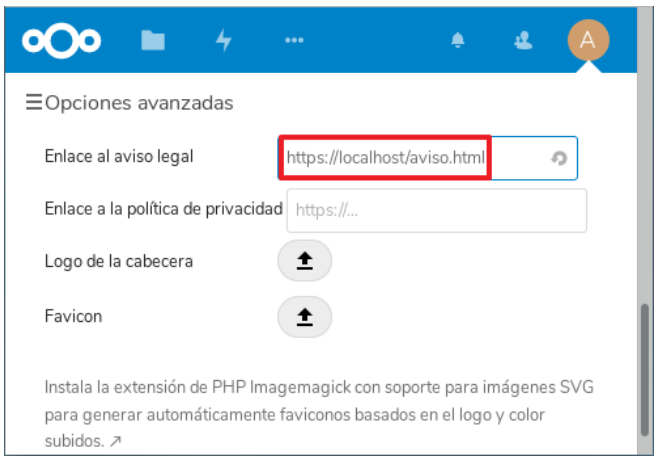
Paso	Descripción
87.	Se procede a configurar usuarios y grupos.
88.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
89.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
90.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.

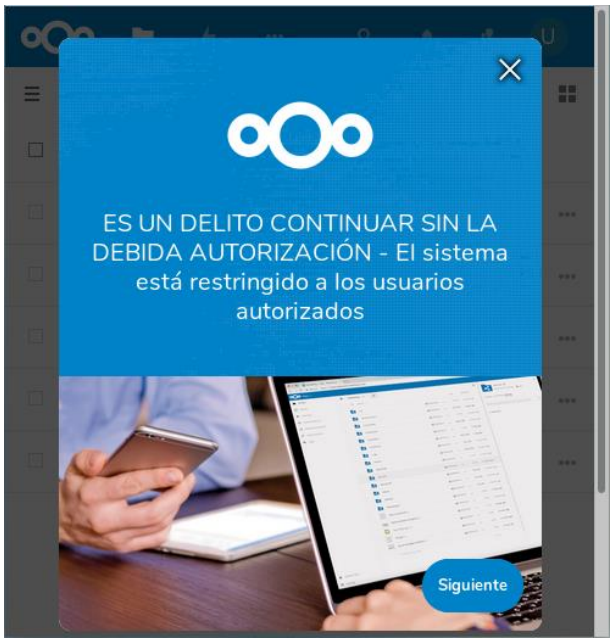
Paso	Descripción
91.	Diríjase al icono de su usuario y en el menú desplegable pulse “Usuarios”. 
92.	En el menú de usuarios, se recomienda empezar con la creación de grupos si no se encuentran creados aún, para ello pulse sobre “+ Añadir grupo” en la parte izquierda de la pantalla. 
93.	Se recomienda crear diferentes grupos identificando posteriormente usuarios comunes de usuarios administradores pertenecientes a cada grupo y teniendo en cuenta las preferencias y necesidades de su organización. 

Paso	Descripción
94.	Una vez creados los grupos necesarios para su organización, se deberán crear los usuarios y asignarles un grupo y un rol dentro de ese grupo. El rol puede ser usuario común del grupo o usuario administrador de ese grupo. Comience creando los usuarios comunes teniendo en cuenta las preferencias y necesidades de su organización. Para ello pulse en el botón nuevo usuario: 
95.	Rellene todos los campos, dejando vacío el apartado “Administrador de grupo para”. Si quisiera configurar cuotas defina éstas en el apartado “Espacio”. 
96.	Cuando finalice de rellenar todos los campos con las preferencias deseadas, diríjase al final de la línea y pulse sobre el icono de verificación para añadir y finalizar. 
97.	Se muestra una captura de ejemplo donde el “usuario_comun1” pertenece al grupo “Grupo1” con 1GB de límite de espacio en disco. En cambio, usuario_común2 pertenece al grupo “Grupo2” con 10GB de límite de espacio en disco. 

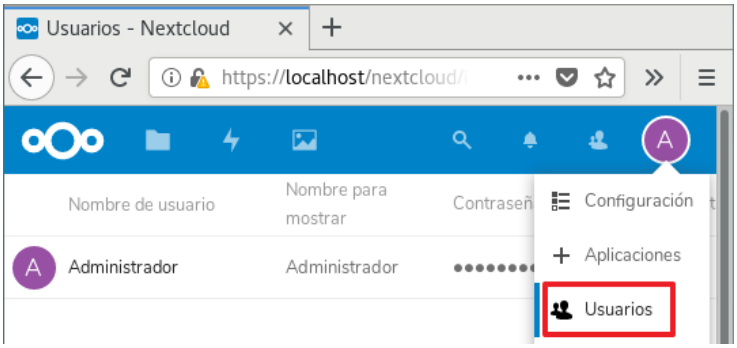
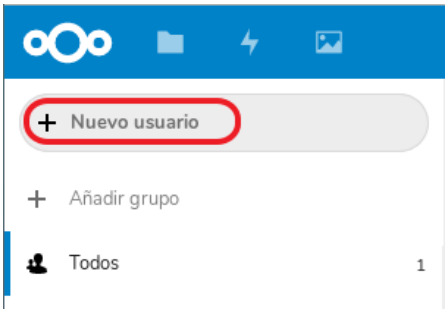
5.3. CONFIGURACIÓN MENSAJE DISUASORIO

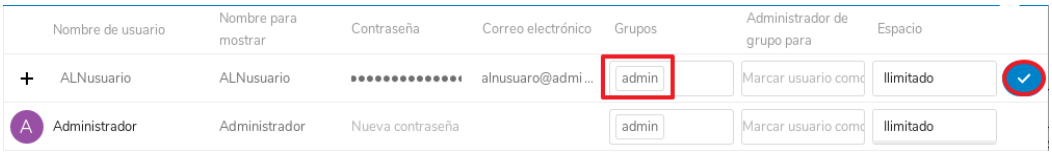
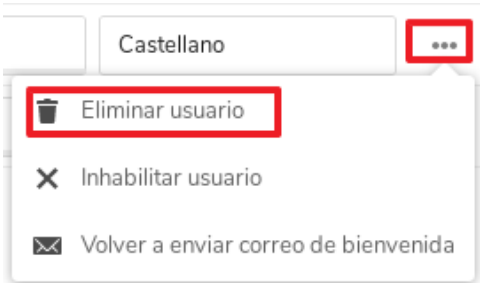
Paso	Descripción
98.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
99.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
100.	Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de “admin”.
101.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
102.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Tema”. 

Paso	Descripción
103.	En el apartado “Nombre”, seleccione el nombre que más convenga a su organización, posteriormente en el apartado “Eslogan” configure el mensaje disuasorio que más se ajuste a las necesidades específicas de su organización.  **Nota:** Nextcloud 15 presenta mecanismos para implementar mensajes que son advertidos al usuario cuando va a realizar el inicio de la sesión. Debe, no obstante, tomarse en consideración que su organización ya está empleando este mecanismo para notificar otros detalles como los marcados por el Reglamento Europeo General de Protección de Datos (GDPR) 2016/679/CE y la Ley Orgánica 15/1999 de protección de datos de carácter personal.
104.	En el apartado “Opciones avanzadas”, si su organización lo posee, se puede añadir un enlace hacia el aviso legal de su organización. Para ello ingrese la URL correspondiente al aviso legal en el apartado “Enlace al aviso legal”. 

Paso	Descripción
105.	Compruebe que se muestra correctamente el mensaje en la pantalla de inicio de sesión. 
106.	Compruebe que se muestra correctamente el mensaje en el primer inicio de un nuevo usuario. 

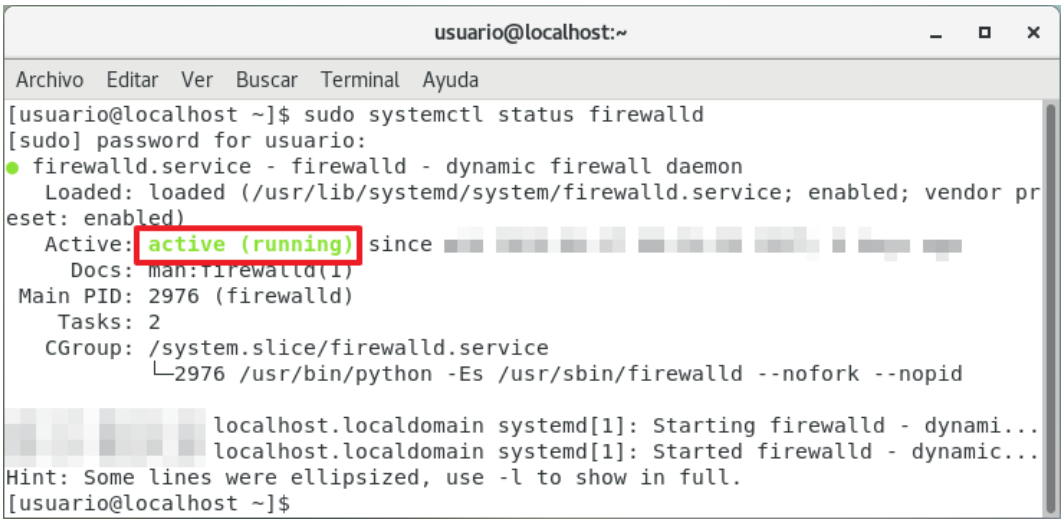
6. POLÍTICA DE SEGURIDAD DE ACCESO PARA ADMINISTRADORES LOCALES

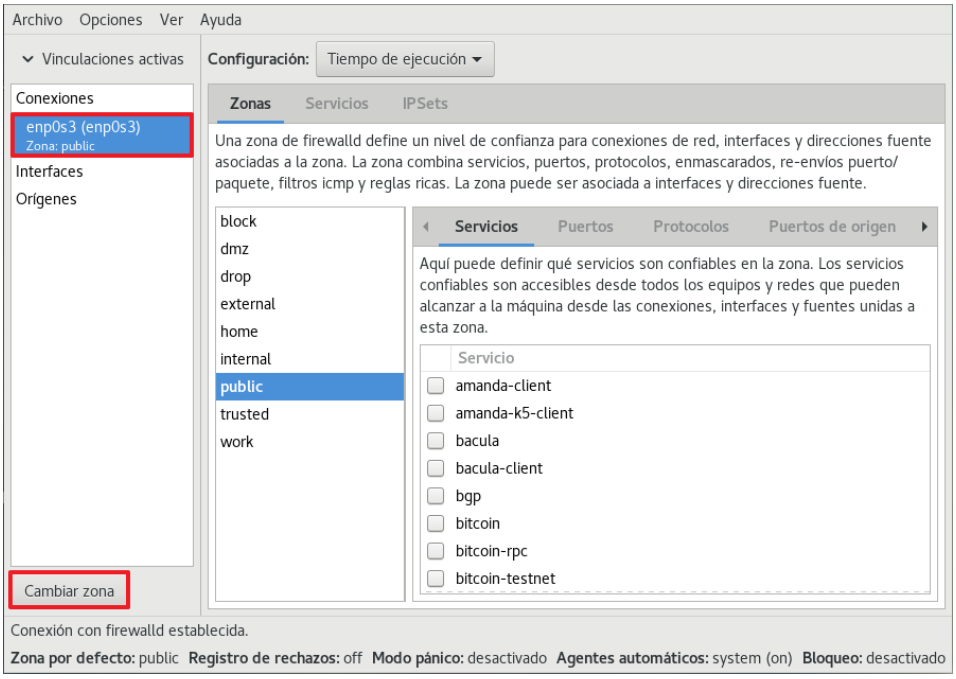
Paso	Descripción
107.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
108.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
109.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
110.	Se va a proceder a modificar el usuario Administrador global del servidor de alojamiento de archivos Nextcloud. Para ello diríjase al icono de su usuario y en el menú desplegable pulse sobre el icono “Usuarios”. 
111.	Como se puede observar en la siguiente imagen, el usuario que se crea en la instalación (en este caso “Administrador”) se añade al grupo “admin”. El usuario que pertenezca al grupo “admin” el sistema lo considerará Administrador global. 
112.	Para modificar el usuario que se creó en la instalación, se debe añadir primero un usuario nuevo y agregarlo al grupo “admin”. En este caso se pondrá un ejemplo con el usuario “ALNusuario”. 

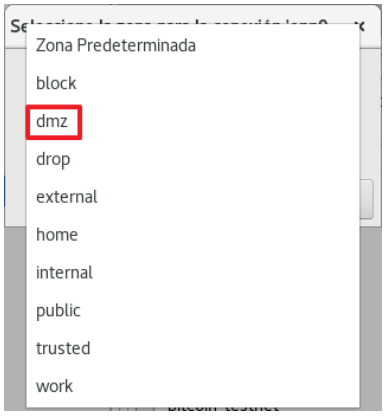
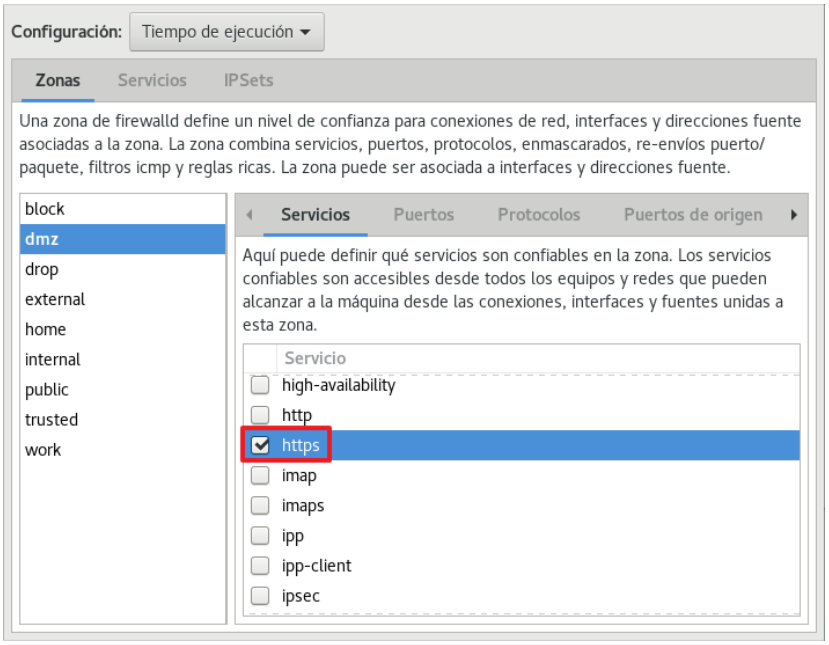
Paso	Descripción
113.	Agregue al usuario “ALNusuario” al grupo “admin”, configure los demás campos con los parámetros que más convengan a su organización y pulse el icono azul de confirmación. 
114.	Pulse sobre el icono de su usuario en el menú desplegable seleccione “cerrar sesión”. 
115.	Inicie sesión con el usuario recién creado “ALNusuario” y en el icono de usuario en el menú desplegable seleccione “Usuarios”. Una vez en el menú de usuarios, elimine el usuario “Administrador” que se creó por defecto en la instalación. Para ello pulse en el icono “…” y seleccione “Eliminar usuario”. 
116.	Posteriormente se creará un usuario administrador de grupos. Para ello se creará el usuario “ALGusuario” y se le asignarán los grupos anteriormente creados. Modifique estos valores con los requerimientos específicos de su organización.  **Nota:** Si necesita revisar el modo de creación de usuarios y grupos, diríjase al punto 53 del apartado 3.2 PERMISOS DE USUARIOS Y ESTRUCTURA DE GRUPOS.

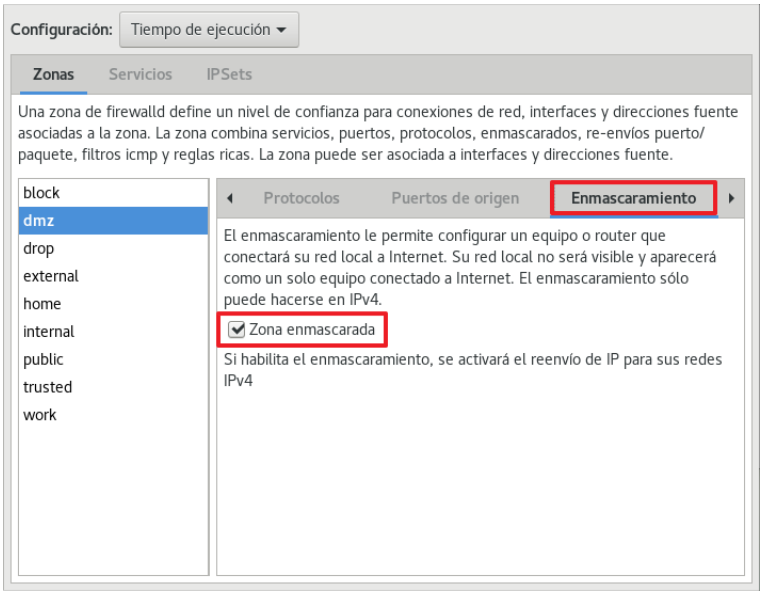
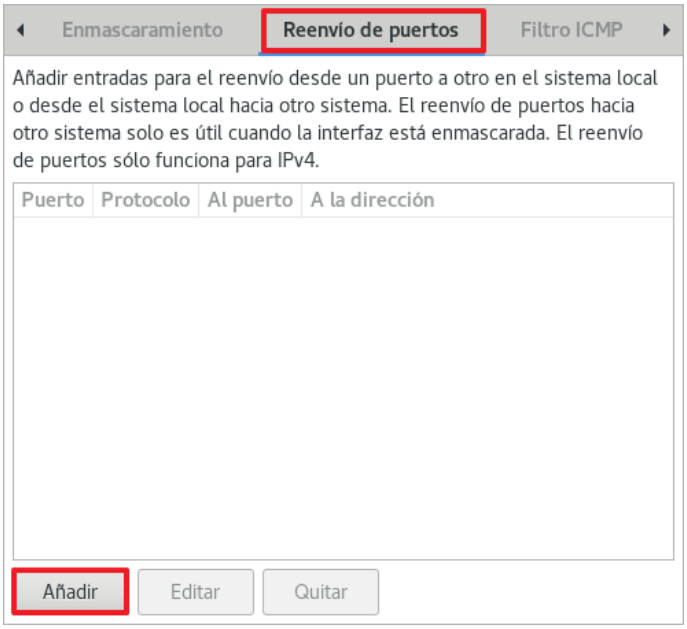
Paso	Descripción
117.	Para finalizar diríjase al final de la línea y pulse sobre el icono de verificación para añadir y finalizar. 

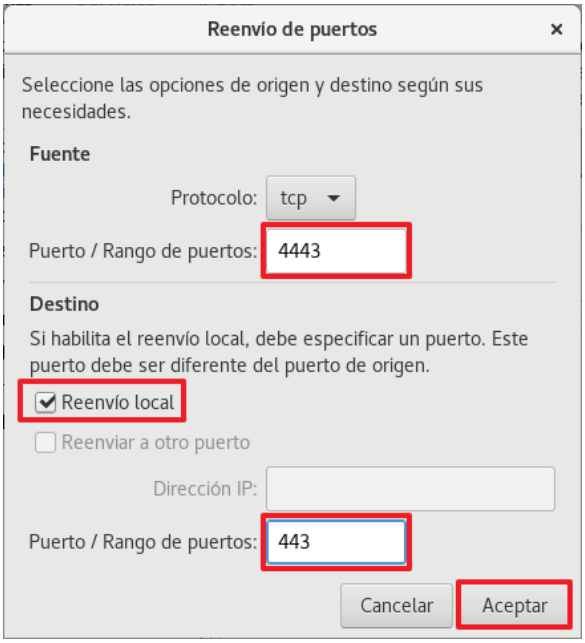
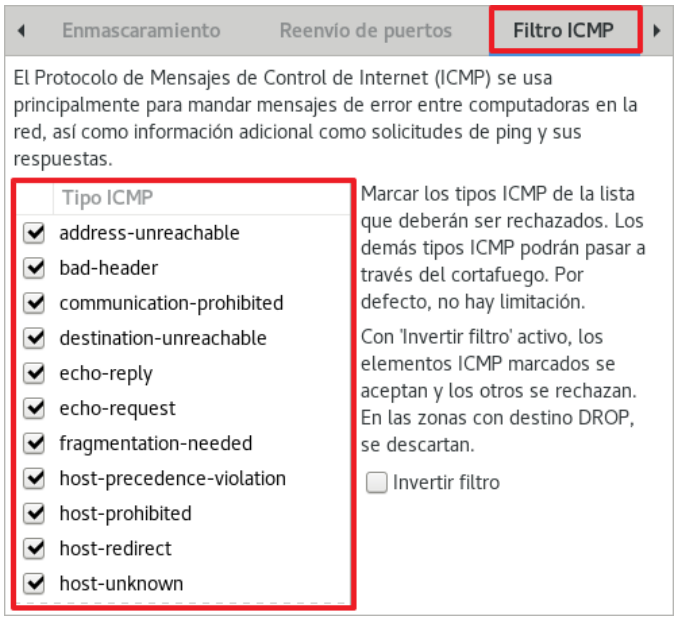
7. CONFIGURACIÓN DE FIREWALLD PARA SERVICIOS NEXTCLOUD

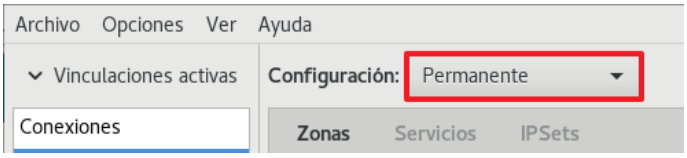
Paso	Descripción
118.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
119.	El primer paso es comprobar el estado del servicio firewalld, además se debe reiniciar y configurar para que arranque al inicio. Para todo ello ejecute los siguientes comandos. **$ sudo systemctl restart firewalld** **$ sudo systemctl enable firewalld** **$ sudo systemctl status firewalld** 

Paso	Descripción
120.	Para iniciar el asistente gráfico diríjase a la barra de tareas, pulse en **"Aplicaciones"** → **"Varios"** → **"Cortafuegos"**. Introduzca la contraseña si se la solicita. 
121.	Seleccione su interfaz y pulse en el botón "Cambiar zona". 

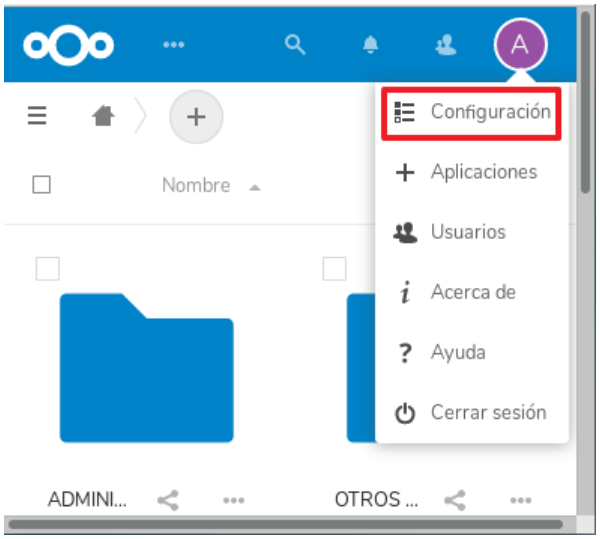
Paso	Descripción
122.	En el menú desplegable podrá seleccionar la zona que más convenga a su organización, en este ejemplo se seleccionará la zona “DMZ”. 
123.	Una vez seleccione la zona deseada, deberá habilitar los servicios y puertos que le sean de aplicación en su entorno, para ello comience dirigiéndose a **“Zonas” → “Servicios”** y habilite los servicios necesarios en su organización, el servicio por **http** deberá encontrarse **desactivado**.  **Nota:** Deberá evaluar la necesidad de servicios, puertos y protocolos activos en el servidor, reduciendo a los mínimos necesarios cumpliendo con el principio de mínima exposición.

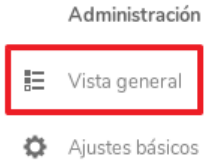
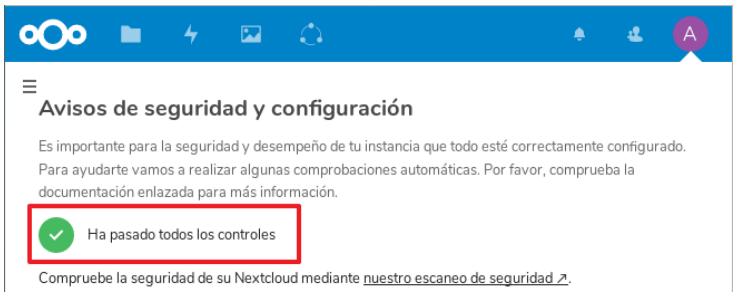
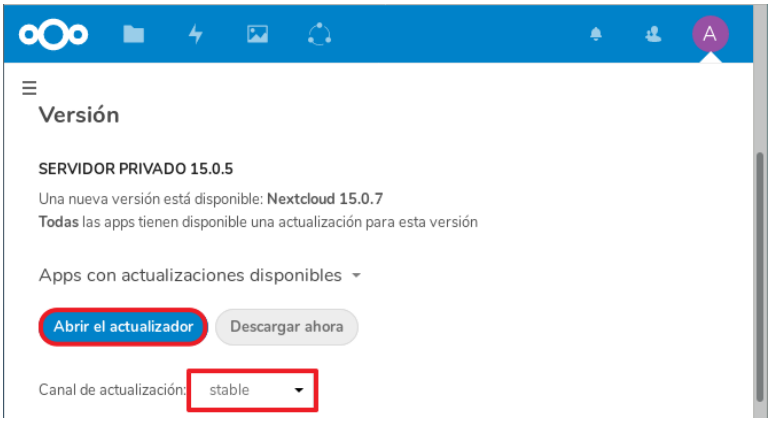
Paso	Descripción
124.	Otro punto de revisión es el de Enmascaramiento. Si le es de aplicación en su organización diríjase al apartado "Enmascaramiento" y seleccione "Zona enmascarada". De esta manera la red local no será visible y se publicará solo un equipo hacia redes externas.  **Nota:** Hay que tener en cuenta que el enmascaramiento solo funcionará en redes IPv4.
125.	Se recomienda modificar los puertos por defecto (443,80…etc.) en los que el servidor acepta solicitudes. Si su servidor Nextcloud acepta solicitudes en un puerto distinto al habitual, diríjase al punto "Reenvío de puertos" para ajustar esta característica en el firewall de CentOS 7. Se va a configurar un ejemplo que fuerza el reenvió al puerto 443 si se realizan peticiones desde el puerto 4443. Para ello pulse en "Añadir". 

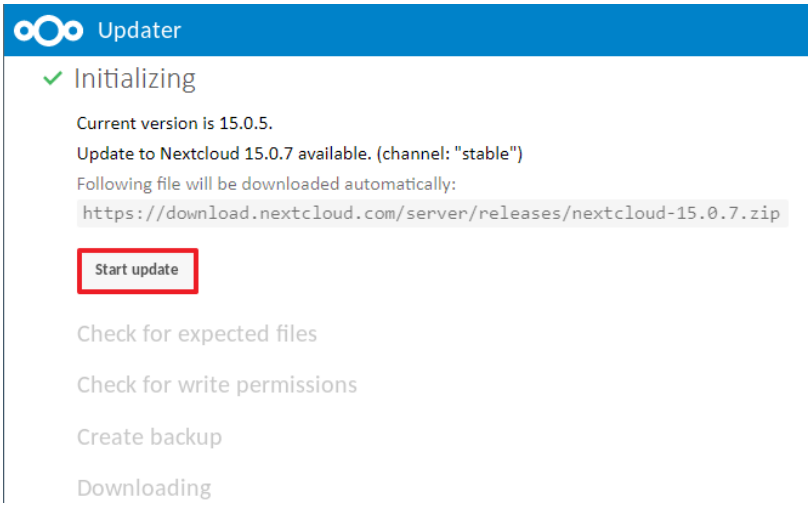
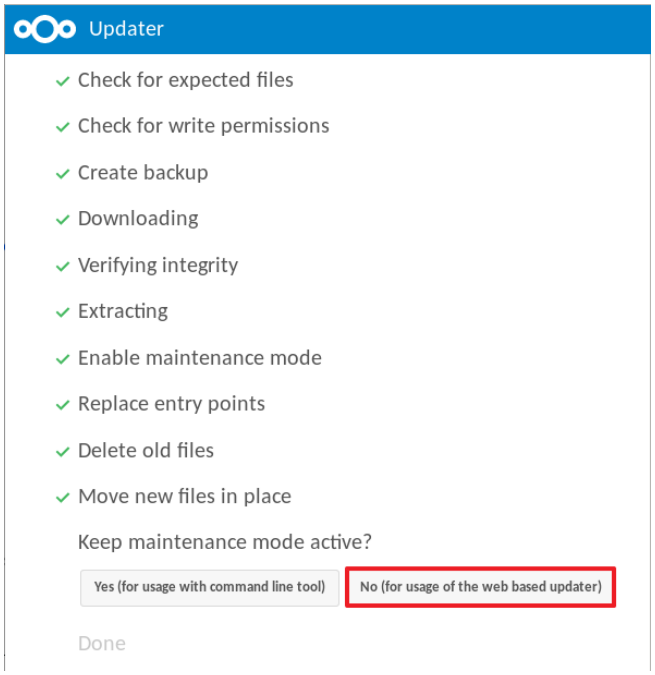
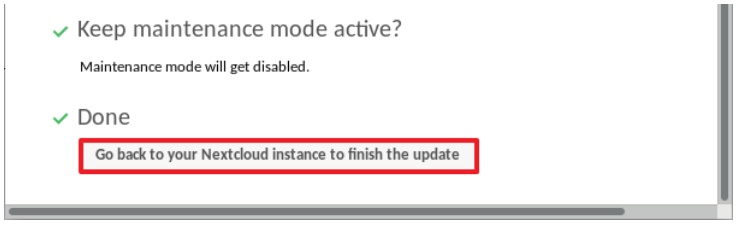
Paso	Descripción
126.	Como se puede observar en la imagen adjunta, se selecciona el puerto tcp 4443 como “Fuente” y en “Destino” se selecciona “Reenvío local” y en “Puerto / Rango de puertos:” el puerto 443 correspondiente al servicio https. Cuando finalice de configurar pulse “Aceptar”. 
127.	Posteriormente se debe revisar el apartado Filtro ICMP. Deberá de realizar un análisis para bloquear o permitir los distintos mensajes de control que sean de aplicación en su organización.  **Nota:** Al seleccionar los diferentes tipos de mensajes de control, se aplicarán automáticamente los bloqueos. Esto se debe a que la configuración del firewall es en “Tiempo de ejecución”.

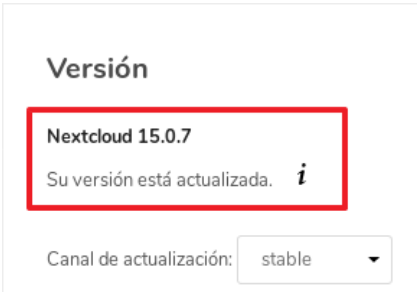
Paso	Descripción
128.	Una vez comprobada la funcionalidad de la configuración realizada anteriormente, deberá de realizarla de nuevo de forma permanente. Para ello vaya al inicio de la pantalla de "Configuración del cortafuegos" y en el desplegable de "Configuración" seleccione "Permanente".  **Nota:** Deberá realizar la configuración desde el paso 91 del punto 6 CONFIGURACIÓN DE FIREWALLD PARA SERVICIOS NEXTCLOUD fijándose que el apartado "Configuración" mantiene seleccionada la opción "Permanente".
129.	Cuando finalice, cierre la ventana de "Configuración del cortafuegos".

8. APLICACIÓN DE ACTUALIZACIONES

Paso	Descripción
130.	Se procede a configurar usuarios y grupos.
131.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Internet" seleccione "**Firefox**" o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
132.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
133.	Debe iniciar sesión en la aplicación Nextcloud con una cuenta administrador que pertenezca al grupo de "admin".
134.	Diríjase al icono de su usuario y en el menú desplegable pulse "Configuración". 

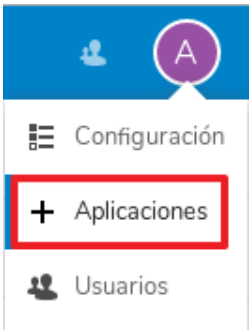
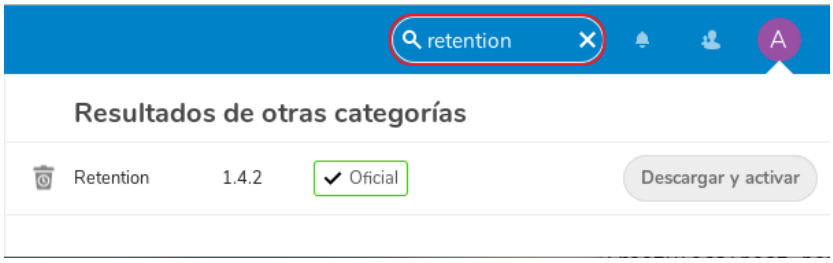
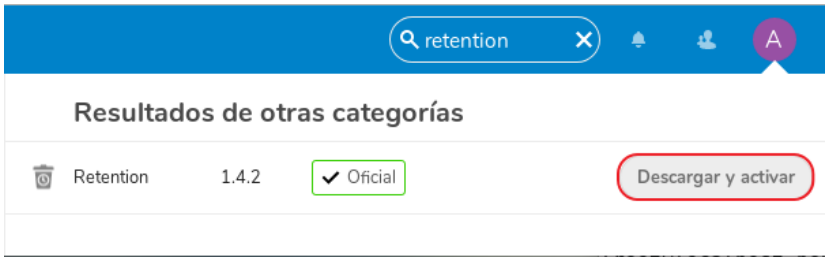
Paso	Descripción
135.	En la barra lateral izquierda seleccione **“Administración” → “Vista general”**. 
136.	Antes de comprobar y comenzar a instalar las actualizaciones, diríjase al apartado inicial “Avisos de seguridad y configuración”. Se recomienda que solvente los problemas que pudiera notificar el servidor Nextcloud antes de comenzar a aplicar actualizaciones. Una vez solventadas las posibles cuestiones a resolver, se le notificará en el mismo apartado mediante un icono de confirmación verde y el siguiente texto “Ha pasado todos los controles”. 
137.	Posteriormente en el siguiente apartado “Versión” se notificarán las actualizaciones disponibles para su servidor. Para comenzar compruebe que en el menú desplegable “Canal de actualización” se encuentra seleccionada la opción “stable”. Posteriormente pulse “Abrir el actualizador”.  **Nota:** Los canales de actualización disponibles son los siguientes. - **production** siempre proporcionará el último nivel de parches, pero no se actualizará a la próxima versión principal de inmediato. Esa actualización generalmente ocurre con la segunda versión menor (x.0.2). - **stable** es la versión estable más reciente. Es adecuada para uso en producción y siempre se actualizará a la última versión principal. - **beta** es una versión preliminar solo para probar nuevas características, no para entornos de producción.

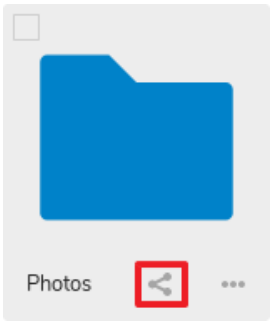
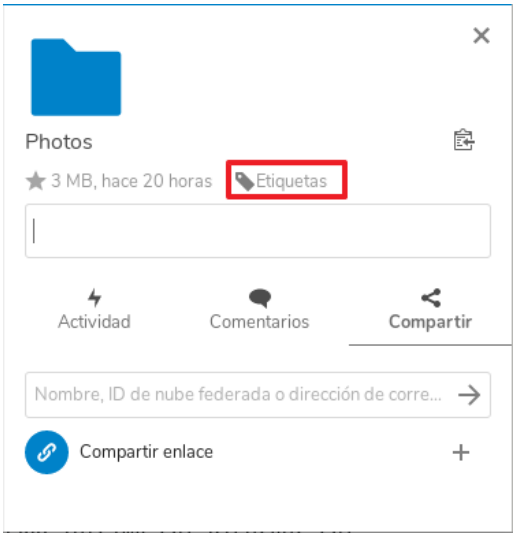
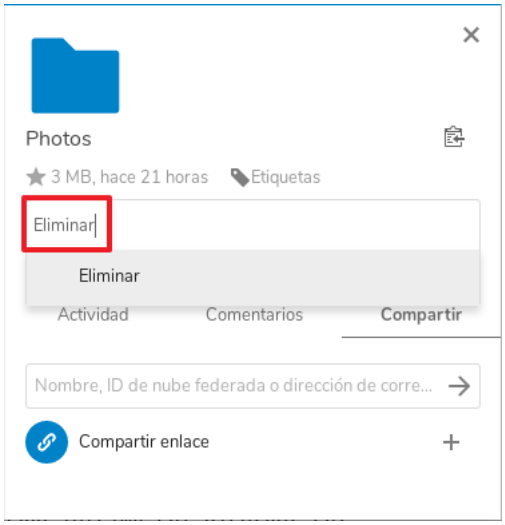
Paso	Descripción
138.	El actualizador realizará varios pasos necesarios para una correcta actualización. Para comenzar pulse “Start update”. 
139.	Cuando finalice de realizar todos los pasos necesarios preguntará si desea mantener activo el modo de mantenimiento, pulse en “No (for usage of the web based updater)”. 
140.	Al realizarlo de este modo, el servidor redireccionará hacia el “updater” basado en WEB. Para ello pulse en “Go back to your Nextcloud instance to finish the update”. 

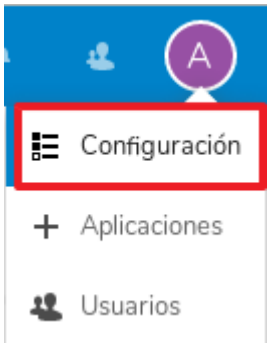
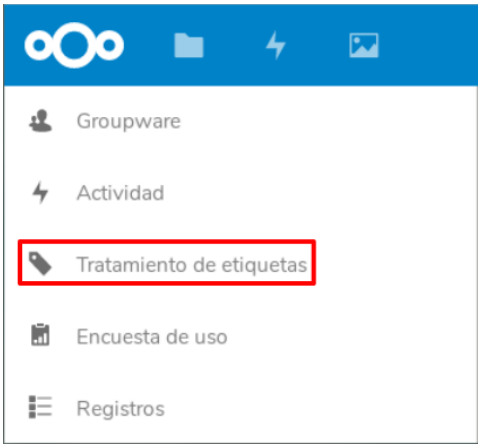
Paso	Descripción
141.	Se mostrará el asistente de actualización de Nextcloud (Updater). Lea detenidamente las advertencias y cuando esté listo pulse el botón “Iniciar actualización” 
142.	El servidor comenzará la actualización y comprobará la integridad del código una vez finalice, al finalizar le redireccionará al servidor si el proceso ha sido satisfactorio. 
143.	Compruebe que no existen nuevas actualizaciones cuando finalice. 

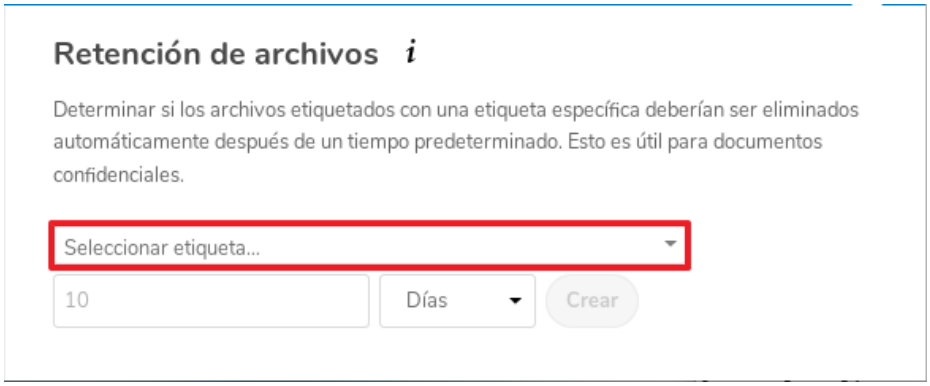
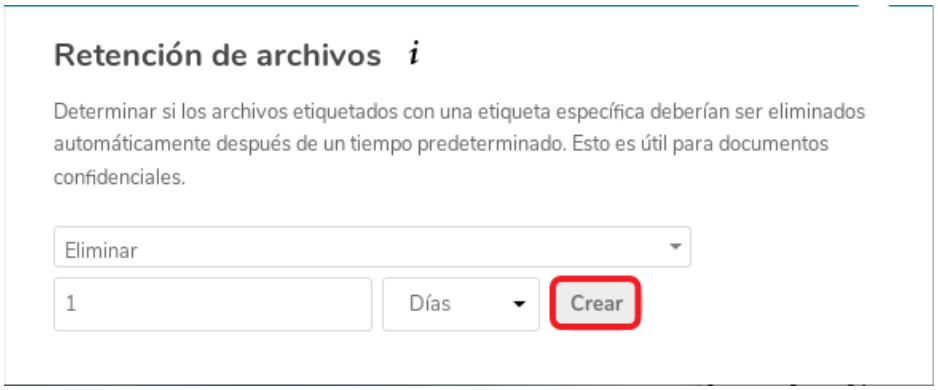
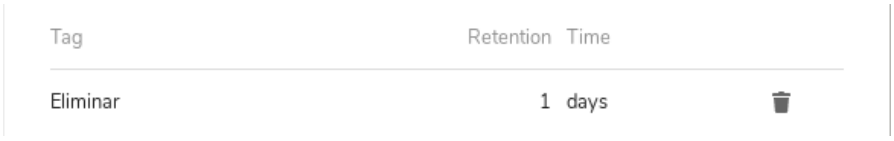
9. CONFIGURACIÓN DEL SISTEMA DE FICHEROS Y PERMISOS

9.1. ELIMINACIÓN AUTOMÁTICA DE ARCHIVOS

Paso	Descripción
144.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “**Firefox**” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
145.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
146.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
147.	Diríjase al icono de su usuario y en el menú desplegable pulse “Aplicaciones”. 
148.	En el panel de navegación superior elija el icono de la lupa para buscar y escriba el siguiente texto: “retention”. 
149.	Pulse el botón “Descargar y activar” para obtener la aplicación y que se encuentre activa en el servidor.  **Nota:** Fíjese siempre que las aplicaciones lleven el recuadro verde que garantice que son aplicaciones **oficiales** y por tanto están aprobadas por los desarrolladores de Nextcloud.

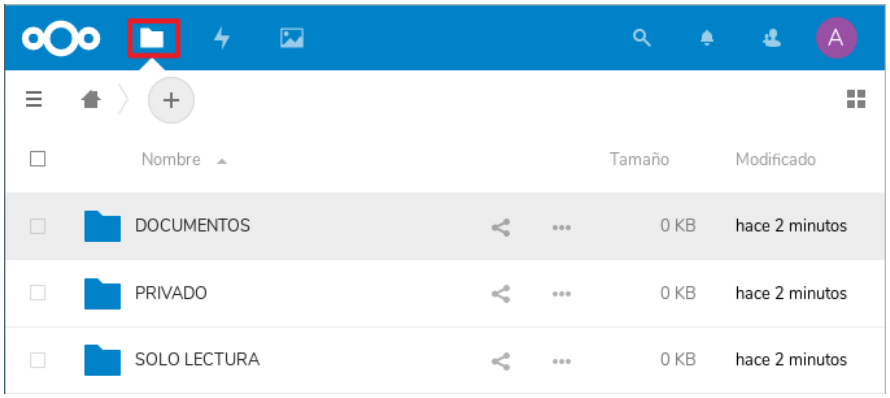
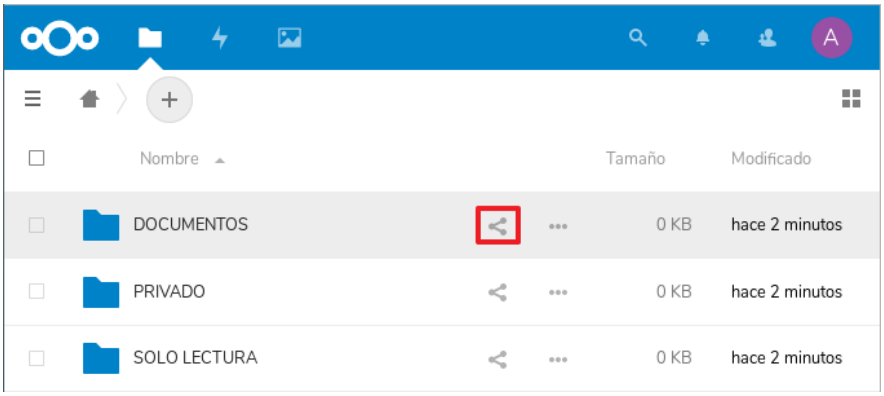
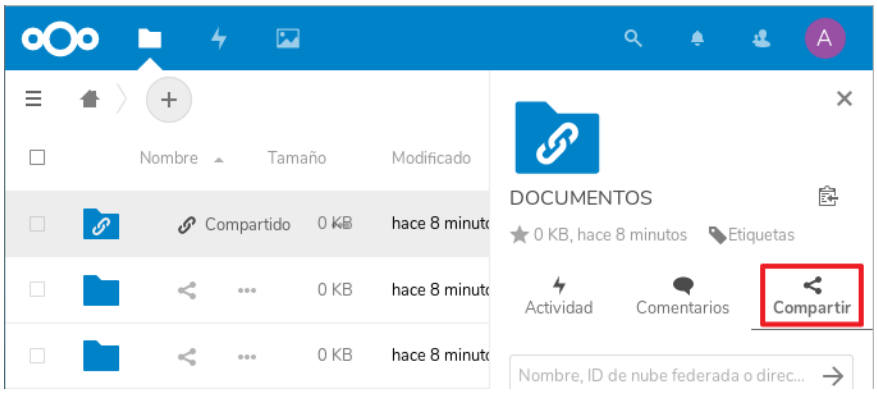
Paso	Descripción
150.	Para programar la eliminación automática de archivos se deben asignar etiquetas anteriormente. Se muestra un ejemplo a continuación de asignación de etiquetas a un archivo alojado en el servidor. Diríjase a los archivos del servidor elija el fichero que quiere programar su eliminación y pulse el icono compartir. 
151.	Se desplegará automáticamente un menú a la derecha de la pantalla. Pulse en “Etiquetas” para añadir una etiqueta. 
152.	Escriba una etiqueta característica para marcar ese fichero o directorio y pulse “Enter”. 

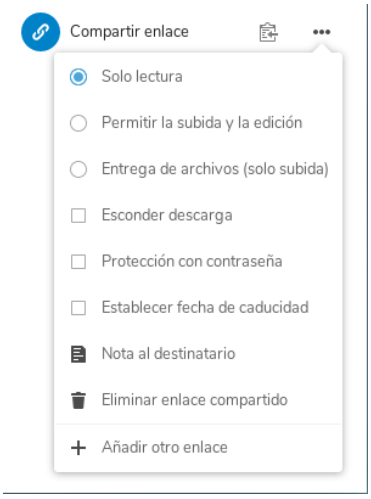
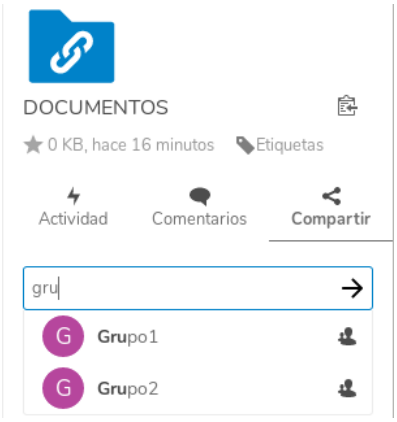
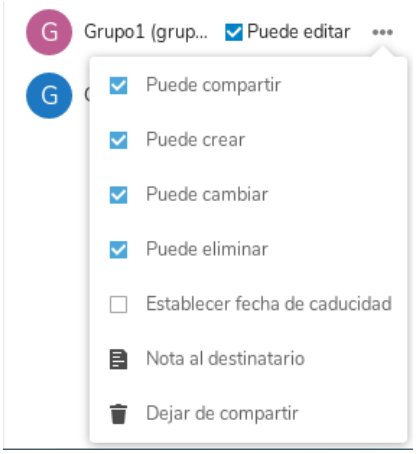
Paso	Descripción
153.	Compruebe que se añade la etiqueta correctamente al fichero o directorio. 
154.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
155.	En la columna de la izquierda seleccione “Flujo de trabajo”.  **Nota:** Debido a las constantes actualizaciones que se producen el producto “**Nextcloud**”, los títulos de las opciones o apartados, podrían sufrir alguna discrepancia con respecto al momento de la elaboración de esta guía. Por ejemplo, en versiones anteriores de la 15.0.7, la aplicación “retention”, en su opción de “Flujo de datos” cambia el nombre a “tratamiento de etiquetas”, manteniendo el mismo icono.

Paso	Descripción
156.	Diríjase al título “Retención de archivos” y en la pestaña “Seleccionar etiqueta…” elija la etiqueta creada anteriormente. En este ejemplo será la etiqueta “Eliminar”. 
157.	Configure la franja de tiempo en la que el fichero o directorio se eliminará y pulse el botón “Crear” para finalizar. 
158.	Se creará la regla en el servidor.  **Nota:** Tenga en cuenta que todo archivo que contenga esta etiqueta se eliminará en la franja de tiempo configurada en la regla.

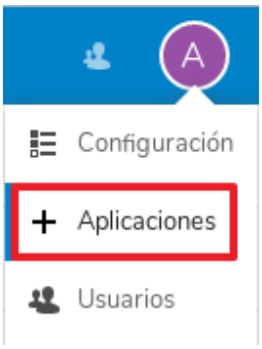
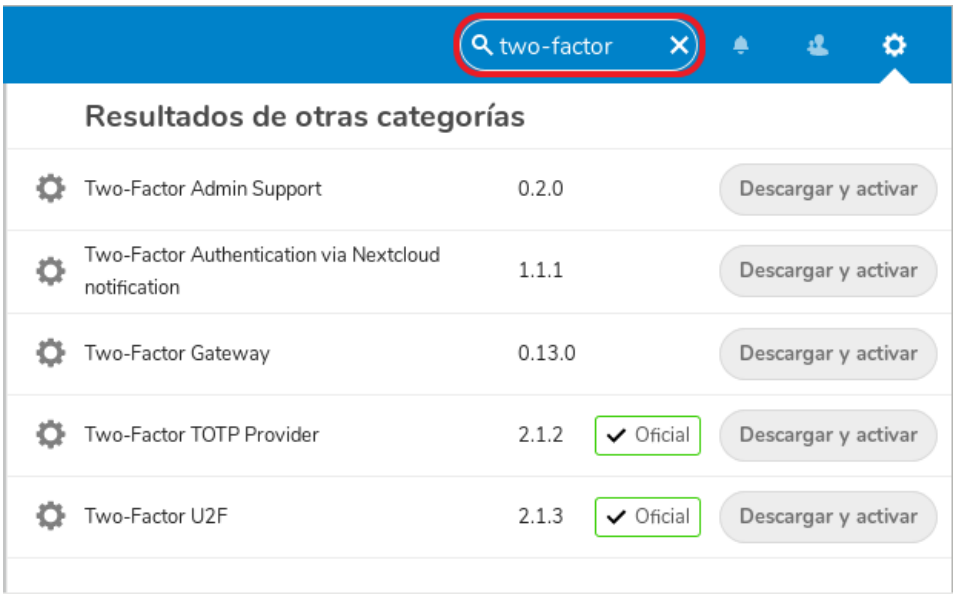
9.2. COMPARTICIÓN DE CARPETAS Y DOCUMENTOS

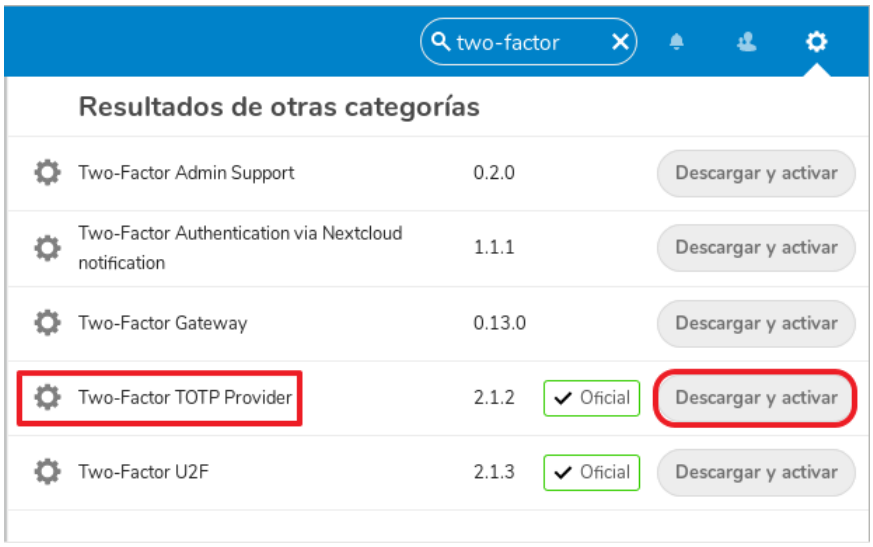
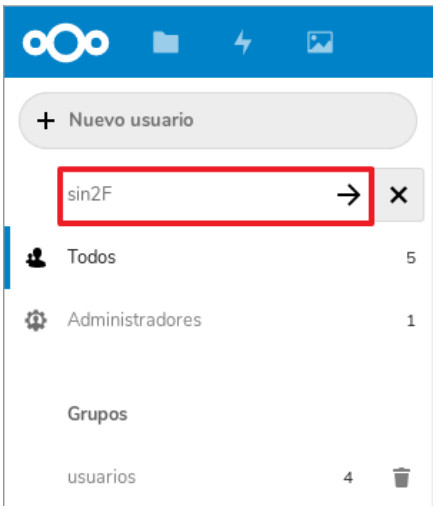
Paso	Descripción
159.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
160.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.

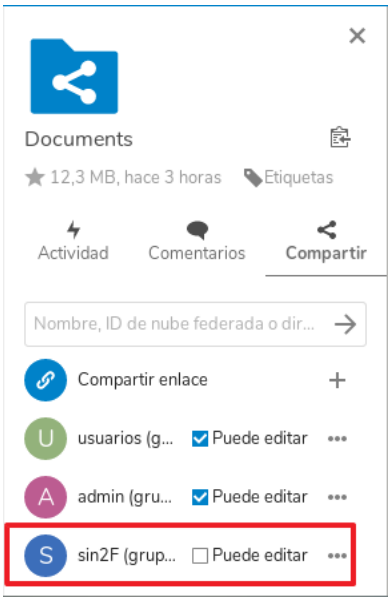
Paso	Descripción
161.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
162.	Diríjase al icono “Archivos” para que se muestren todos los documentos de su usuario. 
163.	Seleccione el icono compartir para desplegar las opciones de compartición. 
164.	Se mostrará el menú de propiedades del directorio, seleccionando el apartado “Compartir”. 

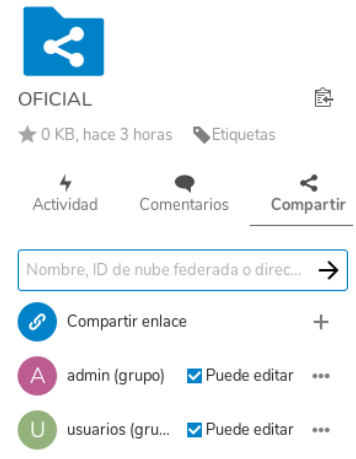
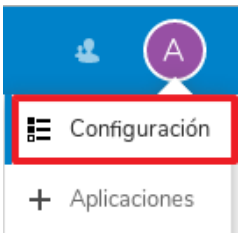
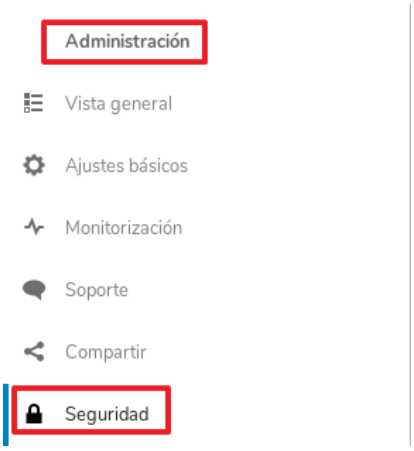
Paso	Descripción
165.	Se crea automáticamente el apartado “Compartir enlace”, pulse sobre “…” y seleccione los permisos que más convengan a su organización. 
166.	Posteriormente diríjase a la barra de búsqueda de usuarios y grupos ubicada justo encima y seleccione los usuarios y grupos a los que se le compartirá la carpeta. 
167.	Una vez seleccionado el Grupo o el usuario, pude permitir o denegar los permisos del mismo en el interior de la carpeta. Además, puede seleccionar una fecha de caducidad para la compartición de la carpeta. 

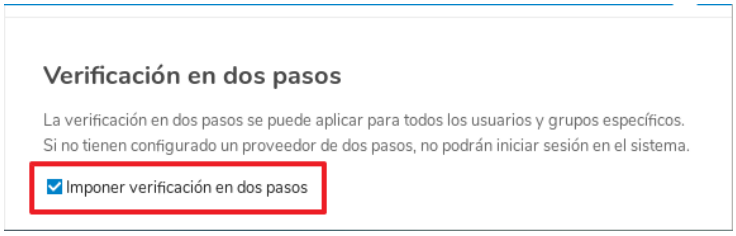
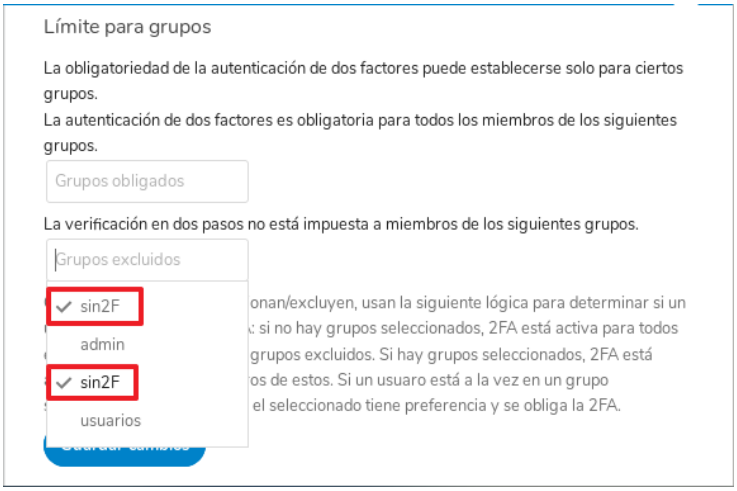
10. AUTENTICACIÓN DE DOBLE FACTOR

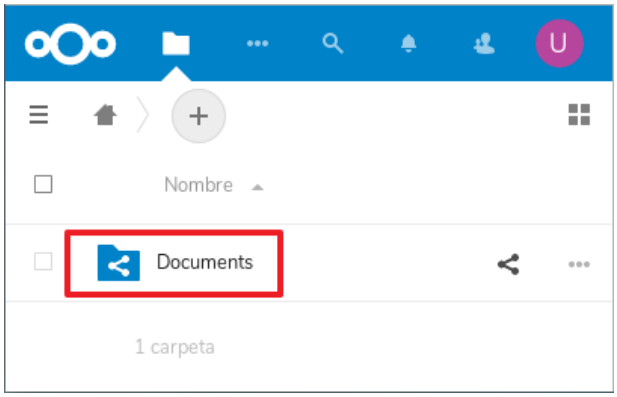
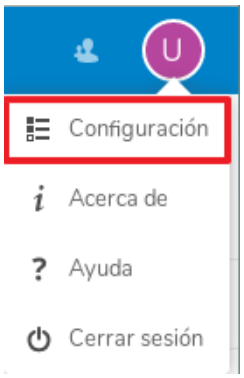
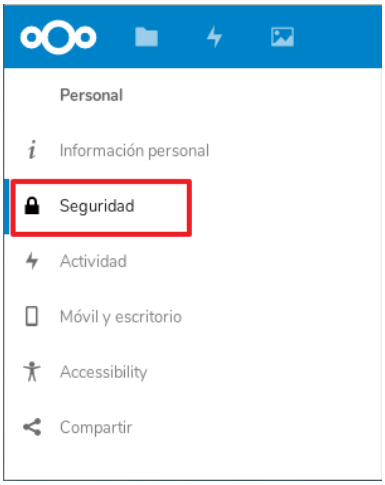
Paso	Descripción
168.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
169.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
170.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
171.	Diríjase al icono de su usuario y en el menú desplegable pulse “+ Aplicaciones”. 
172.	En el panel de navegación superior elija el icono de la lupa para buscar y escriba el siguiente texto: “two-factor”. 

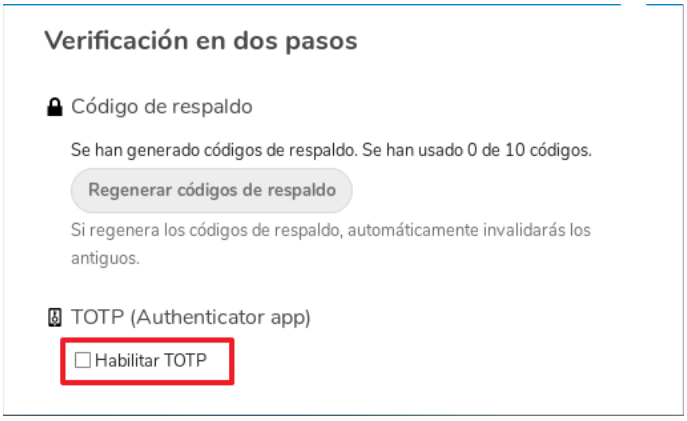
Paso	Descripción
173.	Entre los resultados de la búsqueda, debe elegir la aplicación más acorde con su organización. En este ejemplo se elegirá la aplicación "Two-Factor TOPT Provider" para ello, diríjase a la aplicación elegida y pulse el botón "Descargar y activar" para obtener la aplicación y que se encuentre activa en el servidor. Introduzca la contraseña si se le solicita.  **Nota:** Fíjese siempre que las aplicaciones lleven el recuadro verde que garantice que son aplicaciones oficiales y por tanto están aprobadas por los desarrolladores de Nextcloud.
174.	En primer lugar, se deberá crear un grupo para usuarios que **no tengan habilitado** el doble factor de autenticación. En este ejemplo se le nombrará como "sin2F". Para ello vaya al icono de su usuario y en el menú desplegable pulse **"Usuarios" → "Añadir grupo"**.  **Nota:** El grupo de ejemplo "sin2F" tendrá limitaciones de acceso a documentación más crítica y su principal característica es permitir al usuario configurar la autenticación de doble factor. Cuando un usuario posea la autenticación de doble factor activa, se deberá migrar a su grupo original.

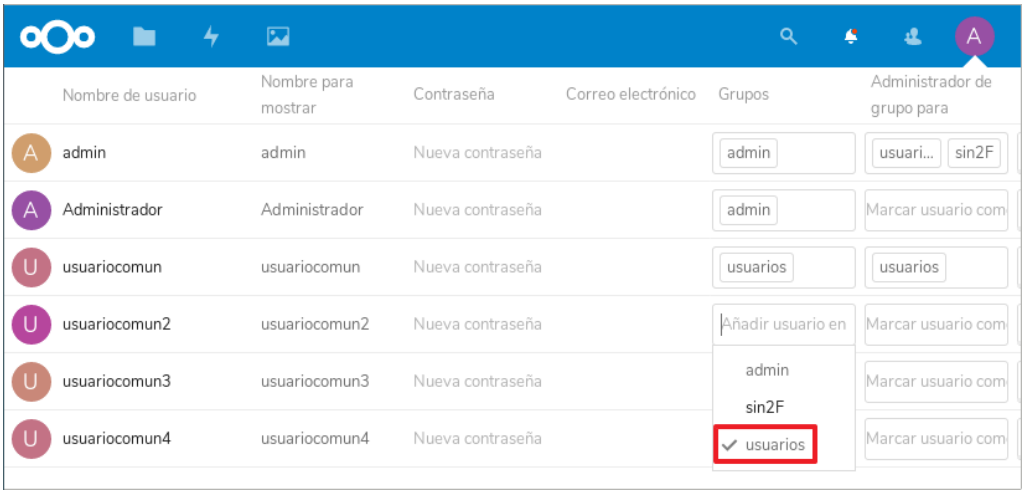
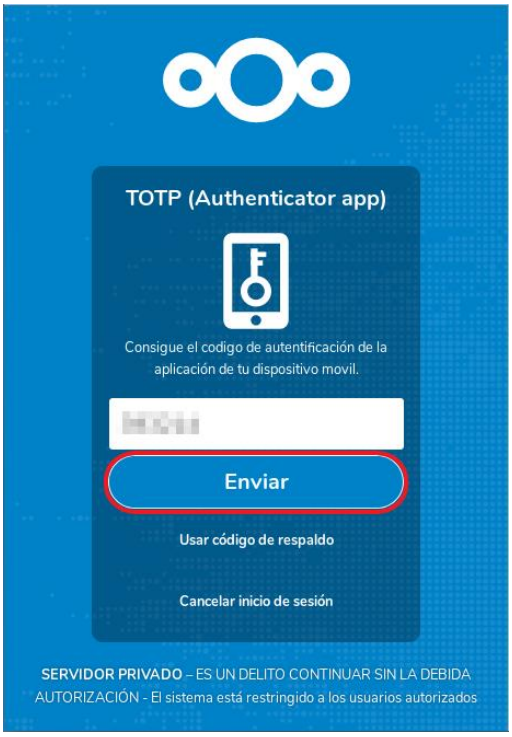
Paso	Descripción
175.	En este ejemplo, existe un usuario creado en el sistema llamado “usuariocomun2”, se va a añadir al grupo “sin2F” y se eliminará la pertenencia al grupo “usuarios” que era su grupo original. 
176.	En las carpetas compartidas se va a permitir la compartición de la carpeta de ejemplo “Documents” con todos los grupos predeterminados incluyendo el grupo “sin2F” con los permisos mínimos. 

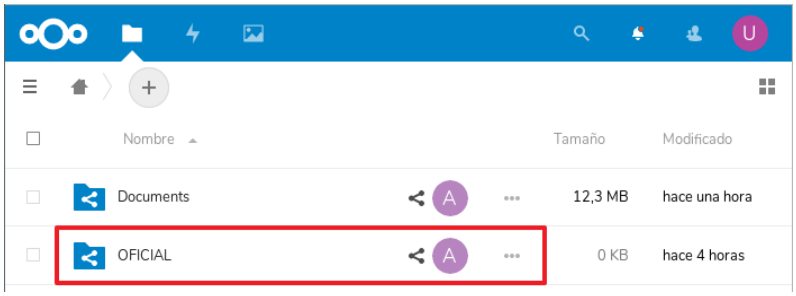
Paso	Descripción
177.	En cambio, la carpeta de ejemplo “OFICIAL” solo se va a permitir a los grupos predeterminados que serán los que poseen el doble factor de autenticación habilitado.  **Nota:** Deberá configurar correctamente todos los permisos acorde con las necesidades específicas de su organización, haciendo hincapié en dotar del menor permiso necesario a los usuarios que no posean la doble autenticación.
178.	Para asegurar que cualquier usuario que inicie sesión en el servidor deba hacerlo por el método de doble factor de autenticación realice los siguientes pasos. Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
179.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Seguridad”. 

Paso	Descripción
180.	Vaya al apartado “Verificación en dos pasos” y seleccione “Imponer verificación en dos pasos”. 
181.	Posteriormente diríjase al apartado “Límite para grupos” y deje vacío el recuadro de “Grupos obligados” para obligar a todos los grupos del servidor a cumplir la verificación de doble factor. En el recuadro de “Grupos excluidos” seleccione el grupo definido anteriormente para la habilitación del doble factor de autenticación. En este ejemplo el grupo añadido será “sin2F”. 
182.	Guarde los cambios para que tenga efecto.  **Nota:** Tenga en cuenta que, si impone la verificación en dos pasos, los usuarios que no posean de la verificación correctamente configurada no podrán acceder al servidor. Si ha impuesto la verificación en dos pasos a los usuarios del grupo **“admin”** y no los ha configurado correctamente **no podrá iniciar sesión en el servidor como Administrador**.

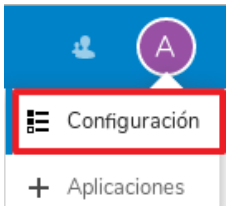
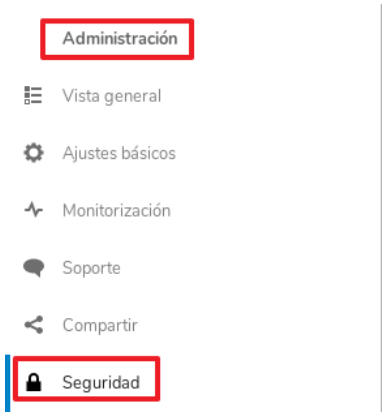
Paso	Descripción
183.	Se debe iniciar sesión en el usuario perteneciente al grupo “sin2F” al que desea configurarle el doble factor de autenticación, en este ejemplo el usuario será “usuariocomun2”. Compruebe que solo tiene acceso a los recursos compartidos exclusivamente para ese grupo de usuarios. 
184.	Para configurar la verificación en dos pasos vaya al icono del usuario y pulse en “Configuración”. 
185.	En la barra lateral izquierda, en el título “Personal” diríjase al apartado “Seguridad”. 

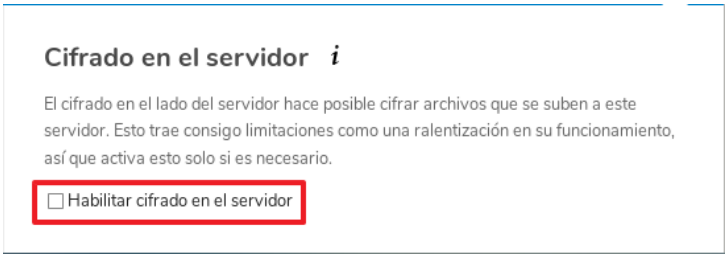
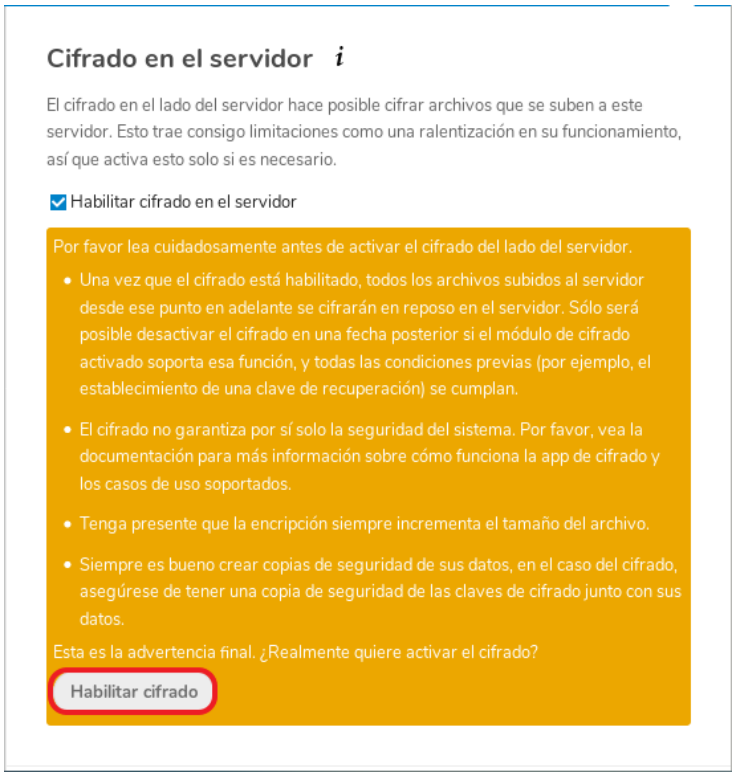
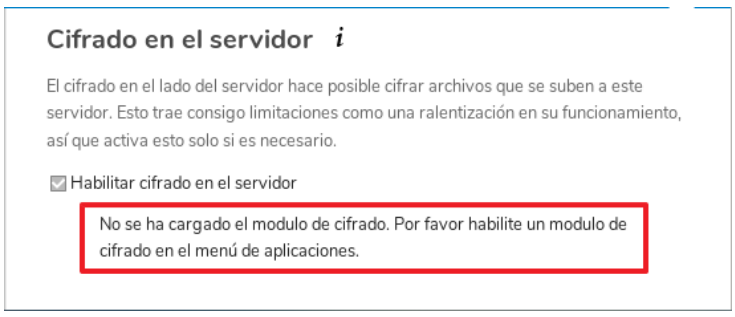
Paso	Descripción
186.	En el título “Verificación en dos pasos” pulse en “Habilitar TOPT”.  **Nota:** Si desea usar una aplicación distinta a la escogida de ejemplo en esta guía deberá adaptar los parámetros y configuraciones a las necesidades de la misma.
187.	La aplicación TOPT generará un código QR para ser detectado mediante la aplicación móvil “TOTP Authenticator” que se puede descargar para IOS y Android. Una vez escaneado el código QR se genera una clave que irá variando cada 30 segundos. Introduzca el “Código de autentificación” y pulse el botón Verificar. 
188.	Si la verificación es correcta se mostrará habilitada la opción “Habilitar TOTP”. 

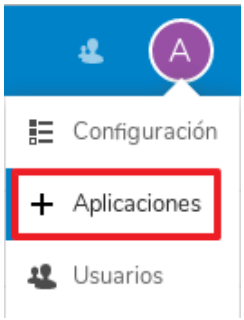
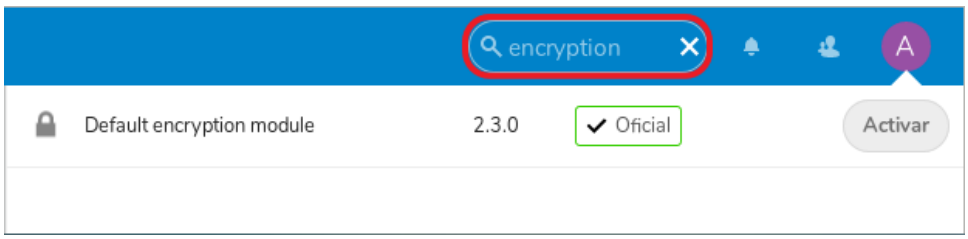
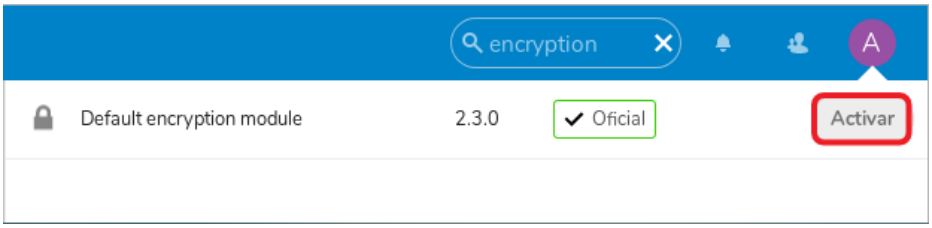
Paso	Descripción
189.	Cierre sesión en el usuario recién configurado e inicie sesión con un usuario Administrador perteneciente al grupo “admin”. Vaya al icono del usuario y pulse en **“Configuración”** → **“Usuarios”** y restaure el grupo original del usuario “usuariocomun2”. 
190.	Cierre sesión con el usuario Administrador e inicie sesión con el usuario configurado para la autenticación de doble factor. Cuando inicie sesión correctamente se le solicitará el código generado en la aplicación “TOTP Authenticator”. Introduzca el código y pulse “Enviar”. 

Paso	Descripción
191.	Compruebe que se le muestran las carpetas compartidas con su grupo predeterminado. 

11. CIFRADO DEL CONTENIDO DE NEXTCLOUD

Paso	Descripción
192.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione **“Firefox”** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
193.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios del ENS.
194.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de “admin”.
195.	Para cifrar el contenido del servidor de alojamientos Nextcloud diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 
196.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Seguridad”. 

Paso	Descripción
197.	Vaya al apartado “Cifrado en el servidor” y seleccione “Habilitar cifrado en el servidor”. 
198.	Una vez seleccione la habilitación de cifrado se desplegará un menú con las distintas cuestiones que hay que tener en cuenta antes de continuar con el cifrado. Lea detenidamente las advertencias y recomendaciones antes de continuar. Si es de aplicación dentro de su organización pulse el botón “Habilitar cifrado”. 
199.	Si no ha habilitado el módulo de cifrado, el servidor notificará la ausencia del mismo. 

Paso	Descripción
200.	Diríjase al icono de su usuario y en el menú desplegable pulse “Aplicaciones”. 
201.	En el panel de navegación superior elija el icono de la lupa para buscar y escriba el siguiente texto: “encryption”. 
202.	Pulse el botón “Activar” para activar el módulo en el servidor.  **Nota:** Fíjese siempre que las aplicaciones lleven el recuadro verde que garantice que son aplicaciones **oficiales** y por tanto están aprobadas por los desarrolladores de Nextcloud.

ANEXO A.5.2. LISTA DE COMPROBACIÓN DEL SERVIDOR NEXTCLOUD 15 PARA LA CATEGORÍA ALTA

Nota: Este anexo es parte de los necesarios para establecer uno de los escenarios elegidos para esta guía. Para ver los que le complementan para una configuración completa se debe consultar el punto de la guía "ANEXO A.5.1 PASO A PASO DE IMPLEMENTACIÓN SEGURA DE SERVIDORES NEXTCLOUD 15 QUE LES SEA DE APLICACIÓN LA CATEGORÍA ALTA DEL ENS".

Este anexo ha sido diseñado para ayudar a los operadores a verificar que se han aplicado las distintas configuraciones de seguridad en los servidores de alojamiento de archivos Nextcloud 15 independientes con implementación de seguridad de categoría alta del ENS.

Para realizar esta lista de comprobación primero deberá iniciar sesión en el cliente con una cuenta de usuario que tenga privilegios de root.

Para realizar las comprobaciones pertinentes en el cliente se deberán ejecutar diferentes consolas con permisos "root" e iniciar sesión con usuarios de Nextcloud pertenecientes al grupo "admin". Éstas estarán disponibles si se ha iniciado sesión en el cliente con una cuenta de usuario perteneciente al grupo de "sudoers". Las consolas y herramientas que se utilizarán son las siguientes:

a) Terminal de Linux

b) Entorno Web Nextcloud 15

Comprobación	OK/NOK	Cómo hacerlo
1. Inicie sesión en el equipo.		En el cliente, inicie sesión con una cuenta con privilegios de root.
2. Inicie la Terminal de Linux		Ejecute la "Terminal". Para ello Diríjase a la barra de tareas, pulse en Aplicaciones y en el apartado "Herramientas del sistema" seleccione "Terminal". 

Comprobación	OK/NOK	Cómo hacerlo

3. Verifique versiones del conjunto de servidores LAMP.		En la "Terminal" ejecute los siguientes comandos y verifique las versiones instaladas.
		$ sudo yum info mariadb
		$ sudo yum info httpd
		$ sudo php -v
		`Paquetes instalados`
		`Nombre : httpd`
		`Arquitectura : x86_64`
		`Versión : 2.4.6`
		`Lanzamiento : 88.el7.centos`
		`Tamaño : 9.4 M`
		`Repositorio : installed`
		`Desde el repositorio : base`
		`Resumen : Apache HTTP Server`
		`URL : http://httpd.apache.org/`
		`Licencia : ASL 2.0`
		`Descripción :The Apache HTTP Server is a powerful,`
		`: web server.`
		Nota: Debe adecuar las versiones a las necesidades y compatibilidad de los diferentes elementos de su organización, teniendo en cuenta que las versiones deben ser las últimas con soporte y recomendadas por el desarrollador.

4. Comprobación de repositorios remi activos.		Abra la Terminal y ejecute el siguiente comando.
		$ sudo ls /etc/yum.repos.d/remi*
		usuario@localhost:~
		Archivo Editar Ver Buscar Terminal Ayuda
		`[usuario@localhost ~]$ sudo ls /etc/yum.repos.d/remi*`
		`/etc/yum.repos.d/remi-glpi91.repo`
		`/etc/yum.repos.d/remi-glpi92.repo`
		`/etc/yum.repos.d/remi-glpi93.repo`
		`/etc/yum.repos.d/remi-glpi94.repo`
		`/etc/yum.repos.d/remi-modular.repo`
		`/etc/yum.repos.d/remi-php54.repo`
		`/etc/yum.repos.d/remi-php70.repo`
		`/etc/yum.repos.d/remi-php71.repo`
		`/etc/yum.repos.d/remi-php72.repo`
		`/etc/yum.repos.d/remi-php73.repo`
		`/etc/yum.repos.d/remi.repo`
		`/etc/yum.repos.d/remi-safe.repo`
		`[usuario@localhost ~]$`
		Nota: Tenga en consideración que a medida que aparezcan nuevas versiones, los repositorios pueden variar.

Comprobación	OK/NOK	Cómo hacerlo

Configuración	OK/NOK
/etc/yum.repos.d/remi-glpi91.repo	
/etc/yum.repos.d/remi-glpi92.repo	
/etc/yum.repos.d/remi-glpi93.repo	
/etc/yum.repos.d/remi-glpi94.repo	
/etc/yum.repos.d/remi-modular.repo	
/etc/yum.repos.d/remi-php54.repo	
/etc/yum.repos.d/remi-php70.repo	
/etc/yum.repos.d/remi-php71.repo	
/etc/yum.repos.d/remi-php72.repo	
/etc/yum.repos.d/remi-php73.repo	
/etc/yum.repos.d/remi.repo	

5. Ficheros de configuración Apache.

Ejecute los siguientes comandos y compruebe que es correcta la configuración según las necesidades específicas de su organización.

```
$ sudo gnome-text-editor /etc/httpd/conf/httpd.conf &>/dev/null
$ sudo gnome-text-editor /etc/httpd/conf.d/nextcloud.conf &>/dev/null
```

6. Ficheros de configuración PHP.

Ejecute los siguientes comandos y compruebe que es correcta la configuración según las necesidades específicas de su organización.

```
$ sudo gedit /etc/php.ini &>/dev/null
$ sudo gedit /etc/php.d/10-opcache.ini &>/dev/null
```

7. Comprobación de cifrado seguro.

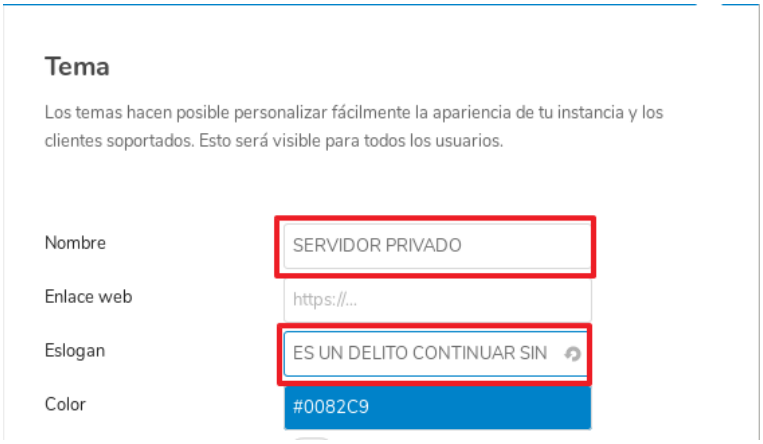
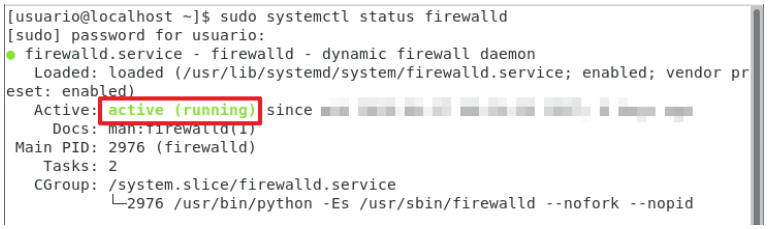
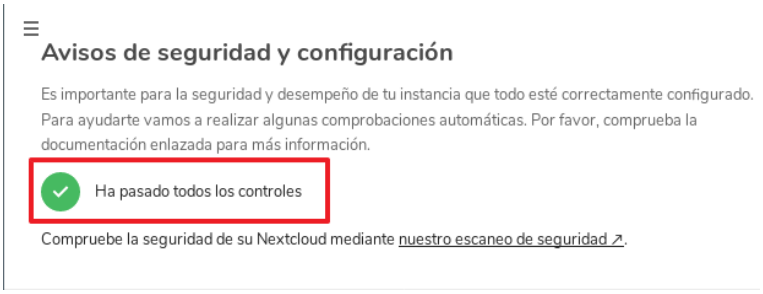
Inicie sesión en la base de datos MariaDB y compruebe los parámetros requeridos, para ello ejecute los siguientes comandos.

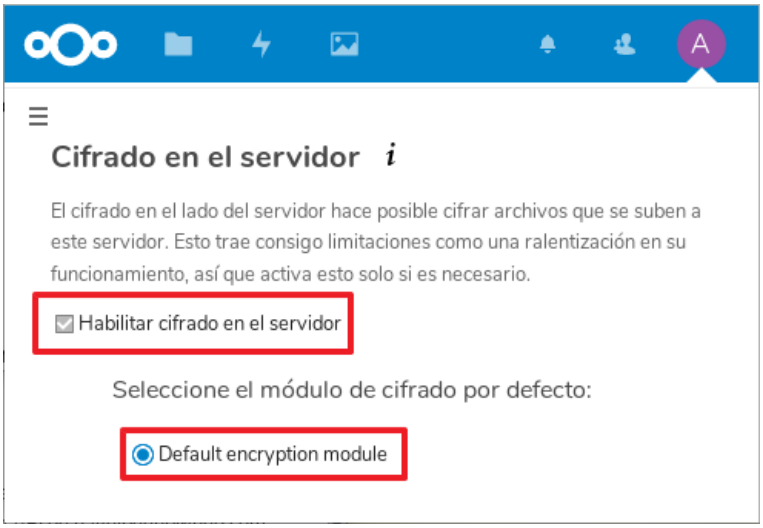
```
$ sudo mysql -u root -p
MariaDB [(none)]> use nextcloud;
MariaDB [nextcloud]>select * from oc_users;
MariaDB [nextcloud]>exit;
```

```
+-------------------------------------------------------------+
| password                                                    |
+-------------------------------------------------------------+
| 2|$argon2i$v=19$m=1024,t=2,p=[redacted]                      |
| 2|$argon2i$v=19$m=1024,t=2,p=[redacted]                      |
| 2|$argon2i$v=19$m=1024,t=2,p=[redacted]                      |
+-------------------------------------------------------------+
```

Configuración	Valor	OK/NOK
Usuario Administrador	2|$argon2i$v=19$m=1024,t=2,	
Resto de usuarios	2|$argon2i$v=19$m=1024,t=2,	

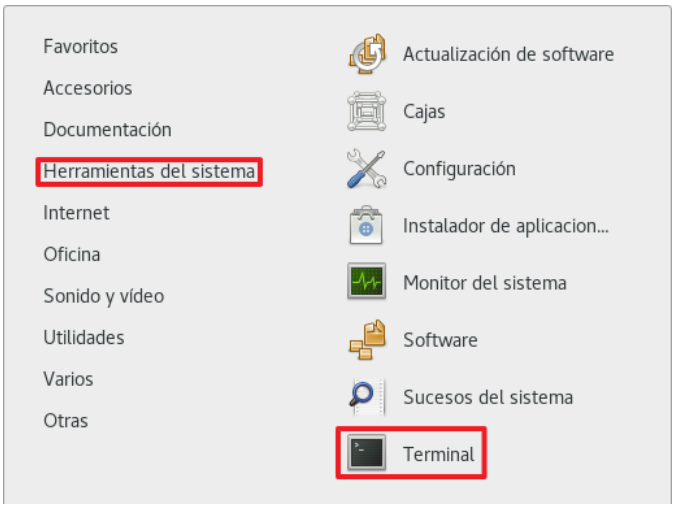
<table>
<tr><th>Comprobación</th><th>OK/NOK</th><th>Cómo hacerlo</th></tr>
<tr><td>8. Aplicaciones instaladas</td><td></td><td>Compruebe que las aplicaciones existentes en el servidor Nextcloud son las mínimas necesarias para su organización. Para ello ejecute el siguiente comando.
$ sudo ls /var/www/html/nextcloud/apps</td></tr>
<tr><td>9. Inicie sesión en el servidor Nextcloud</td><td></td><td>Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Internet” seleccione “Firefox” o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud. Debe iniciar sesión con una cuenta Administrador global que pertenezca al grupo de “admin”.</td></tr>
<tr><td>10. Registros de actividad</td><td></td><td>Vaya al icono de su usuario y en el menú desplegable pulse “Configuración” → “Aplicaciones” → “Tus apps” → “Apps activas” y compruebe que se encuentra instalada y activada la aplicación “Activity”.</td></tr>
<tr><td>11. Control de acceso a los archivos.</td><td></td><td>Vaya al icono de su usuario y en el menú desplegable pulse “Configuración” → “Aplicaciones” → “Tus apps” → “Apps activas” y compruebe que se encuentra instalada y activada la aplicación “File access control”.</td></tr>
<tr><td>12. Reenvío de logs a syslog</td><td></td><td>Abra la terminal y ejecute el siguiente comando para comprobar la correcta configuración de los parámetros establecidos para su organización. Adapte la ruta según su configuración.
$ sudo cat /var/www/html/nextcloud/config/config.php</td></tr>
<tr><td>13. Política de contraseñas</td><td></td><td>Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración” → “Administración” → “Seguridad” → “Política de contraseñas”.
<table>
<tr><th>Configuración</th><th>Valor</th><th>OK/NOK</th></tr>
<tr><td>Longitud mínima</td><td>12</td><td></td></tr>
<tr><td>Imponer caracteres en mayúsculas y minúsculas</td><td>☑</td><td></td></tr>
<tr><td>Imponer caracteres numéricos</td><td>☑</td><td></td></tr>
<tr><td>Imponer caracteres especiales</td><td>☑</td><td></td></tr>
<tr><td>Comprobar contraseña contra la lista de contraseñas filtradas de haveibeenpwned.com</td><td>☑</td><td></td></tr>
</table>
</td></tr>
</table>

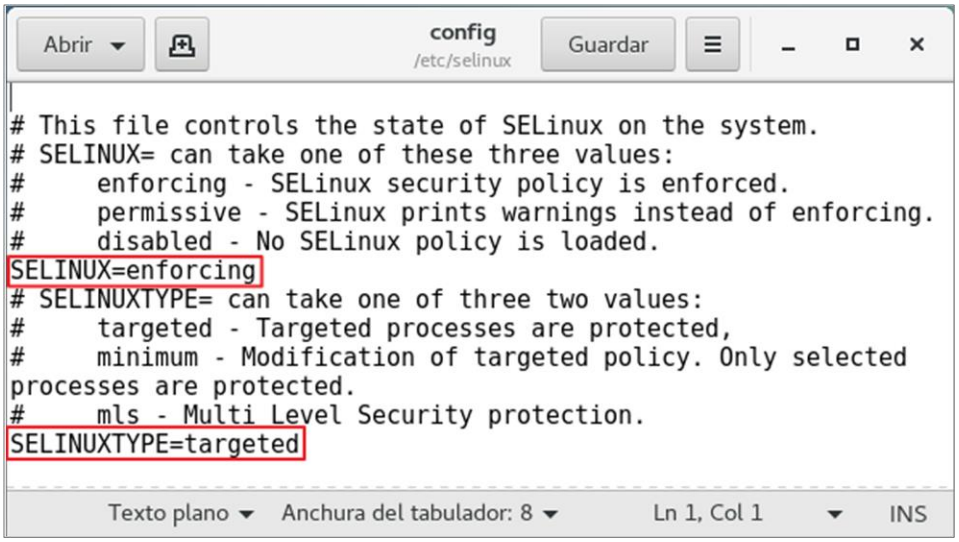
Comprobación	OK/NOK	Cómo hacerlo
14. Mensaje disuasorio		Vaya al icono de su usuario y en el menú desplegable pulse **"Configuración" → "Administración" → "Tema"** y compruebe que se encuentran configurados los apartados remarcados en la siguiente imagen. 
15. Demonio Firewalld		Ejecute el siguiente comando y compruebe que el firewall de CentOS 7 Linux se encuentra activo. **$ sudo systemctl status firewalld** 
16. Firewall CentOS 7 Linux		Vaya a la barra de tareas, pulse en **"Aplicaciones" → "Varios" → "Cortafuegos"**. En el apartado "Configuración:" seleccione en el menú desplegable la opción "Permanente" y revise su configuración.
17. Avisos de seguridad.		Vaya al icono de su usuario y en el menú desplegable pulse **"Configuración" → "Administración" → "Vista general"** y compruebe que se no existen avisos de seguridad y se muestra el mensaje "Ha pasado todos los controles". 

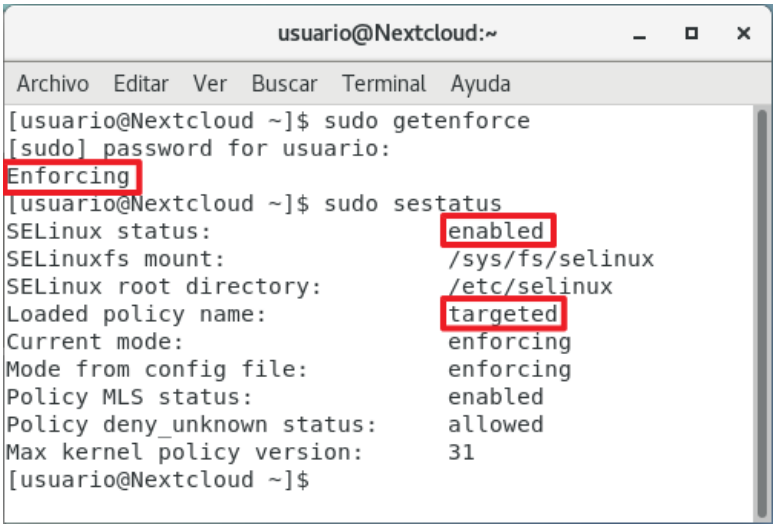
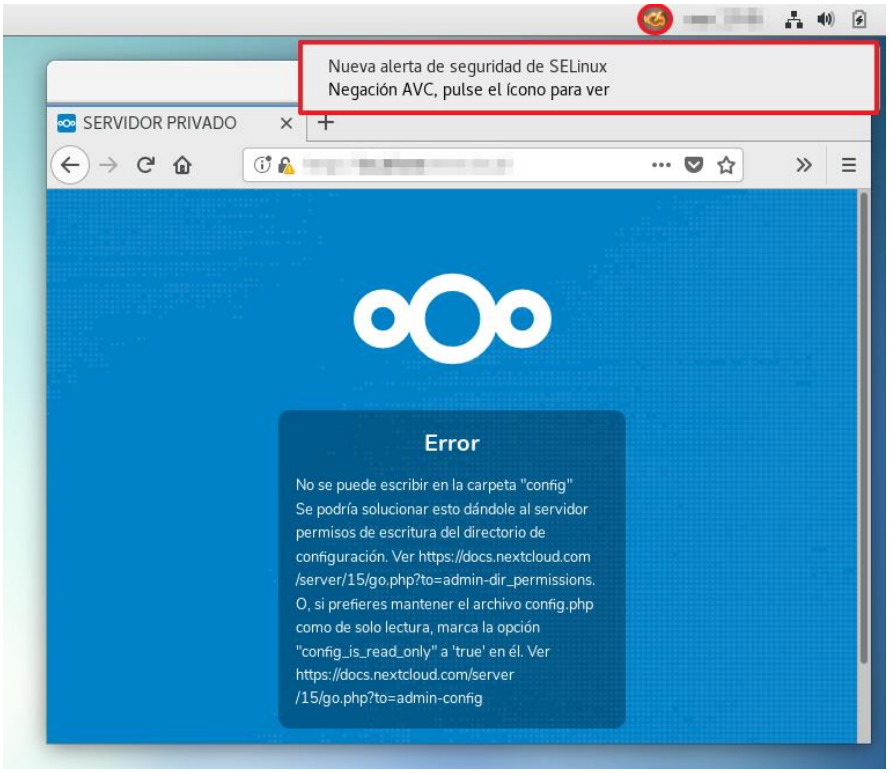
Comprobación	OK/NOK	Cómo hacerlo
18. Retención de archivos		Vaya al icono de su usuario y en el menú desplegable pulse **"Aplicaciones" → "Tus apps" → "Apps activas"** y compruebe que se encuentra instalada y activada la aplicación "Retention".
19. Aplicación doble factor de autenticación		Vaya al icono de su usuario y en el menú desplegable pulse **"Aplicaciones" → "Tus apps" → "Apps activas"** y compruebe que se encuentra instalada y activada una aplicación para autenticación de doble factor, la recomendación de esta guía es la aplicación "Two-Factor TOTP Provider".
20. Configuración de doble factor de autenticación		Vaya al icono de su usuario y en el menú desplegable pulse **"Configuración" → "Administración" → "Seguridad"** y compruebe que en el apartado "Verificación en dos pasos" se encuentra seleccionada la opción "imponer verificación en dos pasos".
21. Cifrado del contenido de Nextcloud.		Vaya al icono de su usuario y en el menú desplegable pulse **"Configuración" → "Administración" → "Seguridad"** y compruebe que en el apartado "Cifrado en el servidor" se encuentra seleccionada la opción "Habilitar cifrado del servidor", y el módulo por defecto "Default encryption module". 

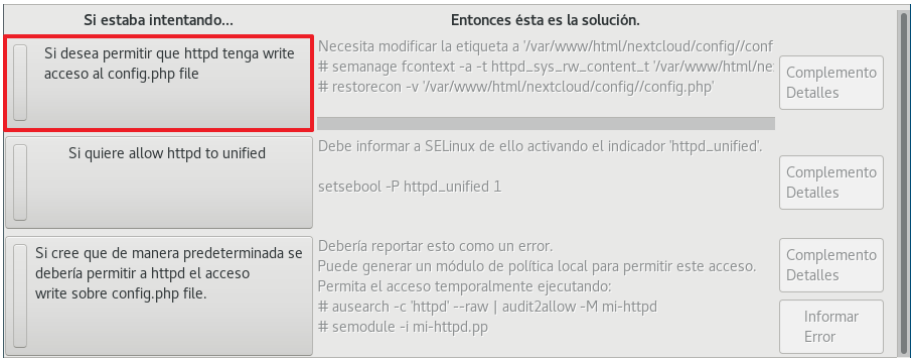
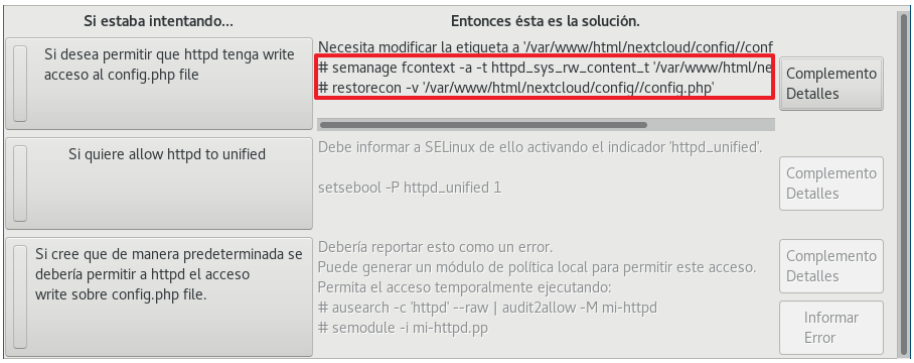
ANEXO A.6. TAREAS ADICIONALES DE SEGURIDAD

ANEXO A.6.1. CONFIGURACIÓN ADICIONAL DE SEGURIDAD – SELINUX

Paso	Descripción
1.	Se va a proceder a revisar el estado de Selinux, así como su configuración.
2.	Inicie sesión en el servidor independiente donde se va a aplicar seguridad según criterios de ENS.
3.	Debe iniciar sesión con una cuenta que pertenezca al grupo de Administradores o Sudoers.
4.	Diríjase a la barra de tareas, pulse sobre “Aplicaciones” y en el apartado “Herramientas del sistema” seleccione “Terminal”. 
5.	Ejecute el comando **“cd /”** y pulse la tecla “Enter”.
6.	Se va a proceder a activar SELinux y configurarlo para que registre los eventos del sistema.

Paso	Descripción
7.	Edite el fichero de configuración "/etc/selinux/config" y modifique los siguientes parámetros: SELINUX=Enforcing, SELINUXTYPE=targeted. Pulse "Guardar", cierre el editor de textos y reinicie el sistema para que los cambios tengan efecto. **$ sudo gnome-text-editor /etc/selinux/config &>/dev/null**  **Nota:** Se comentan a continuación algunos parámetros del fichero de configuración: - SELINUX=enforcing La opción SELINUX pone el modo en el que inicia SELinux. SELinux tiene tres modos: obligatorio (enforcing), permisivo (permissive) y deshabilitado (disabled). Cuando se usa modo obligatorio, la política de SELinux es aplicada y SELinux deniega el acceso basándose en las reglas de políticas de SELinux. Los mensajes de denegación se guardan. Cuando se usa modo permisivo, la política de SELinux no es obediente. Los mensajes son guardados. SELinux no deniega el acceso, pero se guardan las denegaciones de acciones que hubieran sido denegadas si SELinux estuviera en modo obediente. Cuando se usa el modo deshabilitado, SELinux está deshabilitado (el módulo de SELinux no se registra con el kernel de Linux). - SELINUXTYPE=targeted La opción SELINUXTYPE selecciona la política a usar por SELinux. La política Destinada es la predeterminada. Cambie esta opción si quiere usar la política MLS. Para usar la política MLS, instale el paquete selinux-policy-mls; configure SELINUXTYPE=mls en /etc/selinux/config; y reinicie su sistema.

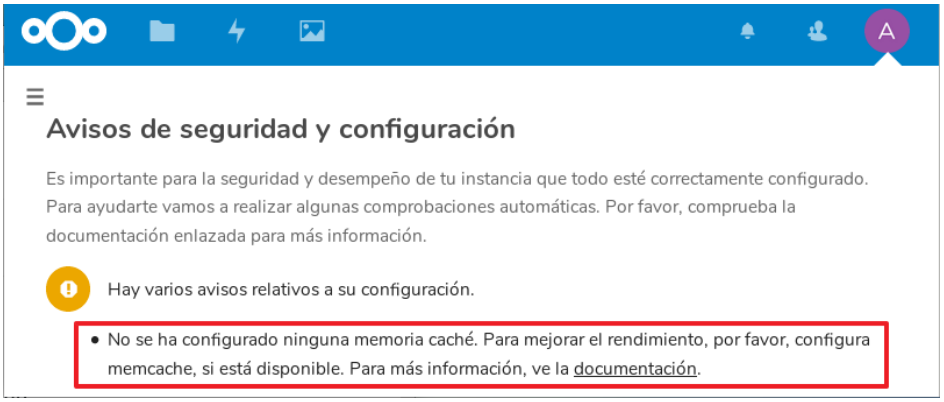
Paso	Descripción
8.	Para comprobar el estado de SELinux ejecute los siguientes comandos. Compruebe que SELinux se encuentre configurado como "**enforcing**", "**enabled**" y "**targeted**". En caso contrario repita los pasos anteriores. **$ sudo getenforce** **$ sudo sestatus** 
9.	Diríjase a la URL del servidor de Nextcloud. Posiblemente si no tiene aún configurados parámetros para SELinux, reciba un error. Si el error es por falta de permisos de SELinux, saltará un aviso de seguridad. 

Paso	Descripción
10.	Pulse en el aviso de seguridad para configurar los parámetros necesarios. Y en la ventana de “Alertas de SELinux” pulse en solucionar. 
11.	Se mostrarán varias soluciones para el mismo suceso, debiendo elegir la opción que más convenga a su organización. En este caso elegiremos la primera opción, permitiendo el permiso de lectura y escritura en “config.php” al demonio httpd (apache2). 
12.	Ejecute los comandos recomendados por SELinux para hacer efectivos los permisos. Si desea conocer más detalles sobre la acción que van a realizar los comando, pulse en el botón “Complemento Detalles”. 
13.	Deberá ejecutar los comandos recomendados por SELinux por cada una de las alertas que se vayan generando en el sistema. Para facilitar esta tarea se van a ejecutar varios comandos con las excepciones más comunes para SELinux en un servidor de alojamiento de archivos Nextcloud.

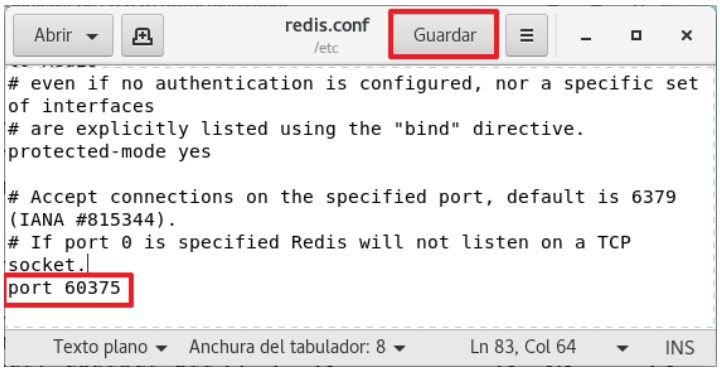
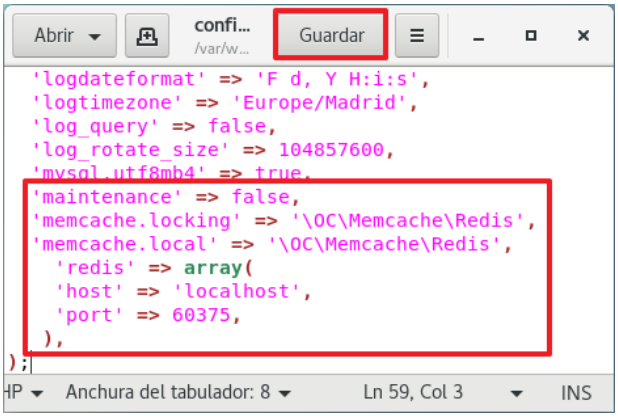
Paso	Descripción
14.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".
15.	Ejecute los comandos para permitir el acceso por SELinux a las rutas de su servidor Nextcloud. Modifique las partes remarcadas en color rojo si fuera necesario y ajuste los parámetros a los más convenientes para su organización. **$ sudo semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/data(/.*)?'** **$ sudo semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/config(/.*)?'** **$ sudo semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/apps(/.*)?'** **$ sudo semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/.htaccess'** **$ sudo semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/.user.ini'** **$ sudo semanage fcontext -a -t httpd_sys_rw_content_t '/var/www/html/nextcloud/3rdparty/aws/aws-sdk-php/src/data/logs(/.*)?'** **$ sudo restorecon -Rv '/var/www/html/nextcloud/'**
16.	Recargue la página de Nextcloud. Y Compruebe que ya tiene acceso a la misma.

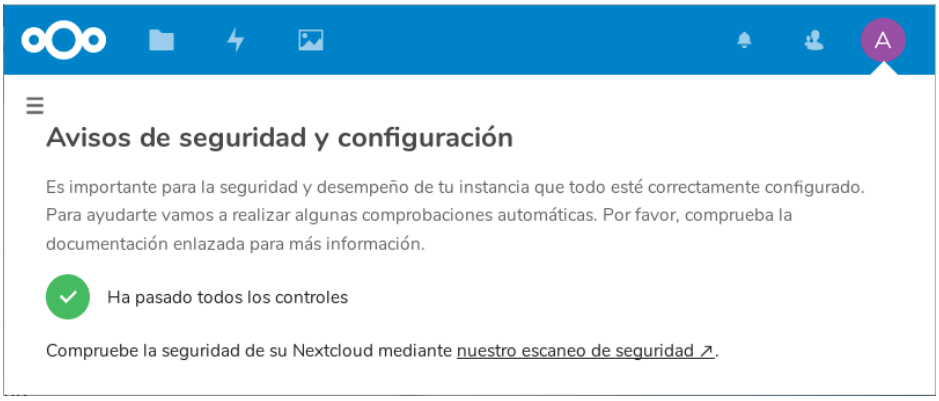
ANEXO A.6.2. REDIS CACHÉ

Paso	Descripción
1.	Si ha cerrado la "**Terminal** "en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Herramientas del sistema" seleccione "**Terminal**". Ejecute el comando **"cd /"** y pulse la tecla "Enter".

Paso	Descripción
2.	En este punto se va a configurar una memoria cache para mejorar el rendimiento del servidor de alojamiento de archivos Nextcloud.  **Nota:** Puede mejorar significativamente el rendimiento de su servidor Nextcloud con el almacenamiento en memoria caché, donde los objetos solicitados con frecuencia se almacenan en la memoria para una recuperación más rápida. Hay dos tipos de cachés para usar: un caché de código de operación de PHP, que comúnmente se denomina caché de datos, y el caché de datos para su servidor web. Si no instala y habilita un memcache local, verá una advertencia en su página de administración de Nextcloud. No se requiere un memcache y puede ignorar la advertencia si lo prefiere.
3.	Se comenzará instalando “redis” y su módulo correspondiente de php. Para ello ejecute el siguiente comando. Introduzca la contraseña si se le solicita. **$ sudo yum install -y redis php-pecl-redis**

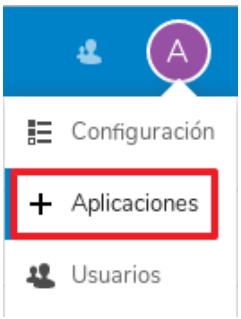
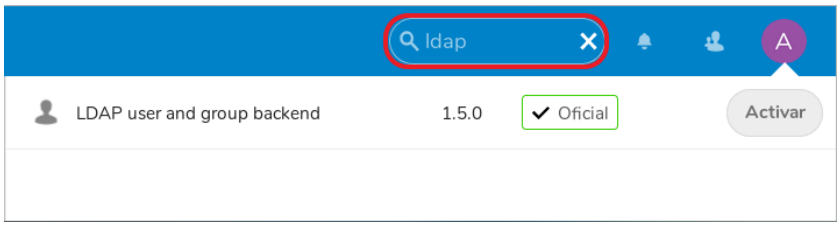
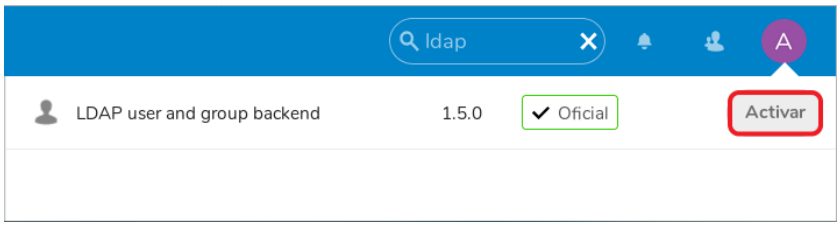
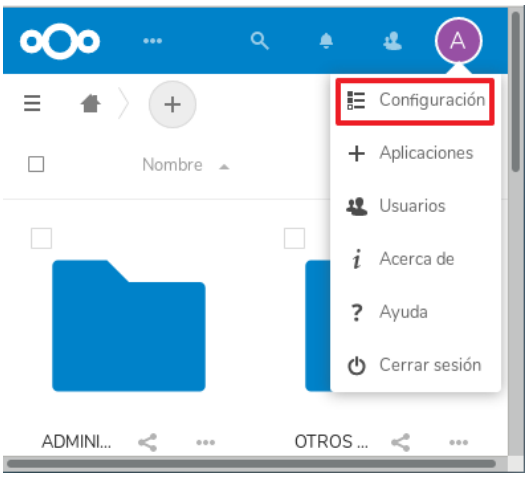
4.	Se va a inicial el servicio “redis” y comprobar que inicia sin errores. Para ello ejecute los siguientes comandos.
	$ sudo systemctl start redis.service
	$ sudo systemctl enable redis.service
	$ sudo systemctl status redis.service
	`[usuario@Nextcloud ~]$ sudo systemctl status redis.service`
	`● redis.service - Redis persistent key-value database`
	`Loaded: loaded (/usr/lib/systemd/system/redis.service; enabled; vendor preset: disabled)`
	`Drop-In: /etc/systemd/system/redis.service.d`
	`└─limit.conf`
	`Active: active (running) since [redacted]`
	`Main PID: 24254 (redis-server)`
	`CGroup: /system.slice/redis.service`
	`└─24254 /usr/bin/redis-server 127.0.0.1:6379`

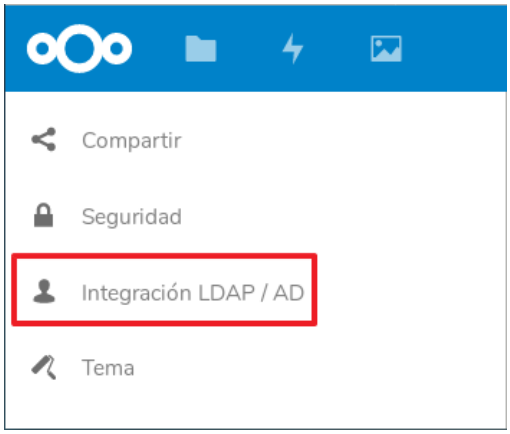
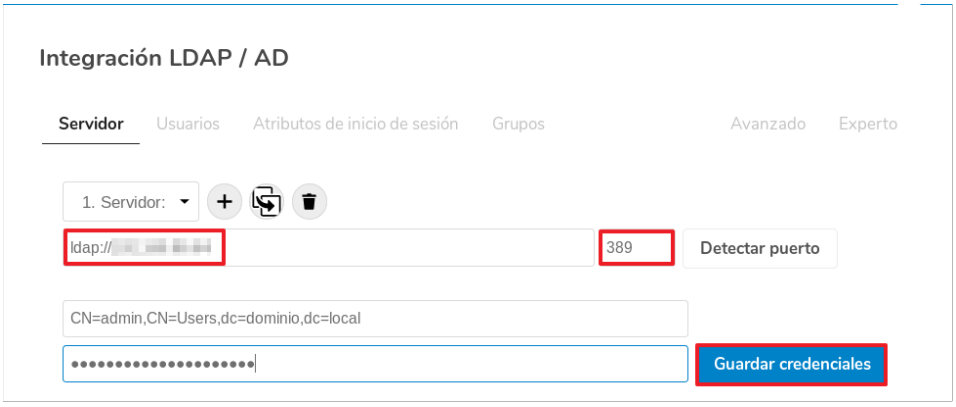
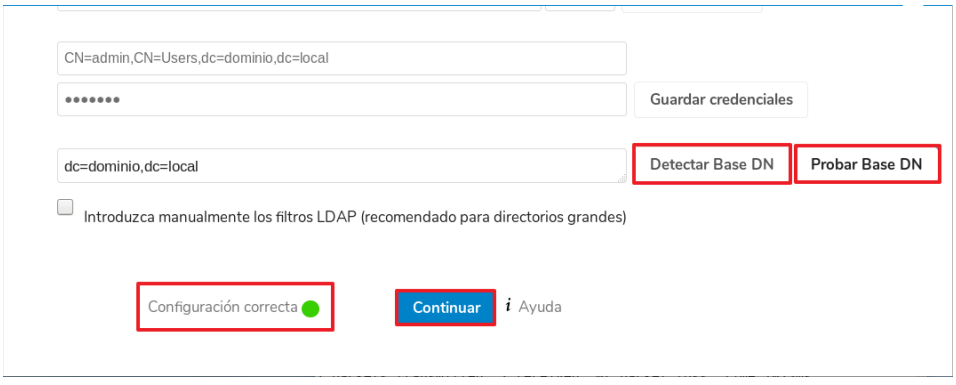
Paso	Descripción
5.	Edite el fichero de configuración de redis modificando el puerto por defecto. Para ello ejecute el siguiente comando y configure las opciones que más convengan en su organización. Cuando finalice pulse “Guardar”. **$ sudo gnome-text-editor /etc/redis.conf &>/dev/null** 
6.	Diríjase al directorio de su servidor de alojamiento de archivos Nextcloud, la ruta por defecto en esta guía es “/var/www/html/nextcloud”. Para ello escriba el siguiente comando, modificando la ruta si fuera necesario. **$ cd /var/www/html/nextcloud**
7.	Edite el fichero de configuración de PHP perteneciente al servidor Nextcloud, para ello ejecute el siguiente comando. **$ sudo gnome-text-editor config/config.php &>/dev/null**
8.	Añada las siguientes líneas al fichero de configuración y modifique acorde a las necesidades de su organización los datos que se remarcan en color rojo. Pulse “Guardar” cuando finalice. **'memcache.locking' => '\OC\Memcache\Redis',** **'memcache.local' => '\OC\Memcache\Redis',** **'redis' => array(** **'host' => 'localhost',** **'port' => 60375,** **),** 

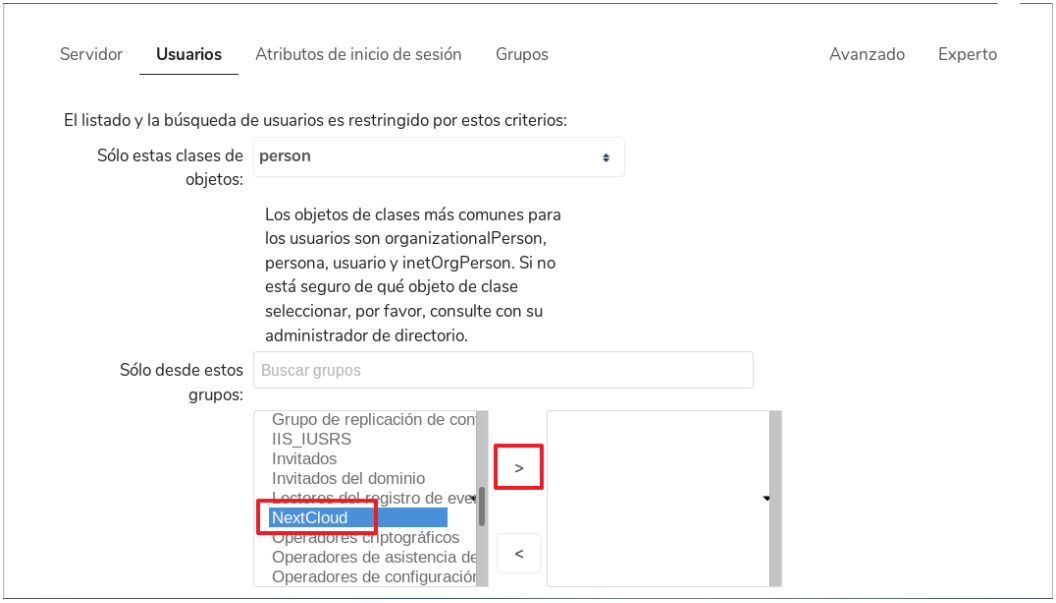
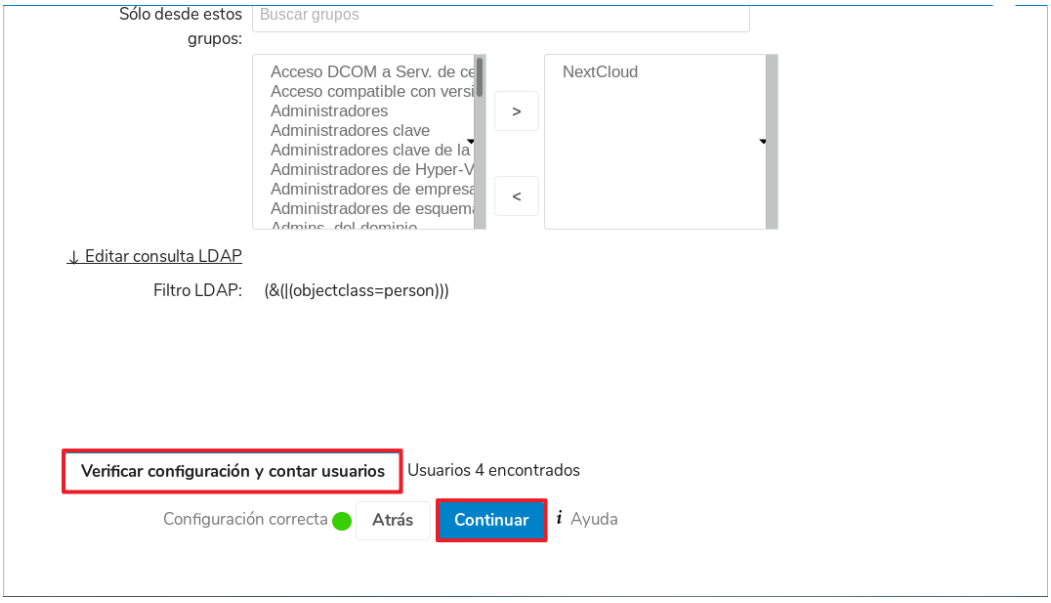
Paso	Descripción
9.	Reinicie los servicios de Apache y redis para que los cambios tengan efecto. Compruebe que reinician sin errores. **$ sudo systemctl restart redis.service** **$ sudo systemctl restart httpd.service**
10.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Internet" seleccione "**Firefox**" o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud. Inicie sesión con una cuenta de Administrador que pertenezca al grupo "admin".
11.	Vaya al icono de su usuario y en el menú desplegable pulse **"Configuración" → "Administración" → "Vista general"** y compruebe que se no existen avisos de seguridad sobre memoria cache. 

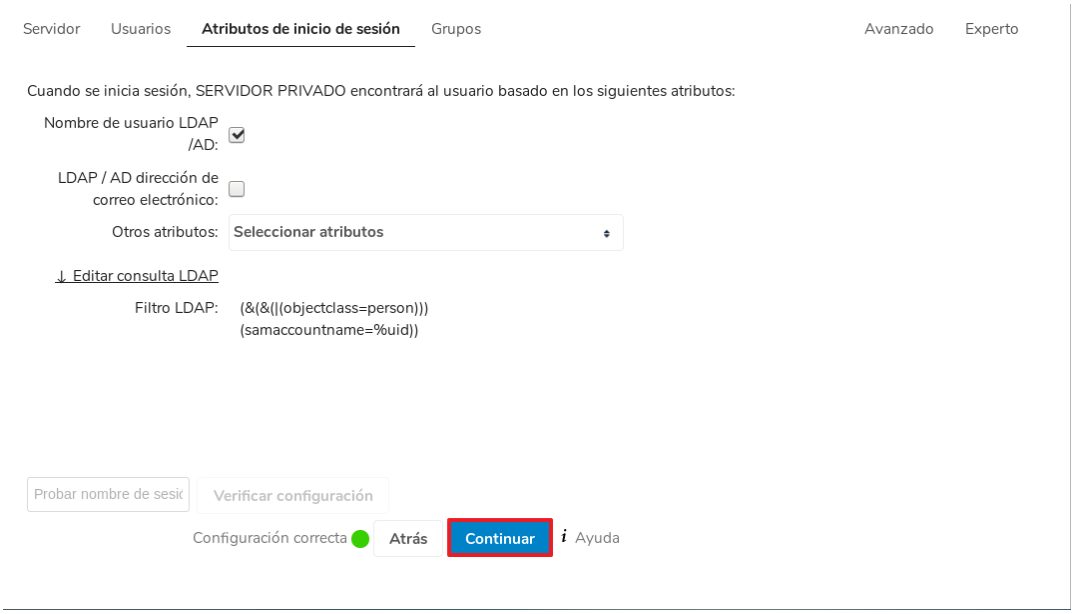
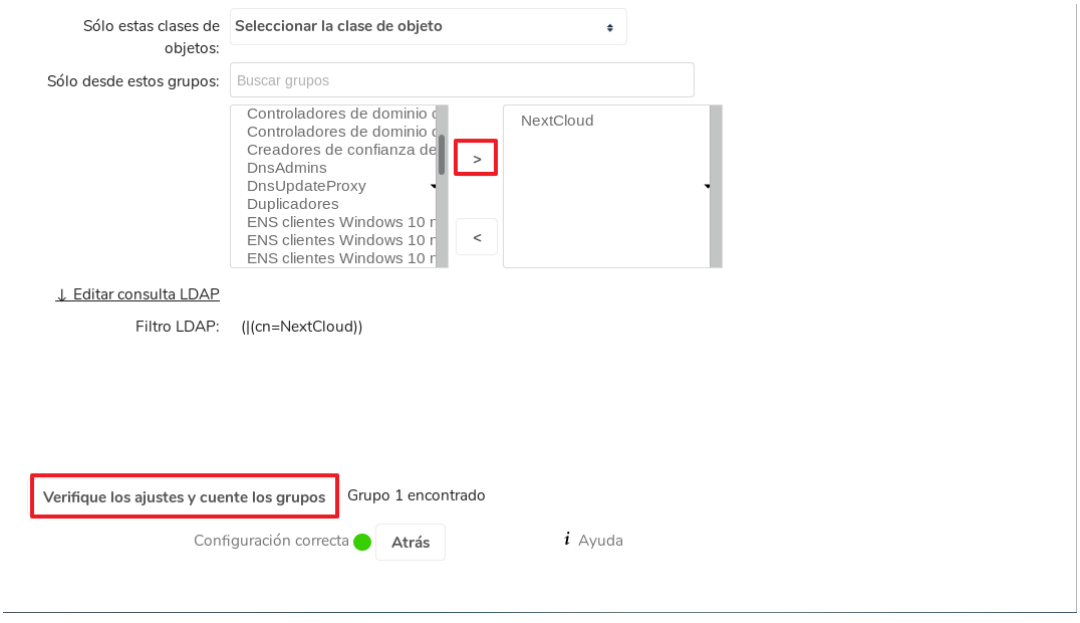
ANEXO A.6.3. INTEGRACIÓN DE USUARIOS CON LDAP

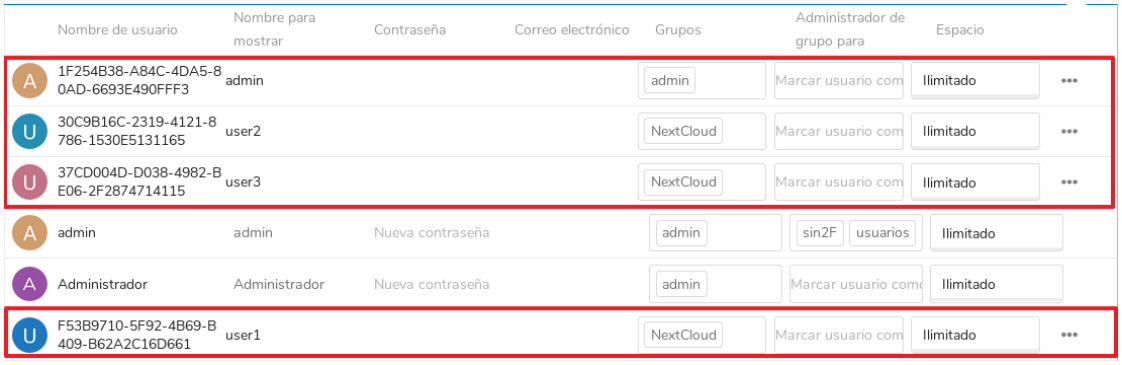
Paso	Descripción
1.	Se procede a configurar la integración de Nextcloud 15 con LDAP.
2.	Si ha cerrado el visor Web del servidor de alojamiento de archivos Nextcloud en algún paso anterior, diríjase a la barra de tareas, pulse sobre "Aplicaciones" y en el apartado "Internet" seleccione **"Firefox"** o su navegador predeterminado e ingrese la URL correspondiente a su servidor Nextcloud.
3.	Inicie sesión en el servidor de alojamiento de archivos Nextcloud donde se va a aplicar seguridad según criterios de ENS.
4.	Debe iniciar sesión con una cuenta Administrador que pertenezca al grupo de "admin".
5.	Para integrar usuarios por medio de LDAP, debe poseer el módulo correspondiente a LDAP de php. Para ello ejecute el siguiente comando. **$ sudo yum install -y php-ldap**
6.	Reinicie el servicio Apache para que detecte el módulo recién instalado. **$ sudo systemctl restart httpd.service**

Paso	Descripción
7.	Una vez instalado el módulo correspondiente deberá instalar la aplicación de Nextcloud para configurar usuarios LDAP en el servidor. Para ello diríjase al icono de su usuario y en el menú desplegable pulse “Aplicaciones”. 
8.	En el panel de navegación superior elija el icono de la lupa para buscar y escriba el siguiente texto: “ldap” 
9.	Pulse el botón “Activar” para continuar. 
10.	Diríjase al icono de su usuario y en el menú desplegable pulse “Configuración”. 

Paso	Descripción
11.	En la barra lateral izquierda en el apartado “Administración”, seleccione el icono “Integración LDAP /AD”. 
12.	En el título “Servidor” configure la dirección de su servidor y el puerto. Posteriormente introduzca las credenciales en el formato correcto y pulse en “Guardar credenciales”. 
13.	Pulse en Detectar Base DN y cuando la detecte, en Probar Base DN, deberá comunicarle que la configuración es correcta. Posteriormente pulse en el botón “Continuar”. 

Paso	Descripción
14.	En el título “Usuarios” en el apartado “objetos”, seleccione los parámetros específicos de su organización y en el apartado “grupos” seleccione los grupos requeridos, en este ejemplo se creó un grupo llamado “Nextcloud” y será el grupo seleccionado para añadir. 
15.	Una vez añadidos los grupos correspondientes, seleccione “Verificar configuración y contar usuarios”. Pulse “Continuar”.  **Nota:** Si al pulsar cualquier botón de verificación detecta que no surte ningún cambio, recargue la página web y vuelva a intentarlo. La configuración se mantendrá desde donde la dejó.

Paso	Descripción
16.	En el título “Atributos de inicio de sesión” seleccione las características que más convengan a su organización y pulse en “Continuar”. 
17.	En el título “Grupos” en el apartado “objetos”, seleccione los parámetros específicos de su organización y en el apartado “grupos” seleccione los grupos requeridos, en este ejemplo se creó un grupo llamado “Nextcloud” y será el grupo seleccionado para añadir. Pulse en “Verificar los ajustes y cuente los grupos”. 

Paso	Descripción
18.	Cuando se compruebe que la configuración está correcta no habrá nada más que hacer en cuanto a la configuración de la aplicación. 
19.	Diríjase al icono de su usuario y en el menú desplegable pulse “Usuarios”. Compruebe que se han añadido correctamente los usuarios de LDAP. 
20.	Cierre sesión con el usuario actual e inicie sesión con un usuario de Directorio Activo. Compruebe que puede ingresar sin problemas.