Universidad Nacional Autónoma de México

Facultad de Ingeniería

xNAS: Appliance de almacenamiento en red por medio de WebDAV

T E S I S

Para obtener el título de

Ingeniero en Computación

Presenta

Andrés Leonardo Hernández Bermúdez

Director de tesis

M.I. Tanya Itzel Arteaga Ricci

Ciudad Universitaria, Febrero 2016

Abstracto

Este trabajo presenta la implementación de un servidor de almacenamiento para la División de Ingenierías Civil y Geomática. Este equipo proporcionará un espacio para que los profesores puedan distribuir el material de sus cursos a los alumnos utilizando las herramientas nativas del sistema operativo.

El proyecto fue implementado en el sistema operativo Debian GNU/Linux utilizando SSH como mecanismo de acceso remoto para la administración del servidor, LDAP como sistema de autenticación para los usuarios, Apache HTTPD para brindar el servicio de HTTPS y el módulo de WebDAV para permitir la gestión de los archivos almacenados en el servidor.

Se reforzó la seguridad del servidor al establecer reglas de *firewall* y ajustar los parámetros de operación del sistema operativo para aplicar las actualizaciones de manera automática y además bloquear los ataques de diccionario. Tras las pruebas realizadas, se modificaron las opciones de `mod_ssl` para mitigar las vulnerabilidades presentes.

Agradecimientos

♥ Te agradezco a tí Yazmin por caminar la vida junto a mi, por apoyarme en todos mis proyectos y por causar siempre ese brillo especial en mis ojos.

✯ Agradezco a mis padres por darme la vida, los valores, la educación y por ser el ejemplo a seguir mostrándome siempre el camino correcto.

❀ A mis abuelos, porque ellos me mostraron que sin importar las condiciones adversas, siempre es posible salir adelante y superarse cada día.

❖ Doy gracias a mis hermanos por todo el apoyo y cariño que me han brindado siempre y por estar al pendiente de mi.

☞ A la Universidad por mi formación y todas las oportunidades que me ha dado para desarrollar mis habilidades haciendo el bien a la comunidad.

¡Lo logramos!

Muchas gracias a todos

— Andrés

Índice

Lista de tablas

Lista de figuras

Introducción

Objetivo

Implementar un servidor dedicado de almacenamiento que incluya las cuentas de usuario desde un directorio LDAP y que transmita la información por medio de WebDAV a través de un canal cifrado.

Estructura de la tesis

Capítulo 1

En el primer capítulo se da a conocer el funcionamiento y clasificación de los medios de almacenamiento que se utilizan en la actualidad, se enuncian los mecanismos de protección para los medios según su tipo y se describen las técnicas de respaldo que se utilizan para el almacenamiento en medios separados, respaldos en red y el uso de *Cloud Storage*.

Por último se aborda una comparativa de los arreglos RAID simples y compuestos, se lista su funcionamiento y se presenta un diagrama que muestra el flujo de los datos en cada tipo de arreglo.

Capítulo 2

En el segundo capítulo se define el problema y se plantea la solución utilizando un servicio de directorio para guardar a los usuarios, un servicio web que implementa el estándar WebDAV para acceder a los archivos y además se mencionan las interfaces para administrar el directorio de usuarios y para que los usuarios puedan cambiar su contraseña.

Capítulo 3

En el tercer capítulo se realiza la configuración de los servicios que forman parte de la solución a implementar, se realiza la configuración del directorio LDAP y se mencionan los mecanismos utilizados para cargar y borrar de forma masiva los usuarios en el directorio.

Se presenta también la configuración del servicio de HTTP con el módulo de WebDAV y la conexión a LDAP, así como la interfaz de administración *LDAP Account Manager* y la interfaz de cambio de contraseña *LDAP Toolbox*.

Por último se aplican las configuraciones de seguridad necesarias para restringir el acceso a la cuenta de administrador `root`, habilitar el envio de reportes de actividad inusual por correo electrónico, habilitar un perfil de reglas de *firewall* en el equipo y aplicar directivas de seguridad para el servicio HTTP.

Capítulo 4

En el cuarto capítulo se muestran las pruebas realizadas tomando como grupo de control los cursos intersemestrales que ofrece la *Unidad de Cómputo* donde se verificó la compatibilidad de la solución con diversas plataformas de escritorio como GNU/Linux, Mac OS X y Windows y sistemas operativos de móviles como Apple iOS y Android.

Capítulo 5

En el quinto capítulo se presentan las conclusiones y se listan los resultados obtenidos durante la implementación y pruebas de la solución propuesta, así como las oportunidades de mejora que puede tener el proyecto en futuras versiones.

Capítulo 1

Marco teórico

1.1. Sistemas de almacenamiento

Los medios de almacenamiento guardan los programas y los datos del usuario para que después puedan ser leídos, modificados o borrados. Los métodos de lectura y escritura dependen en gran medida del tipo de medio que se utilice. A continuación se hace una clasificación de los medios comunes de almacenamiento de acuerdo a su tipo.

1.1.1. Clasificación por tipo de medio

Medios basados en circuitos

Estos medios de almacenamiento son circuitos individuales o arreglos de circuitos que se utilizan para almacenar datos. La información guardada se lee haciendo referencia a la ubicación de memoria y el tamaño de los datos que se lee muchas veces es fijo. En la siguiente figura se muestran algunos de ellos.

- **RAM**

  Es un medio de almacenamiento volátil que se utiliza para guardar datos temporales o como memoria intermedia de un equipo de cómputo. Se compone de arreglos de circuitos y, comparada con cualquier otro medio, tiene una gran velocidad de lectura y escritura [1].

- **NVRAM**

  Es una variante de la memoria RAM donde se almacena la información de manera no volátil, generalmente su capacidad es pequeña y este tipo de memoria se utiliza para fines muy especializados, por ejemplo para guardar las configuraciones de algunos sistemas embebidos [2].

- **ROM**

  Es una memoria de sólo lectura que puede ser grabada una sola vez, generalmente se utilizaba para almacenar el firmware de dispositivos o algún programa embebido en *hardware* que requiere una salida fija para una entrada determinada [1].

- **EEPROM**

  Una variante de la memoria ROM donde el contenido puede ser borrado por varios métodos, ya sea eléctricamente o por medio de la exposición a rayos ultravioleta. En condiciones normales de operación su comportamiento es similar al de la memoria ROM y se debe entrar en un modo especial para grabar nuevos datos en la misma [3].

- **Flash**

  Una variante más de los medios de almacenamiento basados en circuitos es este tipo de memoria que se ha hecho popular en los últimos años gracias a que no depende de partes móviles y es pequeña, por lo que es un medio de almacenamiento portátil y eficiente [4].

- **SSD**

  Un medio de almacenamiento relativamente reciente, utiliza arreglos de circuitos para guardar la información, generalmente se utiliza memoria tipo NAND para mantener los datos y a diferencia de los discos duros no tiene partes móviles por lo que es menos propensa a fallos y disipa menos calor [5].

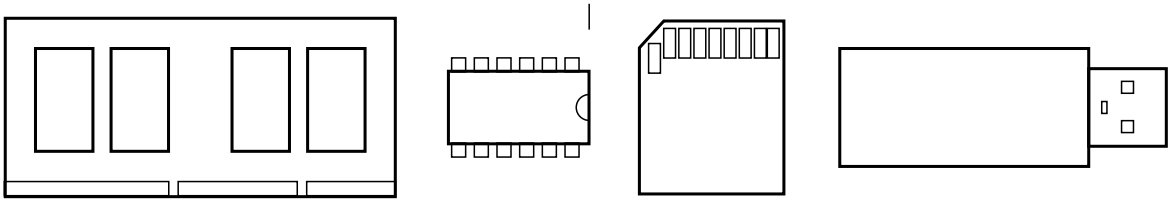


Figura 1.1: Medios de almacenamiento basados en circuitos

Medios magnéticos

Este tipo de medios se caracterizan porque el acceso a los datos se realiza mediante un cabezal que lee o escribe el campo magnético impreso en el material que lo guarda. Son susceptibles a fallar si se exponen a campos magnéticos, golpes o temperaturas extremas. La siguiente figura ilustra la forma que tienen los discos flexibles, discos duros y cintas de almacenamiento.

- **Discos flexibles**

  En este tipo de discos se puede acceder de manera aleatoria a los datos almacenados, tienen un plato magnético rodeado de un material protector que viene contenido en un armazón de plástico y cuenta con con una abertura que permite a la cabeza lectora tener acceso al medio [6].

  Los discos flexibles almacenan los datos dividiendo el plato en círculos concéntricos denominados pistas, que a su vez se subdividen en arcos llamados sectores, de esta manera se puede localizar la información conociendo la pista y el sector donde se encuentra [7]. Su capacidad oscila entre los cientos de KB hasta llegar a 1.44 MB.[1]

- **Discos duros**

  Similar al disco flexible, el disco duro tiene una estructura formada por varios platos, cada uno leído por una cabeza diferente. De manera lógica, el espacio se organiza en círculos concéntricos (cilindros), platos (cabezas) y arcos (sectores), en modelos modernos se utiliza *Logical Block Addressing* para asignar el espacio [8].

  Parecidos a los discos flexibles, estos medios tienen mayor capacidad y actualmente son el medio primordial para almacenar información en los equipos de cómputo. A diferencia de los discos flexibles, tienen los componentes mecánicos dentro del armazón del disco y pueden almacenar grandes cantidades de información gracias a que se apilan varios discos en una estructura cilíndrica.

- **Cintas**

  Las unidades de cinta son medios que almacenan de manera secuencial los datos, dentro de sus componentes internos destacan dos carretes que sirven para almacenar la cinta mientras se lee, para acceder datos en una posición anterior es necesario rebobinar la cinta.

  Generalmente tienen capacidades que oscilan entre los GB y TB [9] y son utilizadas para archivar información.

[1] Existieron otros formatos como *ZIP* de Iomega, *SuperDisk* LS120 de Imation o *HiFD* de Sony.

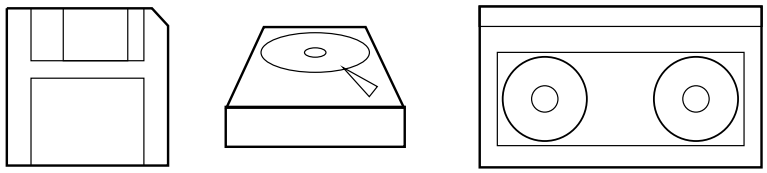


Figura 1.2: Medios de almacenamiento magnéticos

Medios magneto-ópticos

- **Discos MO (Magneto-optic)**

  Los discos magneto-ópticos tienen las bondades de la rapidez de los discos magnéticos y la versatilidad de los discos ópticos.

  Para escribir los datos se calienta la superficie del disco y se aplica un campo magnético para que queden registrados (véase siguiente figura). Al leer los datos el láser reconoce la polaridad y esta se interpreta como cero o uno para la parte del disco que esté leyendo [7].

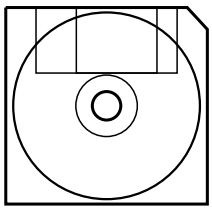


Figura 1.3: Disco magneto-óptico

Medios ópticos

- **Discos de sólo lectura (WORM)**

  Los discos pre-masterizados (CD-ROM, DVD-ROM, BD-ROM) se graban en las fábricas donde se tiene un disco maestro que sirve para transferir los datos al medio final por un proceso de vaciado térmico.

  Los discos grabables (CD-R, DVD+R, DVD-R y BD-R) pueden ser escritos mediante un láser al fundir una capa de policarbonato en la superficie inferior del disco para ingresar los bits (véase figura siguiente). El formato de los bits generalmente va de acuerdo al estándar ISO-9660 [10].

- **Discos regrabables**

  Los discos regrabables (CD-RW, DVD+RW, DVD-RW, BD-RE) tienen una ventaja adicional comparados con los discos grabables de una sola vez, gracias a que es posible borrar la información contenida para almacenar nuevos datos en el medio. Esto se logra al inicializar parcial o totalmente los sectores del disco para que este pueda admitir nuevos datos [11].

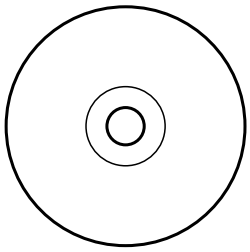


Figura 1.4: Disco óptico

Medios holográficos

- **HVD - Disco Versátil Holográfico**

  Es un nuevo medio de almacenamiento aún en desarrollo que ofrece un método más versátil de escribir los datos, utiliza un mecanismo holográfico donde la información que se obtiene depende de la manera en la que se leen los datos es [12].

1.1.2. Comparativa de medios de almacenamiento actuales

Tabla 1.1: Comparativa de medios de almacenamiento

Medio	Capacidad	Persistencia	Acceso aleatorio	Lectura y escritura	Vulnerabilidades
RAM	MB	✘	✔	✔	Electricidad estática
NVRAM	MB	✔	✔	✔	
ROM	MB	✔	✔	✘	
EEPROM	MB	✔	✔	✘	
Flash / SSD	GB	✔	✔	✔	
Cinta	TB	✔	✘	✔	Campos magnéticos
Disco flexible	MB	✔	✔	✔	
Disco duro	TB	✔	✔	✔	
Disco MO	MB/GB	✔	✔	✔	Campos magnéticos Rayaduras
Disco óptico	MB/GB	✔	✔	✘	Rayaduras
Disco regrabable	MB/GB	✔	✔	✔	
Disco holográfico	GB	✔	✔	✔	

1.1.3. Escenarios de falla

A continuación se presentan dos de las causas más comunes que ocasionan el funcionamiento incorrecto de un medio de almacenamiento:

- **Daño físico del medio**

  Si el medio de almacenamiento presenta daño físico, los datos almacenados pueden aparecer incompletos o ilegibles.

- **Fallo de componentes internos**

  Dependiendo del tipo de medio, la falla de componentes internos puede ser fatal. Por ejemplo, si se tiene un disco óptico y falla el lector de discos, basta con reemplazar la unidad para que el disco pueda ser leído sin problemas, en cambio si falla el cabezal de un disco duro, será necesario un proceso más complicado y costoso para recuperar la información contenida.

1.1.4. Métodos de protección

Los métodos de protección de los medios de almacenamiento varian dependiendo de su tipo, en la tabla 1.1 se muestra una comparativa de los medios y los elementos que pueden dañarlos.

- **Seguro contra escritura**

  El seguro contra escritura previene que los datos sean modificados puesto que el medio se reconoce como de sólo lectura y no es posible escribir en él. Este método es útil cuando se archivan o respaldan datos porque se busca que estos no sean modificados.

- **Protección antiestática y contra campos magnéticos**

  Para evitar el daño por una descarga de electricidad estática o por la presencia de campos magnéticos en los medios de almacenamiento como cintas o discos duros, existen bolsas que evitan que el disco reciba una descarga y cubiertas especiales para salvaguardar el disco de los campos magnéticos.

- **Protección contra daño físico**

  El daño físico se puede prevenir si se maneja el medio de almacenamiento con precaución y se guarda en un lugar fresco y seco que no tenga exposición directa a la luz solar y que esté fuera del alcance de campos magnéticos.

1.1.5. Técnicas de respaldo

En un entorno de hogar u oficina pequeña (SOHO) el número de usuarios es reducido y gradualmente se busca la manera de tener un almacenamiento centralizado. Para resolver este problema, existen varias técnicas que han aparecido a lo largo de los años:

- Grabar la información a discos ópticos como CD y DVD.
- Utilizar discos duros o unidades removibles como medio de respaldo.
- Compartir directorios a través de la red para acceder archivos almacenados en equipos remotos.
- Utilizar dispositivos de bloque compartidos en red (NBD o SAN) para tener acceso a sistemas de archivos remotos.
- Hacer uso de los servicios de almacenamiento en la nube (*cloud storage*) para guardar los archivos en un sitio remoto y acceder a ellos a través de Internet.

- **Respaldo en medios ópticos**

  Guardar información en discos ópticos deja la copia como sólo lectura y aunque sea ideal para respaldos completos o archivado de datos, no es recomendable para guardar datos que van a cambiar porque cada vez que se escriba al disco óptico se guardará una nueva copia del documento en lugar de reemplazar la existente.

- **Respaldo en medios magnéticos y unidades portátiles**

  Desde la masificación de los discos duros externos y las unidades portátiles, estos se han adoptado como medio de almacenamiento para los datos que cambian frecuentemente. Gracias a que dichos medios generalmente son de lectura y escritura, las modificaciones de los archivos pueden guardarse reemplazando la copia original y si un archivo es borrado se recupera el espacio en disco.

  Una desventaja del uso de este tipo de medios radica en que se puede editar tanto la copia local en la computadora como el archivo de respaldo produciendo diferentes versiones y el usuario tendrá que decidir cual versión del archivo es la la más actualizada.

- **Recursos compartidos por red**

  Cuando se cuenta con una red de computadoras se puede utilizar otro mecanismo para almacenar datos en equipos remotos por medio de recursos compartidos en red. Dependiendo de la configuración se pueden asignar permisos de sólo lectura o lectura-escritura.

  A diferencia del método de respaldo anterior, se tiene una sola copia de la información por lo que no existe posibilidad de encontrar una versión desactualizada de los datos. La gran desventaja de los recursos compartidos entre varios equipos es que los datos no se pueden acceder cuando el equipo que los almacena se encuentra apagado o con intermitencias de conectividad. Esta solución funciona mejor cuando los equipos que comparten los recursos están encendidos la mayoría del tiempo.

  Los protocolos que comúnmente se utilizan para compartir recursos a través de la red son NFS y CIFS (SMB), siendo el primero el protocolo más utilizado en sistemas tipo UNIX y el segundo mayormente en sistemas Windows, aunque se puede utilizar también en sistemas UNIX a través de la suite de herramientas de *Samba* [13].

- **Dispositivos de bloque compartidos por red**

  Otra solución popular en sistemas UNIX es compartir dispositivos de bloque a través de la red para acceder a discos remotos como si fuesen locales, ejemplos de esto son NBD (*Network Block Device*) en GNU/Linux y tecnologías SAN como iSCSI (*Internet SCSI*) o AoE (*ATA over Ethernet*). Este tipo de soluciones llegan a ser costosas y no se adaptan bien a ambientes como empresas pequeñas u hogares.

- **Servicios de almacenamiento en la nube (*cloud storage*)**

  En los últimos años los servicios de almacenamiento en la nube han ganado popularidad por ser servicios administrados que no requieren mucha configuración por parte del usuario. Algunos de estos servicios ofrecen una unidad virtual que se monta en el equipo local para acceder al contenido y agregar o modificar los archivos del usuario, mientras que otros sincronizan los archivos locales con el servidor remoto a través de un programa que funge como intermediario.

  Nube pública
  Los servicios de almacenamiento remotos en Internet son denominados *almacenamiento de nube pública*. Son útiles cuando la velocidad de la conexión se ajusta a la demanda de los usuarios. Dado que los archivos residen en otro lugar, es necesario descargar y subir grandes cantidades de datos al servicio de almacenamiento remoto. Si la conexión a Internet no es lo suficientemente rápida, la experiencia del usuario se ve afectada.

  Comúnmente este tipo de servicios ofrece menos de 1TB de almacenamiento y al subir o descargar archivos de gran tamaño la copia es muy lenta.

  Nube privada
  Cuando el servicio de almacenamiento se encuentra en la red local se puede aprovechar de mejor manera gracias a que la velocidad de transmisión es más rápida que entre redes separadas. Además el servicio no está disponible para clientes de otras redes por este motivo se denomina *privada*. En este caso los usuarios tienen una mejor experiencia al utilizar el servicio y los datos se quedan resguardados en un equipo dentro de la organización.

  En este tipo de soluciones se pueden tener grandes volúmenes de datos disponibles para los usuarios, aprovechando así la rapidez de la red local para manipular archivos de gran tamaño.

1.1.6. Arreglos RAID

El término RAID es un acrónimo de *Redundant Array of Independent Disks* (Arreglo Redundante de Discos Independientes)[2] [14]. Es una tecnología que se basa en combinar múltiples discos para que se comporten como uno solo. Dependiendo el modo de operación, ofrece la posibilidad de tomar varios discos y sumar el espacio de almacenamiento o bien replicar los datos escribiéndolos en varios discos para tener tolerancia a fallos [15].

Los arreglos de disco se pueden configurar por tarjetas dedicadas de *hardware* o mediante configuración de *software* en el sistema operativo. En los *arreglos por hardware*, el *firmware* de la tarjeta controladora tiene los algoritmos encargados de leer, escribir y sincronizar los datos, mientras que en los *arreglos por software* el *kernel* del sistema operativo es el encargado de realizar estas operaciones [16].

Tipos de arreglo RAID

A continuación se muestra la descripción de los tipos de arreglo RAID que se pueden implementar tanto en *hardware* y en *software* con las tarjetas controladoras actuales. [3]

- **Linear**

  En esta variante se combinan dos o más discos como si fueran uno solo al *concatenar* el espacio y sólo se escribirá al disco 1 si el disco 0 se encuentra completamente lleno (ver figura).

  Para crear el arreglo no importa el tamaño de los discos. Si se accede a dos archivos que están almacenados en diferentes discos el rendimiento aumenta porque la lectura se realiza en paralelo.

  Este método no ofrece redundancia, por lo que si falla un disco los datos contenidos en este se pierden. Es posible montar el sistema de archivos en un modo especial y recuperar los datos almacenados en los demás discos.

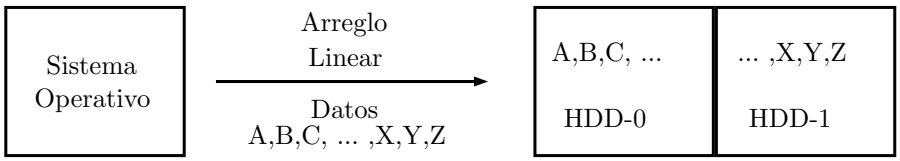


Figura 1.5: Diagrama de funcionamiento del arreglo *Linear*

[2]Dependiendo de la bibliografía el término puede ser también referido como *Redundant Array of Inexpensive Disks* (Arreglo Redundante de Discos Baratos).

[3]Los tipos 2, 3 y 4 de RAID no son comunes y generalmente no son soportados.

- **RAID 0 - *Stripe***

  También llamado *Stripe*, organiza los datos en bloques que se reparten copiando un bloque a cada disco (ver figura).

  Aunque es posible crear el arreglo con discos de diferente tamaño, se recomienda que sean por lo menos dos discos de la misma capacidad. Gracias a la organización de los datos, estos se acceden en paralelo aumentando la velocidad de lectura y escritura.

  No ofrece redundancia porque los bloques se reparten en todos los discos y si uno falla se perderán partes de todos los archivos, haciendo que el contenido no tenga coherencia.

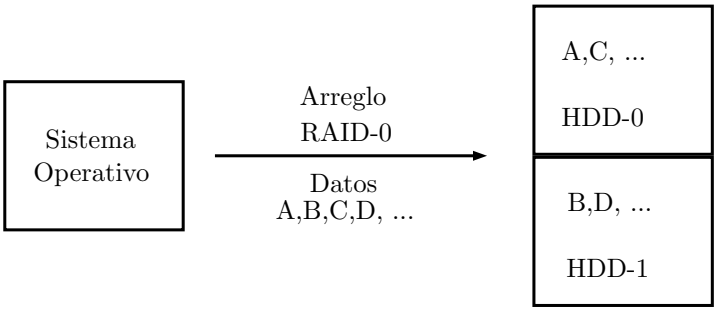


Figura 1.6: Diagrama de funcionamiento del arreglo RAID-0

- **RAID 1 - *Mirror***

  Denominado *Mirror*, guarda una copia exacta de los datos en ambos discos (ver figura). Se requiere un mínimo de dos discos de igual tamaño para hacer este arreglo, si los discos son de diferente capacidad, el espacio del arreglo será el del disco más pequeño.

  Este tipo de arreglo es tolerante a fallos siempre y cuando un solo disco siga funcionando, puesto que contiene una copia exacta de los datos contenidos en los demás medios.

  El rendimiento de escritura es menor al que presenta un solo disco debido a que se deben hacer copias exactas de la información en todos los discos pertenecientes al arreglo.

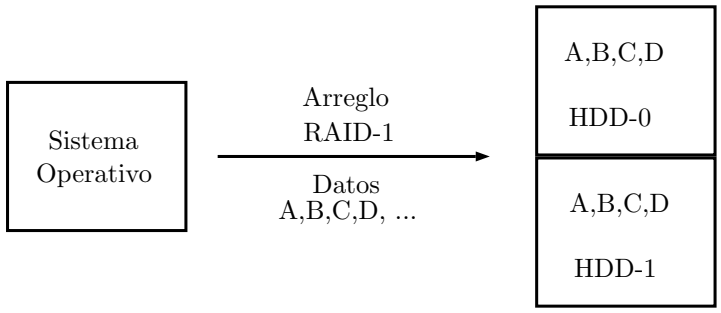


Figura 1.7: Diagrama de funcionamiento del arreglo RAID-1

- **RAID 5 - *Stripe with distributed parity***

  En este tipo de arreglo se dividen los datos en bloques de manera similar a RAID 0 y además se calcula un bloque de paridad que sirve para reconstruir los datos si uno de los discos falla (ver figura).

  Esta configuración de RAID tiene tolerancia a fallos siempre y cuando no falle más de un disco en el arreglo. Se requieren por lo menos tres discos para configurar un arreglo de este tipo.

  Dado que se calcula la paridad de los bloques de datos, se debe restar el tamaño de un disco para obtener el espacio máximo utilizable.

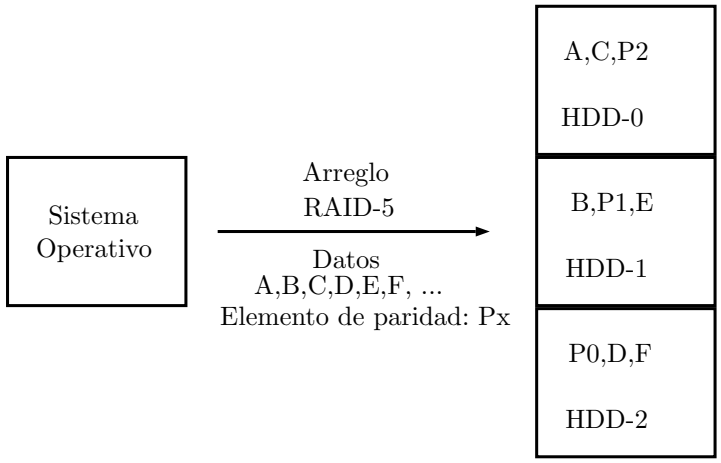


Figura 1.8: Diagrama de funcionamiento del arreglo RAID-5

- **RAID 6 - *Stripe with dual distributed parity***

  Su funcionamiento es similar al de RAID 5 sólo que se calculan dos bloques de paridad para cada bloque de datos (ver figura).

  Esta configuración de arreglo puede tolerar el fallo de hasta dos discos duros, mismos que se reconstruyen utilizando los bloques de paridad. Se requieren al menos cuatro discos para hacer un arreglo RAID 6.

  Las operaciones de escritura tardan más porque se deben calcular dos bloques de paridad, mientras que las operaciones de lectura no se ven afectadas.

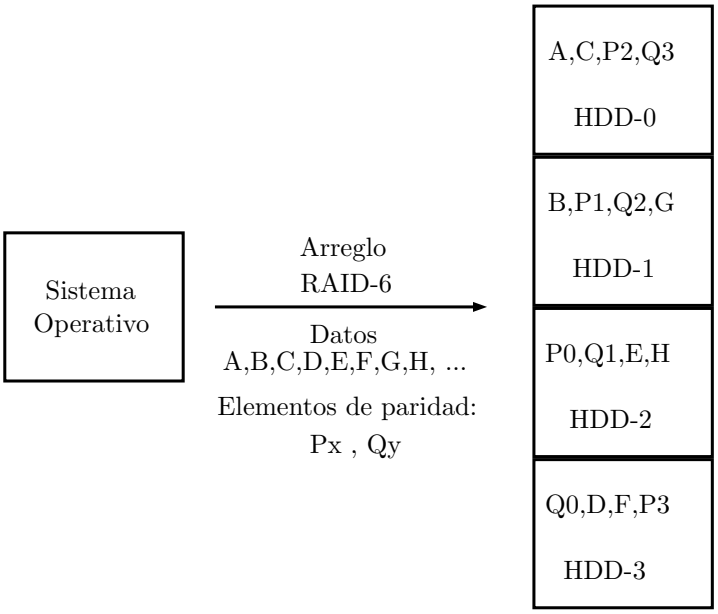


Figura 1.9: Diagrama de funcionamiento del arreglo RAID-6

Arreglos RAID anidados

- **RAID 01 / RAID 0+1**

  Se compone por un arreglo RAID 1 (*Mirror*) que replica los datos contenidos en dos arreglos RAID 0 (*Stripe*). Se requiere un mínimo de cuatro discos para hacer esta configuración (ver figura).

  Si fallan uno o dos discos del mismo arreglo RAID 0, el arreglo RAID 1 entra en modo degradado sin perder los datos. Si además falla un disco de otro arreglo RAID 0, entonces todos los datos se pierden.

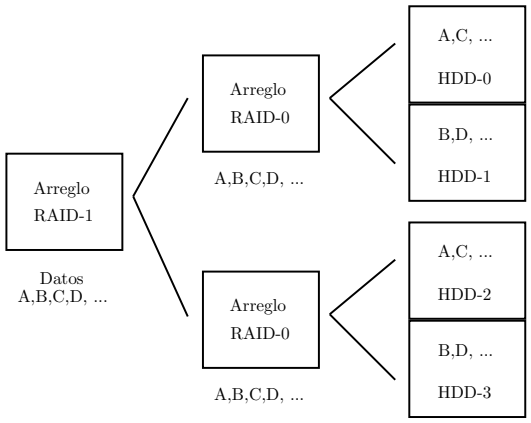


Figura 1.10: Diagrama de funcionamiento del arreglo RAID-01

- **RAID 10 / RAID 1+0**

  Consiste en un arreglo RAID 0 *Stripe* conformado por dos o más arreglos RAID 1 *Mirror*. El sistema operativo detecta la presencia de un solo disco mientras que este se conforma por un arreglo RAID 0 *Stripe* que une los dos arreglos RAID 1 *Mirror* (ver figura).

  Si un disco de algún arreglo RAID 1 falla, este entra en modo degradado y el funcionamiento del arreglo RAID 0 no se ve afectado. [4] Si fallan dos discos del mismo arreglo RAID 1, entonces el arreglo RAID 0 pierde los datos. Se requieren por lo menos cuatro discos para hacer esta configuración.

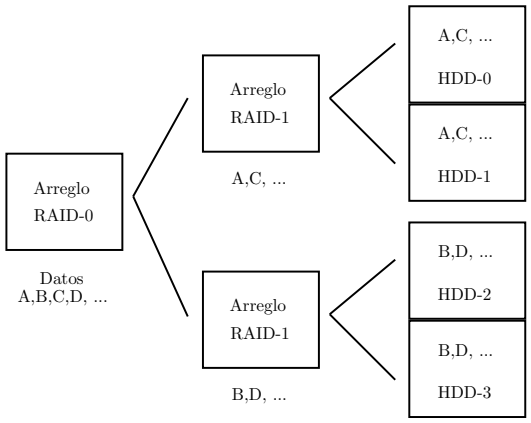


Figura 1.11: Diagrama de funcionamiento del arreglo RAID-10

[4] Salvo por la perdida de rendimiento en el arreglo.

1.1.7. Comparativa de tipos de arreglo RAID

Tabla 1.2: Comparativa de arreglos RAID

Tipo	Redundancia	Paridad	Discos	Capacidad útil	Ventajas
Linear	✘	✘	2+	Todos los discos	Se escribe en el disco *n* cuando *n-1* se llena
RAID 0	✘	✘	2+	Todos los discos	Los bloques se escriben en paralelo en los discos
RAID 1	✔	✘	2+	1 disco	Se tiene una copia exacta de los datos en los discos
RAID 5	✔	✔$_{\text{simple}}$	3+	2 discos	Tolera el fallo de un solo disco del arreglo
RAID 6	✔	✔$_{\text{doble}}$	4+	2 discos	Tolera el fallo de hasta dos discos del arreglo
RAID 01	✔	✘	4+	2 discos	Tolera el fallo de arreglos completos
RAID 10	✔	✘	4+	2 discos	Tolera el fallo de discos de diferentes arreglos

1.2. *Appliances*

Un *appliance* es un conjunto de elementos (*hardware*, *software* y sistema operativo) que trabajan de manera conjunta para realizar un proceso específico [17].

1.2.1. Tipos de *appliance*

- **Hardware**

  Los *appliances* de hardware son sistemas especializados diseñados para realizar tareas específicas. El fabricante los distribuye en servidores independientes y para agregar funcionalidades o aumentar la capacidad puede ser necesario comprar una licencia adicional o incluso comprar un nuevo equipo que realice esta función.

  Regularmente tienen una interfaz web para administración, algunos integran un *shell* para realizar las funciones conectándose a través de SSH y en otros casos integran soporte para SNMP.

- **Software**

  Los *appliances* de *software* pueden ser distribuidos en paquetes descomprimibles (*tarball*) que contienen el instalador y todos los programas necesarios para que funcione la solución [18].

  Integran sólo la interfaz web, puesto que se ejecutan en un equipo existente y son independientes del *shell* o del soporte SNMP que se tenga en el equipo.

- **Virtual**

  Este tipo de *appliances* son imágenes de máquinas virtuales diseñadas para un ambiente específico de virtualización e integran la funcionalidad de los *appliances* de *hardware*. Para aumentar la capacidad de este tipo de equipos se pueden instalar más instancias de la máquina virtual para procesar en paralelo las peticiones de los usuarios [19].

1.3. Seguridad informática

La seguridad informática se refiere a los procesos y metodologías diseñados e implementados para proteger información sin importar que esté en medios impresos, electrónicos o de otro tipo, esta puede ser confidencial, privada o sensible y se debe proteger de accesos no autorizados, mal uso, revelación, destrucción o modificación [20].

1.3.1. Principios de seguridad informática

- **Confidencialidad**

  Este principio busca conservar los datos únicamente para la persona que está destinada a leerlos [21][22].

  Por ejemplo, al cifrar un archivo se garantiza que sólo será visto por la persona que tenga los medios para descifrarlo (ya sea una llave privada o una contraseña).

- **Integridad**

  Este principio busca que la información no pueda ser alterada, ya sea por fallos en el medio de almacenamiento o modificaciones no autorizadas [21][22].

  Por ejemplo, al firmar digitalmente un archivo la firma sólo pasará la prueba de verificación si el mensaje está íntegro, de lo contrario no podrá ser verificado satisfactoriamente.

- **Disponibilidad**

  Este principio dicta que la información debe poder accederse cuando sea necesario o respetando el criterio de los tiempos establecidos [21][22].

  Por ejemplo, un recurso en línea debe estar disponible siempre para que pueda ser accedido por las personas que harán uso de él. En caso de tener horarios de disponibilidad, se debe garantizar que el recurso sea accesible durante ese periodo de tiempo.

1.3.2. Criptografía

El término criptografía proviene de las raíces griegas *kryptos* (oculto) y *grafe* (escritura). Es un conjunto de técnicas utilizadas para *ocultar* (cifrar) el contenido de un mensaje, mismo que solo podrá ser descifrado y leído por la persona a la que va destinado[23].

La criptografía moderna se basa en el uso de las matemáticas para ocultar la información y de los sistemas digitales para realizar la transmisión de la misma [24]. Existen dos tipos de algoritmos que se utilizan para cifrar los mensajes que serán transmitidos a través de un canal inseguro:

1.3.2.1. Algoritmos simétricos

La principal característica de estos algoritmos radica en utilizar la misma llave para cifrar y descifrar el mensaje. Para que la protección de la información sea adecuada, se debe realizar previamente el intercambio de la llave a través de un medio seguro (ej. entregar la llave secreta en persona) y una vez que las dos partes tengan la clave secreta, pueden intercambiar mensajes cifrados.

- **DES y Triple-DES**

  El algoritmo llamado *Data Encription Standard* o DES, se basa en *Lucifer* creado por Horst Feistel. Cifra el mensaje en bloques de 64 bits y la longitud de la llave utilizada es de 56 bits. Utiliza permutaciones, substituciones y aplica la función binaria `XOR` a los datos[23][25].

  Tras el descubrimiento de vulnerabilidades en el algoritmo DES, en 1998 la EFF[5] publicó en Internet la especificación de una máquina capaz de romper el cifrado de este algoritmo[23][26]. La solución interina que fue adoptada consiste en realizar el cifrado DES *tres veces*, es decir, cifrar el mensaje con *Triple-DES*.

[5] *Electronic Frontier Foundation* por sus siglas en inglés.

- **AES**

  Es el algoritmo de cifrado sucesor de DES, se basa en *Rijndael* creado por Joan Daemen y Vincent Rijmen. Tiene una longitud variable de llave que puede ser de 128, 192 o 256 bits y realiza el cifrado en bloques de 128 bits [25][27].

  Gracias a sus características, este algoritmo puede ser utilizado en procesadores de 8 bits como los que se utilizan en los dispositivos *SmartCard*, 16 bits comúnmente utilizados en microcontroladores y además en computadoras de escritorio de 32 y 64 bits.

  Para realizar de manera más rápida el proceso criptográfico, se han incluido instrucciones específicas de AES en algunos modelos de procesadores[28] e incluso se pueden programar las tarjetas gráficas GPU para acelerar el proceso de cifrado y descifrado[29].

1.3.2.2. Algoritmos asimétricos

La criptografía de llave pública se basa en la idea de que cada entidad involucrada tenga un par de llaves que estén matemáticamente relacionadas[30].

Se utiliza la llave pública de una persona para cifrar el mensaje, mismo que se envía a través de un canal inseguro y al llegar al otro extremo el destinatario hace uso de su llave privada para descifrar el mensaje y acceder a la información contenida[31].

- **RSA**

  Creado por Ron **R**ivest, Adi **S**hamir y Leonard **A**dleman, el algoritmo RSA puede ser utilizado para cifrado de mensajes y además puede realizar operaciones de firma digital. Utiliza operaciones de módulo y exponente de números primos de gran tamaño[30][32].

- **Curvas elípticas**

  También denominado ECC[6], utiliza operaciones entre un número primo y una ecuación de curva elíptica dentro de un *campo finito*[33].

  Una de sus ventajas primordiales radica en que el tamaño de las llaves criptográficas se ve reducido, por ejemplo, una llave simétrica de 128 bits es comparable a una llave asimétrica de 3072 bits, mientras que en curvas elípticas, sólo es necesario utilizar una clave con longitud de 256 bits.

[6] *Elliptic Curve Cryptography* por sus siglas en inglés.

1.3.2.3. Algoritmos digestivos

Estos algoritmos, también conocidos como *funciones hash* o *funciones de una vía* producen una suma de verificación a partir de un mensaje dado. Sus principales características son las siguientes:

1. Es rápido calcular el *hash* de un mensaje
2. No es posible regenerar el mensaje a partir de su *hash*
3. Si se cambia el mensaje, el valor del *hash* asociado también cambia

A continuación se describen algunas funciones *hash* empleadas en SSL y TLS:

- **MD5**

  Fue creado por Ron Rivest de RSA y publicado en el RFC1321[34], procesa la entrada en bloques de 512 bits y obtiene como salida una firma con longitud de 128 bits.

  Debido a que se han encontrado *colisiones*[7] en el algoritmo MD5 es considerado **no seguro**[35] y se ha prohibido su uso junto con SSLv2 en el RFC6176[36].

- **SHA1 y SHA256**

  Publicada por el NIST en el RFC3174[37], SHA1 obtiene una salida de 160 bits al procesar de manera secuencial bloques de entrada con longitud de 512 bits.

  SHA256 proviene de la familia SHA-2 publicada en el RFC4634[38], produce una salida de longitud fija con 256 bits y procesa bloques de 512 bits de longitud. Aún no se han encontrado vulnerabilidades o colisiones en esta familia de funciones, por lo que se consideran seguras.

1.3.2.4. Intercambio de llaves

Un paso esencial en un proceso de criptografía asimétrica es realizar el intercambio de las llaves públicas de las partes involucradas[39], algunas técnicas se basan en la confianza que los clientes tienen en una entidad central (Autoridad Certificadora) y existen otros esquemas donde el grado de confianza se mide dependiendo de que tanto confia la comunidad en un individuo (*Web of Trust*)[40].

- **Diffie-Hellman**

  Este método de intercambio de llaves se basa en el problema de la factorización de *logaritmos discretos*, su ventaja principal radica en que la clave secreta nunca es transmitida. Las partes involucradas intercambian números primos y calculan el exponente que será utilizado como clave secreta mediante operaciones modulares[41].

[7] Dos mensajes diferentes que generan el mismo valor de *hash*.

1.3.3. Vulnerabilidades

Una vulnerabilidad es un fallo en la lógica o una situación que se da en condiciones especiales con la que un programa o proceso realiza tareas para las que no fue originalmente destinado. Cuando se alcanzan estas condiciones y se modifica la ejecución del programa se dice que se ha *explotado* la vulnerabilidad [42].

1.3.3.1. BEAST

Descubierto en 2011, este ataque denominado ***B**rowser **E**xploit **A**gainst **S**SL/**T**LS* se aprovecha de los vectores de inicialización del cifrado por bloques CBC para inyectar cadenas en el tráfico cifrado de la víctima[43]. Para mitigar este ataque se recomienda deshabilitar el soporte de SSLv3 y utilizar TLSv1.1 o superior[44].

1.3.3.2. CRIME

El ataque ***C**ompression **R**atio **I**nfo-leak **M**ade **E**asy* fue publicado en 2012, toma ventaja de fallas en la compresión de los protocolos HTTPS y SPDY permitiendo al atacante robar las *cookies* de sesión para hacerse pasar por la víctima. Para mitigarlo es necesario desactivar la compresión realizada con `mod_deflate`[45].

1.3.3.3. BREACH

En 2013 se dio a conocer el ataque llamado ***B**rowser **R**econnaissance and **E**xfiltration via **A**daptive **C**ompression of **H**ypertext* que fue desarrollado por los creadores de CRIME y como su nombre lo indica, utiliza la compresión del tráfico HTTP. En este caso se debe desactivar la compresión de la conexión SSL o TLS y del protocolo HTTP[46].

1.3.3.4. POODLE

La vulnerabilidad conocida como ***P**adding **O**racle **o**n **D**owngraded **L**egacy **E**ncryption* por sus siglas en inglés, fue descubierta en 2014 y toma ventaja de la compatibilidad que implementan los servidores con mecanismos de cifrado débiles como el protocolo SSLv3 y el algoritmo RC4. Se recomienda desactivar el protocolo SSLv3 y el uso de `TLS_FALLBACK_SCSV` en el motor de TLS[47].

1.3.3.5. Heartbleed

Esta vulnerabilidad en la biblioteca de cifrado OpenSSL fue descubierta en 2014 y al explotarla hacía posible leer secciones de memoria privadas donde se aloja la llave privada utilizada para cifrar el tráfico de red[48]. Para mitigar esta vulnerabilidad es necesario actualizar a una versión de OpenSSL mayor o igual a `1.0.1f` o recompilar

utilizando la opción `-DOPENSSL_NO_HEARTBEATS` para deshabilitar la funcionalidad afectada[49].

1.3.3.6. FREAK

El ataque ***F**actoring **R**SA **E**xport **K**eys* publicado en 2015 funciona al interceptar el tráfico HTTPS entre clientes y servidores vunerables, para después forzarlos a establecer la conexión utilizando algoritmos de cifrado débiles denominados `RSA_EXPORT`. Se recomienda deshabilitar el uso de dichos algoritmos y activar una lista de mecanismos de cifrado denominada *Cipher List*[50].

1.3.4. *Hardening*

Se denomina *hardening* al proceso de reforzar las configuraciones del sistema operativo y las aplicaciones para reducir la posibilidad de que una vulnerabilidad sea explotada [42]. El fortalecimiento de las configuraciones se puede realizar en diferentes partes del sistema operativo como:

- Configuración de inicio
- Configuración de acceso físico
- Permisos del sistema de archivos
- Cuotas de espacio en disco
- Configuración de acceso remoto
- Directivas de *firewall* de *host*
- Configuración de las aplicaciones

1.4. GNU/Linux

El sistema operativo GNU/Linux es la combinación del conjunto de utilerías del sistema operativo GNU y el *kernel* Linux [51].

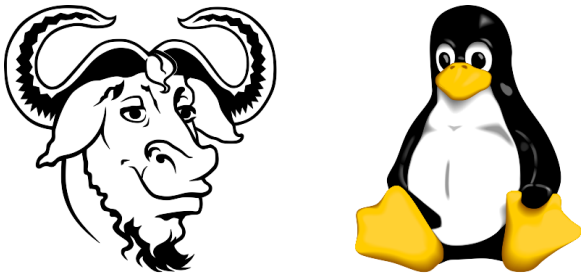


Figura 1.12: Logotipos de GNU y Linux

1.4.1. Historia

En 1983 Richard Stallman inició el proyecto GNU[8], cuyo propósito es hacer un sistema operativo compatible con UNIX que cumpla con las cuatro libertades del *software* y desarrolló junto con otros colegas una serie de utilerías y programas, como el compilador GNU para el lenguage C (*gcc*) [52]. Sin embargo el proyecto tenía prácticamente todos los programas del sistema operativo pero le faltaba la parte escencial: el *kernel*.

En 1987 el profesor Andrew S. Tannenbaum publicó un libro titulado *Sistemas Operativos Diseño e Implementación* [53] donde explica varios conceptos y aspectos clave de los sistemas operativos, la última sección incluye el código fuente del sistema operativo MINIX, que él mismo desarrolló como un clon de UNIX para propósitos educativos[54].

En 1991 Linus Torvalds, que estudiaba la maestría en ciencias de la computación en Helsinki, Finlandia [55], inspirado en MINIX, decidió escribir un sistema operativo compatible con UNIX que cumpliera con el estándar POSIX y el 25 de agosto publicó una entrada en el foro USENET de MINIX [56] explicando su proyecto y pidiendo retroalimentación. Esto dio origen a una ola de desarrollo que hizo que el *kernel* Linux creciera, la licencia original de Linux prohibía el uso comercial pero se cambió para que fuese liberado con la licencia GPL de GNU, que permite el uso comercial siempre y cuando se liberen las modificaciones hechas al *software* y se permita distribuir copias modificadas[9] [58].

[8] Acrónimo recursivo que significa *GNU is Not Unix*.

[9] Visitar [57] para ver la lista completa de mensajes USENET.

1.4.2. Distribuciones de GNU/Linux

Una distribución es un conjunto de paquetes que permiten instalar, actualizar y borrar programas de una manera sencilla gracias a que resuelven las dependencias de forma automática[10]. Generalmente se instalan *paquetes binarios* que contienen los programas ejecutables o *scripts* que conforman la aplicación deseada.

Existen también *paquetes de código fuente* que permiten instalar los archivos de cabecera de un paquete específico. Esto permite compilar un *software* que requiera bibliotecas adicionales sin especificarlas explícitamente gracias a que se resuelven automáticamente porque están en las rutas estándar del sistema.

Aunque todas las distribuciones se apegan al estándar FHS[11] [60], la ubicación de los archivos de configuración y de los binarios varía entre distribuciones y generalmente la estructura del sistema de archivos se hereda entre distribuciones derivadas (ej. Ubuntu es derivado de Debian y tiene una estructura de directorios bastante similar).

Tradicionalmente se utilizaba el sistema de inicio basado en SystemV (*sysvrc*), que lanza los servicios de manera secuencial. Recientemente se han implementado otros sistemas de inicio que pueden lanzar servicios en paralelo si no tienen relación entre sí. Un ejemplo es *insserv* propuesto por LSB[12] [61] [62], *OpenRC* utilizado principalmente en *Gentoo* [63][64][65], *upstart* utilizado en *Ubuntu* y sus derivados [66] y *systemd* utilizado en *Arch Linux* y *Debian 8* [67].

Figura 1.13: Logotipos de las principales distribuciones de GNU/Linux

1.4.3. Uso de GNU/Linux en la industria

El sistema operativo GNU/Linux tiene un gran auge en la industria siendo la plataforma más utilizada para aplicaciones embebidas, *clusters* de supercómputo (con 9 de las 10 computadoras más poderosas), los servicios web más famosos como Google, Twitter, Facebook y Amazon corren sobre GNU/Linux [68].

[10] Las dependencias son programas o bibliotecas adicionales requeridos para que se ejecute el programa.

[11] *Filesystem Hierarchy Standard* por sus siglas en inglés. Estándar publicado que se refiere a la estructura del sistema de archivos en sistemas operativos compatibles con UNIX [59].

[12] *Linux Standard Base* por sus siglas en inglés.

Desde hace más de 15 años el sistema operativo GNU/Linux ha estado presente en diversas aplicaciones como:

- *Clusters* de supercómputo (94 % de los sistemas de cómputo de alto rendimiento se ejecuta sobre GNU/Linux) [69][70]
- Sistemas embebidos con aplicaciones médicas, militares y civiles [71][72]
- Sistemas embebidos de control y RTOS[73][72].
- *Appliances* de red y *firewalls* [74][75]
- Servidores *Proxy* y sistemas de seguridad [76][77][78]
- HTPC (Dispositivos de entretenimiento casero) [79]
- Dispositivos móviles como celulares y *tablets* (Android [80], Firefox OS [81], HP WebOS [82], TizenOS [83], Maemo [84], Ubuntu Phone [85])
- Consolas de videojuegos (PlayStation 2 [86], PlayStation 3 [87], SteamOS y Nvidia Shield)

1.4.4. Debian GNU/Linux

Debian[13] es una de las primeras distribuciones de GNU/Linux que existieron, fue creado en agosto de 1993 por Ian Murdock, quién pensó en hacer un proyecto en el que cualquiera pudiera colaborar sin importar si fuera un usuario o desarrollador [88].

Hoy en día Debian es la distribución más significativa de GNU/Linux sin fines comerciales, esta característica hace posible que el proyecto sea gestionado por una organización de individuos que velan por el proyecto y no por los intereses de la empresa que lo tiene a su cargo.

Figura 1.14: Logotipo de Debian GNU/Linux

[13]El nombre *Debian* proviene de la conjunción del nombre de su creador Ian Murdock (⋆28 de abril de 1973 – †28 de diciembre de 2015) y el nombre de su esposa Debra.

1.5. Protocolo HTTP

El protocolo HTTP permite transferir datos a través de Internet en un esquema cliente-servidor. La primer versión de este protocolo (`HTTP/1.0`) fue descrita en el RFC1945 [89]. Con la evolución de Internet el protocolo fue mejorado y se le agregaron funciones como el control de transferencia o el soporte de mensajes *MIME*, los cuales dieron origen a la versión actual (`HTTP/1.1`) definida en el RFC2616 [90].

1.5.1. HTTPS - *HTTP over SSL*

En el protocolo HTTP los datos se envían y reciben en claro, esto deja la información vulnerable puesto que los mensajes se pueden interceptar o incluso modificar, afectando así la confidencialidad o integidad del mensaje.

Para solventar estas debilidades se definió HTTPS en el RFC2818 [91], que cifra la conexión HTTP utilizando *SSL*[14] o su sucesor *TLS*[15], con el fin de garantizar la confidencialidad e integridad de la información transferida entre el cliente y el servidor.

1.5.2. WebDAV

Web Distributed Authoring and Versioning es una extensión al protocolo HTTP que añade la capacidad de interactuar con archivos almacenados en el servidor web.

Está definido en el RFC4918 [94] y establece un conjunto de extensiones al protocolo HTTP que incluyen métodos, cabeceras y formatos tanto de petición como de respuesta para interactuar con el servidor con la finalidad de crear, modificar y borrar archivos. Además establece un mecanismo denominado *File locking* que previene que dos personas editen el documento al mismo tiempo para no perder cambios.

1.6. Protocolo LDAP

El protocolo LDAP [16] está definido en el RFC4511 [95] y establece el directorio como una colección de objetos que comparte a otros equipos y programas a través de una conexión de red.

Dentro del directorio los objetos se organizan en una estructura jerárquica donde se tiene la raíz del árbol, los contenedores y los objetos, estos últimos además tienen atributos que pueden tener uno o más valores.

[14] Secure Socket Layer por sus siglas en inglés, definido en el RFC6101 [92].
[15] Transport Layer Security por sus siglas en inglés, definido en el RFC5246 [93]
[16] Ligthweight Directory Access Protocol por sus siglas en inglés.

1.6.1. Nomenclatura

La nomenclatura de los objetos es similar a la que utiliza DNS, es decir, el nivel más general se indica a la derecha y el nivel más específico se indica a la izquierda [96]. La raíz del árbol se puede escribir de manera similar al dominio DNS en una notación denominada *Domain Component* (**dc**) o utilizando el nombre de la organización (**o**).

Tabla 1.3: Nomenclatura del nodo raíz de LDAP

Nomenclatura	**Formato del nodo raíz**
Domain Component	dc=tonejito,dc=org
Organization	o=tonejito

Cada objeto tiene un identificador único en el directorio conocido como *Distinguished Name* (**dn**) que ayuda a diferenciar los objetos entre si. Se listan a continuación, a manera de ejemplo, dos de los diferentes nombres distinguidos que se utilizarán en este documento.

```
dn: cn=admin,dc=tonejito,dc=org
dn: uid=user,ou=users,dc=tonejito,dc=org
```

1.6.2. Contenedores

Dentro del directorio se tienen almacenados los objetos en diferentes ramas del árbol que pueden ser vistas como carpetas en un sistema de archivos. Cada contenedor es denominado *Organizational Unit* (**ou**) o Unidad Organizacional y es utilizado para almacenar objetos, incluyendo otras unidades organizacionales para darle estructura al árbol del directorio [96].

1.6.3. Directorio de usuarios

En LDAP los usuarios tienen ciertas propiedades como identificador, nombre de usuario y contraseña, entre otros. Existen dos tipos principales de usuario: `simpleSecurityObject` y `posixAccount`. El primero es utilizado solamente para autenticar un usuario en el directorio y el segundo tiene propiedades parecidas a una cuenta UNIX (*uid*, *gid* y *GECOS*).

1.7. Protocolo SSH

El protocolo SSH[17] sirve para establecer sesiones remotas cifradas entre dos equipos [97]. Utiliza cifrado asimétrico para proteger la conexión y soporta múltiples métodos de autenticación, lo que permite que sea flexible y fácil de incluir en varios sistemas operativos.

Comúnmente se utiliza para conectarse a un servidor y utilizar la interfaz de línea de comandos, aunque el protocolo es muy flexible y se puede utilizar para cumplir las funciones que se listan a continuación:

- Ejecutar un *shell* en el equipo remoto
- Transferencia de archivos desde y hacia el equipo remoto
- Creación de túneles para permitir que el equipo local alcance servicios remotos (*LocalForward*)
- Creación de túneles para que los equipos remotos puedan acceder a los servicios locales (*RemoteForward*)
- Ejecutar programas gráficos en el equipo remoto y visualizar la interfaz como si fuese un programa local (*X11Forward*)
- Generar un *Proxy* SOCKS para enviar el tráfico local al equipo remoto (*DynamicForward*)

Figura 1.15: Logotipo de OpenSSH

[17] *Secure Shell* por sus siglas en inglés.

Capítulo 2

Definición del problema y solución propuesta

2.1. Problemática actual

Los usuarios de la División de Ingenierías Civil y Geomática (DICyG) utilizan memorias USB, discos ópticos y carpetas compartidas en red para acceder a archivos de uso interno como documentos, presentaciones e imágenes que ocupan para realizar sus actividades.

Adicionalmente el personal de la Unidad de Cómputo almacena los archivos de instalación de programas y controladores en dispositivos como memorias USB, discos duros externos o en discos ópticos y los utiliza al dar mantenimiento a los equipos de cómputo de la División.

El problema al mantener los archivos en carpetas compartidas o utilizar un medio de almacenamiento externo es que los datos dejan de estar disponibles si el equipo que comparte la carpeta tiene problemas de conectividad o si el medio de almacenamiento no está conectado al equipo donde se procesa la información.

Por ejemplo, si un profesor necesita compartir algunos archivos con los alumnos parar utilizarlos en clase, los copia a una memoria USB y la pasa a cada uno de los estudiantes para que copien los archivos a su equipo. Este proceso, además de ser tardado, es un proceso propenso a errores donde se puede dañar la memoria *flash* que circula entre los equipos, o bien, se puede infectar con *malware*[1] en un equipo, y al pasar de equipo a equipo se propaga la infección.

Otro caso muy común es el envío de archivos modificados por correo electrónico, generando así una lista de versiones diferentes del mismo archivo que causan confusión porque se desconoce cuál es la versión más actualizada.

[1] *Malware*: *software* malicioso

2.2. Solución propuesta

Para solventar este problema se propone instalar un servidor de almacenamiento que provea espacio para que los usuarios de la DICyG puedan guardar su información y acceder a ella desde los equipos conectados a la red interna a través de una conexión cifrada.

La implementación del servidor de almacenamiento ayudará a liberar espacio en los equipos de cómputo que se utilizan para compartir archivos y proporcionará un repositorio central que guarde la información y la haga accesible a los usuarios sin depender de un equipo o servicio externo.

2.3. Tecnologías a utilizar

Para la implementación de este proyecto se utilizarán las siguientes tecnologías:

- Debian GNU/Linux como sistema operativo del *appliance*
- OpenSSH para el acceso remoto por línea de comandos
- Apache HTTPD para proveer el servicio de HTTPS
- OpenLDAP para implementar el directorio de usuarios

2.4. Arquitectura del prototipo

El prototipo será implementado en un servidor proporcionado por la DICyG que almacenará los archivos que los profesores utilizan en sus clases, así como los programas de instalación y *software* de controladores de dispositivo que la Unidad de Cómputo utiliza para dar mantenimiento a los equipos de la División.

2.4.1. Diagrama funcional

La siguiente figura muestra el diagrama de la interfaz de administración SSH y la interfaz de acceso a los archivos WebDAV sobre HTTPS, ambas utilizan el directorio OpenLDAP para autenticar a los usuarios de manera centralizada.

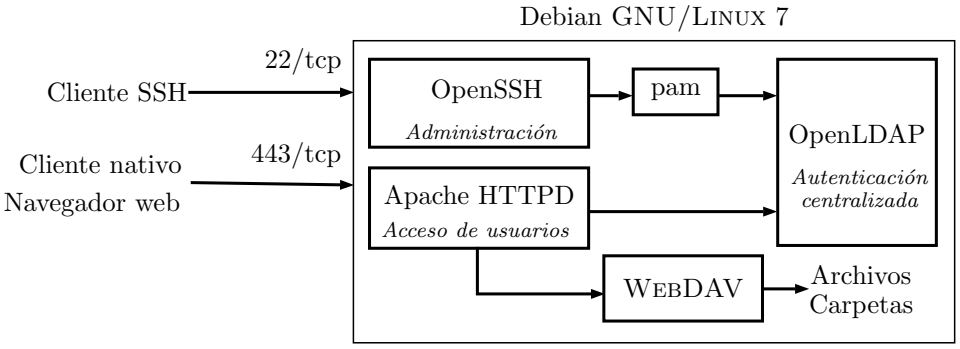


Figura 2.1: Diagrama funcional de la solución propuesta

2.4.2. Autenticación centralizada

El término *autenticación centralizada* se refiere a contar con un repositorio central de usuarios que permita que las aplicaciones puedan verificar las credenciales de acceso *autenticando* así al usuario.

2.4.2.1. Autenticación por medio de directorio

Para tener un esquema de autenticación centralizada se tendrá un directorio de usuarios que implemente el servicio LDAP mediante el *software* OpenLDAP.

2.4.2.2. Estructura del directorio

La estructura propuesta comprende varios contenedores que sirven para separar los tipos de objeto que forman parte del directorio. Cada contenedor está representado

por una *unidad organizacional* cuyo atributo único es el nombre **ou**. Los contenedores principales en la raíz del directorio son los siguientes:

- Contenedor de usuarios
- Contenedor de grupos
- Contenedor de materias
- Contenedor de cuentas de servicio

Contenedor de usuarios

Clasifica los usuarios del sistema por tipo, cada usuario tiene un identificador único asignado llamado **uid**. Se subdivide en tres ramas:

- **Personal de la *Unidad de Cómputo* de la División**

  Estas cuentas de usuario son objetos de tipo *posixAccount* y representan cuentas estándar de UNIX.

- **Profesores**

  Se almacenan en el directorio como objetos de tipo *posixAccount* que representan cuentas estándar de UNIX.

- **Alumnos**

  Su representación en el directorio es un objeto de tipo *simpleSecurityObject* que se utiliza para asignar únicamente un usuario y una contraseña.

Contenedor de grupos

Existen tres clases de grupos de usuarios contemplados en el sistema. Esto ayuda a permitir o negar el acceso a los recursos del servidor, un usuario puede pertenecer a uno o más grupos de los que se listan a continuación.

- **Usuarios de la *Unidad de Cómputo* de la División**

  Existe un grupo único que contiene a todos los usuarios pertenecientes a la *Unidad de Cómputo* y se almacena como un objeto de tipo *posixGroup* que representa un grupo estándar de usuarios UNIX.

- **Profesores**

  Existe un grupo individual para cada usuario y se almacena como *posixGroup*.

- **Alumnos**

  Existen varios grupos que contienen al profesor, la materia y el grupo en el que se imparte, estos permiten dar acceso a la carpeta donde se guardan los archivos de un grupo en particular. Se almacenan internamente como objetos de tipo *groupOfNames*.

Contenedor de materias

Permite almacenar el catálogo de las materias que se imparten en la División. Se requiere para la asignación de grupos a los profesores y alumnos.

Contenedor de cuentas de servicio

Contiene cuentas de usuario asociadas a servicios de sistema. Se utiliza para almacenar las cuentas que realizan búsquedas en el directorio.

Diagrama del árbol de directorio

El siguiente diagrama muestra la estructura del árbol del directorio LDAP:

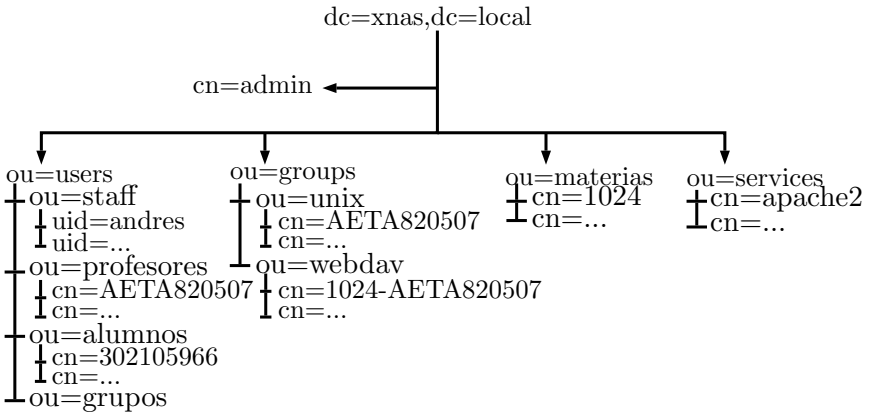


Figura 2.2: Diagrama del árbol de directorio

2.4.3. Mecanismos de acceso a los archivos

Se propone establecer el acceso a los archivos utilizando mecanismos como HTTP estándar y WebDAV.

Acceso por HTTP estándar

Para acceder a los archivos mediante las llamadas estándar del protocolo HTTP sólo se necesita que el usuario tenga un navegador web y que acceda a la URL iniciando sesión. Podrá navegar en los directorios a los que tenga acceso y podrá descargar los archivos si tiene permisos de acceder al directorio.

Acceso por WebDAV

Para el caso del acceso vía WebDAV es necesario un cliente, los sistemas operativos de escritorio como GNU/Linux, Solaris, *BSD[2], Mac OS X y Windows tienen un cliente nativo en sus interfaces gráficas del navegador de archivos.

Aunque en los sistemas operativos es posible instalar clientes de WebDAV para acceder a los archivos, se propone tomar las interfaces nativas del sistema operativo para facilitar el acceso a los archivos.

En los sistemas operativos móviles como Android y Apple iOS es posible instalar clientes para acceder a los archivos vía WebDAV, si no se desea acceder por este medio se puede utilizar la interfaz web estándar.

2.4.4. Interfaces de usuario

Además del acceso por WebDAV y por medio de un navegador web, el *appliance* tendrá una interfaz de administración para ver y modificar los atributos de los usuarios y una interfaz para que los usuarios puedan cambiar su contraseña sin necesidad de acudir con el administrador.

2.4.4.1. Interfaz de administración

La interfaz de administración que se propone permite ver, agregar, modificar y borrar registros del directorio. Se utilizará la interfaz web *LDAP Account Manager* y además se puede instalar la herramienta *Apache Directory Studio*.

2.4.4.2. Interfaz de cambio de contraseña

Esta interfaz permite tanto al personal de la *Unidad de Cómputo* como a los profesores cambiar la contraseña de acceso que tienen asignada, al realizar esta acción envía un correo para notificar que se llevó acabo dicho cambio.

[2]Cualquier versión de BSD como OpenBSD, FreeBSD y NetBSD

2.4.5. Especificación del *appliance*

En la siguiente sección se muestran las configuraciones del *hardware* y *software* que tendrá el *appliance*.

2.4.5.1. Hardware

Tabla 2.1: Recursos de *hardware* utilizados para el *appliance*

Elemento	**Mínimo**	**Recomendado**
CPU	1x 1 GHz	2x 2 GHz
RAM	1 GB	4 GB
Discos Duros	1x 80 GB	2x 500 GB
Arreglo RAID	✘	RAID 1
Fuentes de poder redundantes	✘	✔
Soporte de *TCP Offload Engine*	✘	✔

2.4.5.2. Software

Tabla 2.2: Versiones de *software* utilizados para el *appliance*

Software	**Versión**
Sistema Operativo	Debian GNU/Linux 7 *Wheezy*
OpenSSH	v6.0
Apache HTTPD	v2.2
OpenLDAP	v2.4
PHP	v5.4
LDAP Account Manager	v4.8
LDAP Toolbox: Self Service Password	v0.8

Capítulo 3

Implementación de la solución

3.1. Configuración del sistema operativo

El sistema operativo que será utilizado para la implementación es DEBIAN GNU/LINUX 7 «*wheezy*», se instalará de manera nativa en el servidor y se le aplicarán configuraciones personalizadas para ejecutar el *software* que será implementado, ajustar el rendimiento y reforzar la seguridad de los servicios que ofrezca.

3.1.1. Arreglo de discos RAID

Los discos duros del servidor serán configurados en un arreglo RAID debido a las ventajas que ofrece[1]. La configuración en el servidor de pruebas se realizará con un arreglo RAID 1 por *software* que se configuró de la siguiente manera: [98]

- Instalar el programa para habilitar la compatibilidad con arreglos RAID por *software*:

```
# apt-get install mdadm
```

- Crear las particiones de tipo *Linux RAID Autodetect* en cada disco del arreglo
  - Crear una partición primaria que ocupe todo el espacio del disco:

```
# /sbin/fdisk /dev/sdb

Device contains neither a valid DOS partition table, nor Sun, SGI or OSF disklabel
Building a new DOS disklabel with disk identifier 0x00bab10c.
Changes will remain in memory only, until you decide to write them.
After that, of course, the previous content won't be recoverable.

Warning: invalid flag 0x0000 of partition table 4 will be corrected by w(rite)

Command (m for help): n
```

[1] Ver página 12 sección 1.1.6

```
Partition type:
   p   primary (0 primary, 0 extended, 4 free)
   e   extended
Select (default p): p
Partition number (1-4, default 1): 1
First sector (2048-16777215, default 2048):
Using default value 2048
Last sector, +sectors or +size{K,M,G} (2048-16777215, default 16777215):
Using default value 16777215
```

- Cambiar el tipo de la partición a `0xfd` - *Linux RAID Autodetect* y escribir la tabla de particiones al disco:

```
Command (m for help): t
Selected partition 1
Hex code (type L to list codes): fd
Changed system type of partition 1 to fd (Linux RAID Autodetect)

Command (m for help): w
The partition table has been altered!

Calling ioctl() to re-read partition table.
Syncing disks.
```

- Crear arreglo:

```
# mdadm --zero-superblock /dev/sdb1 /dev/sdc1
# mdadm --create /dev/md0 --level=1 --raid-devices=2 /dev/sdb1 /dev/sdc1
```

- Dar formato al disco que representa el arreglo:

```
# mkfs.ext4 /dev/md0
```

- Asignar tipo y punto de montaje en el archivo `/etc/fstab`:

```
/dev/md0 /opt/xNAS/files ext4 noatime,rw 0 0
```

- Guardar configuración en el archivo `/etc/mdadm/mdadm.conf`:

```
ARRAY /dev/md0 devices=/dev/sdb1,/dev/sdc1 level=1 num-devices=2 auto=yes
DEVICE /dev/sdb1 /dev/sdc1
```

3.1.2. Punto de montaje de sólo lectura

Para evitar el acceso de escritura a los archivos pertenecientes a los profesores, se realizó un montaje de tipo *bind* con permisos de sólo lectura. Debido a que se realizan dos operaciones de montaje, es necesario agregar las siguientes líneas al *script* `/etc/rc.local` [99] [100] [101].

```
PREFIX=/opt/xNAS/files
mount --bind $PREFIX/profesor $PREFIX/p
mount -o remount,ro,bind $PREFIX/profesor $PREFIX/p
```

3.2. Configuración de los servicios

3.2.1. OpenLDAP

3.2.1.1. Instalación de OpenLDAP

Se instala OpenLDAP utilizando el comando `aptitude`, es necesario contestar **NO** en el cuadro de diálogo para seguir el asistente de instalación:

```
# aptitude install slapd
```

```
+---------------------------+ Configuring slapd +----------------------------+
| If you enable this option, no initial configuration or database will be    |
| created for you.                                                           |
|                                                                            |
| Omit OpenLDAP server configuration?                                        |
|                    <Yes>                       <No>                        |
+----------------------------------------------------------------------------+
```

Se pide el nombre DNS del dominio que servirá para conformar la raíz del árbol de LDAP.

```
+---------------------------+ Configuring slapd +----------------------------+
| The DNS domain name is used to construct the base DN of the LDAP           |
| directory. For example, 'foo.example.org' will create the directory with   |
| 'dc=foo, dc=example, dc=org' as base DN.                                   |
|                                                                            |
| DNS domain name:                                                           |
| xnas.tonejito.org_________________________________________________________ |
|                                  <Ok>                                      |
+----------------------------------------------------------------------------+
```

Adicionalmente el instalador pregunta por el nombre de la organización. Aunque este dato no es necesario, se recomienda introducirlo:

```
+---------------------------+ Configuring slapd +----------------------------+
| Please enter the name of the organization to use in the base DN of your    |
| LDAP directory.                                                            |
|                                                                            |
| Organization name:                                                         |
| xNAS______________________________________________________________________ |
|                                 <Ok>                                       |
+----------------------------------------------------------------------------+
```

A continuación se pide que se introduzca la contraseña que será utilizada por el administrador del directorio:

```
+-------------------------+ Configuring slapd +-----------------------------+
| Please enter the password for the admin entry in your LDAP directory.      |
|                                                                            |
| Administrator password:                                                    |
| **********________________________________________________________________ |
|                                 <Ok>                                       |
+----------------------------------------------------------------------------+
```

Se recomienda deshabilitar el soporte del protocolo LDAPv2 puesto que es obsoleto, responder **NO** en el cuadro de diálogo.

```
+---------------------------+ Configuring slapd +---------------------------+
|                                                                            |
| The obsolete LDAPv2 protocol is disabled by default in slapd. Programs and |
| users should upgrade to LDAPv3.  If you have old programs which can't use  |
| LDAPv3, you should select this option and 'allow bind_v2' will be added to |
| your slapd.conf file.                                                      |
|                                                                            |
| Allow LDAPv2 protocol?                                                     |
|                     <Yes>                       <No>                       |
+----------------------------------------------------------------------------+
```

3.2.1.2. Configuración de OpenLDAP

Se configuró el sistema operativo para permitir que los usuarios de LDAP de tipo *posixAccount* puedan iniciar sesión en el equipo.

```
# aptitude install libpam-ldapd
```

Adicionalmente se instalaron los demonios NSCD y NSLCD que se utilizan para guardar en *caché* los resultados de las consultas al directorio y para representar los objetos *posixAccount* de LDAP como cuentas estándar de UNIX.

```
+------------------------+ Configuring libnss-ldapd +-------------------------+
| For this package to work, you need to modify your /etc/nsswitch.conf to    |
| use the ldap datasource.                                                   |
|                                                                            |
| You can select the services that should have LDAP lookups enabled. The new |
| LDAP lookups will be added as the last datasource. Be sure to review these |
| changes.                                                                   |
|                                                                            |
| Name services to configure:                                                |
|    [*] group                                                               |
|    [*] passwd                                                              |
|    [*] shadow                                                              |
|                                  <Ok>                                      |
+----------------------------------------------------------------------------+
```

Para la configuración de PAM, se indica que se utilizarán como fuentes de autenticación la base de datos estándar de UNIX y adicionalmente el directorio LDAP.

```
+---------------------------+ PAM configuration +---------------------------+
| Pluggable Authentication Modules (PAM) determine how authentication,       |
| authorization, and password changing are handled on the system, as well as |
| allowing configuration of additional actions to take when starting user    |
| sessions.                                                                  |
|                                                                            |
| Some PAM module packages provide profiles that can be used to              |
| automatically adjust the behavior of all PAM-using applications on the     |
| system.  Please indicate which of these behaviors you wish to enable.      |
|                                                                            |
| PAM profiles to enable:                                                    |
|    [*] Unix authentication                                                 |
|    [*] LDAP Authentication                                                 |
|                     <Ok>                        <Cancel>                   |
+----------------------------------------------------------------------------+
```

3.2.1.3. Inicialización del directorio LDAP

Una vez instalado el servicio de directorio, es necesario inicializar la estructura básica que comprende los contenedores de usuarios, materias y grupos utilizando el archivo `xNAS-base.ldif` y el comando `ldapadd`. En caso de requerir cambiar la contraseña del administrador del directorio, seguir las indicaciones mostradas en las siguientes referencias [102] [103].

```
# aptitude install ldap-utils
```

Se verifica que no existan objetos adicionales en el directorio. La salida del comando `ldapsearch` debe ser similar a la que se muestra a continuación:

```
# ldapsearch -LLL -Y EXTERNAL -H ldapi:/// -b 'dc=xnas,dc=local'

SASL/EXTERNAL authentication started
SASL username: gidNumber=0+uidNumber=0,cn=peercred,cn=external,cn=auth
SASL SSF: 0

dn: dc=xnas,dc=local
objectClass: top
objectClass: dcObject
objectClass: organization
o: xNAS
dc: xnas

dn: cn=admin,dc=xnas,dc=local
objectClass: simpleSecurityObject
objectClass: organizationalRole
cn: admin
description: LDAP administrator
```

Se procede con la inicialización de la estructura básica del directorio.

```
# ldapadd -x -W -D "cn=admin,dc=xnas,dc=local" -H 'ldapi:///' -f ./xNAS-base.ldif

Enter LDAP Password:

adding new entry "ou=services,dc=xnas,dc=local"
adding new entry "ou=materias,dc=xnas,dc=local"
adding new entry "ou=users,dc=xnas,dc=local"
adding new entry "ou=staff,ou=users,dc=xnas,dc=local"
adding new entry "ou=profesores,ou=users,dc=xnas,dc=local"
adding new entry "ou=grupos,ou=users,dc=xnas,dc=local"
adding new entry "ou=alumnos,ou=users,dc=xnas,dc=local"
adding new entry "ou=groups,dc=xnas,dc=local"
adding new entry "ou=unix,ou=groups,dc=xnas,dc=local"
adding new entry "ou=webdav,ou=groups,dc=xnas,dc=local"
```

3.2.1.4. Carga de datos en el directorio LDAP

Para realizar la carga de la base de datos de usuarios y grupos se desarrolló en el lenguaje de programación *Ruby* una biblioteca y un *script* de carga que lee los datos desde un archivo origen en formato CSV, establece las relaciones entre los objetos y realiza el ingreso de los datos al directorio.

La biblioteca que realiza la carga de objetos funciona de acuerdo al siguiente algoritmo:

- Realiza una conexión al directorio LDAP, a esta operación se le denomina *bind* (ver figura).
- Convierte el archivo de entrada a la codificación UTF-8.
- Lee cada renglón del archivo de entrada y verifica el contenido de cada campo contra una *expresión regular* para identificar problemas.
- Si el renglón cumple con el formato, se continúa con el próximo paso, de lo contrario se guarda en una lista que debe ser revisada manualmente y salta al siguiente.
- Asigna los atributos de cada objeto LDAP de acuerdo al valor de cada campo.
- Establece las relaciones necesarias con otros objetos y realiza una transacción para insertar los datos en el directorio.
- Verifica que la inserción se haya realizado correctamente, en caso de existir algún error, se realiza un *rollback* de las operaciones.

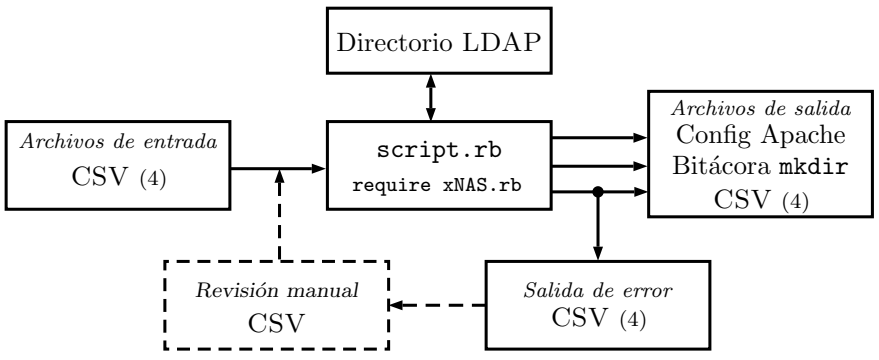


Figura 3.1: Diagrama de bloques de los *scripts* de carga

Cada archivo de entrada CSV tiene varias columnas que contienen información acerca del tipo de objeto que representa, a continuación se muestran las columnas que se requieren en los archivos de entrada:

Tabla 3.1: Formato de los archivos CSV para la carga de datos

Archivo	**Columnas**				
staff.csv	usuario	nombre	correo	curp	
materias.csv	id	grupo	materia	rfc	profesor
profesores.csv	rfc	nombre	correo		
alumnos.csv	cuenta	nombre	correo	asignatura	grupo

Para la correcta ejecución de los *scripts*, es necesario instalar los paquetes `ruby`, `rubygems` y la *Gema*[2] que realiza la conexión con el directorio LDAP.

```
# aptitude install ruby rubygems ruby-json
# gem install net-ldap
```

Utilizando el *script* `./load.rb` se cargan los datos y se crean los objetos en el directorio:

```
# ./load.rb

xNAS - ./load.rb

Enter username, press <ENTER> for default:
    username    [cn=admin]
Enter password (will not echo):
    password
```

Tabla 3.2: *Script* de carga de objetos en el directorio

Tipo	**Objetos creados en el directorio**	
staff	*posixGroup*	*posixAccount*
profesores	*posixGroup*	*posixAccount*
materias	*organizationalRole*	*groupOfNames*
alumnos	*simpleSecurityObject*	

3.2.1.5. Borrado de datos en el directorio LDAP

Se desarrolló un *script* que ayudará a limpiar el directorio cuando se pretenda cargar una nueva base de datos en el mismo.

```
# make clean
# ./clean.rb

xNAS - ./clean.rb

Enter username, press <ENTER> for default:
    username [cn=admin]
Enter password (will not echo):
    password
```

[2]Biblioteca de *Ruby*.

3.2.2. Apache HTTPD

En esta sección se describe el procedimiento que se realizó para configurar el servicio de HTTP con WebDAV sobre SSL.

3.2.2.1. Esquema de configuración

La configuración de Apache HTTPD comprende tres *VirtualHost* que sirven como puntos de entrada para el acceso de sólo lectura o lectura y escritura a los archivos almacenados en el servidor.

Tabla 3.3: VirtualHost configurados en Apache HTTPD

VirtualHost	Función
`xnas.tonejito.org`	Acceso a los archivos por medio de WebDAV
`reset.xnas.tonejito.org`	Interfaz de cambio de contraseña
`admin.xnas.tonejito.org`	Interfaz administrativa del directorio LDAP

Si el usuario accede al *appliance* utilizando el nombre de dominio principal o la dirección IP, se presenta la interfaz de acceso a los archivos. Para acceder a la interfaz de administración del directorio o para cambiar la contraseña se debe acceder utilizando el nombre de dominio designado en la tabla anterior. En la siguiente figura se muestra de manera gráfica la segmentación de los diferentes *VirtualHost*:

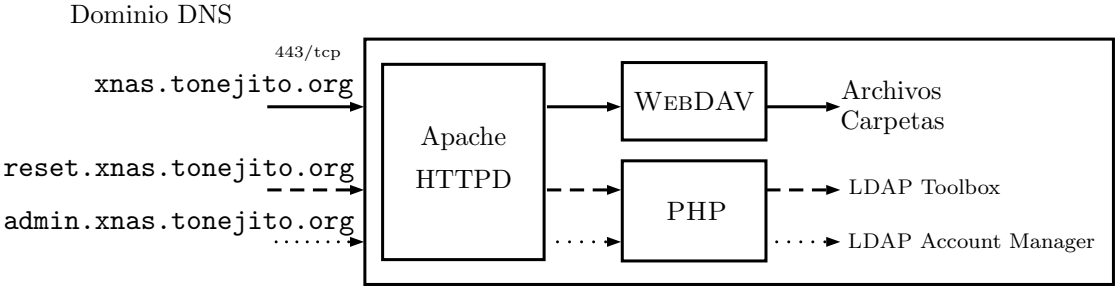


Figura 3.2: Diagrama Apache HTTPD VirtualHost

El conjunto de archivos y configuraciones que forman parte del *appliance* se organizan en diferentes carpetas como se muestra en la siguiente ilustración:

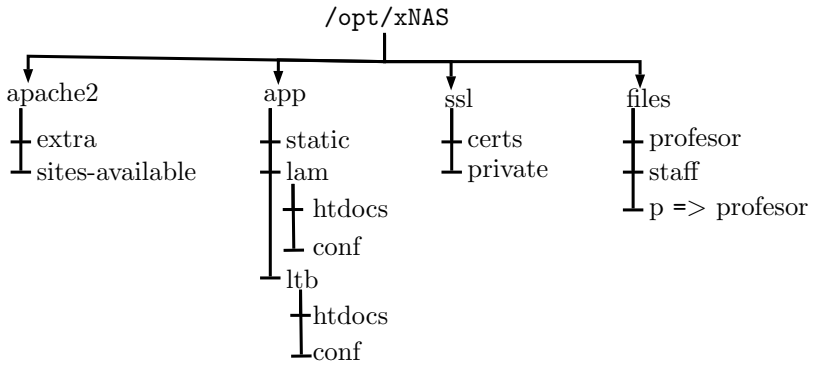


Figura 3.3: Diagrama de configuración de Apache HTTPD

Se ingresaron en el sistema de archivos varias ligas simbólicas que apuntan a las configuraciones de Apache HTTPD que reside en el directorio `/opt/xNAS`.

Tabla 3.4: Archivos de configuración de Apache HTTPD

Liga simbólica	Destino
`/etc/apache2/extra`	`/opt/xNAS/apache2/extra`
`/etc/apache2/sites-available/xnas.local`	`/opt/xNAS/apache2/sites-available/default`
`/etc/apache2/sites-available/reset.xnas.local`	`/opt/xNAS/apache2/sites-available/reset.xnas.local`
`/etc/apache2/sites-available/admin.xnas.local`	`/opt/xNAS/apache2/sites-available/admin.xnas.local`
`/etc/ssl/certs/ca.thesis.tonejito.info.crt`	`/opt/xNAS/ssl/certs/ca.thesis.tonejito.info.crt`
`/etc/ssl/certs/xnas.local.crt`	`/opt/xNAS/ssl/certs/xnas.local.crt`
`/etc/ssl/certs/admin.xnas.local.crt`	`/opt/xNAS/ssl/certs/admin.xnas.local.crt`
`/etc/ssl/certs/xnas.local.key`	`/opt/xNAS/ssl/certs/xnas.local.key`
`/etc/ssl/certs/admin.xnas.local.key`	`/opt/xNAS/ssl/certs/admin.xnas.local.key`

3.2.2.2. Configuración del servicio

Se instala el certificado SSL en `/etc/ssl/certs` y la llave privada en `/etc/ssl/private` mediante los siguientes comandos:

```
# cd /etc/ssl/private
# ln -vsf /opt/xNAS/ssl/xnas.local.key
# cd /etc/ssl/certs
# ln -vsf /opt/xNAS/ssl/ca.thesis.tonejito.info.crt
# ln -vsf /opt/xNAS/ssl/xnas.local.crt
# c_rehash
```

Se copia el archivo `ports.conf` al directorio principal de Apache HTTPD con el objeto de configurar de manera adecuada la directiva `NameVirtualHost` para los sitios de HTTPS.

```
# cd /opt/xNAS/apache2
# cp ports.conf /etc/apache2
# /etc/init.d/apache2 restart
# apache2ctl -S
```

Se habilita el acceso a las configuraciones específicas del *appliance* al hacer una *liga simbólica* al directorio `extra`:

```
# cd /etc/apache2
# ln -vsf /opt/xNAS/apache2/extra
```

Se instalan y habilitan los módulos necesarios para que las funcionalidades del sitio se realicen de manera adecuada, esto incluye la autenticación y la funcionalidad de WebDAV. Por último se reinicia el servicio para aplicar los cambios.

```
# cd /etc/apache2/sites-available
# ln -vsf /opt/xNAS/apache2/xnas.local
# a2dissite default
# a2enmod headers ssl rewrite ldap authnz_ldap dav dav_fs dav_lock
# a2ensite default
# /etc/init.d/apache2 restart
```

3.2.2.3. Compatibilidad con clientes WebDAV

Aunque WebDAV es un estándar definido en el RFC4918 [94], existen varios clientes que ofrecen funcionalidades similares aunque son implementados de manera distinta. Por ejemplo, los clientes de Mac OS X y GNU/Linux son los más completos, mientras que el cliente nativo de Windows (*Microsoft-WebDAV-MiniRedir*) tiene muchos problemas de compatibilidad.

Se utilizaron las directivas `BrowserMatch` y `BrowserMatchNoCase` para distinguir a los clientes problemáticos que se conectan al servidor y darles un tratamiento especial [104] [105]. A continuación se muestran las directivas que se utilizaron para darle un tratamiento especial a los clientes WebDAV nativos de Windows.

```
Header add MS-Author-Via "DAV"
BrowserMatch "Microsoft-WebDAV-MiniRedir" redirect-carefully nokeepalive ssl-unclean-shutdown
```

Para el caso específico de Windows, es necesario deshabilitar la detección automática de *Proxy* en la configuración de *Internet Explorer*, esto debido a que de manera predeterminada intenta encontrar un servidor *Proxy* en cada petición que realiza al servidor [106] [107] [108].

3.2.2.4. Conexión al servidor LDAP

La conexión al servidor LDAP se configura con la directiva `AuthLDAPUrl` que especifica los parámetros de conexión, se compone de dos partes principales:

Tabla 3.5: Parámetros de conexión `LDAP`

Cadena de conexión	Filtro
Protocolo	*Contenedor*
Host	*Atributos de índice*
Puerto	*Profundidad y condiciones de la búsqueda*

3.2.2.5. Búsqueda en el directorio

Esta operación se realiza estableciendo una conexión al servidor para enviar el comando y los parámetros de búsqueda. La respuesta puede ser una lista de los identificadores únicos de cada elemento encontrado o un resultado vacío.

```
AuthLDAPUrl "ldapi:///ou=users,dc=xnas,dc=local?uid,cn?sub?
            (|(objectClass=posixAccount)(objectClass=simpleSecurityObject))"
```

Para esta URL se realizará una búsqueda en el directorio comenzando en el contenedor principal de usuarios, el objetivo es encontrar objetos de tipo `posixAccount` o `simpleSecurityObject` que estén indexados por el atributo *uid* o *cn*. El alcance de la búsqueda se establece para todos los objetos que se encuentren bajo esta rama del árbol, si se desea que únicamente se exploren los objetos en este nivel del directorio, se debe establecer el parámetro *one*.

3.2.2.6. Grupos de LDAP

Para el manejo de permisos de acceso se utilizaron grupos de LDAP que representan a los alumnos que se encuentran inscritos a una materia. Se incluye la directiva `Require` para establecer en la configuración que es necesario pertenecer a determinado grupo para tener acceso al recurso solicitado.

```
Require ldap-group cn=1024-HEBA861228,ou=webdav,ou=groups,dc=xnas,dc=local
```

Al especificar la directiva `Require ldap-group` se realiza la búsqueda del usuario y adicionalmente del grupo, con el objeto de encontrar todos sus miembros y poder verificar si el usuario en cuestión es uno de ellos.

3.3. Implementación de las interfaces de usuario

3.3.1. Acceso mediante el navegador web

Para acceder mediante el navegador web, simplemente se accede a la URL. De manera predeterminada el servidor pide el usuario y la contraseña del usuario para ofrecer el listado de archivos y directorios disponibles dependiendo de su nivel de acceso.

3.3.2. Acceso mediante cliente nativo de WebDAV

Para el acceso mediante el cliente nativo se utilizan los siguientes parámetros. En el Apéndice A se puede consultar el manual de conexión.

Tabla 3.6: Parámetros de conexión WebDAV

Parámetro	Valor
Endpoint	`https://xnas.tonejito.org/profesores`
SSL	`true`
Authentication	BASIC

3.3.2.1. Conector WebDAV desarrollado en *PowerShell*

Se desarrolló una interfaz *frontend* para facilitar a los usuarios de Windows la conexión al servidor WebDAV. Se utilizó el lenguaje de programación *PowerShell* para lograr que el *script* se pueda ejecutar en versiones recientes de Windows sin necesidad de utilizar alguna otra dependencia.

El programa utiliza de manera interna el comando `net use` [109] que permite montar una carpeta del servidor WebDAV con una letra de unidad local (Ej. `Z:`). Es una alternativa a la interfaz estándar que presenta el *Explorador de Windows* [110].

Una vez que se toman los datos de la URL, el nombre de usuario y la contraseña se llama al comando `net use` para montar la unidad de red. La interfaz *frontend* también toma en cuenta si se desea realizar la operación en modo persistente, es decir, que la unidad permanezca montada aún cuando se reinicie el equipo.

```
C:\> net use  *  https://xnas.tonejito.org/profesor/<nombre-del-profesor>  \
                 /user:<usuario>       <password>                          \
                 /persistent:<boolean>
```

3.3.2.2. Instalación del conector WebDAV y certificado raíz

Para hacer uso del conector desarrollado en *PowerShell* o de la interfaz nativa de Windows, es necesario instalar el certificado raíz de la CA para que el dominio pueda ser validado.

El *script bootstrap* de instalación `install.cmd` realiza las siguientes acciones en el equipo:

- Descarga y ejecuta el archivo `install.ps1` con la lógica principal del instalador.
- Crea el directorio `C:\xNAS`.
- Descarga el certificado raíz `ca.crt`.
- Instala el certificado raíz dentro de las *Autoridades Certificadoras de Confianza* utilizando el comando `certutil`.
- Reinicia el servicio `WebClient` puesto que es utilizado para las conexiones a WebDAV.
- Descarga el *script* `xNAS-Connector.ps1` y crea un acceso directo en el escritorio.

3.3.3. Interfaz de administración *LDAP Account Manager*

Se descarga el *tarball* del código fuente y se descomprime en el directorio `lam/htdocs`:

```
# cd /opt/xNAS/app/lam
# wget -c 'http://iweb.dl.sourceforge.net/project/lam/LAM/4.8/ldap-account-manager-4.8.tar.bz2'
# tar -xvvjf ldap-account-manager-4.8.tar.bz2 -C /opt/xNAS/app/lam
# mv ldap-account-manager-4.8 htdocs
```

Se establecen permisos de escritura para el servidor web en los directorios `sess` y `temp`:

```
# chown -cR www-data:www-data /opt/xNAS/app/lam/htdocs/{sess,tmp}
```

Se instalan los archivos de configuración de la herramienta:

```
# cd /opt/xNAS/app/lam/htdocs/config
# ln -vsf ../../lam.conf
# ln -vsf ../../config.cfg
```

Se instala el certificado, la llave privada y la configuración del sitio. Una vez realizado esto, se reinicia el servicio:

```
# cd /etc/ssl/private
# ln -vsf /opt/xNAS/ssl/admin.xnas.local.key
# cd /etc/ssl/certs
# ln -vsf /opt/xNAS/ssl/admin.xnas.local.crt
# c_rehash

# cd /etc/apache2/sites-available
# ln -vsf /opt/xNAS/apache2/admin.xnas.local
# a2ensite admin.xnas.local
# /etc/init.d/apache2 reload
```

3.3.4. Interfaz de cambio de contraseña

Se descarga el paquete de instalación del sitio web oficial y se extrae en el directorio `ltb/htdocs`:

```
# cd /opt/xNAS/app/ltb
# wget -c 'http://tools.ltb-project.org/attachments/download/497/\
  ltb-project-self-service-password-0.8.tar.gz'
# tar -xvvzf ltb-project-self-service-password-0.8.tar.gz -C /opt/xNAS/app/ltb
# mv ltb-project-self-service-password-0.8 htdocs
```

Se instala el certificado, la llave privada y la configuración del *VirtualHost*, hecho esto se reinicia el servicio para reflejar los cambios.

```
# cd /etc/ssl/private
# ln -vsf /opt/xNAS/ssl/reset.xnas.local.key
# cd /etc/ssl/certs
# ln -vsf /opt/xNAS/ssl/reset.xnas.local.crt
# c_rehash

# cd /etc/apache2/sites-available
# ln -vsf /opt/xNAS/apache2/reset.xnas.local
# a2ensite reset.xnas.local
# /etc/init.d/apache2 reload
```

3.4. Hardening

La configuración de seguridad del equipo se realizó con base en las configuraciones de seguridad presentadas en la documentación oficial del sistema operativo Debian GNU/Linux[111], las guias de seguridad publicadas por el *Centro de Seguridad en Internet* (CIS[3])[112] y recomendaciones emitidas por el proyecto OWASP[4][113].

3.4.1. Actualizaciones desatendidas

Una parte importante de la configuración de seguridad de un sistema radica en la instalación periódica de actualizaciones. Al ejecutar el siguiente comando y responder **YES** en el cuadro de diálogo, se configura el sistema para descargar e instalar *automáticamente* las actualizaciones de seguridad que sean liberadas por el fabricante del sistema operativo.

```
# dpkg-reconfigure unattended-upgrades
```

```
+------------------------+ Configuring unattended-upgrades +------------------------+
| Applying updates on a frequent basis is an important part of keeping systems      |
| secure. By default, updates need to be applied manually using package management  |
| tools. Alternatively, you can choose to have this system automatically download   |
| and install security updates.                                                     |
|                                                                                   |
| Automatically download and install stable updates?                                |
|                       <Yes>                          <No>                         |
+-----------------------------------------------------------------------------------+
```

[3] *Center for Internet Security* por sus siglas en inglés.

[4] *Open Web Application Security Project* por sus siglas en inglés.

3.4.2. Reducción de componentes instalados

Como parte de la configuración de seguridad, es recomendable minimizar los paquetes que se instalan en el sistema operativo para disminuir la ventana de posibilidades de tener una intrusión. Con la siguiente configuración del gestor de paquetes se evita la instalación de *software* adicional cuando se agrega un paquete. Esto ayuda a reducir la complejidad del sistema y reduce el espacio en disco utilizado [114].

```
# cat > /etc/apt/apt.conf.d/10Hardening << EOF
Apt::Install-Recommends "false";
Apt::Install-Suggests   "false";
EOF
```

3.4.3. Evitar el apagado o reinicio accidental del equipo

Al administrar un equipo de manera remota se corre el riesgo de ejecutar por error el comando de apagado o reinicio. Al suceder esto se pierde la sesión de todos los usuarios, los servicios se interrumpen, si se dio la órden de apagado, será necesario acudir a la ubicación física del equipo y encenderlo manualmente.

Para mitigar este riesgo se instaló el programa `molly-guard`. Al detectar el uso de comandos para apagar o reiniciar el sistema desde una sesión remota, preguntará el nombre del equipo para hacer una verificación adicional y evitar que un equipo sea apagado o reiniciado accidentalmente de manera remota. El programa se instaló utilizando el siguiente comando:

```
# aptitude install molly-guard
```

3.4.4. Reenvío del correo electrónico de `root`

Se instaló en el equipo el MTA `Postfix` configurado como *Internet Site*. Para habilitar la redirección de los mensajes de correo electrónico dirigidos al administrador del sistema se realizó lo siguiente:

- Especificar la dirección de destino en el archivo `/etc/aliases`:
  ```
  root: xnas@tonejito.org
  ```
- Regenerar la base de datos de *aliases*:
  ```
  # newaliases
  ```
- Recargar la configuración del servicio de correo:
  ```
  # /etc/init.d/postfix reload
  ```

3.4.5. Restricción de acceso para las tareas programadas

Para limitar la capacidad de los usuarios para programar la ejecución de comandos en el sistema operativo se adoptó una política restrictiva que consiste en tener una *lista blanca* donde únicamente los usuarios del sistema[5] pueden hacer uso de trabajos de *cron* y *at* [115] [116] [117].

```
# cd /etc
# getent passwd | sort -g -t ":" -k 3,3 | awk -F: '$3<1000 {print $1}' | tee cron.allow
# ln -v cron.allow at.allow
```

3.4.6. Configuración de seguridad de OpenSSH

Para el servicio de SSH se aplicaron las siguientes opciones en el archivo de configuración `/etc/ssh/sshd_config`. Los valores asignados a las siguientes directivas fueron recomendados por el libro *Securing Debian*[111] y las guias de *hardening* y auditoría publicadas por el CIS[118].

- Quita el nombre del sistema operativo del *banner* inicial de SSH.

  ```
  DebianBanner no
  ```

- Deshabilitar el acceso administrativo utilizando contraseña, únicamente se permite el inicio de sesión como `root` al utilizar autenticación de llave pública.

  ```
  PermitRootLogin without-password
  ```

- Deshabilitar el acceso a cuentas que tengan una contraseña vacía.

  ```
  PermitEmptyPasswords no
  ```

- Permitir el acceso al grupo de usuarios de la *Unidad de Cómputo* de la DICyG.

  ```
  AllowGroups adm staff support
  ```

- Mostrar una pantalla antes de iniciar la sesión en la que se listen las políticas de uso del sistema.

  ```
  Banner /etc/issue.net
  ```

- Evitar la desconexión manteniendo actividad en la sesión.

  ```
  TCPKeepAlive yes
  ClientAliveInterval 30
  ```

- Evitar la redirección de puertos y sesiones gráficas.

  ```
  AllowTCPForwarding no
  GatewayPorts no
  X11Forwarding no
  ```

- Desconectar al usuario si no inicia sesión en 60 segundos.

  ```
  LoginGraceTime 60
  ```

[5] Con **uid** menor a 1000

3.4.7. Reglas de *firewall*

Se adoptó una política que define varias zonas de seguridad con un nivel de acceso diferente a los servicios de LDAP, SSH y HTTPS. Para filtrar el tráfico de red se establecieron las siguientes políticas de *firewall* de *host* en el equipo:

- Se permite todo el tráfico proveniente de la interfaz *loopback*.
- Las conexiones a través de SSH se permiten únicamente desde los siguientes segmentos confiables de red:
  1. Segmentos de RedUNAM: `132.247.0.0/16` , `132.248.0.0/16`
  2. Red interna de la DICyG.
- Se permiten las conexiones por HTTPS desde cualquier *host*, ya sea de la red interna, segmentos de RedUNAM o Internet.
- Las conexiones al demonio de LDAP se permiten únicamente desde *localhost*.

Para implementar las reglas de *firewall* se utilizó `iptables` para el filtrado de paquetes en GNU/Linux y el paquete `iptables-persistent` que sirve para aplicar las reglas guardadas en cada inicio del sistema operativo. El programa se instala con `aptitude` y al configurarlo pregunta si se guardarán las reglas de IPv4 e IPv6.

```
    # aptitude install iptables-persistent
```

```
+--------------------| Configuring iptables-persistent |--------------------+
|                                                                            |
| Current iptables rules can be saved to the configuration file              |
| /etc/iptables/rules.v4. These rules will then be loaded automatically      |
| during system startup.                                                     |
|                                                                            |
| Rules are only saved automatically during package installation. See the    |
| manual page of iptables-save(8) for instructions on keeping the rules      |
| file up-to-date.                                                           |
|                                                                            |
| Save current IPv4 rules?                                                   |
|                                                                            |
|                    <Yes>                       <No>                        |
|                                                                            |
+----------------------------------------------------------------------------+
```

3.4.7.1. Protección contra ataques de fuerza bruta con *fail2ban*

Este *software* realiza un seguimiento de las conexiones que se realizan al equipo e identifica los ataques de fuerza bruta contra el servicio de SSH. Al detectar un ataque, realiza un bloqueo de la dirección IP de origen por un tiempo determinado.

Es necesario instalar el *software* y hacer una copia del archivo `jail.conf` con el nombre `jail.local` donde se realizarán ajustes a la configuración del servicio.

```
# aptitude install fail2ban
# cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
```

Una vez copiado el archivo de configuración, se agregan los bloques CIDR definidos en el RFC1918 y los segmentos de REDUNAM que se definieron en la sección 3.4.7 en la página 55. Adicionalmente se incrementa el tiempo de bloqueo de la dirección IP del atacante de 600 segundos a 3600 (una hora).

```
[DEFAULT]

# "ignoreip" can be an IP address, a CIDR mask or a DNS host
ignoreip = 127.0.0.0/8 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16 132.247.0.0/16 132.248.0.0/16

# seconds
bantime  = 3600
maxretry = 3
```

Al finalizar el ajuste de los parámetros de configuración, se reinicia el servicio.

```
# service fail2ban restart
```

3.4.8. Configuración de seguridad de Apache HTTPD

Se establecieron los valores recomendados en las siguientes directivas con el objetivo de evitar la divulgación de información acerca del *software* del servidor web y del sistema operativo. Estas directivas se encuentran presentes en el archivo `/etc/apache2/conf.d/security`. Se aplicaron las configuraciones publicadas por el CIS en la guía de seguridad para Apache HTTPD[119] y además las recomendaciones de seguridad publicadas por el proyecto OWASP[113].

Tabla 3.7: Directivas de seguridad de Apache HTTPD

Directiva	Valor
`ServerSignature`	Off
`ServerTokens`	ProductOnly
`TraceEnable`	Off

3.4.8.1. Configuración para PHP

Se configuró PHP para que no muestre la versión en las cabeceras del protocolo HTTP, evitar la impresión de errores y para que guarde los errores encontrados en una bitácora. Para lograr esto, se establecieron los siguientes valores en el archivo `php.ini` de acuerdo a la guía de seguridad para PHP publicada por el proyecto OWASP[120].

Tabla 3.8: Directivas de seguridad de PHP

Directiva	Valor
expose_php	Off
display_errors	Off
display_startup_errors	Off
log_errors	On
error_log	/var/log/apache2/error.log

3.4.8.2. Deshabilitar el soporte de archivos `.htaccess`

Se agregó esta directiva de configuración dentro de un bloque `<Directory>` para que el servidor ignore los archivos de configuración `.htaccess`, esto debido a que podrían ser modificados por los usuarios.

```
AllowOverride none
```

3.4.8.3. Restricción de permisos de escritura

Los métodos HTTP se pueden clasificar de acuerdo al tipo de acceso que tienen, ya sea para obtener o enviar datos al servidor. En la siguiente tabla se muestra la clasificación de acuerdo a este criterio:

Tabla 3.9: Clasificación de métodos HTTP

Tipo	Métodos		
Sólo lectura	OPTIONS	PROPFIND	
	HEAD	GET	
Lectura y Escritura	POST	PUT	MKCOL
	COPY	MOVE	DELETE
	LOCK	UNLOCK	PATCH
	PROPPATCH		

Con el fin de establecer una restricción a los métodos HTTP que pueden escribir datos en el servidor, se utilizó la directiva `LimitExcept` para definir los métodos que se permiten en el servidor en determinado directorio [121]. En el siguiente ejemplo se muestra la configuración adoptada para permitir el acceso de sólo lectura.

```
<LimitExcept GET OPTIONS PROPFIND>
  Satisfy ALL
  Require ldap-group _
  Order Allow,Deny
  Deny From ALL
</LimitExcept>
```

3.4.8.4. Configuración de cifrado para HTTPS

Se establecieron los siguientes parámetros de cifrado para HTTPS, a continuación se listan las medidas adoptadas para mitigar los ataques a SSL y TLS. Para la elaboración de la configuración de `mod_ssl` se tomaron las recomendaciones oficiales para deshabilitar la funcionalidad afectada por las vulnerabilidades[44][45][46][47][48][50].

- Deshabilita el mecanismo de compresión de SSL y TLS, mitigando las vulnerabilidades CRIME[122] y BREACH[46]

  ```
  SSLCompression Off
  ```

- Deshabilita explícitamente el uso de SSLv2, SSLv3 y TLSv1, para evitar la vulnerabilidad POODLE[123]

  ```
  SSLProtocol All -TLSv1 -SSLv3 -SSLv2
  SSLHonorCipherOrder On
  ```

- Elige un algoritmo seguro para el cifrado, intercambio de llaves y verificación de mensaje, esto previene los ataques BEAST[43] y BREACH[46]

  ```
  SSLCipherSuite
  ```

- Los algoritmos se listan del más fuerte al más débil y se deshabilitan MD5, RC4, 3DES, DES, así como los algoritmos de tipo EXPORT y NULL

La configuración completa de `mod_ssl` se muestra a continuación:

```
<IfModule ssl_module>
  # CRIME and BREACH
  # http://breachattack.com/

  SSLCompression off

  # POODLE
  # https://poodle.io/servers.html#apache

  SSLProtocol All -TLSv1 -SSLv3 -SSLv2
  SSLHonorCipherOrder On

  # BEAST and FREAK
  # https://ssldecoder.org/
  # https://cipherli.st/
  # https://raymii.org/s/tutorials/Strong_SSL_Security_On_Apache2.html
  # https://freakattack.com/

  SSLCipherSuite ECDHE-RSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES256-GCM-SHA384:
         ECDHE-ECDSA-AES256-GCM-SHA384:DHE-RSA-AES128-GCM-SHA256:DHE-DSS-AES128-GCM-SHA256:kEDH+AESGCM:
         ECDHE-RSA-AES128-SHA256:ECDHE-ECDSA-AES128-SHA256:ECDHE-RSA-AES128-SHA:ECDHE-ECDSA-AES128-SHA:
         ECDHE-RSA-AES256-SHA384:ECDHE-ECDSA-AES256-SHA384:ECDHE-RSA-AES256-SHA:ECDHE-ECDSA-AES256-SHA:
         DHE-RSA-AES128-SHA256:DHE-RSA-AES128-SHA:DHE-DSS-AES128-SHA256:DHE-RSA-AES256-SHA256:
         DHE-DSS-AES256-SHA:DHE-RSA-AES256-SHA:!aNULL:!eNULL:!EXPORT:!DES:!RC4:!3DES:!MD5:!PSK
</IfModule>
```

Capítulo 4

Pruebas

Con el objeto de dar soporte a las plataformas más comunes, se realizaron pruebas sobre los principales sistemas operativos de escritorio y móviles. Gracias a que el protocolo WebDAV es estándar, sólo es cuestión de instalar un cliente en el sistema operativo o verificar si esta funcionalidad ya está incorporada para acceder a servidores de archivos de este tipo.

4.1. Plan de pruebas

A continuación se muestra una lista de las pruebas que se realizaron en el servidor y la descripción de cada una:

- **Pruebas de compatibilidad multiplataforma**

  Se verificó que los usuarios pudieran establecer la conexión al servidor siguiendo los manuales mostrados en el Apéndice A.

- **Pruebas de roles de usuario**

  Se revisó que los perfiles de usuario tuvieran el acceso correspondiente a los archivos y los privilegios necesarios para realizar sus actividades.

- **Pruebas de seguridad web**

  En esta sección se validó que el servidor no contara con servicios adicionales escuchando en puertos de red, además se realizó una prueba automatizada de las cuentas de usuario y sus privilegios de escritura, por último se verificó el nivel de protección que ofrecen los parámetros de cifrado configurados en Apache HTTPD.

4.2. Compatibilidad multiplataforma

En el Apéndice A se muestran los pasos necesarios para realizar la conexión al servidor WebDAV tanto en sistemas operativos de escritorio como en plataformas de móviles.

4.3. Pruebas de roles de usuario

El sistema de almacenamiento presenta tres perfiles de usuario: staff, profesor y alumno. Los dos primeros tienen privilegios de lectura-escritura y el último tiene acceso de sólo lectura.

El personal de la *Unidad de Cómputo* verificó que cada tipo de usario cumpliera con los requerimientos de acceso y además que la conexión al servidor se pudiera realizar de manera exitosa siguiendo los manuales presentados en el Apéndice A.

Tabla 4.1: Perfiles de usuario y tipo de acceso

Perfil de usuario	Descripción
Staff	Acceso de lectura y escritura a su carpeta de usuario Acceso de lectura a la sección de profesores
Profesor	Acceso de lectura y escritura a su carpeta de usuario
Alumno	Acceso de sólo lectura a las carpetas de profesor

4.4. Pruebas de seguridad

4.4.1. Detección de puertos abiertos

Se ejecutó una búsqueda de puertos abiertos en el servidor utilizando el programa *nmap*. El siguiente comando realiza la verificación de todo el rango de puertos TCP enviando paquetes de tipo SYN y además intenta obtener la versión del programa que escucha en el puerto encontrado.

```
# nmap -Pn -sS -sV --version-all -T 5 -p 0-65535 -oA xnas xnas.tonejito.org

Starting Nmap 6.00 ( http://nmap.org ) at 2015-09-28 00:00 EDT
Nmap scan report for xnas.tonejito.org (132.248.139.147)
Host is up (0.064s latency).
Not shown: 65533 closed ports
PORT    STATE SERVICE  VERSION
22/tcp  open  ssh      OpenSSH 6.0p1 (protocol 2.0)
80/tcp  open  http     Apache httpd
443/tcp open  ssl/http Apache httpd

Service detection performed. Please report any incorrect results at http://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 256.32 seconds
```

4.4.2. Autenticación

Las pruebas de autenticación se realizaron de manera automatizada, se utilizó el siguiente algoritmo para iterar entre los usuarios y carpetas utilizando el cliente WebDAV *cadaver*:

```
para cada usuario u
  para cada carpeta c
    intenta acceder como el usuario u a la carpeta c
    el servidor dio acceso
      agrega el usuario y la carpeta a la lista de accesos exitosos
    caso contrario
      agrega el usuario y la carpeta a la lista de accesos fallidos
    fin de condicional
  fin de ciclo de carpetas
fin de ciclo de usuarios
```

4.4.3. Parámetros de cifrado para HTTPS

Al realizar una verificación de seguridad del cifrado SSL utilizado en el *appliance*, se obtuvo una calificación regular **C** y se encontraron los siguientes problemas con la configuración predeterminada:

- Vulnerabilidad al ataque `POODLE`[1] [124] [47] [125] [126] [127]
- El servidor soporta el algoritmo cifrado `RC4`, mismo que es clasificado como débil [128]
- Está habilitado el soporte de SSLv3
- La configuración de SSL aplicada no permite el uso de *Perfect Forward Secrecy* [129]

A comtinuación se muestra una captura de pantalla con los resultados obtenidos tras la primer prueba:

[1]Padding Oracle On Downgraded Legacy Encryption

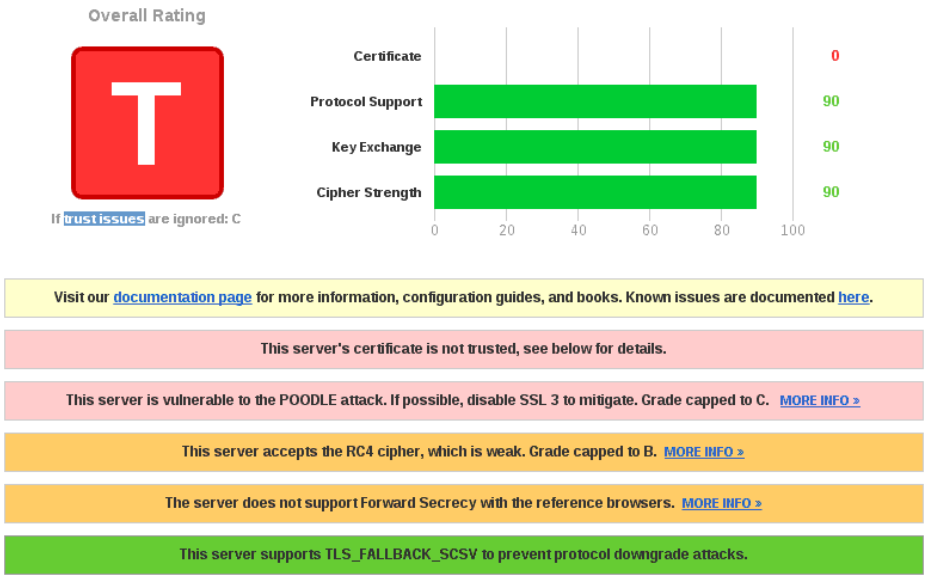


Figura 4.1: Prueba de parámetros de cifrado HTTPS estándar

Para resolver los problemas encontrados se tomaron en cuenta los requerimientos para SSL del estándar PCI-DSS, deshabilitando por completo el soporte de RC4 y SSLv3.

Gracias a la configuración aplicada se obtuvo una calificación buena **A**. En la siguiente imagen se muestra el resultado de las pruebas de seguridad SSL donde la única advertencia mostrada es referente a la autoridad que realizó la firma del certificado. [130]

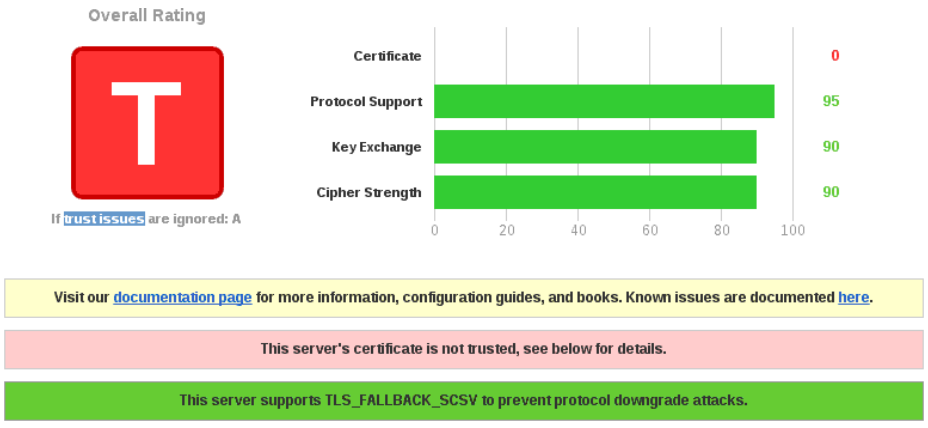


Figura 4.2: Prueba de parámetros de cifrado HTTPS reforzados

Capítulo 5

Conclusiones

5.1. Resultados obtenidos

- **WebDAV**

  Gracias a que la solución desarrollada utiliza el protocolo estándar WebDAV, que es una extensión de HTTP, se tiene un alto grado de compatibilidad con clientes WebDAV, navegadores web y utilidades de línea de comandos, además se puede integrar con otras plataformas.

- **HTTPS**

  Para resguardar la confidencialidad de la contraseña del usuario e integridad de los datos transmitidos, el mecanismo de acceso a los archivos es únicamente a través de HTTPS. Esto además de ser una práctica recomendada, es un requisito para poder utilizar servicios WebDAV en Windows.

- **Compatibilidad multiplataforma**

  Durante el desarrollo de este proyecto se realizaron ajustes de los componentes utilizados en la implementación para que el servidor de archivos fuera compatible con el cliente WebDAV del sistema operativo Windows.

  De igual manera, se investigaron e implementaron mecanismos que permitieran instalar de forma automatizada el certificado de la autoridad raíz en el sistema y que no tuvieran dependencias adicionales para ejecutarse.

- **Directorio LDAP**

  Para agilizar la carga de los usuarios se desarrollaron una serie de *scripts* que realizan la carga desde un archivo separado por comas e insertan los objetos en el directorio LDAP. La carga de usuarios se puede realizar de manera parcial o en una sola operación sin presentar dificultades en el sistema.

5.2. Oportunidades de mejora

Se identificaron los siguientes elementos que se pueden utilizar para extender y mejorar la funcionalidad de este sistema y que pueden ser integrados o implementados en futuras versiones.

- **Implementación de cuotas de usuario**

  Para evitar que un solo usuario ocupe todo el espacio disponible en el disco, se pueden implementar cuotas para los usuarios que tienen permisos de escritura en el sistema, esto requerirá aplicar directivas de ACL en las carpetas de cada usuario para mantener el grupo asociado al usuario en cada archivo que este cree.

- **Apache HTTPD 2.4**

  Utilizar directivas dinámicas de control de acceso puede simplificar las directivas de control de acceso utilizadas en el sistema. Esta característica está disponible en Apache HTTPD 2.4.

- **Integración con bases de datos y directorios de usuarios**

  Como alternativa para evitar el uso de un directorio, es posible utilizar una base de datos para autenticar a los usuarios mediante el módulo `mod_authn_dbd` de Apache HTTPD que se comunica con una base de datos y ejecuta sentencias SQL para autenticar y autorizar al usuario.

  En caso de utilizar un directorio externo de usuarios LDAP, será necesario modificar las directivas de autenticación que utiliza este sistema para realizar la búsqueda del usuario y la validación de sus credenciales.

  Ejemplos de otros sistemas que ofrecen directorios de usuarios son las suites de colaboración *Zimbra* y *Zentyal*. Existen otros servicios de directorio compatibles como *OpenLDAP*, *Apache Directory Server*, *OpenDirectory* de Mac OS X Server, *389 Directory Server* de Red Hat, *Tivoli Directory Server* de IBM y *Active Directory* de Microsoft.

- **Integración con ownCloud**

  Este *appliance* puede ser utilizado como fuente de autenticación en ownCloud para validar las credenciales de los usuarios antes de que accedan al sistema, adicionalmente, cada usuario puede integrar el almacenamiento que provee este proyecto como un *directorio virtual* dentro de su cuenta en ownCloud para expandir el almacenamiento, o bien, mover sus archivos de una plataforma a otra.

Apéndice A

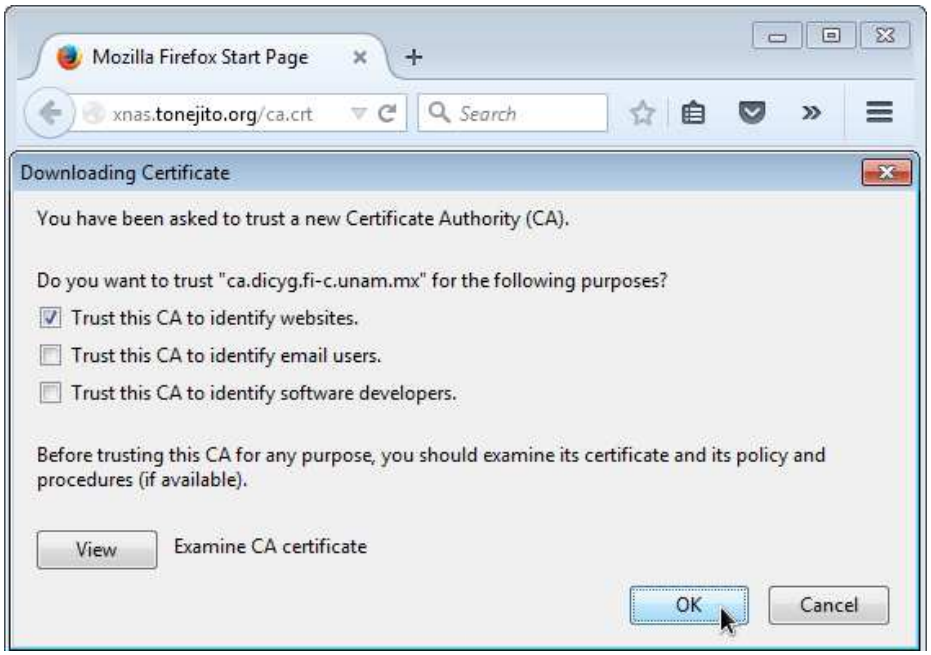
Manuales

A.1. Instalación del certificado raíz

A.1.1. Navegador web Mozilla Firefox

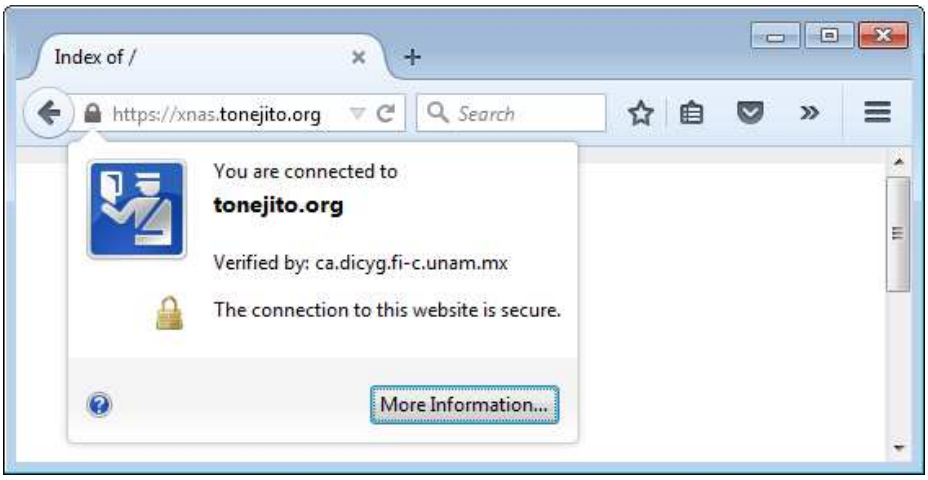
1. Abrir el sitio en el navegador web *Firefox*. Aparecerá una ventana donde se pregunta la función del certificado raíz, seleccionar la primer opción y dar clic en el botón **OK**.

   `http://xnas.tonejito.org/ca.crt`



2. Después de instalar el certificado, el sitio web se mostrará de manera correcta en el navegador web al accederlo por HTTPS.

   `https://xnas.tonejito.org/`

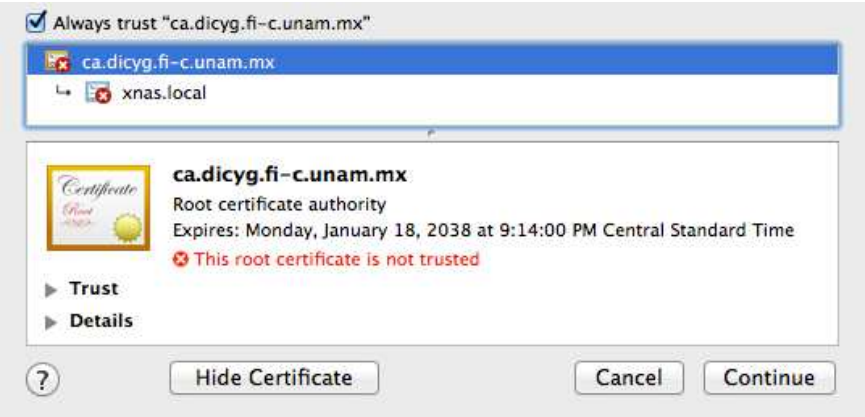


A.1.2. Mac OS X

1. Abrir el sitio en el navegador web *Safari* y dar clic en el botón *Show Certificate*.

   `https://xnas.tonejito.org/`

2. Activar la casilla *Always Trust*, al terminar hacer clic en **Continue**.



3. Escribir la contraseña para aplicar los cambios.

4. Verificar que el sitio cargue a través de HTTPS y cerrar el navegador.

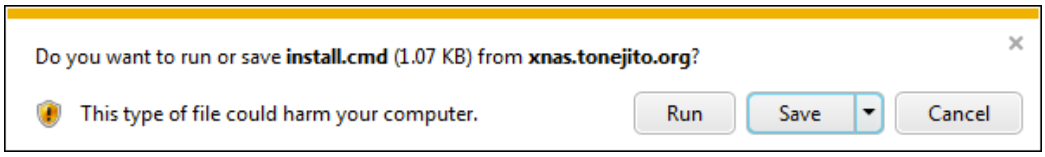
A.1.3. Windows

1. Abrir el navegador de Internet.

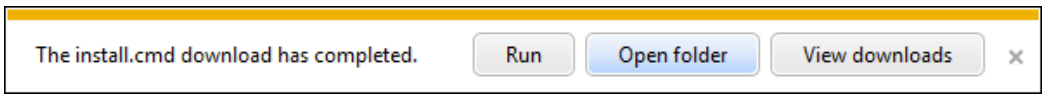
2. Escribir la siguiente URL en la barra de direcciones y presionar `<Enter>`.

   `http://xnas.tonejito.org/install.cmd`

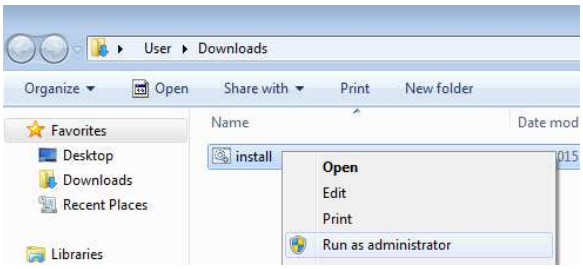
3. El navegador preguntará qué hacer con el archivo, seleccionar la opción **guardar**.



4. El *script* de instalación fue guardado en la carpeta *Descargas*, pulsar en el botón **Abrir carpeta**.



5. Hacer clic derecho en el archivo **install.cmd** y seleccionar la opción *Ejecutar como administrador*.



6. Dar clic en el botón **SÍ** en el cuadro de diálogo de UAC.

7. Al terminar la instalación se creará un icono llamado **xNAS** en el escritorio.

A.2. Acceso de *sólo lectura* para alumnos

El sitio tiene la siguiente estructura de directorios para la sección de *sólo lectura*. El alumno puede navegar en todos los directorios públicos donde la URL tiene el siguiente formato:

Tabla A.1: Formato de la URL de la sección de *sólo lectura*

Elemento	Componente de URL
URL *base*	`https://xnas.tonejito.org/alumno/`
Nombre del profesor	↪ `andres-leonardo-hernandez-bermudez`
ID de materia	↪ `1024`
ID de grupo	↪ `8`
Archivos y carpetas	⟹ archivos ⟹ carpetas

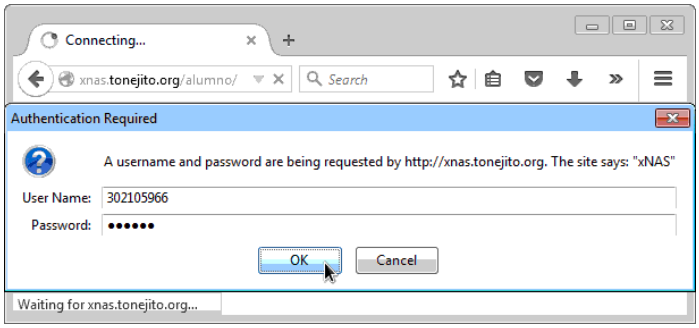
A.2.1. Navegador web

0. Instalar el certificado raíz en el equipo (ver sección A.1.3 en la página 68) y en el navegador web *Mozilla Firefox* (ver sección A.1.1 en la página 65).

1. Abrir el sitio en el navegador web.

   `https://xnas.tonejito.org/alumno/`

2. Escribir el número de cuenta y la contraseña en el cuadro de diálogo. Una vez realizado esto, se podrá navegar en los directorios.



3. Abrir la carpeta que corresponde al nombre del profesor, materia y grupo. Ver sección A.2 en la página 70 para conocer la nomenclatura de las carpetas donde los alumnos pueden acceder a los archivos.

A.3. Acceso de *lectura-escritura* para profesores

El sitio tiene la siguiente estructura de directorios para la sección de *lectura y escritura*. El profesor puede subir archivos al directorio representado por el *ID de materia* y puede generar carpetas adicionales dentro del directorio con el *ID de grupo*:

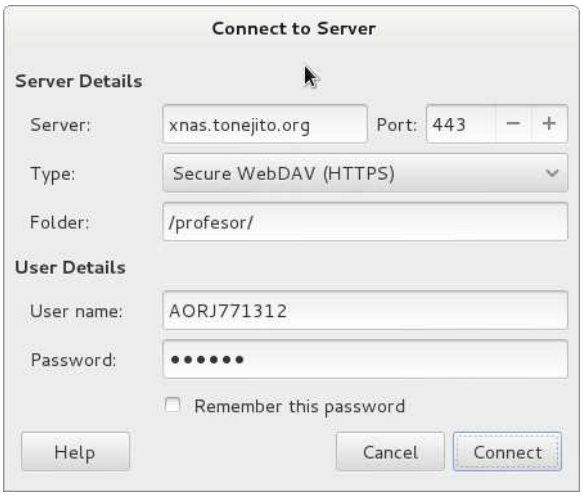
Tabla A.2: Formato de la URL de la sección de *lectura y escritura*

Elemento	Componente de URL
URL *base*	`https://xnas.tonejito.org/profesor/`
Nombre del profesor	↪ `andres-leonardo-hernandez-bermudez`
ID de materia	↪ `1024`
ID de grupo	↪ `8`
Archivos y carpetas	⟹ archivos ⟹ carpetas

A.3.1. GNU/Linux

1. En el escritorio de *Gnome* ir al menú *Places* y seleccionar la opción *Connect to Server*.

2. Escribir los datos de conexión por *Secure WebDAV*, así como las credenciales de usuario y dar clic en el botón *Connect*.

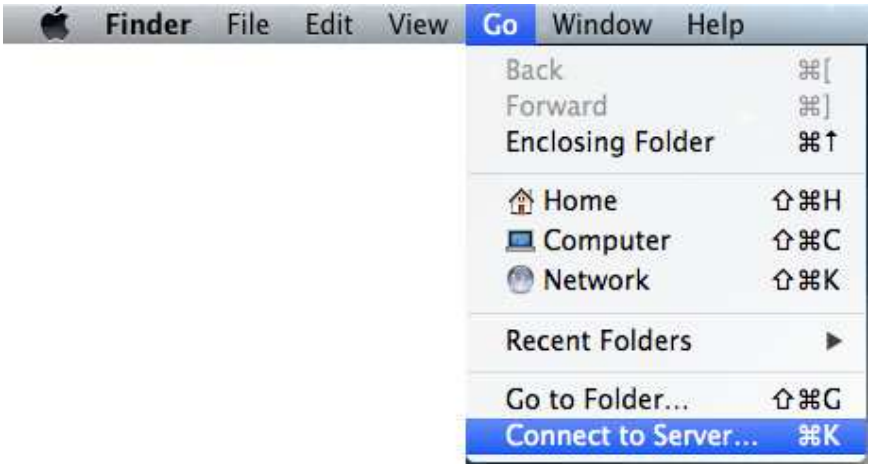


3. Abrir la carpeta que corresponde al nombre del profesor. Ver sección A.3 en la página 71 para conocer la nomenclatura de las carpetas donde se pueden subir archivos.

A.3.2. Mac OS X

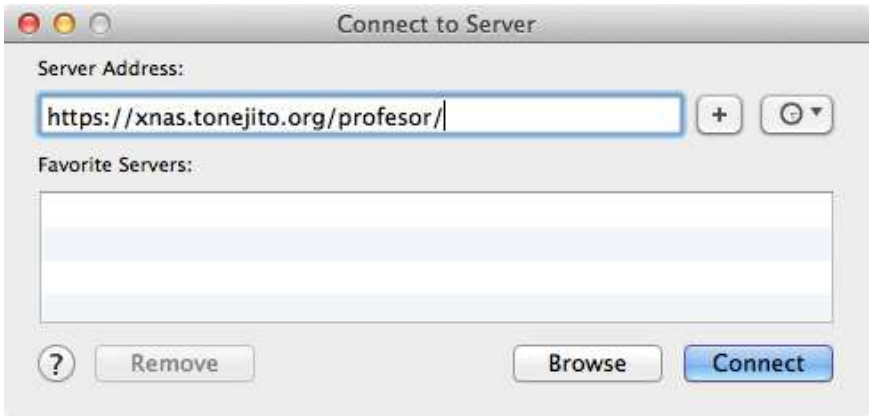
0. Instalar el certificado raíz en el equipo (ver sección A.1.2 en la página 66).

1. En *Finder* ir al menú *Go* y seleccionar la opción *Connect to server*.



2. Escribir la siguiente URL en el campo *Server Address* y dar clic en el botón *Connect*.

   `https://xnas.tonejito.org/profesor/`



3. Esperar a que se inicialice la conexión.

4. Para conectar con el servidor se pedirán las credenciales de acceso, introducirlas y dar clic en el botón *Connect*.

5. Abrir la carpeta que corresponde al nombre del profesor. Ver sección A.3 en la página 71 para conocer la nomenclatura de las carpetas donde se pueden subir archivos.

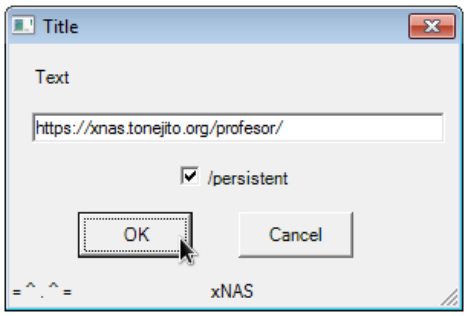
A.3.3. Windows

0. Instalar el certificado raíz en el equipo (ver sección A.1.3 en la página 68).

1. Dar doble clic en el icono **xNAS** ubicado en el escritorio.

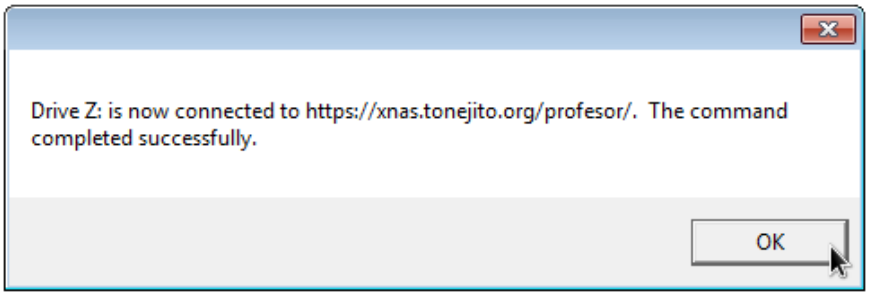
2. Escribir la siguiente URL en el cuadro de diálogo y dar clic en el botón **OK**.

   `http://xnas.tonejito.org/profesor/`

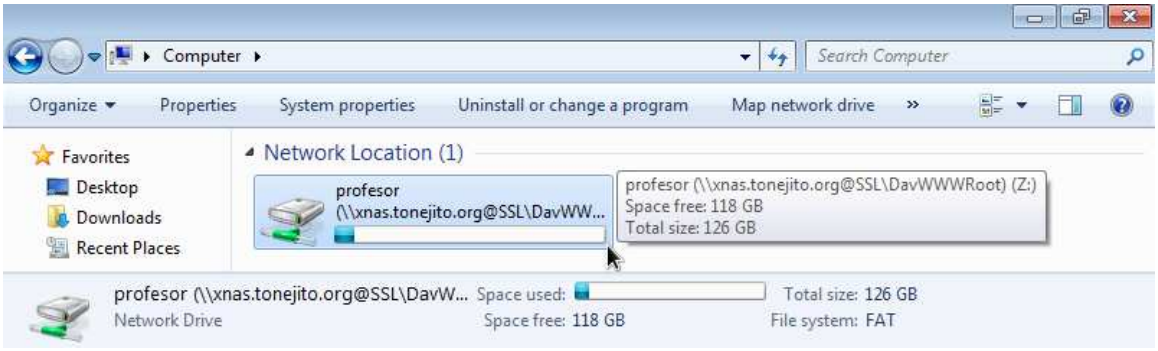


3. Escribir las credenciales de acceso y dar clic en el botón **OK**.

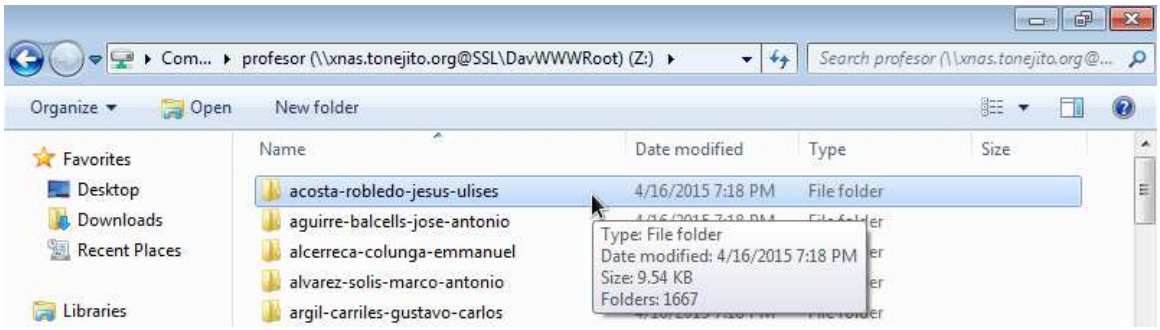
4. Se muestra el siguiente mensaje cuando la unidad pudo conectarse de manera correcta.



5. Iniciar el explorador de windows, seleccionar la unidad de red y dar doble clic.



6. Abrir la carpeta que corresponde al nombre del profesor. Ver sección A.3 en la página 71 para conocer la nomenclatura de las carpetas donde se pueden subir archivos.



Glosario

aliases Archivo de configuración que contiene los alias de correo del sistema, utilizado por el MTA. 53

localhost Nombre de red que se refiere al host actual, está asociado al bloque de direcciones IPv4 `127.0.0.0/8` y a la dirección reservada `::1` de IPv6. 55

root Usuario administrador en sistemas compatibles con UNIX. 54

ACL *Access Control List* por sus siglas en inglés. 64

AT Servicio del sistema que agenda la ejecución de un comando en una fecha específica. 54

Bootstrap Script mínimo de inicialización. 51

CA Autoridad Certificadora, *Certification Authority* por sus siglas en inglés. 51

CIS *Center for Internet Security* por sus siglas en inglés. 52, 54, 56

Cron Servicio del sistema que se utiliza para definir y ejecutar tareas programadas. 54

DNS *Domain Name System* por sus siglas en inglés. 28, 41

ECC *Elliptic Curve Cryptography* por sus siglas en inglés. 20

EFF *Electronic Frontier Foundation* por sus siglas en inglés. 19

FHS *Filesystem Hierarchy Standard* por sus siglas en inglés. 25

Firewall Dispositivofísico o de software que bloquea las conexiones de red entrantes y/o salientes. 23, 26, 55

Firmware Lógica programada de un circuito. 12

Frontend Interfaz de usuario. 50

GB *GigaByte* - 1024^3 bytes = 1073741824 bytes. 5

Gema Paquete de software de Ruby, en este formato se distribuyen las bibliotecas de este lenguaje de programación. 45

GNU Acrónimo recursivo que significa *GNU is Not* Unix. 24

GPL GNU *General Public License*, por sus siglas en inglés. 24

Hardware Partes físicas de un equipo de cómputo. 4, 12, 17, 18, 37

Host Equipo conectado a una red. 23, 55

HTTP *Hypertext Transfer Protocol* por sus siglas en inglés. 22, 27, 36, 46, 56, 57, 63

HTTPS *HTTP over SSL* por sus siglas en inglés. 22, 23, 27, 32, 33, 48, 55, 58, 63

KB *KiloByte* - 1024 bytes. 5

Kernel Núcleo del sistema operativo, ejecuta las tareas en el CPU y administra los recursos del sistema. 12, 24

LDAP *Lightweight Directory Access Protocol* por sus siglas en inglés. 27, 28, 33, 35, 41, 42, 44–46, 49, 55, 63, 64

Loopback Interfaz de red virtual que comunica únicamente al host, utilizada por procesos internos del sistema operativo. 55

LSB *Linux Standard Base* por sus siglas en inglés. 25

MB *MegaByte* - 1024^2 bytes = 1048576 bytes. 5

MTA *Mail Transport Agent* por sus siglas en inglés. 53

OWASP *Open Web Application Security Project* por sus siglas en inglés. 52, 56

PAM *Pluggable Authentication Modules* por sus siglas en inglés. 42

PCI-DSS *Payment Card Industry Data Security Standard* por sus siglas en inglés. 62

PHP *PHP Hypertext Preprocessor* por sus siglas en inglés. 56

PowerShell Lenguaje de programación e intérprete basados en la plataforma .NET, principalmente utilizado para automatización de tareas en Windows. 50, 51

Proxy Servidor que funge como intermediario en la conexión e intercambio de datos entre dos equipos. 26, 29, 48

RAID *Redundant Array of Independent Disks* por sus siglas en inglés. 12, 14–16, 39

RFC *Request for Comments* por sus siglas en inglés. 21, 27, 48, 56

Rollback Acción que deshace los cambios realizados. 44

RTOS *Real-Time Operating System* por sus siglas en inglés. 26

Ruby Lenguaje de programación de propósito general. Soporta múltiples paradigmas como funcional, imperativo y orientado a objetos. 44, 45

Script Programa escrito en un archivo de texto, que es leído y ejecutado por un intérprete. 40, 44, 45, 50, 51, 63

Shell Intérprete de comandos del sistema operativo. 17, 18, 29

Software Sistema operativo y programas instalados en un equipo de cómputo. 12, 17, 18, 24, 25, 31, 33, 37, 39, 53, 55, 56

SSH *Secure Shell* por sus siglas en inglés. 17, 29, 33, 54, 55

SSL *Secure Sockets Layer* por sus siglas en inglés, definido en el RFC 6101 [92].. 21, 22, 27, 46, 47, 58, 61, 62

Tarball Formato del archivo contenedor utilizado para almacenar paquetes de software. 18, 51

TB *TeraByte* - 1024^4 bytes = 1099511627776 bytes. 5, 11

TLS *Transport Layer Security* por sus siglas en inglés. 21, 22, 27, 58

URL *Uniform Resource Locator* por sus siglas en inglés. 36, 49, 50

VirtualHost Configuración de Apache HTTPD que logra diferenciar y aislar diferentes sitios web en un solo servidor físico. 46, 52

WebDAV *Web Distributed Authoring and Versioning* por sus siglas en inglés. 33, 36, 46, 48, 50, 51, 59–61, 63

Referencias

[1] rom vs ram. http://www.escotal.com/memory.html. Fecha de consulta: 2013-02-20. 3, 4

[2] P.K. Veenstra. *Random Access Memory: Testing and Practice*. Eindhoven University of Technology, October 1986. Fecha de consulta: 2013-02-20. 3

[3] ROM, EPROM, and EEPROM Technology - rom-eprom-eeprom-technology.pdf. http://web.eecs.umich.edu/~prabal/teaching/eecs373-f10/readings/rom-eprom-eeprom-technology.pdf. Fecha de consulta: 2013-02-20.
4

[4] FlashMemGuide.pdf. http://media.kingston.com/pdfs/FlashMemGuide.pdf. Fecha de consulta: 2013-02-20. 4

[5] ssd-faq-us.pdf. http://www.seagate.com/files/docs/pdf/ssd-faq-us.pdf. Fecha de consulta: 2013-02-20. 4

[6] Anatomy of Hard Disk Drives – A Deep Look into Hard Drives - TechNet Articles - United States (English) - TechNet Wiki.
http://social.technet.microsoft.com/wiki/contents/articles/13267.anatomy-of-hard-disk-drives-a-deep-look-into-hard-drives.aspx. Fecha de consulta: 2013-02-20.
5

[7] An illustrated Guide toZip, LS120, HiFD and MO-drives.
http://www.karbosguide.com/hardware/module4d.htm. Fecha de consulta: 2013-02-20. 5, 6

[8] An Introduction to Hard Disk Geometry | Tech Juice.
http://www.tech-juice.org/2011/08/08/an-introduction-to-hard-disk-geometry/. Fecha de consulta: 2013-02-20. 5

[9] PowerVault DAT Tape Media Details.
http://www.dell.com/us/enterprise/p/dell-dat-media/pd. Fecha de consulta: 2012-10-31. 5

[10] Further physics - The working principle of CD-ROM.
http://www.hk-phy.org/articles/cdrom/cdrom_e.html. Fecha de consulta: 2013-02-20. 6

[11] ODD SUPPORT.
http://www.samsungodd.com/eng/information/ODDTech/ODDTech.asp?No=5. Fecha de consulta: 2013-02-20. 7

[12] The World's First Movie Recording On a Preformatted Holographic Disc.
http://phys.org/pdf967.pdf, August 2004. Fecha de consulta: 2013-02-20. 7

[13] Samba - opening windows to a wider world. http://www.samba.org/. Fecha de consulta: 2013-01-09. 10

[14] BytePile.com - RAID Classifications. http://www.bytepile.com/raid_class.php. Fecha de consulta: 2012-11-28. 12

[15] RAID (redundant array of independent disks).
http://www.symantec.com/security_response/glossary/define.jsp?letter=r&word=raid-redundant-array-of-independent-disks. Fecha de consulta: 2013-01-15.
12

[16] Chapter 6. Redundant Array of Independent Disks (RAID) - Red Hat Customer Portal. https://access.redhat.com/knowledge/docs/en-US/Red_Hat_Enterprise_Linux/5/html/Deployment_Guide/ch-raid.html. Fecha de consulta: 2013-01-15. 12

[17] B. Smith and J. Hardin. *Linux Appliance Design: A Hands-On Guide to Building Linux Applications*. No Starch Press Series. No Starch Press, 2007. 17

[18] BitNami: The App Store for Server Software. http://bitnami.com/. Fecha de consulta: 2013-04-01. 18

[19] Why Build - Hardware Appliance Vendors. http://www.vmware.com/appliances/getting-started/build/hardware_vendors.html. Fecha de consulta: 2012-11-28. 18

[20] SANS: Information Security Resources. http://www.sans.org/information_security.php. Fecha de consulta: 2013-05-16. 18

[21] NIST SP 800-14, Generally Accepted Principles and Practices for Securing Information Technology Systems - 800-14.pdf. http://csrc.nist.gov/publications/nistpubs/800-14/800-14.pdf. Fecha de consulta: 2013-04-01. 18, 19

[22] Information Security Resource Center Basic Information Security Principles. http://www.oregon.gov/DAS/CIO/ISRC/pages/intro_basics.aspx. Fecha de consulta: 2013-04-01. 18, 19

[23] Criptografía - presentacion_seguridad_1.pdf. http://www.matem.unam.mx/rajsbaum/cursos/web/presentacion_seguridad_1.pdf. Fecha de consulta: 2016-02-02. 19

[24] PowerPoint Presentation - conceptos.pdf. http://delta.cs.cinvestav.mx/~francisco/cripto/conceptos.pdf. Fecha de consulta: 2016-02-02. 19

[25] des.pdf. http://www-math.ucdenver.edu/~wcherowi/courses/m5410/des.pdf. Fecha de consulta: 2016-02-02. 19, 20

[26] Scott G. Kelly <scott@hyperthought.com>. Security Implications of Using the Data Encryption Standard (DES). https://tools.ietf.org/html/rfc4772. Fecha de consulta: 2016-02-02. 19

[27] FIPS 46-3, Data Encryption Standard (DES) (withdrawn May 19, 2005) - fips46-3.pdf. http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf. Fecha de consulta: 2016-02-02. 20

[28] Microsoft Word - AES_wp_2012_09_22_v01.doc - aes-wp-2012-09-22-v01.pdf. https://software.intel.com/sites/default/files/article/165683/aes-wp-2012-09-22-v01.pdf. Fecha de consulta: 2016-02-02. 20

[29] GPU Gems 3 - Chapter 36. AES Encryption and Decryption on the GPU. http://http.developer.nvidia.com/GPUGems3/gpugems3_ch36.html. Fecha de consulta: 2016-02-02. 20

[30] Eric W. Weisstein. RSA Encryption. http://mathworld.wolfram.com/RSAEncryption.html. Fecha de consulta: 2016-02-02. 20

[31] Yevgeny.pdf. https://www.math.washington.edu/~morrow/336_09/papers/Yevgeny.pdf. Fecha de consulta: 2016-02-02. 20

[32] slides12.dvi - Lecture12.pdf. https://engineering.purdue.edu/kak/compsec/NewLectures/Lecture12.pdf. Fecha de consulta: 2016-02-02. 20

[33] SafeCurves: Fields. https://safecurves.cr.yp.to/field.html. Fecha de consulta: 2016-02-02. 20

[34] R. Rivest. The MD5 Message-Digest Algorithm. http://tools.ietf.org/html/rfc1321. Fecha de consulta: 2016-02-03. 21

[35] The People of the GnuPG Project. Weak Digest Algorithms — GnuPG.org. https://www.gnupg.org/faq/weak-digest-algos.html, November 2013. Fecha de consulta: 2016-02-03. 21

[36] Sean Turner <> and Tim Polk <>. Prohibiting Secure Sockets Layer (SSL) Version 2.0. http://tools.ietf.org/html/rfc6176. Fecha de consulta: 2016-02-10. 21

[37] Donald E. Eastlake 3rd and Paul E. Jones. US Secure Hash Algorithm 1 (SHA1). https://tools.ietf.org/html/rfc3174. Fecha de consulta: 2016-02-03. 21

[38] Tony Hansen and D. E. Eastlake 3rd. US Secure Hash Algorithms (SHA and HMAC-SHA). https://tools.ietf.org/html/rfc4634. Fecha de consulta: 2016-02-03. 21

[39] Keyless SSL: The Nitty Gritty Technical Details. http://blog.cloudflare.com/keyless-ssl-the-nitty-gritty-technical-details/. Fecha de consulta: 2016-01-27. 21

[40] Building your web of trust. https://www.gnupg.org/gph/en/manual/x547.html. Fecha de consulta: 2016-02-10. 21

[41] SampleSections.pdf. https://www.math.brown.edu/~jhs/MathCrypto/SampleSections.pdf. Fecha de consulta: 2016-02-04. 21

[42] Miriam Padilla. Buenas practicas para proteger datos confidenciales en las aseguradoras. http://meta-bidi.cichcu.unam.mx/ptd2009/junio/0645141/, 2009. Fecha de consulta: 2013-02-19. 22, 23

[43] BEAST.pdf. http://www.hit.bme.hu/~buttyan/courses/EIT-SEC/abib/04-TLS/BEAST.pdf. Fecha de consulta: 2016-02-10. 22, 58

[44] SSL ATTACKS - InfoSec Resources. http://resources.infosecinstitute.com/ssl-attacks/. Fecha de consulta: 2016-02-09. 22, 58

[45] Dan Goodin. Crack in Internet's foundation of trust allows HTTPS session hijacking. http://arstechnica.com/security/2012/09/crime-hijacks-https-sessions/, September 2012. Fecha de consulta: 2016-02-09. 22, 58

[46] BREACH ATTACK. http://breachattack.com/. Fecha de consulta: 2016-02-04. 22, 58

[47] This poodle bites: Exploiting the ssl 3.0 fallback. https://www.openssl.org/~bodo/ssl-poodle.pdf. Fecha de consulta: 2015-10-07. 22, 58, 61

[48] Heartbleed Bug. http://heartbleed.com/. Fecha de consulta: 2016-02-04. 22, 58

[49] Vulnerabilidad Heartbleed en OpenSSL | Boletines - UNAM-CERT -. http://www.cert.org.mx/boletin/?vulne=6487. Fecha de consulta: 2016-02-09. 23

[50] Tracking the FREAK Attack. https://freakattack.com/. Fecha de consulta: 2016-02-04. 23, 58

[51] The Linux Foundation - YouTube. http://www.youtube.com/user/TheLinuxFoundation?feature=watch. Fecha de consulta: 2013-05-29. 24

[52] About the GNU Operating System - GNU Project - Free Software Foundation. http://www.gnu.org/gnu/about-gnu.html. Fecha de consulta: 2013-05-20. 24

[53] Andrew S. Tanenbaum and Albert S. Woodhull. *Operating Systems Design and Implementation*. Prentice Hall, third edition, 2006. 24

[54] The Complete Concise History of GNU/Linux | All about Linux. http://www.aboutlinux.info/2005/11/complete-concise-history-of-gnulinux.html. Fecha de consulta: 2013-02-19. 24

[55] Staff | The Linux Foundation. http://www.linuxfoundation.org/about/staff#torvalds. Fecha de consulta: 2013-05-23. 24

[56] History of Linux.
http://web.archive.org/web/20060910125820/https://netfiles.uiuc.edu/rhasan/linux/. Fecha de consulta: 2013-05-23. 24

[57] LINUX's History by Linus Torvalds. http://www.cs.cmu.edu/~awb/linux.history.html. Fecha de consulta: 2013-05-23. 24

[58] Linux Foundation Video Site. http://video.linux.com/. Fecha de consulta: 2013-05-29. 24

[59] FHS - The Linux Foundation. https://wiki.linuxfoundation.org/en/FHS. Fecha de consulta: 2013-05-29. 25

[60] Filesystem Hierarchy Standard. http://www.pathname.com/fhs/. Fecha de consulta: 2013-05-29. 25

[61] LSBInitScripts - Debian Wiki. http://wiki.debian.org/LSBInitScripts. Fecha de consulta: 2013-05-29. 25

[62] LSBInitScripts/DependencyBasedBoot - Debian Wiki.
http://wiki.debian.org/LSBInitScripts/DependencyBasedBoot. Fecha de consulta: 2013-05-27. 25

[63] Gentoo Linux Documentation – Baselayout and OpenRC Migration Guide.
http://www.gentoo.org/doc/en/openrc-migration.xml. Fecha de consulta: 2013-05-27. 25

[64] OpenRC - ArchWiki. https://wiki.archlinux.org/index.php/OpenRC. Fecha de consulta: 2013-05-27. 25

[65] OpenRC - Debian Wiki. http://wiki.debian.org/OpenRC. Fecha de consulta: 2013-05-27. 25

[66] upstart - event-based init daemon. http://upstart.ubuntu.com/. Fecha de consulta: 2013-05-27. 25

[67] systemd - ArchWiki. https://wiki.archlinux.org/index.php/Systemd. Fecha de consulta: 2013-05-29. 25

[68] How Linux is Built | The Linux Foundation Video Site.
http://video.linux.com/videos/how-linux-is-built. Fecha de consulta: 2013-05-29. 25

[69] TIC. http://www.tic.unam.mx/kan-balam.html. Fecha de consulta: 2013-05-29. 26

[70] 94 Percent of the World's Top 500 Supercomputers Run Linux | Linux.com.
https://www.linux.com/news/enterprise/high-performance/147-high-performance/666669-94-percent-of-the-worlds-top-500-supercomputers-run-linux-/. Fecha de consulta: 2013-05-29. 26

[71] eLinux.org. http://elinux.org/Main_Page. Fecha de consulta: 2013-05-29. 26

[72] RTOS (Real-Time Operating System) and virtualization security software for embedded real-time systems from LynuxWorks, formerly Lynx Real-Time Systems.
http://www.lynuxworks.com/. Fecha de consulta: 2013-05-29. 26

[73] uClinux™ – Embedded Linux Microcontroller Project – Home Page.
http://www.uclinux.org/. Fecha de consulta: 2013-05-29. 26

[74] Router/Bridge Linux Firewall. http://www.zeroshell.org/. Fecha de consulta: 2013-05-29. 26

[75] Endian - Open Source Firewall Appliance - UTM Linux Security Distribution.
http://www.endian.com/en/community/overview/. Fecha de consulta: 2013-05-29. 26

[76] F5 Friday: What's Inside an F5? | F5 DevCentral.
https://devcentral.f5.com/blogs/us/f5-friday-what-rsquos-inside-an-f5#.UaWdGut-oy4. Fecha de consulta: 2013-05-29. 26

[77] Junos Network Operating System - Consistent Operating Environment - Juniper Networks.
http://www.juniper.net/us/en/products-services/nos/junos/. Fecha de consulta: 2013-05-29. 26

[78] Infoblox NIOS Security. http://www.infoblox.com/sites/infobloxcom/files/resources/infoblox-note-nios-security-implementation.pdf. 26

[79] OpenELEC Mediacenter - Home. http://openelec.tv/. Fecha de consulta: 2013-05-29. 26

[80] Android. http://www.android.com/. Fecha de consulta: 2013-05-29. 26

[81] Firefox OS - Mozilla | MDN. https://developer.mozilla.org/en/docs/Mozilla/Firefox_OS. Fecha de consulta: 2013-05-29. 26

[82] HP WebOS official website. http://www.hpwebos.com/us/. Fecha de consulta: 2013-05-29. 26

[83] Tizen | An open source, standards-based software platform for multiple device categories. https://www.tizen.org/. Fecha de consulta: 2013-05-29. 26

[84] maemo.org - maemo.org: Home of the Maemo community. http://maemo.org/. Fecha de consulta: 2013-05-29. 26

[85] Ubuntu for phones | Ubuntu. http://www.ubuntu.com/phone. Fecha de consulta: 2013-05-29. 26

[86] PS2 - LinuxMIPS. http://www.linux-mips.org/wiki/PS2#Running_Linux_on_the_Playstation_2. Fecha de consulta: 2013-05-29. 26

[87] Open Platform for PLAYSTATION®3. http://www.playstation.com/ps3-openplatform/index.html. Fecha de consulta: 2013-05-29. 26

[88] Debian – About Debian. http://www.debian.org/intro/about. Fecha de consulta: 2013-05-27. 26

[89] RFC 1945 - Hypertext Transfer Protocol – HTTP/1.0. http://tools.ietf.org/html/rfc1945. Fecha de consulta: 2013-04-01. 27

[90] RFC 2616 - Hypertext Transfer Protocol – HTTP/1.1. https://tools.ietf.org/html/rfc2616. Fecha de consulta: 2013-04-01. 27

[91] RFC 2818 - HTTP Over TLS. https://tools.ietf.org/html/rfc2818. Fecha de consulta: 2013-04-01. 27

[92] RFC 6101 - The Secure Sockets Layer (SSL) Protocol Version 3.0. http://tools.ietf.org/html/rfc6101. Fecha de consulta: 2013-04-01. 27

[93] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2. http://tools.ietf.org/html/rfc5246. Fecha de consulta: 2013-04-01. 27

[94] RFC 4918 - HTTP Extensions for Web Distributed Authoring and Versioning (WebDAV). https://tools.ietf.org/html/rfc4918. Fecha de consulta: 2013-04-01. 27, 48

[95] RFC 4511 - Lightweight Directory Access Protocol (LDAP): The Protocol. https://tools.ietf.org/html/rfc4511. Fecha de consulta: 2013-04-01. 27

[96] Appendix A: LDAP: DN and RDN. http://www.zytrax.com/books/ldap/apa/dn-rdn.html. Fecha de consulta: 2013-05-12. 28

[97] SSH, SSL, TLS. http://gwolf.org/files/pki/node9.html. Fecha de consulta: 2013-05-12. 29

[98] SoftwareRAID - Debian Wiki. http://wiki.debian.org/SoftwareRAID. Fecha de consulta: 2012-11-28. 39

[99] mount. http://manpages.debian.org/cgi-bin/man.cgi?manpath=Debian+7.0+wheezy&query=mount. Fecha de consulta: 2015-07-06. 40

[100] Read-only bind mounts [LWN.net]. https://lwn.net/Articles/281157/. Fecha de consulta: 2015-07-06. 40

[101] Karel Zak's blog: bind mounts, mtab and read-only. http://karelzak.blogspot.mx/2011/04/bind-mounts-mtab-and-read-only.html. Fecha de consulta: 2015-07-06. 40

[102] Change Root DN Password on OpenLDAP | The RoarinPenguin Techiezone. http://techiezone.rottigni.net/2011/12/change-root-dn-password-on-openldap/. Fecha de consulta: 2015-04-09. 43

[103] OpenLDAP Software 2.4 Administrator's Guide: Configuring slapd. http://www.openldap.org/doc/admin24/slapdconf2.html. Fecha de consulta: 2015-04-09. 43

[104] WebDav with Apache 2.2 - Simply won't work - Server Fault. http://serverfault.com/questions/478528/webdav-with-apache-2-2-simply-wont-work. Fecha de consulta: 2015-04-27. 48

[105] Fixing WebDAV support in MacOS X and on iPad. http://blog.toxa.de/archives/387. Fecha de consulta: 2016-04-27. 48

[106] Chief Oddball. Fix Slow WebDAV Performance in Windows 7. http://oddballupdate.com/2009/12/fix-slow-webdav-performance-in-windows-7/. Fecha de consulta: 2015-04-27. 48

[107] Slow response working with WebDAV resources on Windows Vista or Windows 7. http://support.microsoft.com/kb/2445570. Fecha de consulta: 2014-06-09. 48

[108] Using the WebDAV Redirector : The Official Microsoft IIS Site. https://www.iis.net/learn/publish/using-webdav/using-the-webdav-redirector. Fecha de consulta: 2015-04-27. 48

[109] Net use. https://technet.microsoft.com/en-us/library/gg651155.aspx. Fecha de consulta: 2015-12-30. 50

[110] Create a shortcut to (map) a network drive - Windows Help. http://windows.microsoft.com/en-us/windows/create-shortcut-map-network-drive. Fecha de consulta: 2015-12-30. 50

[111] Securing Debian Manual - Securing services running on your system. https://www.debian.org/doc/manuals/securing-debian-howto/ch-sec-services.en.html#s5.1. Fecha de consulta: 2016-01-28. 52, 54

[112] Center for Internet Security :: Security Benchmarks Division :: CIS Download Form. https://benchmarks.cisecurity.org/downloads/multiform/index.cfm. Fecha de consulta: 2016-01-27. 52

[113] SCG WS Apache - OWASP. https://www.owasp.org/index.php/SCG_WS_Apache. Fecha de consulta: 2016-02-02. 52, 56

[114] Configuration file reference. http://aptitude.alioth.debian.org/doc/en/ch02s05s05.html. Fecha de consulta: 2015-05-23. 53

[115] Debian GNU/Linux System Administrator's Manual (Obsolete Documentation) - Managing User Accounts. https://www.debian.org/doc/manuals/system-administrator/ch-sysadmin-users.html#s8.1.1. Fecha de consulta: 2016-01-06. 54

[116] crontab. http://manpages.debian.org/cgi-bin/man.cgi?manpath=Debian+7.0+wheezy&query=crontab. Fecha de consulta: 2016-01-06. 54

[117] at. http://manpages.debian.org/cgi-bin/man.cgi?manpath=Debian+7.0+wheezy&query=at. Fecha de consulta: 2016-01-06. 54

[118] Benchmarks Overview | Benchmarks | Center for Internet Security. http://benchmarks.cisecurity.org/downloads/benchmarks/index.cfm. Fecha de consulta: 2016-01-27. 54

[119] CIS_apache_http_server_2.2_benchmark_v3.3.1. https://benchmarks.cisecurity.org/tools2/apache/CIS_Apache_HTTP_Server_2.2_Benchmark_v3.3.1.pdf. Fecha de consulta: 2016-01-28. 56

[120] PHP Configuration Cheat Sheet - OWASP.
https://www.owasp.org/index.php/PHP_Configuration_Cheat_Sheet#PHP_error_handlling.
Fecha de consulta: 2016-01-28. 56

[121] core - Apache HTTP Server Version 2.2.
http://httpd.apache.org/docs/2.2/mod/core.html#limit. Fecha de consulta: 2016-01-06. 57

[122] CRIME against TLS? — Graceful Security.
https://www.gracefulsecurity.com/crime-against-tls/. Fecha de consulta: 2016-02-09. 58

[123] POODLE Attack and SSLv3 Deployment. https://poodle.io/. Fecha de consulta:
2016-02-04. 58

[124] SSL 3.0 Protocol Vulnerability and POODLE Attack | US-CERT.
https://www.us-cert.gov/ncas/alerts/TA14-290A. Fecha de consulta: 2015-10-07. 61

[125] This POODLE bites: exploiting the SSL 3.0 fallback.
https://googleonlinesecurity.blogspot.com/2014/10/this-poodle-bites-exploiting-ssl-30.html.
Fecha de consulta: 2015-10-07. 61

[126] Richard Barnes. The POODLE Attack and the End of SSL 3.0.
https://blog.mozilla.org/security/2014/10/14/the-poodle-attack-and-the-end-of-ssl-3-0/.
Fecha de consulta: 2015-10-07. 61

[127] Security Labs: SSL 3 is dead, killed by the POODLE attack.
https://community.qualys.com/blogs/securitylabs/2014/10/15/ssl-3-is-dead-killed-by-the-poodle-attack. Fecha de consulta: 2015-10-07.
61

[128] Security Labs: RC4 in TLS is Broken: Now What?
https://community.qualys.com/blogs/securitylabs/2013/03/19/rc4-in-tls-is-broken-now-what. Fecha de consulta: 2015-10-07.
61

[129] Forward secrecy.
https://en.wikipedia.org/w/index.php?title=Forward_secrecy&oldid=697804805, January
2016. Fecha de consulta: 2015-10-07. 61

[130] SSL Server Test: xnas.tonejito.org (Powered by Qualys SSL Labs).
https://www.ssllabs.com/ssltest/analyze.html. Fecha de consulta: 2015-10-07. 62