

DOCUMENTACIÓN FINAL

AUTORES

- José María Viúdez Parra
- José Antonio Cervantes Fernández
- Jorge Luis Pérez Martínez
- Karim El Bissari Dakdaki

ÍNDICE

Introducción

Escenario

UD1. Máquina IPFire.

1. Instalación y configuración de IPFire.

UD2. Máquina Ubuntu Server.

1. Instalación y configuración de Ubuntu Server.
2. Instalación Apache2.

UD 3. Máquina Debian.

1. Instalación y configuración de Debian.
2. Importación de scripts para las copias de seguridad

UD 4. Máquina Windows.

1. Instalación y configuración de Windows.
2. Instalación BitDefender.

UD 5. Máquina Lubuntu.

1. Instalación y configuración de Lubuntu.
2. Instalación Clamtk.

UD 6. Implantación de soluciones de seguridad física.

1. Informe sobre nuestra empresa.

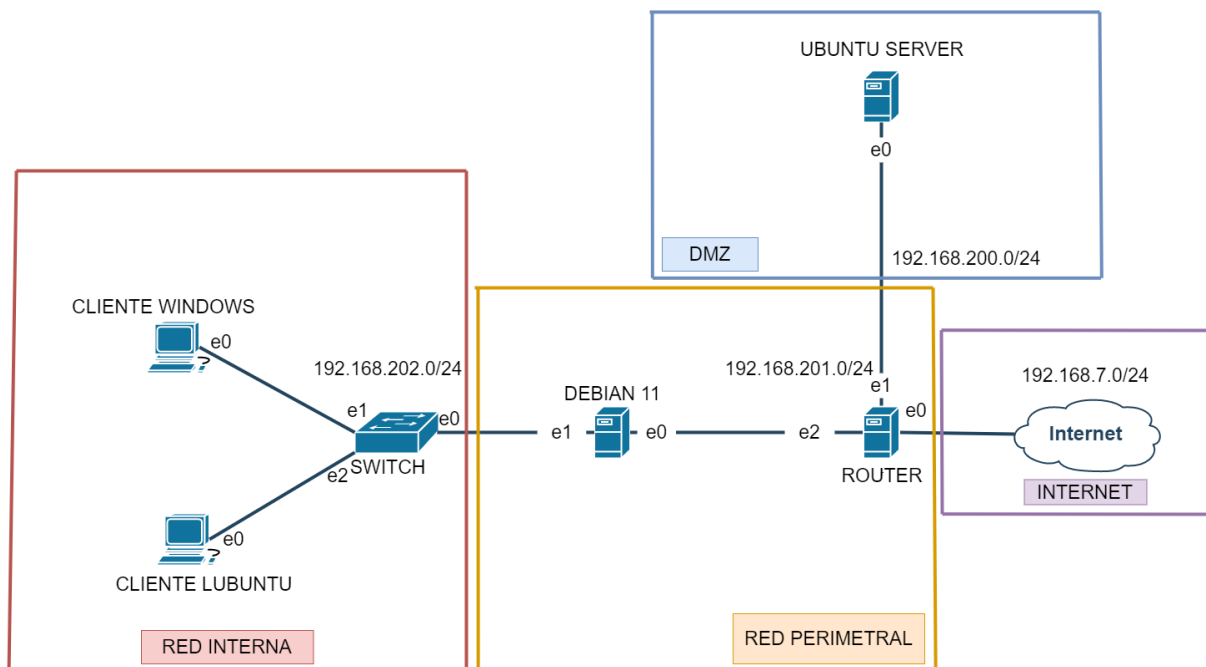
Conclusión

Introducción

Hoy llegó el gran día de juntar todo lo esencial de la asignatura de Seguridad y Alta Disponibilidad en un solo escenario y proyecto. A lo largo de todo este documento podremos ver y demostrar que todo lo que hemos hecho a lo largo de las prácticas anteriores han servido y sirven para algo. Para ello, qué mejor que en el proyecto final de la asignatura SAD. Aplicaremos lo aprendido y este documento servirá de ejemplo para configurar en una empresa o nuestra casa una red considerable y lista para el público.

Escenario

El escenario escogido ha sido el que aparece a continuación. Podemos ver como lo hemos preparado y está listo para ser usado y configurado.



UD1. Máquina IPFire

1. Instalación y configuración de IPFire

En la configuración tenemos que elegir la ISO de IPFIRE y seleccionar el sistema operativo Linux en versión Ubuntu 64 -bits.

Debemos tener tres adaptadores de red (porque en la configuración del IPFire en el tipo de configuración de red tendremos que elegir GREEN+RED+ORANGE).

Cuando arranquemos con la instalación, tenemos que definir el idioma, también debemos de definir el tipo de teclado, la zona horaria, el nombre del host de la máquina y el nombre del

dominio del sistema operativo. Después nos pedirá introducir una contraseña tanto para *root* como para *admin*

A continuación debemos seleccionar el tipo de configuración de red GREEN+RED+ORANGE, en la configuración de dirección es donde debemos seleccionar la interfaz que deseamos configurar;

- GREEN: e2 (Debian)
- RED: e0 (Internet)
- ORANGE: e1 (Ubuntu Server)

En cuanto completamos esto automáticamente se arrancará el sistema operativo con todas las configuraciones aplicadas.

UD2. Máquina Ubuntu Server

1. Instalación y configuración de Ubuntu Server

- Iniciamos la instalación y lo primero que nos aparece es la selección del idioma y la distribución del teclado.
- Después deberemos seleccionar la variante del servidor de Ubuntu donde tendremos que elegir el estándar *Ubuntu Server*. (Lo dejamos por defecto).
- A continuación configuraremos la red y proxy y configuraremos el espejo del archivo Ubuntu (Lo dejamos por defecto).
- Una vez hechos los anteriores pasos toca configurar el perfil donde pondremos el nombre, nombre de servidor, usuario y contraseña.
- Por último saldrá la configuración del SSH donde lo dejamos por defecto.
- Con esto completamos la instalación del Ubuntu Server.

2. Instalación Apache2

- Hemos instalado el servidor web Apache desde los repositorios de la propia distribución, por lo que los actualizamos (`sudo apt update`).
- E instalamos el paquete *apache2* con *apt* (`sudo apt install -y apache2`).
- Tras la descarga e instalación de este paquete y sus dependencias se crea un nuevo servicio en Ubuntu, el servicio *apache2* o *apache2.service* que queda iniciado y habilitado para su arranque automático junto al sistema.
- Podemos comprobar el estado del servicio Apache en cualquier momento con el comando `systemctl status apache2`.
- El servicio queda escuchando peticiones para el protocolo HTTP estándar en el puerto 80 TCP, como podemos comprobar con el comando `ss`.

UD3. Máquina Debian

1. Instalación y configuración Debian

- Iniciamos la instalación y lo primero que nos aparece es la selección del idioma y la distribución del teclado.

- Después deberemos establecer tanto la clave del superusuario (root) como el disco que se le asignará a dicho sistema operativo.
- Hecho esto, comenzará el proceso de instalación.
- Una vez se haya completado, configuraremos la red y comprobamos que haya internet en la máquina.
- Con esto completamos la instalación de Debian.

UD4. Máquina Windows

1. Instalación y configuración Windows

- Metemos la Iso y arrancamos la máquina
- Una vez arrancada la máquina elegimos el idioma y elegimos teclado
- A continuación deberemos poner un nombre a la máquina, nombre completo para el nuevo usuario, nombre de usuario para la cuenta e introducimos una contraseña
- Por último deberemos seleccionar el particionado de discos

2. Instalación BitDefender

Bitdefender Total Security es uno de los mejores antivirus que puedes adquirir: ofrece un diseño excelente y una protección increíblemente avanzada. Además, la VPN ha sido mejorada dramáticamente para cualquier sistema operativo.

Ventajas

- Protección antimalware: junto con Norton y Kaspersky, Bitdefender obtiene la máxima puntuación en las pruebas antimalware de AV-Test.
- Excelente VPN: Bitdefender ha hecho mejoras significativas en su VPN: es rápida, segura, con una política de cero registros y funciona con Netflix y torrents.
- Protección completa en Windows: ofrece protección antimalware, un gestor de contraseñas, protección web, un cortafuegos, una VPN, el navegador SafePay, protección de la cámara web y mucho más.
- Protección completa en Android: ofrece protección antimalware, protección web, una VPN, protección antirrobo, privacidad de cuentas, bloqueo de aplicaciones y mucho más.
- Excelente diseño en Windows y macOS: Bitdefender es tan avanzado como fácil de usar. Además, hay que decir que cuando el modo oscuro está activado, se ve genial.
- Navegador SafePay: Bitdefender incluye un navegador extraseguro para sus operaciones bancarias en línea, con un teclado virtual para protegerse de los keyloggers.
- Protección antirransomware: Bitdefender puede restaurar los archivos que los ataques de ransomware han cifrado.

- Herramientas antirrobo: en Windows y Android, puedes localizar, bloquear o borrar los datos de tus dispositivos de forma remota, algo que Norton no ofrece.
- Asequible: en comparación con la mayoría de los competidores, Bitdefender tiene un buen precio, lo que le confiere una excelente relación calidad-precio.

Desventajas

- Funciones limitadas en macOS: Bitdefender no ofrece un cortafuegos ni un gestor de contraseñas en Mac. Si esto es algo importante para ti, te recomendamos [Norton 360 Deluxe](#) para Mac.
- Gestor de contraseñas solo para Windows: al no ser compatible con Android, iOS o macOS, el gestor de contraseñas al final es un poco inútil.
- Controles parentales decepcionantes: no todas las funcionalidades que Bitdefender ofrece funcionan bien. De hecho, un adolescente algo inteligente podría burlar los controles parentales fácilmente.
- La VPN ilimitada tiene un coste adicional: la VPN de Bitdefender es excelente. No obstante, a diferencia de Norton y McAfee, no incluye su VPN de forma gratuita.

Para su instalación accederemos al siguiente enlace [Bitdefender Free Antivirus for Windows - Descarga de software](#)

UD5. Máquina Lubuntu

1. Instalación y configuración Lubuntu

- Metemos la Iso y arrancamos la máquina
- Una vez arrancada la máquina elegimos el idioma y elegimos teclado
- A continuación deberemos poner un nombre a la máquina, nombre completo para el nuevo usuario, nombre de usuario para la cuenta e introducimos una contraseña
- Por último deberemos seleccionar el particionado de discos

2. Instalación Clamtk

Diseño de la interfaz

El diseño de ClamTk es bastante simple, se dispone de una sola ventana en la que se diferencia un menú con las funciones comentadas, un panel de acciones donde se localizan en un botón las funciones más comunes en un escaneo, así como preferencias a seleccionar para un análisis. En el panel de estado muestra la versión del motor antivirus, versión de la interfaz, fecha de las últimas

definiciones de virus instaladas, fecha del último análisis realizado y último fichero infectado. Además para las versiones del motor antivirus, interfaz y últimas definiciones instaladas indica con una cruz roja si no está actualizado o con un tick verde si está al día. Por último al ejecutar un análisis se activa el panel analizar donde muestra el directorio o fichero analizándose actualmente, el progreso del escaneo, cantidad de archivos analizados y cantidad de virus encontrados. Se podrá cerrar este panel pulsando sobre la X de éste o con la opción Limpiar Salida.

Consumo de memoria

Para realizar una aproximación acerca del consumo de memoria de ClamTk habrá que diferenciar dos casos, si tan solo se ejecuta sin realizar ningún análisis o arrancamos un análisis que será el caso más interesante de estudio pues es cuando mayor carga soporta la aplicación. Tanto los datos de consumo como los de velocidad variarán atendiendo al número de directorios y ficheros que la aplicación tenga que escanear por lo que los datos aquí reflejados son meramente orientativos, en nuestro caso al empezar un análisis recursivo de nuestro home el consumo de memoria oscilaba entre 16'5 - 16'9 MB.

Velocidad de ejecución

La velocidad de ClamTk dependerá de diversos factores, como se ha comentado anteriormente variará atendiendo al número de directorio y ficheros a escanear además en momentos de carga máxima, mientras se está analizando varios directorios, la velocidad puede bajar significativamente, hasta el punto que la aplicación parece no responder durante varios segundos.

La aplicación es muy sencilla de usar, manejar e instalar. Además la facilidad de uso se incrementa gracias al diseño de aplicación que la hace muy intuitiva, pues está completamente integrada con GNOME.

Para su instalación podemos hacerlo desde la tienda de aplicaciones de lubuntu o desde el terminal.

UD6. Implantación de soluciones de seguridad física.

1. Informe sobre nuestra empresa.

Nuestro escenario podría mejorarse de muchas maneras, entre ellas destacaremos las siguientes:

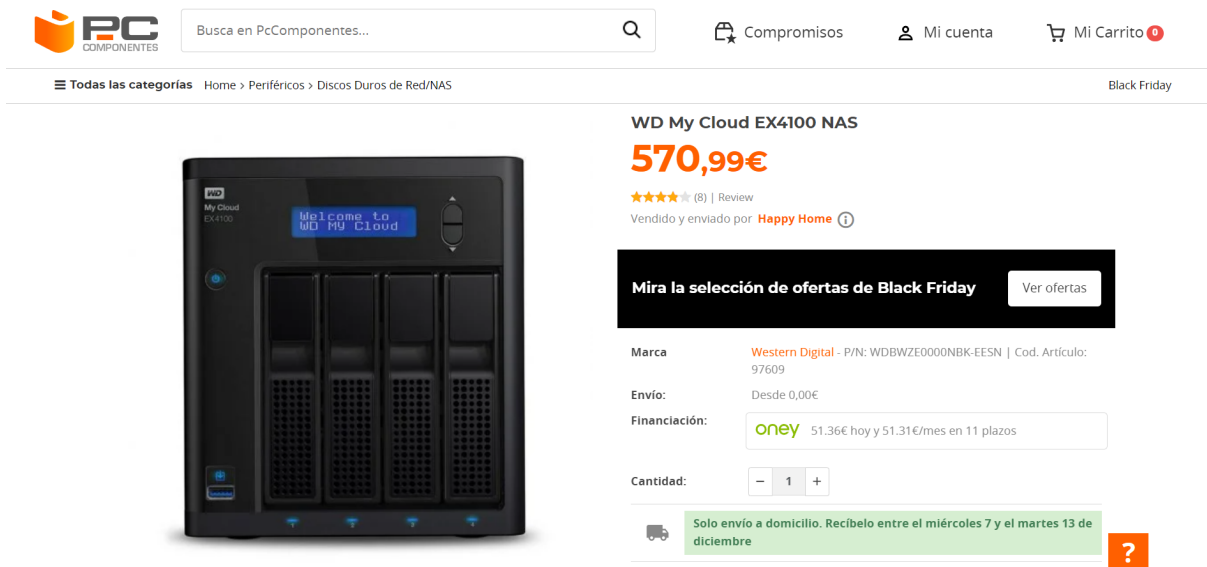
- Un Cisco ASA proporciona una seguridad aún mayor a la red. El Cisco ASA podría ser sustituido por el servidor Linux que actúa de firewall entre otros servicios más. En

caso de no querer sustituir el equipo Linux que actúa de firewall, el Cisco ASA podría ser puesto entre nuestro firewall y nuestro router estando la DMZ conectado a este. Esto nos proporciona una seguridad grandísima en la red, pero claro, el precio y coste sería mucho mayor. Un Cisco ASA vale en torno a los 600€ lo que es un gran desembolso teniendo en cuenta que las actualizaciones son costosas también. Aun así, es una de las mejores opciones. Habría que contactar con Cisco para poner un precio.

- Otra podría ser en lugar de un servidor único DMZ tener varios servidores o incluso varios servidores NAS donde repartir estos servicios. Un servidor NAS no es muy caro y estos podrían estar interconectados ofreciendo balanceo de carga. Los NAS dependen de lo que se quiera y según el volumen de datos que reciban podrían salir por menos de 500€ los dos, un precio muy apetecible por lo que ofrece a cambio.

Estos NAS podrían tener configurado unos RAID para en caso de pérdida de datos no sea algo catastrófico o crítico. Normalmente al comprar un NAS incluye ya de por sí varias bahías o incluso RAID 5 ya hechos.

Aquí podemos ver un NAS empresarial que además no es caro.



The screenshot shows the PCComponentes website interface. At the top, there's a search bar and navigation links like 'Compromisos', 'Mi cuenta', and 'Mi Carrito'. Below the navigation bar, the breadcrumb trail reads: 'Todas las categorías > Home > Periféricos > Discos Duros de Red/NAS'. The main product featured is the 'WD My Cloud EX4100 NAS'. The price is prominently displayed as 570,99€. Below the price, there's a star rating of 4.5 from 8 reviews. A banner indicates it's sold and shipped by 'Happy Home'. A Black Friday promotion banner says 'Mira la selección de ofertas de Black Friday' with a 'Ver ofertas' button. The product details section shows the brand 'Western Digital', P/N: WDBWZE0000NBK-EESN, and a code. Shipping is 'Desde 0,00€'. Financing options are provided by 'oney' with a monthly payment of 51.36€ today and 51.31€/mes in 11 installments. The quantity is set to 1. A green banner at the bottom states 'Solo envío a domicilio. Recíbelo entre el miércoles 7 y el martes 13 de diciembre'.

Un servidor en condiciones podría costar 4 veces más que este NAS, aunque claro, con las limitaciones que realmente podría ofrecer. En la siguiente imagen podemos ver una serie de servidores empresariales HP para rack de 2U. Vemos que el más barato comienza en 2.111€ siendo la configuración más básica (8GB de RAM, sin RAID con solo un disco duro SSD de 240GB y sin licencia de Windows Server que serían +1.000€ o "gratis" si escogemos alguna versión Linux).

CONFIGURAR TU SERVER


RESUMEN DEL SISTEMA

1.744,63 € excl. IVA

2.111,00 € incl. IVA

CONTINUAR →


1) SELECCIONAR UNA CARCASA




1.529 €




1.752 €



2.102 €




2.102 €



2.463 €

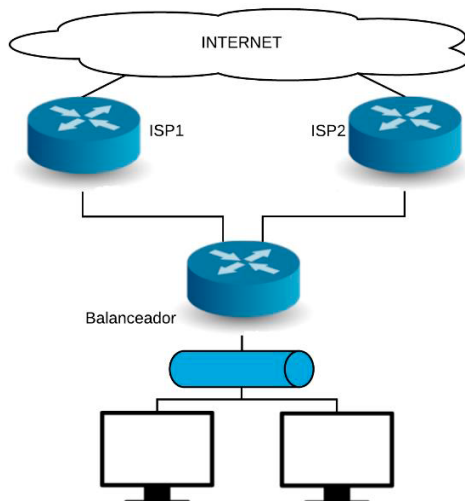


2.752 €



5.317 €

- Una configuración acompañante podría ser tener redundancia en la red con algún otro router para la salida a internet. Este router no tendría que ser tan potente como el principal y podría ser incluso un router cisco para mayor administración y facilidad de monitorización en la red. Un router cisco podría costar unos 500€ - 1.200€ dependiendo el modelo que se escoja y las funcionalidades que tenga. Habría que contactar con Cisco para ver qué solución extra podrían ofrecer también. Esto podría ir acompañado y beneficiándose totalmente del siguiente punto lo cual aumenta aún más la disponibilidad en la red.
- Otra medida podría ser tener un balanceo de carga con dos ISP para que en caso de



que falle uno el otro esté disponible o incluso para repartir el tráfico. Esto no es muy barato y más dependiendo de lo que necesitemos. Quizás esta medida es muy excesiva según la importancia del sector de la empresa o si la empresa no es muy grande y no puede afrontar gastos como estos. Habría que valorar cada detalle para saber si es necesario o no. Esto además conlleva otros costes extra como una tarjeta de red extra para nuestro router cisco lo cual no son baratas dependiendo del modelo. En el caso busque en la página de Cisco y no provee ninguna información remitiéndose siempre a llamarles o contactarnos por correo. Buscando en internet de forma externa la tarjeta de red más simple

y barata puede llegar a costar 200€ siendo de dos interfaces, algo que no es muy apetecible y barato.

- Para finalizar, pondría algún SAI potente para el servidor y los equipos. Podríamos optar por poner un SAI para cada dispositivo o un SAI potente tanto para el servidor firewall como para el de la DMZ (en nuestro caso, hemos elegido esta última opción). Este SAI podríamos programar un script que guarde y cierre todos los servicios antes de que se le acabe la batería.

El consumo de un servidor tiene distintos factores de por medio de los que depende. Depende de la potencia y del consumo también, pero por regla general un servidor puede llegar a consumir desde 180W a 220W de media.

Servidor con uso moderado

En este caso, el servidor es de gama media con un uso moderado que consume de media unos 180W. También contamos que está encendido unas 5 horas al día. Su monitor supone un consumo de 40W y, además, el usuario no apaga nunca la regleta.

Encendido: $22W \times 5 \text{ horas/días} = 1.1kWh$.

Apagado: $4W \times 19 \text{ horas/días} = 0.076kWh$.

Con esto, llegamos a la conclusión de que el equipo consume aproximadamente 1,176kWh al día. Al día nos cuesta 17 céntimos de euro tenerlo encendido; unos 62,24€ al año.

Servidor con uso constante

En este supuesto, disponemos de un equipo que cumplirá la función de servidor multimedia o HTPC equipado con una APU de bajo consumo y un único disco duro mecánico.

Además, no tiene monitor conectado porque se utiliza para almacenar archivos y vídeos a través de la red local, así que su consumo es simplemente ese.

Consumo total: $28W \times 24 \text{ horas/días} = 0.672kWh$.

Qué potencia de SAI necesito

Pongamos que hemos medido que cuando lo utilizamos al máximo rendimiento el consumo es de 300W. Lo ideal es que el SAI tenga una potencia de 400W, para así tener un margen por si hay más carga o tenemos más cosas conectadas. Pero, los SAI aparecen expresados en potencia aparente (VA). Entonces, ¿cómo sé que SAI debo comprar?

Con las fórmulas que hemos utilizado anteriormente en clase, podemos saber la potencia de SAI que necesitamos fácilmente. Es tan sencillo como dividir la potencia activa con el factor de potencia. La fórmula sería tal que así: $S=P/FP$.

Vale, no sabemos cuál es el factor de potencia y realmente no es necesario. La mayoría de SAI del mercado se mueven en un factor de potencia (FP) de entre 0.7 y 0.6. Lo ideal es optar por un factor de potencia conservador, siendo lo ideal elegir el valor de 0.6, para ir sobre seguro. Si elegimos un SAI de una marca conocida y confiable, podemos elegir el factor de potencia de 0.7. Cuidado, porque si elegimos un SAI chino de precio muy bajo, lo ideal es considerar un FP de tan solo 0.5.

Pues bien, para un consumo de 400W, cogiendo el factor de potencia de 0.6, nos da que el SAI debe ser de al menos 666.66VA. No hay SAI de esta potencia, así que elegiremos uno de 700VA.

Finalmente, he decidido incorporar un SAI para los dos servidores, por lo que el SAI que elegiremos será uno de entre 1400 y 1500VA. En mi opinión, los que aparecen debajo son las mejores opciones calidad-precio del mercado a día de hoy:

Ejemplo de SAI con hasta 20 minutos de duración, sin tener en cuenta la potencia consumida:



PC COMPONENTES

Busca en PcComponentes...

Compromisos Mi cuenta Mi Carrito

Todas las categorías Home > Periféricos > SAIS Black Friday

Talius POW1500 SAI 1500VA UPS

132,09€

★★★★★ (3) | Review

Vendido y enviado por **Futura Teck**

Otros vendedores 16

Mira la selección de ofertas de Black Friday Ver ofertas

Marca **Talius** - P/N: TAL-POW1500 | Cod. Artículo: 209676

Envío: Desde 0,00€

Financiación: **oney** 22.84€ hoy y 22.78€/mes en 5 plazos

Cantidad: - 1 +

Solo envío a domicilio. Recíbelo el lunes 28 de noviembre

Ejemplo de SAI que dispone de software de gestión y monitorización para cierre de ficheros y aplicaciones. Es gratuito y descargable desde www.salicru.com disponible tanto para Windows, como para Linux y Mac.



 Compromisos
  Mi cuenta
  Mi Carrito

Todas las categorías Home > Periféricos > SAIS Black Friday



Salicru SPS One 1500VA V2 SAI

137,92€ PVP 190,26€ DTO. -27%

★★★★★ (57) | Review

Vendido y enviado por **Infopavon**

Otros vendedores 37 desde 135.89€

Mira la selección de ofertas de Black Friday [Ver ofertas](#)

Marca: Salicru - P/N: 662AF000005 | Cod. Artículo: 259666

Envío: Desde 0,00€

Devolución: **Devolución GRATIS**




Financiación: **oney** 23.87€ hoy y 23.78€/mes en 5 plazos

Servicios disponibles: ☐ Extensión de garantía + 3 años **por 19,00€ + info**

Cantidad: - 1 + 

Ejemplo de SAI para meter en los racks de la empresa.



 Compromisos
  Mi cuenta
  Mi Carrito

Todas las categorías Home > Periféricos > SAIS Black Friday



Salicru SPS Advance RT2 SAI Line 1500VA

602,72€ PVP 642,87€ DTO. -6%

★★★★★ (3) | Review

Vendido y enviado por **Infopavon**

Otros vendedores 11 desde 594.37€


Mira la selección de ofertas de Black Friday [Ver ofertas](#)

Marca: Salicru - P/N: 6A0CA000003 | Cod. Artículo: 163013

Envío: Desde 0,00€

Devolución: **Devolución GRATIS**

Financiación: **oney** 54.34€ hoy y 54.15€/mes en 11 plazos

Cantidad: - 1 + 

 **Solo envío a domicilio. Recíbelo el lunes 28 de noviembre**

Conclusión

Por fin el final de un proyecto que me ha llevado a dedicarles unos días muy importantes. El proyecto me ha servido para calentar antes del gran proyecto de SRI. Gracias al proyecto de SAD llevado a cabo puedo decir que afianza totalmente los conocimientos aprendidos a lo largo del curso y puedo decir también tras haber llevado a cabo el proyecto y haberlo realizado que estoy contento conmigo mismo. Este proyecto fue distinto al realizado en 1ºASIR ya que al tener los conocimientos claros y saber lo que hacía he podido resolver problemas muy fácilmente (con el tema ACL, NAT o enrutamiento) o incluso en algunas

cosas no tener problemas. Realizar todo esto a lo largo del curso ayuda a que en el proyecto final se haga automáticamente casi sin fallos. Puedo decir que cada vez veo más el fin de la asignatura tras haber realizado el proyecto de SAD.