

— EMPRESA —

NAPOLÉS

Realizado por:

- Pedro Benítez Fuentes
- Alba Villanueva Oller
- José María Sánchez Haro
- Bruno Lorente Martínez



ÍNDICE

ANÁLISIS EMPRESA

3

SERVIDOR FTP

3

Instalación

3

Configuración

5

Permitir servidor FTP a través de Firewall

7

CRIPTOGRAFÍA

7

SEGURIDAD FÍSICA Y ALMACENAMIENTO

8

Sistemas de almacenamiento redundante

8

Planes de copias de seguridad

9

Seguridad física

10

SAI

10

POTENCIA

11

BATERÍA

11

PESO Y DIMENSIONES

12

VOLTIOS Y BATERÍAS

12

PUERTOS Y CONECTORES

12

INFORMACIÓN EXTRA

12

PRECIO

12

MALWARE

13

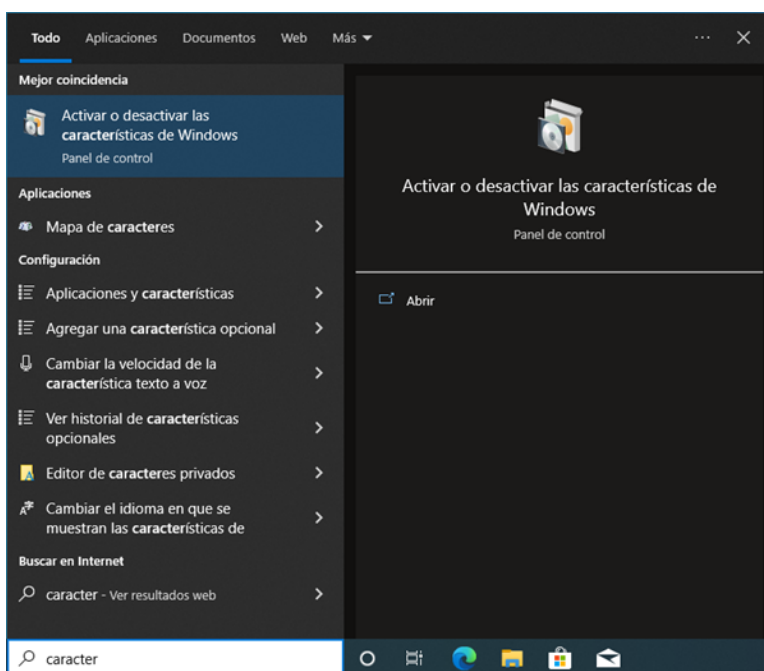
ANÁLISIS EMPRESA

Nuestra empresa ofrecerá un servicio ftp para que los usuarios de la red puedan disfrutar de subir archivos, como por ejemplo sus proyectos o ideas que tengan y quieran compartir con el resto de usuarios. Además, podrán descargar contenido del resto de usuarios. Aunque parezca que es una nube por sus funciones, el servidor no podrá ser utilizado como un sitio privado para guardar archivos personales.

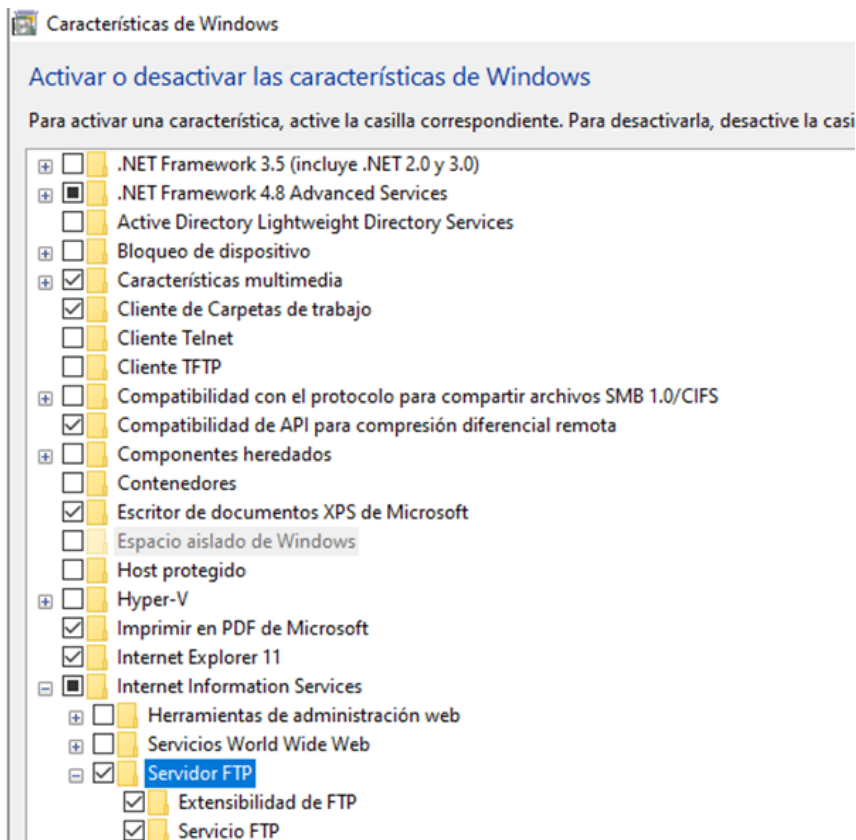
SERVIDOR FTP

Instalación

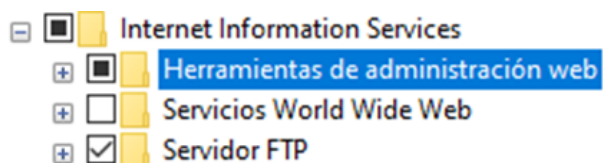
Buscamos activar y desactivar características de Windows.



Buscamos la característica de Internet Information Services y desplegamos las opciones, ahora marcamos servidor FTP y dentro de este activamos todas sus opciones.



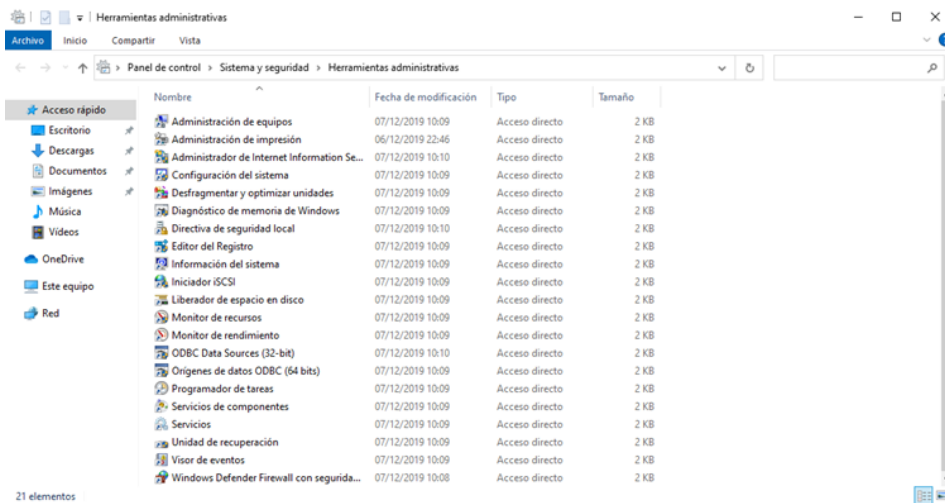
También activamos herramientas de administración web.



Le damos a aceptar y se instalarán ambas características.

Configuración

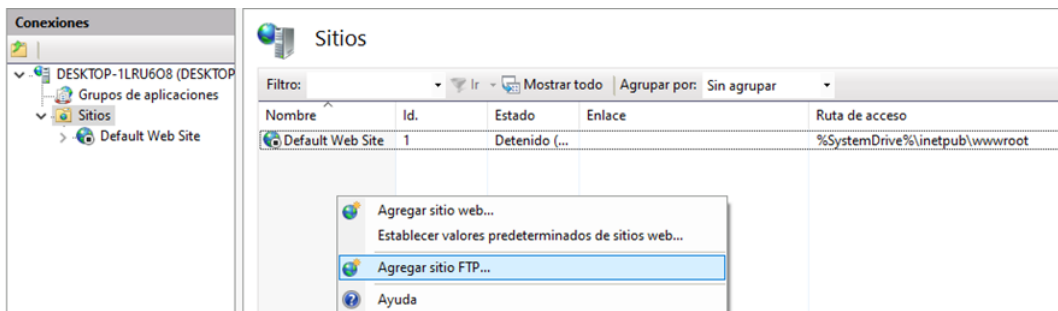
Abrimos Panel de control > Herramientas administrativas



Entramos en “Administrador de Internet Information Services (IIS)”.


| Nombre | Fecha de modificación | Tipo | Tamaño |
|--|-----------------------|----------------|--------|
| Administración de equipos | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Administración de impresión | 06/12/2019 22:46 | Acceso directo | 2 KB |
| Administrador de Internet Information Services (IIS) | 07/12/2019 10:10 | Acceso directo | 2 KB |
| Configuración del sistema | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Desfragmentar y optimizar unidades | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Diagnóstico de memoria de Windows | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Directiva de seguridad local | 07/12/2019 10:10 | Acceso directo | 2 KB |
| Editor del Registro | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Información del sistema | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Iniciador iSCSI | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Liberador de espacio en disco | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Monitor de recursos | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Monitor de rendimiento | 07/12/2019 10:09 | Acceso directo | 2 KB |
| ODBC Data Sources (32-bit) | 07/12/2019 10:10 | Acceso directo | 2 KB |
| Orígenes de datos ODBC (64 bits) | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Programador de tareas | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Servicios de componentes | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Servicios | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Unidad de recuperación | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Visor de eventos | 07/12/2019 10:09 | Acceso directo | 2 KB |
| Windows Defender Firewall con seguridad avanzada | 07/12/2019 10:08 | Acceso directo | 2 KB |

Le damos a Sitios > Agregar sitio FTP...



Asignamos nombre al sitio y definimos la carpeta que utilizaremos para enviar y recibir archivos.

Agregar sitio FTP ? X

 **Información del sitio**


Nombre del sitio FTP:

Directorio de contenido
Ruta de acceso física:
 ...

Anterior Siguiente Finalizar Cancelar

Siguiente y ahora configuración de enlace y SSL (Hay que señalar que en un ambiente de negocios o en un servidor FTP que será el anfitrión de los datos sensibles, se recomienda configurar el sitio para requerir SSL).

Agregar sitio FTP ? X

 **Configuración de enlaces y SSL**

Enlace

Dirección IP: Puerto:

☐ Habilitar nombres de host virtuales:
Host virtual (ejemplo: ftp.contoso.com):

☒ Iniciar sitio FTP automáticamente

SSL

☒ Sin SSL
☐ Permitir SSL
☐ Requerir SSL

Certificado SSL:
 Seleccionar... Ver...

Anterior Siguiente Finalizar Cancelar

Agregamos la información de autenticación y autorización.

The screenshot shows a Windows-style dialog box titled 'Agregar sitio FTP' with a globe icon. The main section is titled 'Información de autenticación y autorización'. It contains three sections: 'Autenticación' with checkboxes for 'Anónima' (unchecked) and 'Básica' (checked); 'Autorización' with a dropdown menu set to 'Usuarios especificados' and a text box containing 'empresa.ftp.napoles@gmail.com'; and 'Permisos' with checkboxes for 'Leer' (checked) and 'Escribir' (checked). At the bottom are buttons for 'Anterior', 'Siguiente', 'Finalizar' (highlighted with a blue border), and 'Cancelar'.

Permitir servidor FTP a través de Firewall

Entramos al Firewall > Permitir aplicación o característica > Cambiar configuración> Buscamos servidor FTP, marcamos y activamos privada y pública.



CRIPTOGRAFÍA

Guardaremos las copias de seguridad de los datos de los usuarios y toda la información en una base de datos fuera de la DMZ.

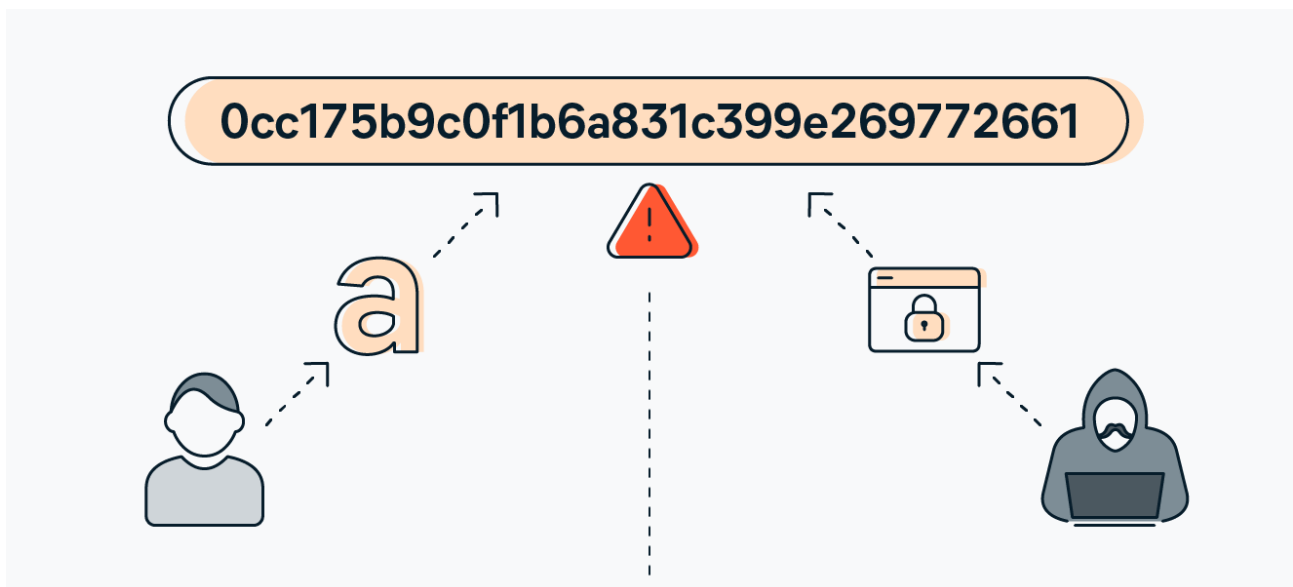
Necesitaremos encriptar las copias de seguridad del servidor, ya que hay información de todos los datos de nuestros clientes, por lo tanto, tenemos que protegerlos por ley y para darles mayor seguridad con nuestro servidor. Para esta encriptación usaremos el programa “Acero Docs”.

Además, encriptaremos todas las contraseñas de los usuarios con el fin de preservar su seguridad. Para ello utilizaremos un cifrado MD5.

Este tipo de cifrado es solo de un único sentido, por lo tanto, no podemos descriptar el contenido una vez encriptado. La validación también debe hacerse en MD5, es decir, tenemos que convertir las dos cadenas a MD5 y realizar la validación.

Como en la base de datos se guarda la contraseña encriptada, cuando un usuario quiere acceder, habrá que realizar una comparación entre la contraseña que introduce encriptado en MD5, y la que tenemos en la base de datos (que es la contraseña encriptada en MD5), si coincide se le permite el acceso, si no, se rechaza.

MD5 se utiliza también para que cuando un usuario olvida su contraseña, si quiere recuperarla, debe introducir el correo electrónico, por ejemplo, y se le envía un mail con una URL, tal que si entra en ella genere una nueva contraseña que se le indica al usuario y se reescribe en MD5 en la base de datos.



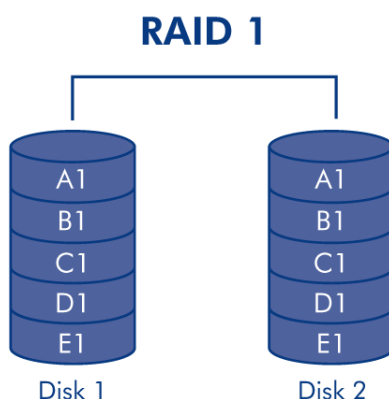
SEGURIDAD FÍSICA Y ALMACENAMIENTO

Sistemas de almacenamiento redundante

El sistema de almacenamiento redundante que utilizaremos será el RAID 1, en otras palabras, tipo espejo.

Necesitaremos dos discos para poder duplicar los datos y tenerlos en ambos. De esta manera, si el disco principal se estropea tendremos el segundo para poder trabajar con él sin problemas.

Para asegurarnos de que tenemos los mismos datos en ambos discos, se realizarán copias de seguridad periódicas.



Planes de copias de seguridad

Vamos a realizar copias de seguridad tanto completas e incrementales, de forma que nuestro servidor cuente siempre con un respaldo que nos permitirá, en caso de emergencia, recuperar todos los datos.

Las copias de seguridad serán realizadas, mediante crontab, de la siguiente manera:

- Se realizarán copias completas el día 1 de cada mes a las 03:00
- También se realizarán copias incrementales todos los días a las 03:00

De esta forma, todos los meses crearemos la copia completa, para tener un respaldo total de toda la información.

Hemos decidido realizar copias incrementales en vez de copias diferenciales ya que estas son más ligeras de hacerse y requieren menos espacio. Aunque son más lentas a la hora de restaurar, nos proporcionará la garantía de que no perderemos ningún tipo de dato.



Seguridad física

La base de datos donde se guardarán todos los datos del servidor ftp y dicho servidor se encontrarán en una habitación aparte cada uno donde sólo podrán acceder el personal autorizado que se encargará de la administración.

Dicho personal podrá entrar en la habitación mediante sistemas biométricos, como la huella digital y la identificación mediante el iris, aunque tendrá a parte una contraseña manual por si hay algún tipo de fallo con las otras formas de acceso.

Junto con ellos habrá un SAI por seguridad física, un aire acondicionado 24 horas a temperatura entre 21 y 23 grados centígrados, además de estar en sobre altura para evitar cualquier problema en caso de que haya alguna inundación.

SAI

Se han seleccionado los SAIs teniendo en cuenta las necesidades de la empresa.

Los servidores estarán conectados a la corriente 24/7 todo el año y, por lo tanto, haciendo un gasto estimado de lo que se consume por cada uno, son 1800 KWh aproximadamente.

Se debe poner uno en cada una de las zonas donde se encuentra cada servidor, de tal forma que serán SAIs independientes uno del otro.

En base a esto, se ha seleccionado un SAI.

V7UPS1RM2U3000-1E



[Enlace de compra en Amazon](#)

[Enlace de compra en CCLonline](#)

POTENCIA

El SAI seleccionado es el V7 UPS1RM2U3000-1E, el cual tiene una potencia de 3000VA. Por esto, podremos conectar un servidor a cada uno y dejaremos un margen por si necesitamos colocar algún equipo extra en un futuro, y ya estaríamos preparados para solo conectarlo y no gastar mucho más dinero.

BATERÍA

El SAI tiene un tiempo de carga de batería de 4 horas aproximadamente.

PESO Y DIMENSIONES

- Peso: 29.3 Kg
- Dimensiones: 43.8 x 63 x 8.8 centímetros.

VOLTIOS Y BATERÍAS

12 voltios, requiere 6 baterías de 12V.

PUERTOS Y CONECTORES

Posee los siguientes puertos:

- 1 recuento de procesos
- 1 puerto USB 2.0 Ports
- 1 puerto Ethernet
- 8 conectores para equipos

INFORMACIÓN EXTRA

- UPS de montaje en rack de 3000 VA con salida de onda sinusoidal pura con 8 salidas IEC.
- ECO para operación de ahorro de energía.
- Función EPO
- Señales de advertencia acústicas y visuales para problemas con la batería, el nivel de carga y otros problemas
- Los zócalos programables maximizan el tiempo de respaldo para los sistemas críticos al establecer tiempos de respaldo más cortos para los sistemas no críticos.

PRECIO

Precio aproximado de 400€.

MALWARE

En nuestro servidor y empresa necesitaremos un antivirus para que nos proteja ante posibles ataques y tanto nuestros clientes como los empleados, puedan estar seguros. Por todo esto, hemos decidido instalar y aplicar la aplicación de "Trend Micro Server Protect", ya que, en relación calidad-precio, es de los mejores.

Ofrece lo siguiente:

- Protección frente a malware fiable y eficiente
- Cuenta con un motor de análisis de tecnología galardonada y con un extenso historial de protección completa frente al malware
- Combina tecnologías de reconocimiento de patrones con tecnologías basadas en reglas para detectar eficazmente el malware
- Incluye API nuevas para detectar y limpiar mejor spyware y rootkit
- Protege los canales de comunicación interna para evitar los trastornos que ocasiona el malware
- Ofrece asistencia anti-malware ininterrumpida por parte de los científicos de datos e investigadores de amenazas globales de Trend Micro Research
- Exploraciones automatizadas para la optimización de la protección
- Permite personalizar por tarea para cumplir con las necesidades de flujos de trabajo específicos en lo concerniente al análisis en tiempo real, ad-hoc y programado, además de despliegue, registro y estadísticas
- Descompone las tareas de exploración programadas para analizar los directorios más utilizados con una frecuencia diferente a la de los directorios menos usados
- Reduce el impacto sobre los recursos al permitir el análisis de tráfico y la creación de políticas de RTS personalizadas para las diferentes horas del día
- Implementación y gestión centralizadas
- Agiliza la implementación inicial y la gestión en curso de los principales servidores de Microsoft® Windows® y Novel® NetWare®
- Gestiona de forma centralizada la supervisión del sistema, las actualizaciones de software, los cambios de configuración y los informes sobre eventos mediante una consola remota
- Controla varios servidores de información de ServerProtect e implementa actualizaciones producto en todos los servidores desde una única consola
- Despliega programas y actualizaciones en varios servidores simultáneamente y supervisa el estado del servidor en tiempo real
- Gestiona de forma centralizada las estrategias de seguridad que se han implementado en una red de varios sitios
- Funciones de protección y limpieza inmediatas

- Elimina restos de malware de todos los servidores mediante limpieza y reparación automatizada de malware para minimizar la reinfección
- Analiza y limpia los archivos comprimidos de malware evitando así una descompresión innecesaria
- Gracias a la función de análisis de vulnerabilidades (disponible si la solicita), identifica los fallos del sistema de seguridad

