

Carlos del Cerro, Óscar Ramírez y David Burgos

# Índice

- 1. Introducción
  - Empresa Code Or Digit
  - Equipo COD
  - Asignaturas y tecnologías
  - Metodología ágil
- 2. Implantación y configuración de servidores
- 3. Implantación y configuración de Raspberry Pi
  - Conexión remota a las Raspberrys con Putty
  - Administración (cron, tar, instalación de paquetes)
  - Configuración de la red /etc/host
- 4. Conexiones remotas
- 5. Administración de los servidores (Active Directory y Samba)
- 6. Red Esquema de red
- 7. Packet Tracer
- 8. Instalación de servicios de red
- 9. Implantación de las BBDD
- 10. Cluster entre las Raspberrys
- 11. Seguridad en el proyecto
- 12. Plan de contingencias
- 13. Copias y restauración de los equipos
- 14. Configuración del proxy
- 15. Implantación web
  - Creación formulario de entrada (HTML, CSS, PHP, MySQL)
  - Instalación de paquetes PHP y MySQL en las Raspberrys
- 16. CRUD
  - CMS con Wordpress
  - Implantación final de Blog redireccionado.
- 17. Auditoría de las máquinas
- 18. Auditoría web de nuestro sitio COD

# Introducción

La empresa Pother (Project on the rack) ha solicitado los servicios a nuestra empresa COD para poner en marcha el proyecto Project On The Rack. El proyecto se realizará en la UEM en el campus de Villaviciosa, concretamente el proyecto estará en el aula C308 y desde ahí se dará el servicio.



Nosotros les ofreceremos las soluciones hardware y software para resolver este supuesto que nos plantean y resolver así el supuesto que nos plantean. Este proyecto tendrá como objetivos principales:

- Poner a punto los servidores.
- Instalar, configurar y administrar los SO.
- Configurar las Raspberrys.
- Instalar, configurar y administrar la BBDD.

- Creación de un portal que dará servicio de entrada a los CMS de Wordpress.
- Implantar un cluster de alta disponibilidad.
- Implantar seguridad física y lógica.
- Realizar auditoria del proyecto.
- Usar las tecnologías utilizadas en clase.
- Dar seguridad a los sistemas que pondremos en marcha.

# Empresa Code Or Digit

Somos una empresa de consultoría y soporte IT que da soluciones a PYMES fundada en Enero de 2017. Queremos satisfacer las necesidades que el mercado tecnológico demanda en la actualidad, aportando soluciones tanto software como hardware.

Utilizamos las tecnologías más avanzadas, aportamos personas idóneas para cada proyecto y con un alto nivel de cualificación.

Nuestro portfolio de actividades abarca desde:

- Mantenimiento y soporte tecnológico.
- Gestión de aplicaciones y desarrollo del software.
- Análisis y Diseño de soluciones.

El conocimiento de nuestros técnicos abarca las principales entornos tecnológicos utilizados en el mercado: Bases de datos (Oracle, SQL Server, MySQL), Lenguajes de Programación (Javascript, PHP, HTML, CSS, XML, Scripting), Aplicaciones de gestión empresarial.

Para ello basamos nuestra metodología en 4 pilares fundamentales:

- -Trabajo en Equipo
- -Cercanía
- -Proactividad
- -Flexibilidad



# Miembros del equipo COD

El equipo asignado para realizar el proyecto Pother es el equipo de técnicos COD está formado por tres alumnos de 2º Administración de Sistemas Informáticos en Red, los cuales, darán una solución al proyecto integrador Project On The Rack.

Carlos del Cerro Tenorio Óscar Ramírez David Burgos

# Asignaturas que engloban el proyecto

- Administración de Sistemas Operativos
- Servicios de Red e Internet
- Seguridad y Alta Disponibilidad
- Implantación de Aplicaciones Web
- Sistemas Gestores de Bases de Datos

# Tecnologías utilizadas

- Servidores Rack, sobremesa y Raspberrys.
- Sistemas operativos Windows y Linux.

- Equipos y material de red (switchs, routers, cableado, ...).
- Software HTTP, FTP, proxy...
- Software opensource para la implantación del sistema y desarrollo de la aplicación web.
- HTML, CSS, Javascript y PHP.
- MySQL y DIA.
- Software de clonezilla para la implantación de la maquetas de los equipos por red y equipo a equipo.
- Aplicación web kanban https://waffle.io .

# Metodología ágil

Para ser buenos gestores de nuestro proyecto integrador utilizaremos los métodos y técnicas ágiles como Scrum o Kanban (popularizada en Japón). Esta metodología de post-it que se mueven en un tablero es de gran ayuda para el trabajo en equipo. Nosotros utilizaremos Waffle que es una herramienta que está enlazada con GitHub para proyectos software. Para ello crearemos un tablero donde el responsable o Scrum Master pondrá las tareas e irá actualizando el tablero. Un buen Scrum Master necesita saber cómo integrar estos métodos dentro de su proceso de desarrollo en el equipo COD para el buen resultado del proyecto integrador. Algunos miembros del equipo trabajamos el año pasado con una herramienta llamada Trello para realizar el proyecto integrador Star Walls de 1ºASIR.



# Implantación y configuración de servidores

Lo primero que haremos será realizar un inventario de los servidores que tenemos disponibles para realizar el proyecto. Para ello instalaremos Ubuntu en los

servidores y una vez hecho esto, entraremos en el terminal de comandos. Realizaremos un inventariado con el comando "Ishw" podremos ver todos los componentes conectados al equipo, pero a esto se le puede añadir el parámetro "-hml", lo que hará que el inventariado del equipo se muestre en código HTML para así poder verlo desde un navegador con un mejor diseño, además, hay que indicar en que se quiere exportar a un archivo .html.

Así que el comando utilizado para inventariar el servidor ubuntu fue **lshw -html > invent.html**.

id:	ubuntu
descripción:	Chasis de montaje rack
producto:	Precision WorkStation R5400 ()
fabricante:	Dell Inc.
serie:	8PPQX4J
anchura:	64 bits
capacidades:	smbios-2.5 dmi-2.5 vsyscall32

(Todos los inventariados los tenemos en el anexo de inventarios).

# STARK (NAS)

# Instalación Ubuntu 16.04 Server.

Inventario Stark

Seleccionamos lenguaje y comenzamos la instalación de Ubuntu Server 14.04.

	Lar	nguage	#
Amharic	Français	Македонски	Tamil
Arabic	Gaeilge	Malayalam	0 0383
Asturianu	Galego	Marathi	Thai
Беларуская	Gujarati	Burmese	Tagalog
Български	עברית	Nepali	Türkçe
Bengali	Hindi	Nederlands	Uyghur
Tibetan	Hrvatski	Norsk bokmål	Українська
Bosanski	Magyar	Norsk nynorsk	Tiếng Việt
Català	Bahasa Indonesia	Punjabi (Gurmukhi)	中文(简体)
Čeština	Íslenska	Polski	中文(繁體)
Dansk	Italiano	Português do Brasil	
Deutsch	日本語	Português	
Dzongkha	ქართული	Română	
Ελληνικά	Қазақ	Русский	
English	Khmer	Sámegillii	
Esperanto	ಕನ್ನಡ	ສົ•ກຣ	
Español	한국어	Slovenčina	
Eesti	Kurdî	Slovenščina	
Euskana	Lao	Shaip	
يس اف	Lietuviškai	Српски	
Suomi	Latviski	Svenska	

Podemos ver el Asistente Gráfico de Ubuntu Server 14.04 (GUI, Graphical User Interface).



A continuación, elegimos el idioma que vamos a usar, la ubicación del teclado y a continuación nos detectará el HW.



Ponemos un nombre a la máquina y registramos un usuario. Durante la instalación tendrás que introducir una clave para el usuario (recomendado al menos 8 caracteres incluyendo números y letras). Podemos además cifrar nuestra carpeta personal. Y comenzaría la instalación del SO propiamente dicho.

	Instalando el sistema	
	22%	
Copiando datos a disco	•••	

Nos pregunta si necesitamos un proxy, en nuestro caso se queda en blanco. Comienza la instalación de los programas y aplicaciones. De primeras le decimos que no queremos actualizaciones. Seleccionamos otros programas si queremos instalarlos. Lo hacemos pulsando la barra espaciadora y presionamos continuar. Para configurar el sitio de correo seleccionamos Sitio de Internet. Instala además el gestor de arranque GRUB.

Ya tenemos la instalación completa, solo debemos retirar la iso del arranque y podremos entrar a nuestro nuevo SO Ubuntu Server 14.04.



LANNISTER

En este servidor configuraremos el proxy. Después de buscar una solución al problema con el servidor, instalaremos un sistema en una raspberry e instalaremos squid para que haga de servidor proxy.

La raspberry utiliza Ubuntu 14.04. Crearemos el usuario llamado lannister, después añadiremos el usuario lannister al grupo sudoers y modificamos el usuario por defecto. Una vez hecho esto descargamos Squid3 y editaremos el archivo /etc/network/interfaces y asignaremos la ip fija 192.168.1.2 para la interfaz de red eth0. Editamos el archivo /etc/hostname cambiando el nombre por defecto por lannister y por último haremos un apt-get update para actualizar nuestro sistema.

Además hemos modificado la distribución del teclado de inglés a español.

# TARGARYEN

# Instalación Windows Server 2012 en una de las máquinas compartidas en el rack para Active Directory

Seleccionamos la imagen (iso que hemos descargado previamente) y arrancamos la máquina desde donde la tengamos.

Loading files...

Seleccionamos leguaje, hora y teclado para posteriormente introducir la clave de activación del producto.

-0	Windows Setup	0.6	Windows Setup	0.0
	Windows Server 2012 R2		H Windows Server 2012 R2	2
	Language to install English (United States)	-		
	Imme and cummery formate Spanish (Spain, International Sort)			
39	(ayboard or input method and a second and a se		Install now	
	Enter your language and other preferences and click "Next" to continu	<b>9</b> 2		
e data Mer	and Engenders All spits manual	Not		

Elegimos Server con entorno gráfico (GUI, Graphical User Interface).

A continuación, aceptamos los términos de la licencia.

Operating system	Architecture	Date modified
Windows Server 2012 R2 Standard (Server Core Installation)	хб4	3/18/2014
Windows Server 2012 K2 Standard (Server with a GUI)	X04	3/18/2014
escription:	ovide hackward	romnatibility for an
scription:		14 Mar - 1

Seleccionamos dónde vamos a instalar el SO y comienza la instalación del mismo.

🖉 Windows Setup				📫 🙀 Windows Setup	101.30
Where do you	want to install Wi	ndows?		Installing Windows	
Neme	1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 - 1990 -	Total vice	The space Type	Your computer will restart several times. This might take a while	
Drive O Une	Hocated Space	40.0 08	40.0 08	Copyling Windows Files (190%) Senting fract works for installation Installing fractions Installing lightnes Finishing up	
fy Beliush Di Louet driver	X Orlens Di Esterni	Hornal	é hipe		
				ljest	

Durante la instalación tendrás que introducir una clave de Administrador (al menos 8 caracteres incluyendo números y letras).

Setting	js	*	Press Ctrl+Alt+Delete to sign in.
Type a password for t	he built-in administrator account that y	ou can use to sign in	
User name	Administration		
Password			22:09
Reenter password		*	miércoles, 21 de septiembre
			6 A

Con esto ya tendríamos la instalación completada y nuestro SO listo para empezar a trabajar con él.

Esta es la apariencia que tiene nuestro escritorio al entrar por primera vez a Windows Server 2012 R2. Salta directamente el Server Manager.

		Server Manager
€⊙ - Serve	er Manager 🔸 Dash	board
Dashboard	WELCOME TO SERV	ER MANAGER
All Servers	₽3	1 Configure this local serve
	QUICK START	2 Add roles and features
		3 Add other servers to manag
	WHAT'S NEW	4 Create a server group
	LEARN MORE	
	ROLES AND SERVER Roles: 0   Server group	s; 1   Servers total: 1
	Local Serve	r 1 All Servers
	Manageabilit Events	y Manageability Events
	Services	Services

# RASPBERRY PI



# Documentación Raspberry Pi Lite COD 2

Hardware

Procesador:

- Chipset Broadcom BCM2387.
- 1,2 GHz de cuatro núcleos ARM Cortex-A53 GPU

Conectividad

- Ethernet
- Salidas
  - HDMI
  - RCA
  - jack de 3,5 mm de salida de audio, HDMI
  - USB 4 x Conector USB 2.0
- Ranura de tarjeta de memoria SDIO

Sistemas Init User: Pi Password: Raspberry

Nuevo user y contraseña: "cod2" "doc" Damos todos los permisos al nuevo user con "usermod -g sudo cod"

#### Documentación Raspberry Pi Pixel COD 1

Hardware

Procesador:

• Chipset Broadcom BCM2387.

• 1,2 GHz de cuatro núcleos ARM Cortex-A53 GPU Conectividad

- Ethernet
- Salidas
  - HDMI
  - RCA
  - jack de 3,5 mm de salida de audio, HDMI
  - USB 4 x Conector USB 2.0
- Ranura de tarjeta de memoria Micro SDIO

# Sistemas

Instalación de los sistemas Lite y Pixel, con los que probaremos versión TUI y GUI. Después dejaremos en las dos Raspberrys solamente el entorno en modo texto. Estos sistemas operativos están basados en la distribución Debian 8 Jessie.

Seguiremos los siguientes pasos:

- 1. Descargar SO en nuestro PC desde https://www.raspberrypi.org/downloads/raspbian/
- 2. Insertamos o conectamos la tarjeta SD en nuestro PC
- 3. Descomprimimos el SO que descargamos como fichero zip en la SD.
- 4. Una vez termina de copiarse todo, sacamos la tarjeta SD y la insertamos en la Raspberry Pi
- 5. Conectamos el cable HDMI, pantalla, teclado, ratón y cable de red.
- 6. Conectamos el cable de alimentación eléctrica y empezará a arrancar la Raspberry Pi.
- 7. Elegimos el idioma de instalación y el idioma del teclado.
- 8. Comenzamos a instalar y ya tendremos nuestras Raspberrys preparadas.

Inicialmente entraremos con estas credenciales a nuestras Raspberrys.

User: Pi

# Password: Raspberry

La primera tarea que hemos realizado es instalar los SO a las Raspberrys y posteriormente hemos creado un usuario con las iniciales de los integrantes del equipo en cada Raspberry (COD) y le hemos incluido en el grupo sudo utilizando el comando "usermod -g sudo cod"

Crearemos nuevo user y contraseña, para eliminar las que vienen por defecto: "cod" "\*\*\*\*\*\*"

Damos todos los permisos al nuevo usuario con "usermod -g sudo cod"

Definimos dos IPs una estática y una virtual (ver ejemplo abajo) por DHCP en cada Raspberry así como DNS local en /etc/hosts asignando nombres a las dos máquinas COD1 y COD2.

```
codl@raspberrypi:~$ cat /etc/network/interfaces
# interfaces(5) file used by ifup(8) and ifdown(8)
# Please note that this file is written to be used with dhcpcd
# For static IP, consult /etc/dhcpcd.conf and 'man dhcpcd.conf'
# Include files from /etc/network/interfaces.d:
source-directory /etc/network/interfaces.d
auto lo
iface lo inet loopback
auto eth0
iface eth0 inet dhcp
auto eth0:1
iface eth0:1 inet static
       address 192.168.1.41
       netmask 255.255.255.0
allow-hotplug wlan0
iface wlan0 inet manual
    wpa-conf /etc/wpa supplicant/wpa supplicant.conf
allow-hotplug wlan1
iface wlan1 inet manual
    wpa-conf /etc/wpa_supplicant/wpa_supplicant.conf
cod1@raspberrypi:~$
```

Administración



Comenzamos a trabajar de manera directa con las Raspberrys. Configuramos las pantallas, teclados y ratón a las Raspberrys para poder trabajar en ellas, instalar el sistema operativo Rasp Lite y Rasp Pixel para probar las interfaces de este sistema, TUI y GUI. Como hemos podido comprobar el sistema gráfico consume más recursos de las Raspberrys. Por lo que hemos decidido pasar las dos Raspberrys al interfaz en modo texto.

# Trabajando con las Raspberrys

Lo primero de todo es listar el HW de los servidores y las Raspberrys con: lshw -html > invent.html

Con esto tendremos un listado del Hardware en formato HTML.

Además chequeamos ambas máquinas con los comandos: nmap,iftop, (ASOpedia).

En clase hemos creado un NAS (Network Attached Storage) con un server ubuntu para dar servicio a todos los grupos y provisionalmente las Raspberrys se conectaran y almacenarán en él las copias de seguridad.

Para trabajar de forma remota cada miembro del grupo COD tenemos instalado en nuestro portátil el software Putty para conectarnos de manera remota a las Raspberrys y los servidores.

Como vemos en la siguiente captura nos vamos a conectar a la Raspberry COD1.

tegory:	1	
∃ Session	Basic options for your Pu	ITY session
	Specify the destination you want to	connect to
	Host Name (or IP address)	Port
Bell	192.168.1.41	22
- Features - Window - Appearance - Behaviour - Translation - Selection	Connection type:	● SSH ○ Serial
	Load, save or delete a stored sessions	n
Colours	Default Settings	Load
- Data		Save
- Telnet		Delete
ia SSH Serial	Close window on exit: Always Never  On	ly on clean exit

Crear par de claves para conexión sin password entre Raspberrys, para ello utilizaremos ssh keygen y vamos a sincronizar entre Raspberrys COD1 y COD2 para generar confianza entre ellas. Creamos así el par de claves para conexión sin password entre Raspberrys. Haremos los mismos pasos con el servidor NAS.

🚰 192.168.1.41 - PuTTY

login as: cod1 cod1@192.168.1.41's password: The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright. Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Mon Jan 30 17:24:29 2017 from 192.168.1.112 codl@raspberrypi:~\$ ssh-keygen Generating public/private rsa key pair. Enter file in which to save the key (/home/cod1/.ssh/id rsa): Enter passphrase (empty for no passphrase): Enter same passphrase again: Your identification has been saved in /home/cod1/.ssh/id rsa. Your public key has been saved in /home/cod1/.ssh/id rsa.pub. The key fingerprint is: f1:c6:3e:c4:8e:7a:f6:44:ae:06:76:5a:69:66:fe:e8 cod1@raspberrypi The key's randomart image is: ---[RSA 2048]----+ S.B o BO .=Eoo codl@raspberrypi:~\$ ssh-copy-id cod2@192.168.1.42

codl@raspberrypi:~\$ ssh-copy-id cod2@192.168.1.42
/usr/bin/ssh-copy-id: INF0: attempting to log in with the new key(s), to filter out any that are already installed
/usr/bin/ssh-copy-id: INF0: 1 key(s) remain to be installed -- if you are prompted now it is to install the new keys
cod2@192.168.1.42's password:

Number of key(s) added: 1

Now try logging into the machine, with: "ssh 'cod2@192.168.1.42'" and check to make sure that only the key(s) you wanted were added.

cod1@raspberrypi:~\$ ssh cod2@192.168.1.42

The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Mon Jan 30 17:30:28 2017 from 192.168.1.101 cod2@raspberrypi:~\$ Haremos los mismo con los servidores, exportar claves públicas desde las Raspberrys sobre el NAS para acceso sin contraseña.

Enviar imágenes de las copias de seguridad de las Raspberrys como tarea de cron. Para ello crearemos un script dentro de Crontab que empaquetará las copias o bien con tar o con tgz.



10 18 tar -zcvf /home/cod1/bak/homecod1.tgz /home/cod1 && scp /home/cod1/bak/homecod1.tgz

192.168.1.6:/mnt/greyjoy/bak/cod/cod1/homecod1.tgz

Cambiamos los permisos de la carpeta cod del NAS donde se guardan las copias de seguridad.

```
codl@stark:/mnt/greyjoy/bak$ chmod 774 cod
codl@stark:/mnt/greyjoy/bak$ sudo chgrp cod cod
codl@stark:/mnt/greyjoy/bak$ ls -1
total 20
drwxr-xr-x 2 bdj sudo 4096 feb 3 19:54 bdj
drwxrwxr-- 4 codl cod 4096 feb 3 20:07 cod
drwxrwxr-- 4 dj1 djgroup 4096 feb 3 20:08 dj
drwxr-xr-x 2 jmc sudo 4096 feb 3 20:13 jmc
drwxr-xr-x 2 root root 4096 feb 3 19:34 nd
codl@stark:/mnt/greyjoy/bak$
```

Cambiamos el grupo y los permisos del mismo de la carpeta donde están las copias de seguridad.

cod1@stark:/mnt/greyjoy/bak/cod\$ chmod 774 cod1 cod2 cod1@stark:/mnt/greyjoy/bak/cod\$ sudo chgrp cod cod1 cod1@stark:/mnt/greyjoy/bak/cod\$ sudo chgrp cod cod2 cod1@stark:/mnt/greyjoy/bak/cod\$ ls -1 total 8 drwxrwxr-- 2 cod1 cod 4096 feb 4 19:20 cod1 drwxrwxr-- 2 cod1 cod 4096 feb 4 19:20 cod2 cod1@stark:/mnt/greyjoy/bak/cod\$

Modificamos el fichero /etc/hosts para poner nombre a cada una de las IP's de los servidores y Raspberrys.

GNU nano 2.2	.6 Fichero: /etc/hosts
127.0.0.1	localhost
::1	localhost ip6-localhost ip6-loopback
ff02::1	ip6-allnodes
ff02::2	ip6-allrouters
127.0.1.1	raspberrypi
192.168.1.41	codl
192.168.1.42	cod2
192.168.1.6	stark
192.168.1.4	targaryen
192.168.1.2	lanister
	[ 11 líneas escritas ]
^G Ver ayuda ^	Guardar AR Leer Fich AY Pág Ant AK CortarTxt AC Pos actual
^X Salir ^	Justificar W Buscar V Pág Sig A PegarTxt A Ortografia

# **Conexiones remotas**

Para acceder de manera remota a los servidores utilizaremos conexión a escritorio remoto de Windows. Entraremos a través de los puntos de acceso Wi-Fi, utilizando una IP fija previamente asignada a los miembros del grupo COD e introduciendo la IP, nombre y contraseña en el programa de Conexión a Escritorio remoto.

😼 Conex	ión a Escritorio remoto	-	画	×
-	Escritorio remoto Conexión			
<u>E</u> quipo:	192.168.1.4	Ŷ		
Usuario:	MicrosoftAccount\cod			
Se solicitar	án credenciales al conectarse.			
Mostra	ar <u>o</u> pciones	Conectar	Ауц	īqa

Después de esto podemos ver el escritorio (en este caso Targaryen) desde el portátil de los miembros del equipo COD.



# Ubuntu-Ubuntu



# **Ubuntu-Windows**

L		Server Manager		
🐨 🗧 Server Ma	nager • Local Sei	rver • ⊛ I	Managai Taols	Vew Help
E Dashboard	PROPERTIES For TARGARYEN		I	TASKE V
M Servers  AD CS  AD DS	Compater name Domain	Takcarven asispedier	Last metallist updates Window Update Last checked for spilates	
1월 DHCP ▲ DNS W File and Storage Services Mo Its 약, NAP @ Remote Desktop Services 1	Windows Energiest Apricela surragement Terristic Devicting SAC Teaching Ethernet Ethernet 2	Semara OH Enabled Saabled Saataled Saataled 102,003,14	Weidows Error Reporting Continent Experience Improve El Ennotation Society, Configura Time serve Product III	ert Poys int III
	Opending system version Hamburn information	Microsoft Windows Sever 2012 KZ Standard Del Inc. Precision WorkStation R3400	Processori Isstalled memory (RAM)	
	4			1643]

# Administración de los servidores

# Active Directory

Lo primero que haremos es la instalación DNS en el servidor. Para ello entramos en Añadir roles y características y seguiremos los pasos de instalación que hemos seguido en las prácticas realizadas a lo largo del curso. Escogemos añadir DNS Server y añadimos sus características. Vemos que nos ofrece DNS y damos a next para proceder a instalar. En la siguiente imagen podemos ver el panel del DNS con los ficheros creados para la web y ftp.

å,	DNSI	Manager	_	
File Action View Help				
🔶 🔿 🙋 🛅 🛅 🙆 😽				
<ul> <li>DNS</li> <li>TARGARYEN</li> <li>Global Logs</li> <li>DNS Events</li> <li>Forward Lookup Zones</li> <li>msdcs.asir.pother</li> <li>asir.pother</li> <li>asir.pother</li> <li>asir.pother</li> <li>asir.pother</li> <li>asir.pother</li> <li>asir.pother</li> <li>Trust Points</li> <li>Conditional Forwarders</li> </ul>	Name (same as parent folder) (same as parent folder) (ftp cod1 cod2 (vwww	Type Start of Authority (SOA) Name Server (NS) Host (A) Host (A) Host (A) Host (A)	Data [1], targaryen.asir.pother., targaryen.asir.pother. 192.168.1.41 192.168.1.41 192.168.1.42 192.168.1.41	Timestam static static
QUICK START	nfigure this local s Add rolas and features	erver		

Confirmamos la instalación y ya comenzaría a instalarse el rol. Haremos lo mismo con el rol de directorio activo.

elect server ro	les	DESTINATION SERVE WIN-1HGL3K298
Before You Begin Installation Type Server Selection Server Roles	Select one or more roles to install on the selected server. Roles	Description Active Directory Certificate Services (AD CS) is used to create
Features Confirmation Results	Active Directory Domain Services     Active Directory Federation Services     Active Directory Lightweight Directory Services     Active Directory Rights Management Services     DHCP Server     DNS Server     Fax Server     Fax Server     Fax Server     File and Storage Services (1 of 12 installed)     Hyper-V     Network Policy and Access Services     Print and Document Services     Remote Access	certification authorities and related role services that allow you to issue and manage certificates used in a variety of applications.



Debemos crear un nuevo bosque donde tendremos los grupos de los equipos y dentro los usuarios de los mismos. El nombre de dominio se llamará asir.pother.



Además le pondremos una contraseña.



Una vez tengamos esto seleccionado podemos dar a next. La descripción que tenemos de Active Directory nos explica que tendremos unos usuarios administrados por admin (nosotros) y que les daremos una serie de permisos y accesos.



Una vez hechos estos pasos podemos ver en el Dashboard los nombres de los grupos del proyecto incluido el nuestro.



La primera vez que nos conectamos remotamente nos pedirá un usuario y contraseña del servidor. Por lo que hay que hacerlo directamente en el servidor.

Ven	Propiedades del sistema
con	Cambios en el dominio o el nombre del equipo
gurida	d de Windows
Caml Escriba al dom	bios en el dominio o el nombre del equipo a el nombre y la contraseña de una cuenta con permiso para unirse ninio.
F	Nombre de usuario
	Dominio: asir.pother
	Aceptar Cancelar
Vea	Aceptar Cancelar Aceptar Cancelar Aceptar Cancelar Aplicar

Una vez realizado esto ya estaremos logueados en el dominio del proyecto.



Después de tener todo esto configurado, nos conectaremos de manera remota. Desde allí podemos configurar los usuarios, los haremos miembros del grupo COD y además los podemos ver en los usuarios que están registrados en el ordenador.

<b>d</b> 1	Active Directory Users and Computers		- 🗆 X	COD-PC Properties ? X
File Action View Help	1 Q 🔒 🛛 🗔 % % în 🖷 🚨 %			General Operating System Member Of Delegation Location Managed By Dialin
Active Directory Users and Comput         Saved Queries         asin pother         Boli         Builtin         COD         Computers         Domain Controllers         ForeignSecurity-Principals         Jown Managed Service Accounts         Users	Name DANIEL-PC MG-AD MSI-PC ND-NICO COD-PC.	Type Computer Computer Computer Computer Computer	Description	Neine       Active Directory/Domain Services Folder         CDD group       Sart.cohiat         Domain Computers       Sart.points/Users         Add       Remove         Prinsty group:       Domain Computers         Set Prinsty Group       There is no need to change Prinsty group unless you have Macintath Clerks of PDSD-complant applications.
< III >	C	1	X	OK Carcel Apply Help

Después de tener los usuarios conectados empezaremos a crear las políticas de grupo COD.

# Creación de las GPO

Group Policy Management	Politicas COD						
	Scope Details Settings Delegation						
A Stational Domains	Links						
Default Domain	Display links in this location:	esir.pother			5		
a 🗐 BDJ	The following sites, domains, and	OUx are linked to this GPO:					
Politicas BD	Location	Enforced	Link Enabled	Path			
A E COD	L COD	No	Yes	asir.pother/COD			
Politicas CC							
b al JMC							
p 📅 Group Policy O	e l						
WMI Filters							
👂 🋄 Starter GPOs	Comity Filming						
b Sites	The estimatic this GBD can only	, mellete the following groups :	ware and another provi				
Group Policy Modeling	The salings in this and can only	A apply to the following groups. I	isais, and computers				
Group Policy Results	Nome 62 Authority and Users						
	& COB-gloup ITABGARYEN1	COD-group (TARBARYEN1\COD-group)					
			2200				
	Add	Temove Property	17				
	WMI Filtering						
	This GPO is linked to the follow:	ng WMI filter:					
	Economea	v	Doen				
< 111. >		104U S					

La primera política de grupo que crearemos será quitar las opciones de apagado, restart, hibernar...

Remove and p	revent access t	the Shut Down, Restart, Sleep, and Hibernate comm 💻 🗖 🎫
Remove and prev	vent access to the Next Setting	ut Down, Restart, Sleep, and Hibernate commands
<ul> <li>Not Configured</li> <li>Enabled</li> </ul>	Comment:	
O Disabled	Supported on:	At least Windows 2000
Options:		Help:
		This policy setting prevents users from performing the following commands from the Start menu or Windows Security screen: Shut Down, Restart, Sleep, and Hibernate. This policy setting does not prevent users from running Windows-based programs that perform these functions.         If you enable this policy setting, the Power button and the Shut Down, Restart, Sleep, and Hibernate commands are removed from the Start menu. The Power button is also removed from the Windows Security screen, which appears when you press CTRL +ALT+DELETE.         If you disable or do not configure this policy setting, the Power button and the Shut Down, Restart, Sleep, and Hibernate commands are available on the Start menu. The Power button setting with the Shut Down, Restart, Sleep, and Hibernate commands are available on the Start menu. The Power button setting the Power button and the Shut Down, Restart, Sleep, and Hibernate commands are available on the Start menu. The Power button on the Windows Security screen is also available.
		OK Cancel Apply

La siguiente política de grupo que implementamos es la prohibición de acceso de los usuarios al panel de control.

Prohibit access to Control Panel and PC settings 📃 🗕 💌 🗙				
📑 Prohibit access to	o Control Panel an	d PC settings Previous Setting Next Setting		
O Not Configured	Comment:	· · · · · · · · · · · · · · · · · · ·		
Enabled				
O Disabled		×		
	Supported on:	At least Windows 2000		
		· · · · · · · · · · · · · · · · · · ·		
Options:		Help:		
		Disables all Control Panel programs and the PC settings app.         This setting prevents Control.exe and SystemSettings.exe, the program files for Control Panel and PC settings, from starting. As a result, users cannot start Control Panel or PC settings, or run any of their items.         This setting removes Control Panel from:         The Start screen         File Explorer         This setting removes PC settings from:         The Start screen         Settings charm         Account picture         Search results         If users try to select a Control Panel item from the Properties		
		item on a context menu, a message appears explaining that a		

Esta política de grupo lo que hace es impedir las actualizaciones a los usuarios.

Remc	e access to use all Windows Update features	×
Remove access to use all Window	Jpdate features Previous Setting Next Setting	
<ul> <li>Not Configured Comment:</li> <li>Enabled</li> <li>Disabled</li> <li>Supported on:</li> </ul>	Windows XP Professional Service Pack 1 or At least Windows 2000 Service Pack 3	
Options:	Help:	
Configure notifications: 1 - Show restart required notifications	<ul> <li>This setting allows you to remove access to Windows Update.</li> <li>If you enable this setting, all Windows Update features are removed. This includes blocking access to the Windows Update Web site at http://windowsupdate.microsoft.com, from the Windows Update hyperlink on the Start menu, and also on the Tools menu in Internet Explorer. Windows automatic updating is also disabled; you will neither be notified about nor will you receive critical updates from Windows Update. This setting also prevents Device Manager from automatically installing driver updates from the Windows Update web site.</li> <li>If enabled you can configure one of the following notification options:</li> <li>Do not show any notifications</li> <li>This setting will remove all access to Windows Update features and no notifications will be shown.</li> </ul>	<

Por último podemos ver las políticas de grupo ya implantadas desde un usuario cliente que está dentro del grupo de política de COD. Las políticas que hemos implementado son:

- El usuario del Directorio Activo sólo puede cerrar sesión (no tiene permisos para reiniciar, apagar o suspender).
- El usuario del Directorio Activo no puede hacer actualizaciones en el sistema.





# Samba en el servidor Stark

En primer lugar, en UBUNTU 16.04 ya tenemos algunos paquetes SAMBA instalados (podemos comprobarlo con dpkg -l nombrepaquete) si no fuera así instalaremos: sudo apt-get install samba samba-common smbclient samba-doc samba - Servidor de archivos e impresoras samba-common - Archivos comunes de samba utilizados para clientes y servidores. smbclient - Cliente simple swat - Herramienta de administración de Samba vía web samba-doc - Documentación de Samba. smbfs - Comandos para montar y desmontar unidades de red samba system-config-samba: interfaz gráfica de configuración para samba



#### A continuación editamos el archivo de configuración /etc/samba/smb.conf



(para que los cambios surjan efecto se ha de reiniciar servicio # service smbd restart)

stark@stark:~\$ sudo service smbd restart
stark@stark:~\$ sudo service smbd status
<ul> <li>smbd.service - LSB: start Samba SMB/CIFS daemon (smbd)</li> </ul>
Loaded: loaded (/etc/init.d/smbd; bad; vendor preset: enabled)
Active: active (running) since mie 2017-02-15 18:56:26 CET: 6s ago
Docs: man:systemd-sysy-generator(8)
Process: 18908 ExecStop=/etc/init d/smbd stop (code=exited status=0/SUCCESS)
Process: 18921 EverStart=/etc/init d/smbd start (code=evited_status=0/SUCCESS)
Tasks: 3
Memory: 3 1M
CDII: 320me
Course (Journam elicatembet carvica
19040 June (biological de la constance)
Choice 13940 /usr/sbirl/smbd -D
-18941 /usr/spin/smbd -D
-18946 /UST/SDIA/Smbd -D
feb 15 18:56:26 stark systemd[1]: Starting LSB: start Samba SMB/CIFS daemon (smbd) feb 15 18:56:26 stark smbd[18921]:   * Starting SMB/CIFS daemon smbd feb 15 18:56:26 stark smbd[18921]:  done.
feb 15 18:56:26 stark systemd[1]: Started LSB: start Samba SMB/CIFS daemon (smbd).

Necesitamos crear una carpeta en Ubuntu Server para compartir, por ejemplo, creamos

Hacemos por defecto de propiedad pública y asignamos todos los permisos en smb.conf lo restringimos ya al usuario winuser y esta configuración es predominante, se pedirán claves!)

En el sistema LINUX necesitamos convertir un usuario en usuario samba para ello primero lo creamos en el sistema: # adduser winuser Y ahora para que sea usuario samba: # smbpasswd -a winuser (facilitamos una contraseña segura para la conexión desde Windows, puede ser otra) # smbpasswd -e winuser (lo habilitamos, enable).



Por último hacemos un service smbd restart.

# En el cliente WINDOWS

Administrar Recursos Compartidos

Conectar a unidad de red y facilitamos la IP o el Dominio de nuestra máquina UBUNTU en red (podemos asignarle una letra de Unidad)

← 🧟 Conectar a unidad de red

# ¿Qué carpeta de red desea asignar?

Especifique la letra de unidad para la conexión y la carpeta a la que desea conectarse:

id:	Y: ~					
Carpeta:	\\192.168.1.6\samba_asir ~	Examinar				
	Ejemplo: \\servidor\recurso_compartido					
	Conectar de nuevo al iniciar sesión					
	Conectar con otras credenciales					
	Conectarse a un sitio web para usarlo como almacén de documentos e imáger					

	Finalizar	Cancelar
Ya podemos ver el recurso compartido.		
V Ubicaciones de red (1)		
asir_samba (\\192.168.1.6) (Z:)		
427 GB disponibles de 453 GB		

Por lo que ya podemos entrar en la carpeta compartida con nuestro usuario y contraseña.

Seguridad de Windows

# Escribir credenciales de red

Escriba sus credenciales para conectarse a: 192.168.1.6

X

asiruser	
Dominio:	
Dominio:	
Recordar mis cred	lenciales
Aceptar	Cancelar

# Redes

# Montaje del Rack dentro del CPD (Centro de Proceso de Datos o aula 308)

Lo primero que haremos será comprobar todos los elementos que tenemos. Comprobaremos que todos los cables que tenemos siguen el estándar y son cables directos que siguen la norma a ambos extremos del cable. Seguiremos la norma T-568B de cables directos utilizados para conectar routers, switches y hubs. Para realizar la comprobación utilizaremos los tester de los que disponemos en el aula.



Para el diseño y despliegue de esta red, hemos pensado en la manera más simple y sencilla. De esta manera se encontrará todo en el rack:

Tendremos el acceso de los usuarios COD a dos puntos.

El cableado se hará en el rack usando cables directos con un sistema administrativo horizontal.

# RACK

Stark, Targaryen y Lannister (de arriba a abajo). Debajo las Raspberrys conectadas y los switches y dentro los puntos de acceso (no aparecen en la imagen).

# Unidades del rack

Stark y Targaryen  $\rightarrow$  2U (1,75" x 2) Lannister y dos switches  $\rightarrow$  1U (1,75" x 1) Raspberrys  $\rightarrow$  (0,625")

En el rack, a parte de los servidores, también tenemos pantalla y teclado para la configuración, además de las regletas para alimentar todos los dispositivos.



# Diagrama del Rack

Como podemos ver tenemos todos los dispositivos en el rack, además tenemos los dos puntos de acceso que no están visibles en este diagrama.



Definimos IPs estáticas flotantes en Raspberry Lite y Pixel.

#### COD1 192.168.1.41

eth0:1 Link encap:Ethernet HWaddr b8:27:eb:8c:45:0a inet addr:192.168.1.41 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

#### COD2 192.168.1.42

eth0:1 Link encap:Ethernet HWaddr b8:27:eb:0c:f4:43 inet addr:192.168.1.42 Bcast:192.168.1.255 Mask:255.255.255.0 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1

#### Configuración de la red

Elegimos los elementos que vamos a utilizar para crear la red de Pother. Una vez seleccionados creamos un esquema que nos muestre cómo debemos conectar los elementos.

# Esquema de red



Configuramos dos puntos de acceso uno para el frontal que dará los servicios (Raspberrys) y otro para configuración. Los puntos de acceso tendrán las direcciones de clase C 192.168.1.1 y 192.168.4.1. Desde este punto de acceso podremos entrar a configurar los servidores y las Raspberrys de manera remota. Cogemos los routers que utilizaremos y los configuramos, de tal manera que nos de una IP dentro de los rangos de nuestro equipo. Además introducimos nuestras MAC Address para que solamente tengamos acceso los miembros del grupo.

# Prueba de acceso Wi-Fi a la red

Buscamos el SSID de los puntos de acceso que hemos creado y a los que hemos nombrado como ASIR-P1 y ASIR-P2. Previamente hemos realizado un filtrado de MAC-Adress para que sólo puedan acceder nuestros dispositivos.



En el punto de acceso ASIR-P1 la IP ha de ser estática, en el punto de acceso ASIR-P2 se asigna por DHCP.

Adaptador de LAN inalámbrica Vi-Fi:	
Sufijo DNS específico para la conexión: homestation Descripción	
192.168.1.1 Servidor DHCP	

Configurar en LAN con la IP 192.168.1.6 para el NAS

Desde nuestros equipos personales podremos entrar con Putty estableciendo una IP estática en nuestra tarjeta de red.

den 192.168	8.1.41 - PuTTY			×
permitte Last log	d by applicable law. in: Mon Jan 30 17:44:20 2017 from 192.168.1.6			^
eth0	<pre>DEFrypl:~\$ 11Config Link encap:Ethernet HWaddr b8:27:eb:0c:f4:43 inet addr:192.168.1.102 Bcast:192.168.1.255 Mask:255. UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1 RX packets:18110 errors:0 dropped:0 overruns:0 frame:0 TX packets:11036 errors:0 dropped:0 overruns:0 carrier: collisions:0 txqueuelen:1000 RX bytes:1615270 (1.5 MiB) TX bytes:1408989 (1.3 MiB)</pre>	255.25 0	5.0	
eth0:1	Link encap:Ethernet HWaddr b8:27:eb:0c:f4:43 inet addr:192.168.1.42 Bcast:192.168.1.255 Mask:255.2 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1	55.255	.0	
10	Link encap:Local Loopback inet addr:127.0.0.1 Mask:255.0.0.0 UP LOOPBACK RUNNING MTU:65536 Metric:1 RX packets:0 errors:0 dropped:0 overruns:0 frame:0 TX packets:0 errors:0 dropped:0 overruns:0 carrier:0 collisions:0 txqueuelen:1 RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)			
cod2@ras	pberrypi:~\$ 📒			~

# Instalación de servicios

Instalación de Apache2

login as: cod1 cod1@192.168.1.41's password: The programs included with the Debian GNU/Linux system are free software; the exact distribution terms for each program are described in the individual files in /usr/share/doc/\*/copyright. Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent permitted by applicable law. Last login: Mon Feb 6 17:15:36 2017 from 192.168.1.45 cod1@raspberrypi:~\$ sudo apt-get install apache2 [sudo] password for cod1: Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho Se instalarán los siguientes paquetes extras: apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0 ssl-cert Paquetes sugeridos: apache2-doc apache2-suexec-pristine apache2-suexec-custom openssl-blacklist Se instalarán los siguientes paquetes NUEVOS: apache2 apache2-bin apache2-data apache2-utils libapr1 libaprutil1 libaprutil1-dbd-sqlite3 libaprutil1-ldap liblua5.1-0 ssl-cert 0 actualizados, 10 nuevos se instalarán, 0 para eliminar y 124 no actualizados.

#### El fichero de apache se almacena en /etc/apache2

codl@raspb	erry	pi:/e	tc/ap	ache2\$	ls	-lat	E,	
total 88								
drwxr-xr-x	111	root	root	4096	feb	7	18:56	
drwxr-xr-x	2	root	root	4096	feb	7	18:52	sites-enabled
drwxr-xr-x	2	root	root	4096	feb	7	18:52	conf-enabled
drwxr-xr-x	2	root	root	4096	feb	7	18:51	mods-enabled
drwxr-xr-x	2	root	root	4096	feb	7	18:51	sites-available
drwxr-xr-x	8	root	root	4096	feb	7	18:51	
drwxr-xr-x	2	root	root	12288	feb	7	18:51	mods-available
drwxr-xr-x	2	root	root	4096	feb	7	18:51	conf-available
-rw-rr	1	root	root	7115	ago	7	2016	apache2.conf
-rw-rr	1	root	root	1782	jul	5	2016	envvars
-rw-rr	1	root	root	31063	jul	5	2016	magic
-rw-rr	1	root	root	320	jul	5	2016	ports.conf
codl@raspbe	erry	pi:/et	tc/ap	ache2\$				

#### Creamos los enlaces simbólicos

cod1@raspberrypi:/etc/apache2/mods-enabled\$ sudo ln -s ../mods-available/ssl.conf cod1@raspberrypi:/etc/apache2/mods-enabled\$ sudo ln -s ../mods-available/ssl.load cod1@raspberrypi:/etc/apache2/mods-enabled\$

Activamos el puerto 8080 para escuchar a través de él.

GNU nano 2.2.6	Fichero:	ports.conf			Modifi
<pre># If you just change the port or # have to change the VirtualHost # /etc/apache2/sites-enabled/000</pre>	add more statemen -default	e ports here, nt in .conf	you will	likely	also
Listen 80					
Listen 8080					
<ifmodule ssl_module=""></ifmodule>					
<ifmodule mod_gnutls.c=""> Listen 443</ifmodule>					
<pre># vim: syntax=apache ts=4 sw=4 s</pre>	ts=4 sr 1	noet			

Modificamos los ficheros de sites-enabled

1000

GNU	nano 2.2.6	FICHERO: COD.es.CONT
<virtu< th=""><th>ualHost *:80&gt;</th><th></th></virtu<>	ualHost *:80>	
	<pre># The ServerName direct # the server uses to id # redirection URLs. In # specifies what hostna # match this virtual ho # value is not decisive # However, you must set ServerName www.cod.es</pre>	ive sets the request scheme, hostname and port that entify itself. This is used when creating the context of virtual hosts, the ServerName me must appear in the request's Host: header to st. For the default virtual host (this file) this as it is used as a last resort host regardless. it for any further virtual host explicitly.
	ServerAdmin webmaster@l DocumentRoot /var/www/h DirectoryIndex index.ph	ocalhost tml/es p
	# Available loglevels: # error, crit, alert, e # It is also possible t # modules, e.g. #LogLevel info ssl:warn	trace8,, tracel, debug, info, notice, warn, merg. o configure the loglevel for particular
	ErrorLog \${APACHE_LOG_D CustomLog \${APACHE_LOG_	IR}/error.log DIR}/access.log combined
<td><pre># For most configuratio # enabled or disabled a # include a line for on # following line enable # after it has been glo #Include conf-available tualHost&gt;</pre></td> <td>n files from conf-available/, which are t a global level, it is possible to ly one particular virtual host. For example the s the CGI configuration for this host only bally disabled with "a2disconf". /serve-cgi-bin.conf</td>	<pre># For most configuratio # enabled or disabled a # include a line for on # following line enable # after it has been glo #Include conf-available tualHost&gt;</pre>	n files from conf-available/, which are t a global level, it is possible to ly one particular virtual host. For example the s the CGI configuration for this host only bally disabled with "a2disconf". /serve-cgi-bin.conf



Creamos un index dentro de la carpeta cod para que sea la página a la que accedemos. Tendrá dos dominios .com y .es y dentro la página principal o index.

/var/www/	html/
├── com	
- a	ilta.php
- b	aja2.php
- t	aja.php
	conexion.php
- c	lesconexion.php
— i	ndex.html
— i	.ndex.php
<u>⊢</u> 1	istado.php
	.ogin.php
- n	odificar2.php
— п	odificar.php
	rocesaLogin.php
l i i	egistroUsuarios.php
— es	
- a	lta.php
- t	aja2.php
b	aja.php
- c	onexion.php
- 0	onexion.php.bueno
	onexion.php.old
- c	lesconexion.php
— i	ndex.html.old
— i	.ndex.php
	istado.php
	.ogin.php
- n	nodificar2.php
n	odificar.php
- p	rocesaLogin.php
- r	egistroUsuarios.php

En /etc/apache2/sites-enabled se crean enlaces simbólicos de los ficheros de configuración creados en sites-avaliable ejecutando desde sites-enabled "sudo In -s ../sites-available/cod.es.conf cod.es.conf" y lo mismo con el .com.



Reiniciamos el servicio Apache2 restart

codl@raspberrypi:/etc/apache2\$ sudo service apache2 start codl@raspberrypi:/etc/apache2\$

Instalación de vsftpd

codl@raspberrypi:~\$ sudo apt-get install vsftpd Leyendo lista de paquetes... Hecho Creando árbol de dependencias Leyendo la información de estado... Hecho Se instalarán los siguientes paquetes extras: dialog Se instalarán los siguientes paquetes NUEVOS: dialog vsftpd 0 actualizados, 2 nuevos se instalarán, 0 para eliminar y 124 no actualizados. Se necesita descargar 373 kB de archivos. Se utilizarán 1.001 kB de espacio de disco adicional después de esta operación. ¿Desea continuar? [S/n]

Configuración de vsftpd.conf -anonymous\_enable=NO -local\_enable=YES -write\_enable=YES -chroot\_local\_user=YES -allow\_writeable\_chroot=YES

Lo único que hemos modificado para su correcto funcionamiento son estas 5 características de la configuración. Hecho esto ya funciona el ftp correctamente.

# Seguridad en el proyecto

#### Explicación ¿por qué es importante la seguridad en el aula del proyecto?

La seguridad en un aula donde tendremos los equipos del proyecto es muy importante ya que la entrada de alumnos y profesores de diferentes ámbitos pueden afectar a la misma (puede suceder que entre gente no autorizada). Debido a esto cada usuario tiene una forma de tratar los equipos, diferentes cuentas y formas de acceso a los equipos. Además puede haber material sensible como software, aplicaciones, bbdd del proyecto y se debe cuidar la E/S a Internet. Todo esto es lo más habitual en el aula 308 y puede haber otro tipo de riesgos que veremos.

### Seguridad física

- Control de acceso y seguridad de los edificios.
- Control de acceso al aula 308 donde trabajamos: Personas y equipos autorizados tendrán llave para entrar a trabajar en la clase.
- Extintor anti incendios homologado, señales luminosas y acústicas, manguera y activación de incendios







- Seguridad de equipos y periféricos que utilizaremos en el proyecto. Las Raspberrys, cables y demás hardware a utilizar están guardados con llave en los armarios.
- Seguridad de la red interna, conexiones y cableado (switches, patch panel, regletas, cables Ethernet, etc.).
- Paneles indicativos y de emergencia.



- Doble filtro para controlar la electricidad del aula con dos cuadros.
- Implementación del SAI (finalmente no aplicado en este proyecto).
- Copias de Seguridad en almacenamiento o soporte físico con los servidores (uso de NAS, Almacenamiento Conectado en Red). Volcamos las copias de seguridad en un periodo de tiempo al servidor.

# Monitorización HW de los servidores que utilizamos

# Planificación de la Seguridad lógica

- NAS (Ubuntu Server 16.04. Almacenamiento de copias de seguridad)
  - Contraseña de login de nuestro equipo
  - Actualizaciones automáticas
  - Comprobar la integridad del sistema con rkhunter
  - Configuraciones DNS, IP.
  - Comprobación de la disponibilidad del sistema (comprobación de puertos, escuchas... con nmap).
  - Cifrar copias de seguridad y guardarlas
  - Auditoría de seguridad
- Servidor proxy (Ubuntu 16.04) + Firewall  $\rightarrow$  squid 3
  - Contraseña de login de nuestro equipo
  - Actualizaciones automáticas
  - Comprobar la integridad del sistema con rkhunter
  - Configuraciones DNS, IP

- Comprobación de la disponibilidad del sistema (comprobación de puertos, escuchas... con nmap).
- Auditoría de seguridad
  - Firewall: IPTABLES o UFW
- Active Directory (Windows Server 2012, Dominio)  $\rightarrow$  sfc
  - Políticas y directivas de seguridad
  - Contraseña de login de nuestro equipo
  - Actualizaciones automáticas
  - Comprobar la integridad del sistema con rkhunter
  - Configuraciones DNS, IP
  - Comprobación de la disponibilidad del sistema (comprobación de puertos, escuchas... con nmap).
  - Auditoría de seguridad
- Raspberry (Pixel y Lite) + Servidor web
  - Seguridad Web
  - Certificado SSL
  - Apache 2
  - Contraseña de login en BBDD (mysql)
  - Permisos FTP (no permitir anónimos)
  - Actualizaciones automáticas
  - Comprobar la integridad del sistema con rkhunter
  - Configuraciones DNS, IP
  - Comprobación de la disponibilidad del sistema (comprobación de puertos, escuchas... con nmap).
  - Auditoría de seguridad
- Seguridad con las contraseñas y datos del equipo COD
  - Una de esas técnicas que podemos utilizar es el uso adecuado de contraseñas que estén compuestas por números, mayúsculas, minúsculas y símbolos.
  - Mínimo 8 caracteres
  - El uso de software de seguridad informática como firewall, proxy...
  - Encriptación de los datos.

# Problemas encontrados

Se podía acceder a las Raspberrys debido a que el usuario que viene por defecto "pi" no fue eliminado y cualquiera que conociera o usara Raspberrya el software podía conectarse por Wi-fi, probar las contraseñas y acceder a ellas fácilmente.

- Normas para los componentes de COD en el proyecto integrador

- Respetar normas en todo momento (no permitir comer, beber o fumar en el aula...).



- Limpieza de los equipos (paños y productos adecuados).
- Sólo acceso de personal autorizado en el proyecto.
- Evitar entrar a páginas de internet poco seguras (el centro puede tener un proxy o utilizar uno externo).
- De cara al usuario de los equipos: Prevención de riesgos laborales (Posición correcta, protector de pantalla, cuidar que los cables estén en buen estado).

# Plan de Contingencias de copia de seguridad

# Objetivos del Plan de Contingencias

Los objetivos principales de un Plan de Contingencias son los de planificar y describir la capacidad para respuestas rápidas. Su finalidad es la de permitir el funcionamiento del sistema Pother implementado, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la organización. Los principales objetivos específicos son:

- Establecer un procedimiento formal y por escrito que indique las acciones a seguir frente a determinados riesgos.
- Optimizar el uso de recursos humanos y materiales.
- Un control adecuado para cumplir con las normas y procedimientos establecidos.

Las copias de seguridad de las Raspberrys se harán mediante un script en crontab a diario. La copia de seguridad se guardará donde hayamos elegido al principio de la copia de seguridad indicado en el anterior punto como un servidor o un disco extraíble o en la red. Dicha parte se establece en las configuraciones de las Raspberrys (ver apartado configuración de las Raspberrys).

# Copias de seguridad y restauración

 Copia Total (diaria): 10 18 tar -zcvf /home/cod1/bak/homecod1.tgz /home/cod1 && scp /home/cod1/bak/homecod1.tgz 192.168.1.6:/mnt/greyjoy/bak/cod/cod1/homecod1.tgz
 (Este apartado está dentro de crontab en ASO).

Ubicación /mnt/greyjoy/bak/cod

#### Lugar donde se ha realizado la maqueta Pother

Ubicación CPD en la clase 308. Colocación: Dentro del rack del proyecto. Servidores: Stark, Targaryen y Lannister. Raspberrys de los equipos y COD1, COD2. 2 Switches y 2 puntos de acceso.

# Configuración del proxy

# Configuración en /etc/squid/squid.conf

Nombre, puerto, caché, log, listas acl y accesos al proxy.

```
GNU nano 2.2.6
                                       File: /etc/squid/squid.conf
isible hostname lannister
nttp_port 3128
cache_mem 64 MB
cache_log /var/log/squid/cache.log
acl pother src 192.168.1.0/24
acl all src 0.0.0.0/0.0.0
acl bloqueadas url_regex "/etc/squid/bloqueadas.acl"
acl dominios dstdomain "/etc/squid/dominios.acl"
acl puerto_1 port 0-79
acl puerto_2 port 81-65535
nttp_access allow pother
http_access deny bloqueadas
http_access deny dominios
http_access deny puerto_1
http_access deny puerto_2
```

Páginas bloqueadas por el proxy

GNU nano 2.2.6	File: /etc/squid/bloqueadas.acl
google.es .youtube.com .facebook.com .www.facebook.com .www.twitter.com .twitter.com	

Palabras de búsqueda bloqueadas

GNU nano 2.2.6	File: /etc/squid/dominios.acl
porno youtube sexo series videos peliculas	

Implantación de las BBDD

Creación de la Base de Datos para el CRUD. Lo primero que haremos será crear el diagrama con el modelo Chen de la BBDD que queremos implementar. De esta forma nos hacemos una idea de lo que queremos implementar a la hora de hacer el script que implemente nuestra solución.



USUARIO {<u>id\_usuario</u>, nombre, contrasena, <u>id\_grupo</u>} grupo\_id hace referencia a id\_grupo en GRUPO. GRUPO {<u>id\_grupo</u>, tipo} Después de crear esto implementaremos en un script .sql este modelo que contendrá a los usuarios dentro de un grupo que nos dirá si son administradores o son usuarios normales de dicha base de datos.

GNU nano 2.2.6 Fichero: bbdd.sql create database cod; use cod; create table usuario (id usuario int(10) not null auto increment, nombre varchar(255) not null, contrasena varchar(255) not null, grupo id int(10) not null, primary key (id usuario) ); create table grupo (id\_grupo int(10) not null auto increment, tipo varchar(255) not null, primary key (id\_grupo) ); alter table usuario add foreign key (grupo id) references grupo (id grupo); insert into grupo (id grupo, tipo) values (1, "administrador"), (2, "usuario"); create user admin@localhost identified by 'doc'; create user codl@localhost identified by 'doc'; grant select, insert, update, delete on cod.\* to admin@localhost; grant select on cod.\* to cod1@localhost;

Configuración mysql en las Raspberrys. Primeramente entramos en mysql:

codl@raspberrypi:~\$ mysql -u root -p Enter password:

Después de esto cargamos el script de la BBDD en las Raspberrys y comprobamos que se ha cargado.

```
mysql> source bbdd.sql
Query OK, 1 row affected (0.20 sec)
Database changed
Query OK, 0 rows affected (0.98 sec)
Query OK, 0 rows affected (0.07 sec)
Query OK, 0 rows affected (0.19 sec)
Records: 0 Duplicates: 0 Warnings: 0
Query OK, 2 rows affected (0.04 sec)
Records: 2 Duplicates: 0 Warnings: 0
Query OK, 1 row affected (0.03 sec)
Query OK, 0 rows affected (0.00 sec)
```

Comprobamos que está la BD en MySQL.

my	ysql>	sho	ow d	atabas	es;
Ī	Datak	base	ş		
	infor cod mysql perfo	cmat L Drma	ion	schem schem	+ a     a
+-	rows	in	set	(0.00	+ sec)
my	ysql>				

Y después vemos las tablas que tenemos.

my_	ysql>	show	<i>i</i> ta	bles	;	
	Table	es_ir	_cc	d		
+	grupo usuai	o cio		1		
2	rows	in s	set	(0.0	0 sec	:)
my	ysql>					

Mostramos los atributos de la tabla grupo y de usuario de manera descendente.

	rupo;				L të
Field	Туре	Null	Кеу	Default	Extra
id_grupo   tipo	int(10)   varchar(255)	NO   NO	PRI	NULL NULL	auto_increment
rows in set	: (0.01 sec)				
Judith gene g	+	-+	+		+
Field	Туре	Null	Key	Default	Extra

Vemos los grupos que hemos creado para esta BD, en este caso un grupo de administradores que tendrán todos los privilegios y otro para usuario normales.

id_grupo	tipo
1	administrador
2	usuario

Implantación Web

#### Primera idea para acceder a una web creada con CMS

El trabajo está desarrollado con Wordpress, que es un CMS, del inglés Content Management System. Este CMS está enfocado a la creación de blogs y portales web. Está desarrollado en PHP y MySQL, bajo licencia GPL y código modificable.

La creación de nuestros CMS fue utilizando muchas herramientas que nos ofrece Wordpress para plantillas, crear una tienda, SEO, Cookies, Seguridad, copia de seguridad...

Para crear el sitio web principal utilizaremos los lenguajes aprendidos HTML, CSS, Javascript, PHP.

PHP es, junto con mysql, el complemento ideal del servidor web apache ya que dota al servidor de un lenguaje script de ejecución en el servidor lo que facilita la creación de aplicaciones web y sitios web dinámicos.

Lo primero para poder trabajar con PHP debemos instalar en las Raspberrys el módulo PHP. Para ello seguiremos los siguientes pasos:

# Instalación de PHP

Para instalar PHP en nuestra Raspberry utilizaremos apt-get. El paquete a instalar depende de la versión que deseemos instalar y la versión de apache que tengamos, en nuestro caso utilizamos la versión 2 de apache e instalamos la versión 5 de php con  $\rightarrow$  sudo apt-get install libapache2-mod-php5



Al instalar libapache2-mod-php5 mediante apt-get, automáticamente se configura para integrarse perfectamente en apache, creando los archivos necesarios en la carpeta (/etc/apache2/mods-available) y creando los enlaces necesarios para habilitarlos en (/etc/apache2/mods-enabled).

Si vamos a conectar a bases de datos mysql desde php, necesitamos instalar el módulo php5-mysql:

sudo apt-get install php5-mysql



Además, tendremos que editar el archivo /etc/php5/apache2/php.ini y añadir la línea **extension=mysql.so** como veremos en el siguiente apartado.



# Configuración de PHP

El archivo de configuración de php5 es el archivo:

// Archivo de configuración de php5

/etc/php5/apache2/php.ini

```
cod1@raspberrypi:/etc/php5/apache2$ ls
conf.d php.ini
cod1@raspberrypi:/etc/php5/apache2$ sudo nano php.ini
```

Los parámetros más destacables a configurar son:

- Safe Mode = Off (Modo Seguro. Si el Modo seguro está desactivado, se habilitan todas las funciones del PHP. Para un uso educativo es mejor ser funcional y no activar el modo seguro. Si el Modo seguro está activado, se deshabilitan todas las funciones del PHP consideradas peligrosas. Para servicios de hosting se recomienda activar el modo seguro)
- **Display errors = On** (Mostrar Errores. Muestra los errores en las mismas páginas, cuando les haya. Cuando hay errores en los scritps, es más fácil encontrarlos si se muestran en las páginas)
- max\_execution\_time=30 (Tiempo máximo en segundos, de ejecución de un script. Si dejamos que un script se ejecute indefinidamente, podría colapsar el sistema)

```
; Maximum execution time of each script, in seconds
; http://php.net/max-execution-time
; Note: This directive is hardcoded to 0 for the CLI SAPI
max_execution_time = 30
```

- **post\_max\_size=8M** (Tamaño máximo de datos que se pueden enviar al servidor mediante POST)
- **upload\_max\_filesize = 8M** (Tamaño máximo de archivo que se puede subir al servidor. Si vamos a trabajar con archivos grandes, debemos subir este parámetro)
- **extension=mysql.so** (Activa el acceso a bases de datos MySQL desde PHP)

# **Probando PHP**

Una vez instalado y configurado, antes de probar debemos reiniciar el servidor web apache:

sudo /etc/init.d/apache restart

Ahora crearemos una página php que utilice la función phpinfo que además de comprobar que apache y php están funcionando, nos mostrará una información de la versión. Crearemos el siguiente archivo:

// Probando PHP. Crear archivo /var/www/phpinfo.php - permisos 644

<HTML> <H1>Probando PHP</H1> Salida del comando phpinfo:

<?php phpinfo();

?>

</HTML>

Ahora tan solo necesitamos arrancar el navegador e ir a la URL: http://ip-del-servidor/phpinfo.php. Si nos aparece la información de la versión de PHP significa que está correctamente instalado.

En el siguiente ejemplo vemos un programa escrito en PHP que, mediante un **bucle for** que va desde 1 hasta 10, muestra la tabla de multiplicar del 7. Si después observamos la página desde el cliente, no vemos más que la respuesta del programa PHP pero nunca el programa.

// Programa PHP para generar la tabla del 7. Se almacena en el servidor. Se mezcla el HTML con el código PHP

<html> <body> <? // Tabla de multiplicar del 7 echo "<h2>Tabla del 7</h2>";

```
// Bucle de 1 a 10
for($i=1; $i<11; $i++)
echo "7 x $i = ".(7*$i)."<br>\n";
?>
</body>
</html>
```

// Lo que ve el cliente, una vez ejecutado el programa en el servidor: HTML

puro

```
<html>
<body>
<h2>Tabla del 7</h2>7 x 1 = 7<br>
7 x 2 = 14<br>
7 x 3 = 21<br>
7 x 4 = 28<br>
7 x 5 = 35<br>
7 x 6 = 42<br>
7 x 7 = 49<br>
7 x 8 = 56<br>
7 x 9 = 63<br>
7 x 10 = 70<br>
</body>
</html>
```

#### Instalación MySQL Server

Lo primero que haremos es instalar mysql-server

```
codl@raspberrypi:~$ sudo apt-get install mysql-server
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes extras:
libaio1 libdbd-mysql-perl libdbi-perl libhtml-template-perl libmysqlclient18
libterm-readkey-perl mysql-client-5.5 mysql-common mysql-server-5.5
mysql-server-core-5.5
Paquetes sugeridos:
libclone-perl libmldbm-perl libnet-daemon-perl libsql-statement-perl
libipc-sharedcache-perl mailx tinyca
```

Durante la instalación nos pedirá una contraseña para el servidor mySQL.

Configuración de mysql-server-5.5 Se recomienda que configure una contraseña para el usuario «root» (administrador) de MySQL, aunque no es obligatorio.
No se modificará la contraseña si deja el espacio en blanco. Nueva contraseña para el usuario «root» de MySQL:

Una vez instalado actualizaremos la lista de paquetes disponibles.

codl@raspberrypi:~\$ sudo apt-get update

Verificamos que esté realizada la instalación y vemos que está escuchando y el puerto.



Comprobamos el fichero de configuración que esté haciendo el bind a la propia máquina



GNU nano 2.2.6 Fichero: my.cnf

# # The MySQL database server configuration file. #

Hacemos un restart a mySQL



Y por último accedemos a la consola de mySQL.

codl@raspberrypi:/\$ mysql -u root -p Enter password:



Estos pasos anteriores de instalación de Apache y MySQL, los podemos hacer también instalando solamente LAMP dónde viene todo esto integrado.

Para ofrecer este servicio hemos programado un CRUD (altas, bajas, modificaciones y consultas). Este CRUD dará acceso a la página web mediante un registro previo (o un login si ya estamos registrados). El usuario administrador tendrá acceso al panel CRUD donde podrá gestionar y administrar a los usuarios. Un usuario registrado cualquiera accederá directamente al servicio de Wordpress.

Nuestro Wordpress es un sitio con un pequeño curso de SEO (con lo que se cumplirá otra parte del curso de IAW) en el que se subirán noticias mediante un blog en el que se actuará con los usuarios y se publicarán las últimas novedades sobre SEO. Además contiene una tienda creada con WooCommerce.



# Publicaciones y descripción de todos los apartados del portal

*Inicio:* Página principal de mi portal web con un menú con las diferentes entradas,tienda y aspectos legales. En él se puede ver el tema utilizado. Encontramos una descripción de lo que nos vamos a encontrar, una serie de enlaces a laspáginas del sitio web, un formulario de contacto y un pie de página. Incluye elapartado blog donde se incluirán nuevas noticias sobre posicionamiento.

Todo lo que ves aquí es adaptable y amigable. Busca la creatividad.	Norma Lavian Red Mala or Takan conversion geballions: Alignmentation 12.452 Anno an exception data in the September 2018 and the orthogon and the September 2018 and the orthogon and the September 2018 and the orthogon and the set of the September 2018 and the orthogon and the set of the September 2018 and the orthogon and the set of the September 2018 and the set of the September 2018 a taken to a set of the September 2018 a taken to	2) 1000 2) HALTHARM 2) HERCHARM 2) HERCHARM 2) DIREND 010000

# SEO, SEM, Móviles:

Entradas sobre los temas de SEO, SEM y móviles en modo blog. Estas páginas tienen submenús, que son:

SEO: Escribir bien, Primeros pasos y Consejos, Metatags, Robots.

SEM: Marketing, Publicidad y Anuncios y e-commerce.

*Móviles:* SEO en Móviles y ASO.

Además tenemos la Tienda que tiene una cuenta, un carrito y finalizar compra.Y que veremos en el dossier de Tienda.

La última página es sobre nosotros donde están además las páginas fijas de Condiciones de envío, Política de Privacidad y Aviso legal.

En este sitio se podrá navegar de manera cómoda, en un entorno amigable y atendiendo a la usabilidad en un navegador web.

# Idea final para acceder a una web creada con Blogger

Al final el acceso que daremos desde el CRUD a los usuarios será a un blog creado con Blogger. En nuestro caso utilizaremos el blog:

# http://cetme77.tk/

El blog es del grupo de música de uno de los miembros COD, Carlos. El blog CETME 77, incluye:

Menú, Archivo PDF, Sonido Soundcloud, Pop-Up a Youtube, Slide & FanBox Twitter y Facebook, Script, Favicon, Adsense, Analytics, Subscripción, Cursor, Template modificado, Pie de página con Copyrigth, Contador de visitas, Enlaces a otros blogs, buscador, vídeo, archivo del blog, tags y revista. Hay varios post subidos actualmente y tiene un diseño responsive.



# Auditoría de las máquinas

Realizaremos la auditoría a las máquinas que tenemos. Empezaremos con las máquinas que llevan Linux y Debian Jessie. Para realizar la auditoría en estas máquinas utilizaremos Lynix. Lo primero de todo será crear un directorio dentro de /etc . Una vez hecho esto nos cambiamos a este directorio. Lo siguiente será conseguir de la web el paquete Lynis que viene comprimido.

```
cod2@raspberryp1:/$ sudo mkdir /etc/lynis/
mkdir: no se puede crear el directorio «/etc/lynis/»; El fichero ya existe
cod2@raspberryp1:/$ cd /etc/lynis
cod2@raspberryp1:/$ cd /etc/lynis$ sudo wget http://cisofy.com/files/lynis-1.3.7.tar.gz
--2017-03-09 15:55:13-- http://cisofy.com/files/lynis-1.3.7.tar.gz
Resolviendo cisofy.com (cisofy.com)... 37.97.224.115, 2a01:7c8:aac4:309::1
Conectando con cisofy.com (cisofy.com)[37.97.224.115]:80... conectado.
Petición HTTP enviada, esperando respuesta... 301 Moved Permanently
Localización: https://cisofy.com/files/lynis-1.3.7.tar.gz [siguiendo]
--2017-03-09 15:55:13-- https://cisofy.com/files/lynis-1.3.7.tar.gz
Conectando con cisofy.com (cisofy.com)[37.97.224.115]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 134683 (132K) [application/octet-stream]
Grabando a: ~lynis-1.3.7.tar.gz ''
lynis-1.3.7.tar.gz 100%[====>] 131,53K --.-KB/s en 0,1s
```

2017-03-09 15:55:13 (1,31 MB/s) - "lynis-1.3.7.tar.gz" guardado [134683/134683]

#### Después de esto desempaquetamos y descomprimimos



Nos movemos a la carpeta Lynis y ejecutamos un escaneo rápido de nuestro sistema

cod2@raspberrypi:/etc/lynis\$ cd /etc/lynis/lynis-1.3.7
cod2@raspberrypi:/etc/lynis/lynis-1.3.7\$ sudo ./lynis -c -Q

Una vez realizado el escaneo ya podemos ver como se encuentran nuestros equipos y los warnings que nos muestra.

```
Copyright 2007-2013 - Michael Boelen, http://rootkit.nl
Enterprise support and plugins available via CISOfy - http://cisofy.com
[+] Initializing program
                                                           [ DONE ]
 - Detecting OS...
  - Clearing log file (/var/log/lynis.log)...
                                                           [ DONE ]
    _____
 Program version: 1.3.7
Operating system: Linux
 Operating system: Linux
Operating system name: Linux
 Operating system version: 4.4.38+
Kernel version:4.4.38+Hardware platform:armv61Hostname:raspberrypiAuditor:[Unknown]Profile:./default.prfLog file:/var/log/lynis.logReport file:1.0
  - Checking profile file (./default.prf)...
                                                           [ WARNING ]
 - Program update status...
     Notice: Lynis update available
        Current version : 137 Latest version : 240
         Please update to the latest version for new features, bug fixes, tests
        and baselines.
[+] System Tools
  - Scanning available tools...
  - Checking system binaries...
                                                           [ FOUND ]
   - Checking /bin...
```

En nuestro caso hemos detectado errores en las actualizaciones del kernel de Linux en las Raspberrys. Todo lo demás lo encuentra y está actualizado dentro de nuestros sistemas Linux.

Este error de actualización puede que sea el causante de no haber podido realizar con éxito tareas como el cluster de alta disponibilidad y otras tareas parecidas.

[+] Logging and files	
<ul> <li>Checking for a running log daemon</li> <li>Checking Syslog-NG status</li> <li>Checking Metalog status</li> <li>Checking RSyslog status</li> <li>Checking RFC 3195 daemon status</li> <li>Checking minilogd instances</li> <li>Checking logrotate presence</li> <li>Checking log directories (static list)</li> <li>Checking open log files</li> <li>Checking deleted files in use</li> </ul>	[ OK ] [ NOT FOUND ] [ NOT FOUND ] [ FOUND ] [ NOT FOUND ] [ NONE ] [ OK ] [ DONE ] [ DONE ] [ FILES FOUND ]
[+] Insecure services	
- Checking inetd status	[ NOT ACTIVE ]
[+] Banners and identification	
<pre>- /etc/motd - /etc/motd permissions - /etc/motd contents - /etc/issue - /etc/issue contents - /etc/issue.net - /etc/issue.net contents</pre>	[ FOUND ] [ OK ] [ WEAK ] [ FOUND ] [ WEAK ] [ FOUND ] [ WEAK ]
[+] Scheduled tasks	
<ul> <li>Checking crontab/cronjob</li> <li>Checking atd status</li> </ul>	[ DONE ] [ NOT RUNNING ]
[+] Accounting	
<ul> <li>Checking accounting information</li> <li>Checking auditd</li> </ul>	[ NOT FOUND ] [ NOT FOUND ]
[+] lime and Synchronization	
<ul> <li>Checking running NTP daemon (ntpd)</li> <li>Checking running NTP daemon (timed)</li> </ul>	[ FOUND ] [ NOT FOUND ]



Después de hacer estos test esta es la puntuación que nos da Lynix.

Los mismos pasos los hemos seguido con el servidor Stark

stark@stark:/etc/lynis/lynis-1.3.7\$ sudo ./lynis -c -Q

🛃 stark@stark: /etc/lynis/lynis-1.3.7	- D >
Result: found 6 shells (valid shells: 6).	
[+] File systems	
- Checking mount points	
- Checking /home mount point	[ SUGGESTION ]
- Checking /tmp mount point	[ SUGGESTION ]
- Checking LVM volume groups	[ FOUND ]
- Checking LVM volumes	[ FOUND ]
- Checking for old files in /tmp	[ OK ]
- Checking /tmp sticky bit	[ OK ]
- ACL support root file system	[ ENABLED ]
- Checking Locate database	[ FOUND ]
[+] Storage	
	[ NOT DISABLED ]
- Checking firewire ohci driver (modprobe config)	[ DISABLED ]
[+] NFS	
- Check running NFS daemon	[ NOT FOUND ]
[+] Software: name services	
- Checking default DNS search domain	[ NONE ]
- Checking search domains	[ FOUND ]
- Checking /etc/resolv.conf options	[ NONE ]
- Searching DNS domain name	[ UNKNOWN ]
- Checking nscd status	[ NOT FOUND ]
- Checking BIND status	[ NOT FOUND ]
- Checking PowerDNS status	[ NOT FOUND ]
- Checking ypbind status	[ NOT FOUND ]
[+] Ports and packages	
- Searching package managers	
- Searching dpkg package manager	[ FOUND 1
- Ouerving package manager	
- Ouerv unpurged packages	[ NONE ]
- Checking security repository in sources, list file	[ OK ]
- Checking APT package database	I OK 1

Por último entramos en el servidor Targaryen y le hacemos un checkeo viendo los eventos, del sistema los logs que tenemos, los warnings que se han producido...

Event Viewer (Local)	Administrative Events	Number of events: 2.503	_	_		Action	Actions		
Image of the second secon	Y Number of events: 2	2.503				Adm	Administrative Events		
	J         Optimizer of exertisk action           B         Warning         09/03/2017 17:16:14           M         Warning         09/03/2017 17:16:13           M         09/03/2017 17:16:14<		Event Properties - Event 201, DeviceSetupManager           General Details         A connection to the Windows Metadata and Internet Services (WMIS) could not be established.           Log Name         Microsoft-Windows-DeviceSetupManager/Admin           Source:         DeniceSetupManager           Log Name         Microsoft-Windows-DeviceSetupManager/Admin           Source:         DeviceSetupManager           Level:         Warning           Level:         Warning           Usen         SYSTEM           OpCode         Info           More Information:         Source:			Saved Log Custom View Custom View Current Custom View Custom View Custom View Custom View Custom View n Task To This Custom View h 1 1, DeviceSetupManager - Properties			
	Generat Details A connection to the V Log Name: M Source Dr Event ID: 20 Level W Ilser SS	Vindows Metadata and Internet Servi icrosoft: Vindows-DeviceSetupManag exceSetupManager Logged: 1 Task Categ aming Kaywords STEAd Communication	Copy er/Admin 09/03/2017 17:18 jory: None TABCARVENI wir	14 sether		Close	Task To This Event		

El visor de eventos nos muestra errores que se han producido o determinadas alertas.

Además, vemos los recursos que utiliza o consume nuestro sistema tanto de memoria como CPU

File Monitor Help					Resource Monitor								
the second se													
Dverview CPU Memory	Disk N	letwork											
CPU	📕 3% CPU Usage	10	T 100% Maximum Frequency				<u>^</u> >	Views 🖛					
Image	PID	Description	5	itatus *	Threads	CPU	Average CPU	CPU	1005				
perfmon.exe	6252	Resource and Performance Monitor	F	Running	17	2	1.90						
salsenviexe	2332	SOL Server Windows NT - 64 Bit	r	Running	57	0	0.66						
sychost.exe (termsycs)	2996	Host Process for Windows Services	1	Running	40	0	0.10						
System Interrupts	and a second sec	Deferred Procedure Calls and Interrupt Service Routines	F	Running		0	0.05						
CSISS-exe	5568		F	Running	9	0	0.01		وي و و و و و				
explorer.exe	3896	Windows Explorer	F	Running	44	0	0.01						
Isass.exe	528	Local Security Authority Process	1	Running	32	0	0.01	60 Cassada	08/				
System	4.	NT Kernel & System	F	Running	114	0	0.01	Diale	100 100 (000				
rdpclip.exe	4956	RDP Clipboard Monitor	F	Running	9	0	0.01	L/ISK	TUU KB/SEC				
dwm.exe	4676	Desktop Window Manager		Running	12	D	0.01						
 Disk		8 KB/sec Disk I/O		0% Highest Acti	ve Time		0						
Metunde	_	E of Share Mahanak (17)		OF Mahuark Little			Tesefi (A)		4				
vetwork		B to kops network tro		Use network out	ezation		100	O DISTAN	A A A A A				
mage	PD	Address			Send (B/sec)	Receive (B/sec)	Total (B/sec)	=	0				
svchost.exe (termsvcs)	2996	DESKTOP-KAPTXOS			10.551	1,246	11.797	Network	1 Mbps				
vchost.exe (termsvcs)	2995	TARGARYEN.asir.pother			0	279	279		ين ک کر ک ک ک				
ins exe	1476	TARGARYEN.asir.pother			727	96	223		و و و و و و				
sass.exe	528	TARGARYEN.asir.pother			90	127	217		کے کے ایک کے لیے اور اور				
System	4	192,168,2,255			0	174	174						
wchost.exe (DHCPServer)	1460	255,255,255,255			5	136	141						
ins.exe	1476	TARGARYEN.asir.pother			0	75	75	MA ALA					
wchost.exe (NetworkService)	1064	224.0.0.252			0	62	62	Concernance of the	0				
dns.exe	1476	DESKTOP-643106A			62	0	62	Memory -	100 Hard Faults/sec				
sass.exe	528	TARGARYEN.asir.pother			12	50	61 4						
Memory		I O Hard Faults/sec		38% Used Physical Memory									
mage	PD		Hard Faults/sec	Commit (KB)	Working Set (KB)	Shareable (KB)	Private (KB)						
ServerManager.exe	4356		0	141.968	180.656	85.536	94.120						
ServerManager.exe	5624		0	148.495	121,372	34,724	86.548						
dns.exe	1476		0	89.772	87.528	7.536	79.992		يركد بيرك يوج				
solsenv.exe	2332		0	267.384	89,148	21.864	67.284		L				
wchost.exe (termsycs)	2996		0	64.055	72,860	30,704	42,156						
sass.exe	528		0	49,405	59,900	18,428	41.472						
typiotet eve	3896		0	49.848	101.050	61.192	39.868						
	5005			+33,646		53,645	33,440	~					

Como podemos ver tenemos suficientes herramientas y muy visuales en Windows para monitorear el sistema, ver los recursos que consumimos y como afecta esto a nuestro servidor.

<u>8</u> /				Resource Moni	tor					- 6
File Monitor Help										
Overview CPU Memory	y Disk Network									
Processes		📕 38% Used Physical Me	mory						3	Views 🔽
_ Image	PID			Hard Faults/sec	Commit (KB)	Working Set (KB)	Shareable (KB)	Private (KB) 🗠	Used Physical N	lemony 100% -
ServerManager.exe	4356			0	141.916	180.620	86.536	94.084		
ServerManager.exe	5624			0	154.396	125,740	34.724	91.016		
dns.exe	1476			0	90.048	87.540	7.536	80.004		و بر بر بر بر بر
sqisenmexe	2332			0	267.384	89,148	21.588	67.560		وي و بر و و
sychost exe (termsycs)	2996			٥	64.224	74.452	31.212	43.240		
lsass.exe	528			0	49,304	59.732	18.424	41.308		
explorer.exe	3896			0	47.892	100.076	61.204	38,872	60 Seconds	0%
sychost exe (netsycs)	892			0	30.832	47.42B	23.956	23.472	Commit Charge	e 100% 7
explorer.exe	4780			0	35.620	87.548	65.612	21.936		وي و و و و
ServerManager.exe	5280			0	123,100	38,220	15,424	21.796 *		
Physical Memory		📕 1577 MB in Use			2365 MB Availab	le	_	$\odot$		
Hardware Rest 3 MB	nved E	in Use 1577 MB	Modified 131 MB Cached Total Installed	2385 MB 2285 MB 927 MB 4095 MB 4095 MB		1589 N	46		Hard Faults/sec	0% J
								~	-	17/05



Auditoría web de nuestro sitio COD

# Bibliografía

Apuntes y documentación de las asignaturas del proyecto <u>http://kanbantool.com/es/metodologia-kanban</u> <u>https://www.raspberrypi.org/downloads/raspbian/</u> Edrawsoft → Diagramas

Método Kanban https://github.com/CODasir16/COD https://waffle.io/CODasir16/COD https://subefotos.com/

# Video animado sobre el proyecto Pothers

https://www.youtube.com/watch?v=x4ZI7UOZu9U&feature=youtu.be

Creado con: <u>http://wideo.co/</u> → <u>http://www.wideo.co/view/18880501486307347686?utm\_source=CopyPaste&utm\_m</u> <u>edium=share&utm\_campaign=sharebox</u> MusicMaker Imágenes y gifs (Google)

Música: Code Or Digit - Digital Pop, MusicMaker, Carlos del Cerro