



salesianos

ATOCHA

Departamento de Electrónica e Informática



NacreDECK

Dispositivo Proxy Portátil

- Proyecto fin de ciclo ASIR -

Autor

Jorge Gonzalez

Tutor

Samuel Arranz de Andrés

Junio de 2021

Manual Operativo de Usuario

1. Introducción.....	4
1.1. Terminal Futurista. Sistema y Administración.....	4
1.1.1. Servidor Proxy.....	6
1.1.2. Sistema IDS.....	7
2. NacreDECK. Equipo Futurista.....	8
2.2. Disposición y puesta en marcha.....	10
3. NacreADMIN. Servicio Web.....	14
3.1. Introducción.....	14
3.2. NacreADMIN tipo 0.....	15
3.3. NacreADMIN tipo 1.....	16
3.4. Manual de Uso.....	17
3.1.1. PROXY.....	18
3.1.2. USERS.....	20
3.1.3. MISCELLANY.....	22
4. Conclusiones Personales.....	23
4.1. Introducción.....	23
4.2. Conclusiones sobre el trabajo realizado.....	23
4.3. Ampliaciones y Mejoras.....	24

Memoria Ilustrativa de Trabajo

1. Introducción.....	26
1.1. NacreDECK, visión de concepto.	26
1.1.1. Propuesta.....	26
2. Planificación y costes de desarroll.....	27
2.1. Estado de arte y Valoración de Alternativas.	27
2.2. Costes de Desarrollo.....	29
3. Diseño Estructural.....	31
3.1. Diseño Arquitectónico.....	31
3.1.1. Hardware interno.....	37
4. Diseño de Datos.....	39
4.1. Servicios del NacreDECK.....	39
4.1.1. Apache, Core web. PHP.....	40
4.1.2. MariaDB, Base de Datos SQL.....	41
4.1.3. SQUID.....	42
4.1.4. BASH.....	43
5. Pruebas de Control.....	45
5.1. Esquematización.....	45
5.2. Depuración y scripts.....	47
6. Bibliografía.....	65
6.1. Direcciones web / Referencias.....	65
6.2. Comentarios finales.....	66

1. Manual Operativo de Usuario

Por Jorge Gonzalez Gallego

UN
R

ユーザー !!

1. Introducción

1.1. Terminal Futurista. Sistema y Administración.

Presentando un concepto que aúna el vigor de la tecnología en los 80 con la eficiencia del presente, **NacreDECK (ND)** cuenta en su exterior con un elegante cuerpo de madera resistente al agua, con un teclado y ratón trackball, así como una sucesión de interfaces y puertos frontales. En su interior ofrece un sofisticado sistema de proxy operable portátil, con múltiples funciones enfocadas a la seguridad y la protección de tus equipos.

Con él será capaz de gestionar de forma eficiente y veloz el tráfico entrante y saliente de su red, así como asignar parámetros de control en función de sus necesidades.

Este equipo es manejado en su núcleo por un potente servicio de monitorización y prevención de usos dañinos en su red. **NacreADMIN**, un **software exclusivo** que unifica las facilidades de proxy y monitorización respectivamente. Unifica las prestaciones de *SQUID* y de sus *registros de empleo de red*.

Dicho servicio actúa bajo un **debian** modificado y simplificado. Añadiendo múltiples servicios de seguridad y pentesting:

Como ya se ha mencionado, El ND ofrece la posibilidad de regular y controlar las operativas de red de todos los equipos, todo ello a través de **NacreADMIN**. Un sencillo pero completo servicio gestor web capaz de monitorizar a tiempo real y desde cualquier lugar el flujo de paquetes entre IP, (Ver 2.2.2. NacreAdmin tipo 0 / 1)

Administración del ND:

- **Control de ACLs por Sistema jerárquico de monitorización.**
 - NacreAdmin permite a los administradores de red facilitar control de proxy Externo (Ver 1.1.1. Servicio Proxy), será capaz de regular minuciosamente que pueden o no hacer sus equipos en Internet.
- **Listado de tráfico personalizado.**
 - Podrá filtrar por IP el trafico de cada equipo de su red. Dispondrá de forma simplificada el numero y el tipo de peticiones, siendo asi capaz de reconocer movimiento sospechoso o no deseado. (Ver 1.1.2. Servicio IDS).
- **Gestión de usuarios de red.**
 - Regule quien puede o no usar NacreAdmin y sus funciones. Como administrador podrá consultar el registro de accesos de usuarios al organismo administrativo.

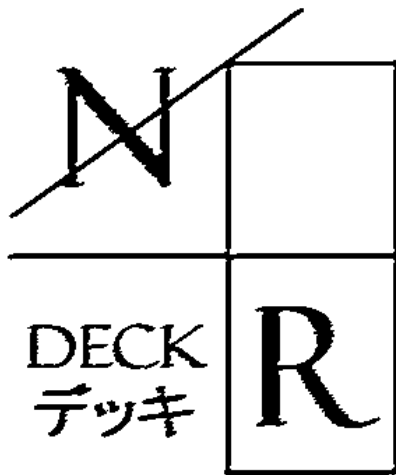


Ilustración 1

NacreDECK. El IDS Proxy portátil

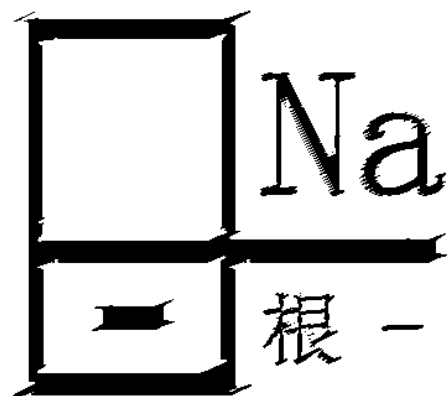


Ilustración 2

NacreAdmin. La herramienta administrativa web.

1.1.1. Servidor Proxy

Se entiende generalmente por Proxy como el ‘intermediario’. Este efectúa el rol de puente entre emisores y receptores en una red, filtrando los paquetes que pasan por la misma a través de su propia dirección IP.

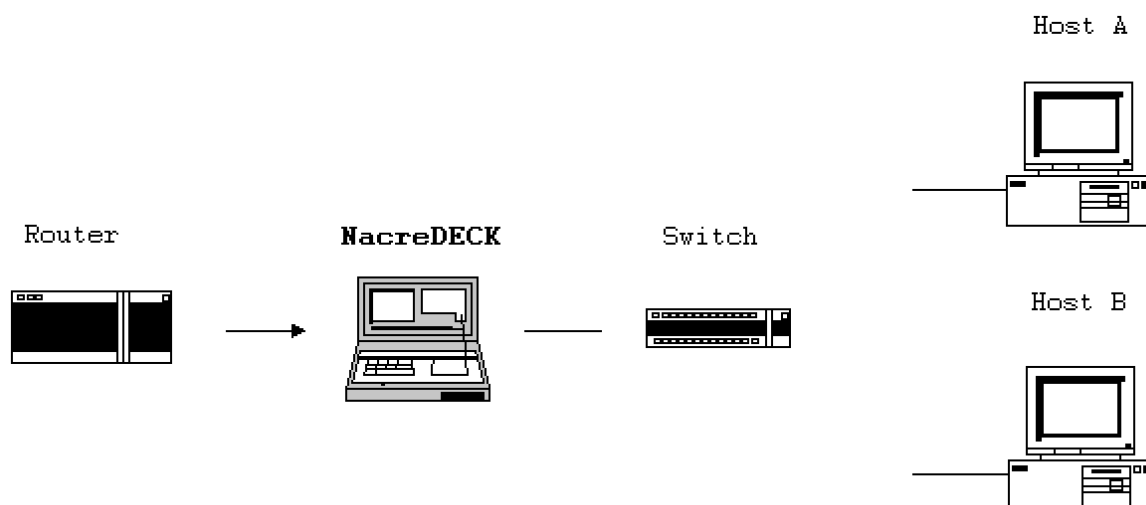
Un proxy puede:

- Controlar Accesos.
- Registrar el tráfico.
- Restringir en función del tráfico.
- Mejorar el rendimiento.
- Cache web.
- Anonimato.

Una mala gestión de proxy puede provocar flujo de datos con paginas maliciosas, resultando en malware y/o visitantes no deseados. No solo el riesgo acontece las paginas que no queremos acceder, si no aquellas que son ajenas al carácter profesional de la empresa (ocio o distracciones) y por tanto, conviene restringir al acceso de sus empleados.

Existen, en función de si la petición es ajena o no. tanto **Proxy Internos** como **Proxy Externos**, El ND es un ejemplo de lo segundo. A través de un proxy Externo pasa todo el contenido exterior a la red local, siendo así filtrado en el proceso con las reglas que se deseen estipular. (Para reglas aplicables ver 1.2. Requisitos e instalación).

ND actuará sobre todos los equipos del sistema, permitiendo al administrador filtrar todo el contenido que entra y sale de su empresa.



1.1.2. Sistema IDS

La información privada circulante en redes de sistemas TI es un objetivo tentador frente a ciberdelincuentes y extorsionadores. Asegurar la integridad de sus datos y los de su equipo es primordial a la hora de trabajar en la red y es por ello por lo que hoy contamos con los **servicios de detección y/o prevención (IDS / IPS)**.

Los delincuentes de la red casi siempre dejan un rastro notable por donde quiera que ambulen, un sistema IDS será capaz de notificar dichas trazas sospechosas monitorizando la red y anticipándose de forma preventiva al ataque.

El NacreAdmin permite una gestión IDS completa en su red de equipos. Contará así con un sólido **software de gestión** cuyo uso puede detectar accesos no autorizados en un sistema o red de ordenadores, y en base a ello, **generar alertas (logs)** que podrá gestionar

2. NacreDECK. Equipo Futurista.

2.1. Introducción

No olvide que su dispositivo ND también **funciona como un terminal independiente y operable**. Significa que para trabajar con el únicamente deberá accionar los **interruptores frontales** y suministrarle 5 V por su entrada USB tipo C (Podrá utilizarlo en cualquier parte haciendo uso de una batería portátil).

2.1.1. Hardware

En el frontal encontrará dos interruptores. **Pantalla y Energía general** respectivamente.

El ND iniciará como un equipo corriente, podrá interactuar con su interfaz a través del **teclado y trackball**. O si lo desea, hacer uso de las **capacidades táctiles** de la **pantalla Full HD de 7 pulgadas**.

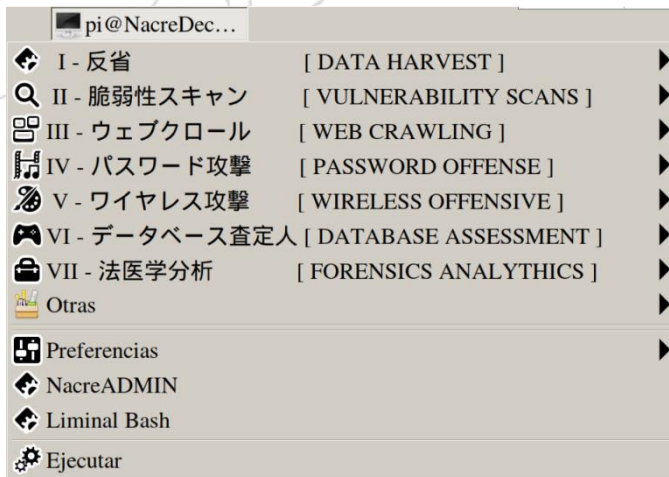
Posee un **hub de puertos USB**, así como dos **interfaces de red (0,1)** operables.

2.1.2. Software

Como ya se ha mencionado, **El NacreDECK opera en base** a una distribución de **Linux**; un **Debian 32x** modificado.

En su menú principal, encontrará una serie de subcategorías con herramientas enfocadas a la seguridad ofensiva.

Herramientas como **Maltego** o **Nmap**, separadas por categorías distintivas, podrá emplear su ND como un equipo *custom* de haking ético.



Tendrá acceso directo a las principales aplicaciones de *linux* por **interfaz grafica** a través de este menú. Haga click en el **recuadro transparente** de la esquina superior izquierda, o presione la tecla de **Windows** (o su equivalente en el teclado que desee usar) para desplegarlo

El sistema del NacreDECK incluye como obsequi la ultima versión de **Liminal_Bash.sh**. Una aventura de texto generada proceduralmente en base **bash**. ¡No olvide probarla!.

```
pi@NacreDeck:/$ ./Liminal_3_6.sh
-----
LIMINAL SPACES RNG GAME. Nacre Repo 2/6
-----

*) Consultar status
1) Nuevo evento / Explorar otro mundo
2) Buscar en el Mundo actual
3) Pelear
d) Lanzar un dado
e) Esconderse
r) Meditar
h) Comandos
m) Manual, Como jugar
-) Generar un personaje nuevo
s1 Modificar mi salud
s2 Modificar salud enemigo
a1 Explorar evento concreto (debug)
k) Liquidar enemigo (debug)
.) Salir.
-----
SALUD:          1
ATAQUE:        4
-----
He despertado en una sala oscura
```

2.2. Disposición y puesta en marcha.

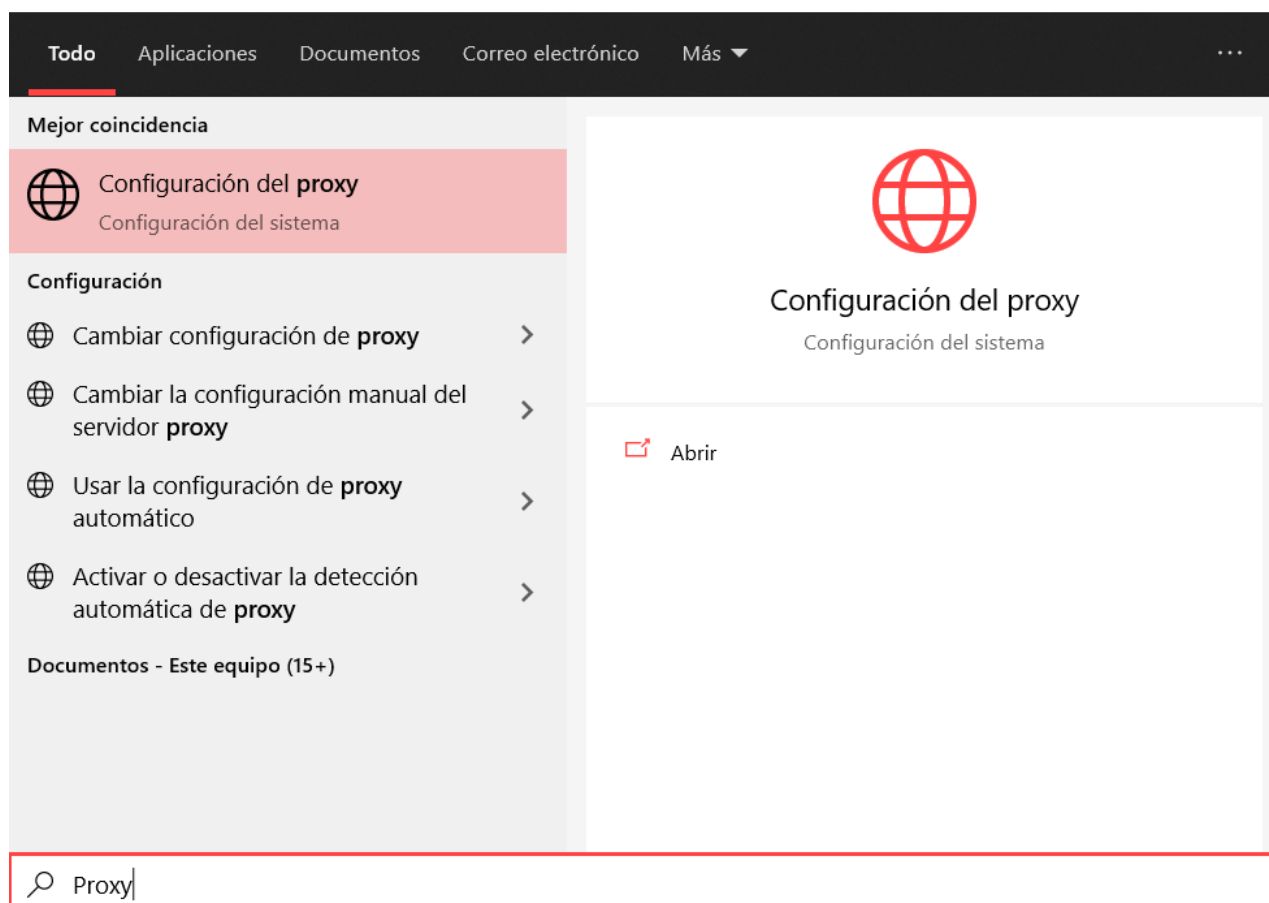
El ND **no requiere de configuración inicial**. Su servicio proxy estará disponible desde el minuto 1 de acción, tan solo **necesitará conectarlo a su red** y conocer la **IP local**.

No obstante. **Para identificar el ND. Necesitará configurar un proxy en sus equipos**. Tarea sencilla y no llevará mas de un minuto.

2.2.1. Proxy ND en Windows.

Acceda desde el menú inicio a la configuración de *Proxy*.

También puede usar la ruta *Configuración/Red e internet/Proxy*



A continuación. Deberá indicar la **IP Local** del NacreDECK, así como el **puerto de Proxy Squid**. (Por defecto 3128).

Configuración manual del proxy

Usa un servidor proxy para conexiones Ethernet o Wi-Fi. Esta configuración no se aplica a conexiones VPN.

Usar servidor proxy **IP Local. ND Puerto**

Activado

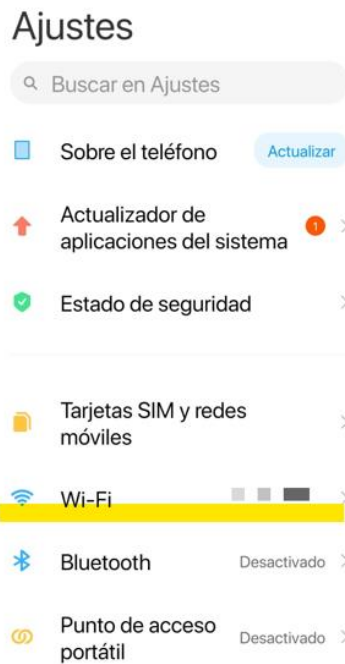
Dirección	Puerto
<input type="text" value="192.168.1.59"/>	<input type="text" value="3128"/>

Usar el servidor proxy excepto para direcciones que empiecen con las siguientes entradas. Usa el punto y coma (;) para separar las entradas.

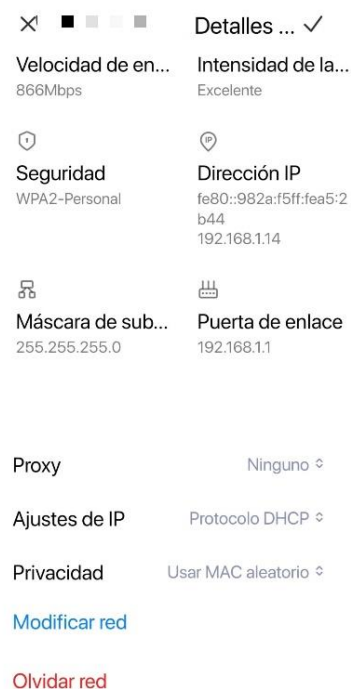
No usar el servidor proxy para direcciones locales (intranet)

2.2.2. Proxy ND en Android.

Acceda desde el menú de **configuración** del terminal a **ajustes de Wi-Fi**.



Acto seguido. Seleccione la **red Wi-Fi a la que se encuentre conectado** y baje hasta el **final de la pagina**.



Verá que no hay ningún proxy conectado, toque la opción en cuestión. E indique **Proxy Manual**.

A continuación. Deberá indicar la **IP Local** del NacreDECK, así como el **puerto de Proxy Squid**. (Por defecto 3128).

The screenshot shows a network configuration window with a title bar containing a close button (X), a window control bar with four colored squares (black, grey, light grey, dark grey), and a maximize button (checkmark). Below the title bar, there are two sections: 'Máscara de sub...' with the value '255.255.255.0' and 'Puerta de enlace' with the value '192.168.1.1'. The main section is titled 'Proxy' and has a dropdown menu set to 'Manual'. Below this are three input fields: 'Nombre de host' with the value '192.168.1.59', 'Puerto' with the value '3128', and 'Derivar a' with the value 'example.com,mycomp...'. At the bottom, there are two more dropdown menus: 'Ajustes de IP' set to 'Protocolo DHCP' and 'Privacidad' set to 'Usar MAC aleatorio'. Below these are two buttons: 'Modificar red' in blue and 'Olvidar red' in red.

3. NacreADMIN. Servicio Web.

3.1. Introducción.

El ND permite una configuración completa y accesible desde **NacreADMIN (NA)**. Este servicio consiste en una plataforma web alojada en el equipo, llevado por una base de datos de usuarios con varios privilegios de acción. (ver 3.2.1. y 3.2.2. NacreADMIN tipo 0 y 1).

NA Podrá ser **accesible desde:**

- El mismo **Nacre Deck:**
Introduciendo *localhost* o <https://127.0.0.1/> en cualquier navegador. NA se hospeda a través del servicio Apache, Será accesible desde la dirección de *loopback del dispositivo*.
- Equipos de la **misma red:**
Introduciendo la **IP Local** del ND en cualquier navegador. Desde ordenadores y equipos ofimáticos hasta tablets y telefonos Android o IOS. NA.

Nada más acceder, encontrará un formulario de acceso, en caso de no tener una cuenta, podrá **crear una** para acceder como usuario (*tipo 1*).



NacreADMIN
Administrative Service.

A screenshot of a web login form. At the top, there is a black header with the text 'Log in' in white. Below the header, there are two input fields: 'Nickname' and 'Password'. To the right of the 'Password' field is a 'Log in' button. Below the input fields, there is a horizontal line and a link that says 'Create a new account into the Nacre Deck here.'

Podemos diferenciar dos tipos de usuario en NacreADMIN; El usuario genérico (*tipo 1*) y el usuario administrador o root (*tipo 0*).

3.2. NacreADMIN tipo 0

Existe un único usuario tipo 0, El usuario **Admin/123**.

Será necesario usar esta cuenta para poder gestionar enteramente NA. No se pueden crear cuentas nuevas con privilegio 0 y solo puede haber una. Es la única capaz de aplicar reglas de acceso y modificar como super-usuario el NacreDECK

En caso de querer cambiar la contraseña o nombre de esta cuenta, podrá hacerlo desde la sección *USERS/NacreADMIN*.

NacreADMIN User Database Entries.
Logger of NacreADMIN database general users.

User	Hash	Role
Admin	6116afedcb0bc31083935c1c262ff4c9	Administrator

Haga click sobre su rol, en color verde. Se abrirá un formulario.

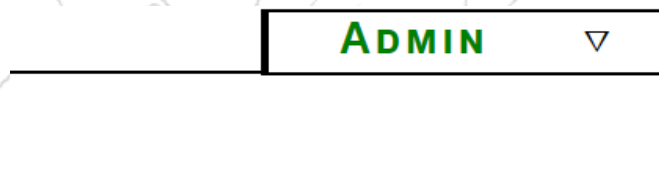
Modify Type 0 Account

Nickname

Password

[Get back](#)

El tipo 0 es el **usuario maestro**, tiene acceso a todas las funcionalidades del servicio, Será distinguible por el **color verde** de la pestaña superior derecha



3.3. NacreADMIN tipo 1

Los usuarios tipo 1 son todos aquellos que quieran usar NacreADMIN como **herramienta de consulta** de aquellas directrices establecidas por el tipo 0. **Cualquiera puede crear una cuenta con este nivel de acceso.**

En la pantalla de inicio de sesión. Haga click en **crear una nueva cuenta**.

Log in

Nickname

Password

Create a new account into the Nacre Deck **here**.

Introduzca un **nombre** que no esté ya en la base de datos seguido de una **contraseña**

Create Account

Nickname

Password

Como podrá comprobar, el usuario tipo 1 posee un color **rojo**

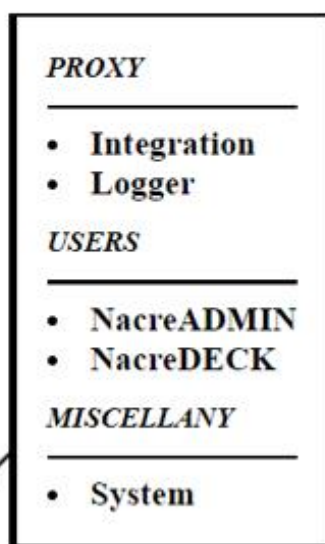
TEST ▾

3.4. Manual de Uso

Independientemente del tipo de usuario. NacreADMIN separa sus posibilidades a través de un **menú contextual con forma de recuadro**. Esquematizado en tres grupos principales.

NacreADMIN.

Administrative Service. **ROOT**



<i>PROXY</i>
• Integration
• Logger
<i>USERS</i>
• NacreADMIN
• NacreDECK
<i>MISCELLANY</i>
• System

- **PROXY**

Comprende los menús principales de *integración* de parámetros en la red y de *consulta* de estos.

- **USERS**

Permite **gestionar los usuarios** presentes en la base de datos de *NacreADMIN* y del propio equipo *NacreDECK*.

- **MISCELLANY**

Ofrece la **configuración general** tanto del NA como del ND.

3.1.1. PROXY

Como ya sabe, la principal característica del NacreDECK es su función como proxy de fácil configuración.

a) En la pestaña **Integration**. Podrá interactuar con las reglas de proxy:

- **Permitted IPs** consiste en una tabla ampliable con las IP locales que el administrador **desea habilitar en la red**. El NacreDECK hará cómputo de la tabla y aplicará la directriz a los pocos segundos.

Ej) al indicar la IP 192.168.1.50. El sistema dará acceso fuera de red local al equipo asociado a dicha dirección.

- **Denied Expressions** se trata de otra lista ampliable contando por el contrario con **expresiones regulares** prohibidas.

Ej) Al indicar palabras como Facebook o Youtube. El ND denegará el acceso a cualquier página que contenga en su URL dicha expresión en cualquier formato o tipo a toda IP permitida.

The screenshot shows a web interface with a top navigation bar containing the text 'ADMIN' and a dropdown arrow. Below the navigation bar, there are two main configuration sections. The first section is titled 'Permitted IPs' and includes a horizontal line, a descriptive text 'This is the list of addresses which will be allowed from the ND network.', and a table with a single header 'IPs' and a blacked-out content area. The second section is titled 'Denied Expressions' and includes a horizontal line, a descriptive text 'The next list tells ND which words has to exclude from it's network.', and a table with a single header 'Expression' and a blacked-out content area. A plus sign is centered between the two sections.

b) En la pestaña **Logger**. Se mostrará **Un registro completo** de la actividad de los equipos conectados a la red a través del ND.

Verá que a través de tres columnas, se segmenta la **información de IP, Dirección de la petición** y el **estatus** de la misma respectivamente

Con rol de administrador. Podrá filtrar la información por número de filas. Pudiendo así ver registros tan antiguos como desee.

Ej) La IP .83 es la de un equipo concreto de su oficina. Sospecha que pueda merodear paginas ajenas al carácter de la empresa. Tan solo deberá listar las últimas líneas y observar sus últimos movimientos.

Network Log

Last activity entries in proxy network. Filter by number of lines below.

15 Filter

IP	Address	Status	Date
192.168.1.83	http://192.168.1.59/class.css?	MISS	Wed Jun 16 10:19:31
192.168.1.83	http://192.168.1.59/index.php?	MISS	Wed Jun 16 10:19:31
192.168.1.83	af.opera.com:443	TUNNEL	Wed Jun 16 10:19:31
192.168.1.83	speeddials.opera.com:443	TUNNEL	Wed Jun 16 10:19:28
192.168.1.83	speeddials.opera.com:443	TUNNEL	Wed Jun 16 10:19:28
192.168.1.83	http://192.168.1.59/class.css?	MISS	Wed Jun 16 10:19:25
192.168.1.83	s.pwt.soundcloud.com:443	TUNNEL	Wed Jun 16 10:19:25
192.168.1.83	error:transaction-end-before-headers		Wed Jun 16 10:19:25
192.168.1.83	http://192.168.1.59/index.php?	MISS	Wed Jun 16 10:19:25

Un usuario corriente de NacreADMIN podrá consultar las implementaciones de proxy y los registros de acción. Pero no podrá ni crear ACLs ni filtrar en profundidad. Nuevamente, tan solo el tipo 0 es capaz de tomar control del NacreDECK.

3.1.2. USERS

La segunda división de opciones comprende a los **usuarios de ambos servicios**, *NacreDECK* y *NacreADMIN*.

a) NacreADMIN


- Aquí podrá listar todos los usuarios que forman la base de datos de la administración de su equipo, tendrá tres columnas, **Nombre de usuario**, **Hash de contraseña MD5** y el **Rol** determinando.

Ej) Cree que alguien no deseado ha creado una cuenta en NacreADMIN, Desea consultar algún cambio

- Recuerde que puede cambiar los parámetros de su cuenta tipo 0 desde esta tabla, **clikando en el rol de Administrador**

NacreADMIN User Database Entries.

Logger of NacreADMIN database general users.

User	Hash	Role
Admin	6116afedcb0bc31083935c1c262ff4c9	<u>Administrator</u>
	6116afedcb0bc31083935c1c262ff4c9	User

b) NacreDECK

- Esta sección es exclusiva al tipo 0. Podrá ver en una tabla **todos los usuarios del sistema Linux** del ND. Encontrará el **nombre y directorio de conexión**, así como el **UID y GUID** asociados.

Como verá, se trata del fichero *passwd* del sistema. Filtrado y esquematizado para una correcta lectura.

Ej) Similar al anterior. En caso de manipulación al sistema general del proxy, aquí podrá consultar nuevos usuarios y el GUID asociado. Patrones sospechosos o simplemente irregularidades, todo a un click.

NacreDECK User OS Entries.

Logger of NacreDECK system general users.

Name	Folder	UID	GUID
root	/root	0	0
daemon	/usr/sbin	1	1
bin	/bin	2	2
sys	/dev	3	3
sync	/bin	4	65534
games	/usr/games	5	60
man	/var/cache/man	6	12
lp	/var/spool/lpd	7	7
mail	/var/mail	8	8
news	/var/spool/news	9	9
uucp	/var/spool/uucp	10	10
proxy	/bin	13	13
www-data	/var/www	33	33
backup	/var/backups	34	34
list	/var/list	38	38

3.1.3. MISCELLANY

Este ultimo segmento ofrece la **configuración general**. Aquellos parámetros que disten de los anteriores, **opciones que se agrupan en una sola tabla** para la comodidad del administrador o usuario.

a) System

System Settings

Hostname

1) **Nombre del NacreDECK en la red.**

Ethernet(0)

2) **IP del puerto proxy actual.**

Proxy Port

3) **Puerto proxy actual.**

Server Status

4) **Estatus del proxy y tiempo.**

Reload Services

5) **Recargar servicios manualmente**

Hostname

6) **Cambiar nombre del ND en la red**

System Time

Current System Time

7) **Habilita y deshabilita el protocolo NTP asociado a la hora actual**

Listen Settings

HTTP Port

8) **Modifica los puertos de escucha**

HTTPS Port

NacreADMIN Appearance

Display Color

9) **Personalización visual de NA.**

Background Color

NacreADMIN Miscellany

Reboot the NacreDECK.

10) **Reiniciar o apagar el sistema NacreDECK**

Turn Off the NacreDECK.

4. Conclusiones Personales

4.1. Introducción.

Me gustaría, para terminar este manual al uso de mi proyecto. Aportar lo que son mis visiones y mi perspectiva general del proceso. Ahondando en motivaciones y conclusiones tanto finales como iniciales

4.2. Conclusiones sobre el trabajo realizado.

NacreDECK viene de mis ganas por ofrecer un proyecto acorde con mis expectativas ante el curso, y también ante mi futuro profesional. Pretende ser un equipo único, a medida, en el que aplicar todo lo que he aprendido en el centro y lo que no.

Mi pasión por el estilo antes que la sustancia me ha hecho tropezar varias veces con las mismas piedras. Encontrando un duro conflicto a la hora de aplicar mis capacidades, años atrás siempre he preferido que algo sea bonito que a que sea verdaderamente útil.

He pasado en Salesianos de Atocha 4 años. Cursando 2 ciclos formativos; Telecomunicaciones e informática. Durante todo ese tiempo, he aprendido no solo a enfrentarme a nuevos retos, si no a enfrentarme a mi mismo. Puedo decir que soy otra persona completamente diferente a la despedida del colegio Salesiano.

Bien. Esta es mi aportación. *NacreDECK* unifica todo lo que he aprendido, ya sea a nivel informático como electrónico. Y lo plasma como un equipo completamente funcional del que me siento orgulloso y feliz de poder mostrar tras tanto tiempo en mi cabeza. La mezcla que buscaba entre estilo y aplicación.

4.3. Ampliaciones y Mejoras

EL ND dista mucho de ser perfecto. Sus sistemas, pese a ser funcionales, son básicos en la ejecución. **En la segunda parte de la memoria plantearé como ha sido el desarrollo de este proyecto.**

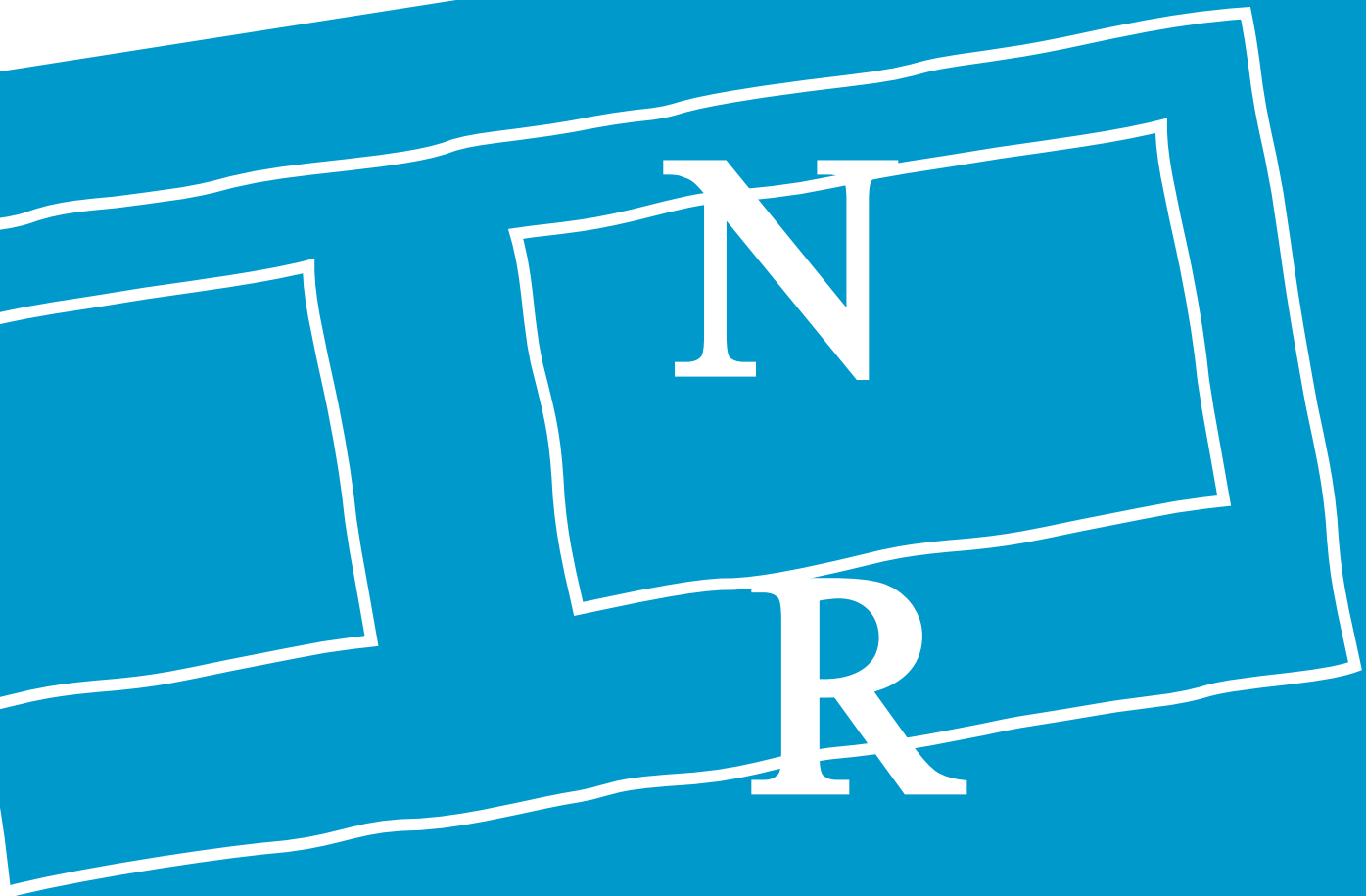
Honestamente, deseo seguir trabajando en este proyecto, para ello aun he de seguir avanzando como persona y como profesional. Tal vez algún día tenga el conocimiento necesario para hacer del NacreDECK el equipo Retro futurista de mis sueños.

Podría ampliar la sección *Miscelánea*, así como la *aplicación de ACLS* y la *consulta de las interacciones de red*. La verdad y visto con perspectiva, las **posibilidades son infinitas.**

Bien. Volviendo al presente, creo que he aplicado todo lo que se de la mejor forma posible. Este proyecto lo siento solido y capaz de hablar por si solo.

2. Memoria Ilustrativa de Trabajo

Por Jorge Gonzalez Gallego



ユーザー !!

1. Introducción

La siguiente sección pretende reflejar punto a punto mi desempeño en este proyecto, desde el primer momento en que se pasó por mi cabeza este concepto hasta estos escasos días antes de su presentación.

1.1. NacreDECK, visión de concepto.

1.1.1. Propuesta

Continuando mis conclusiones previas pero ahora ahondando en lo técnico. Este proyecto apareció en mi cabeza poco después de finalizar el Grado Medio. Visualizaba un servicio o servicios, pero siendo llevado a cabo por una máquina, algo creado o estructurado plenamente por mí.

Se fijó un concepto en mi cabeza, el género literario *cyberpunk*. Tenía en mente crear un sistema que fuera resistente a todo, completamente portátil. Algo así como un superviviente de guerra nuclear. Siempre girando en mi cabeza este concepto de *Netrunning*. La seguridad informática llevada al futurismo.

Los primeros prototipos aparecían en mi mente. **Un maletín**. Adquiriré un maletín de herramientas o un contenedor horizontal pequeño con el que comenzar a hacer electrónica y poner el huevo que podría ser una RB Pi o un Arduino.

2. Planificación y costes de desarrollo

2.1. Estado de arte y Valoración de Alternativas.

En etapas muy tempranas de desarrollo, planteo hacerme con uno de estos y modificarlo hasta conseguir lo que quería. Mirando con retrospectiva puedo decir que no fue una idea muy brillante

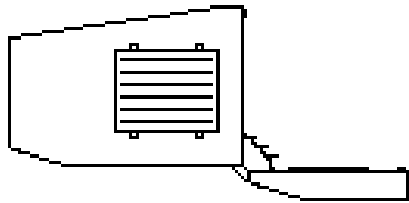


Yato YT-0882 - Caja para herramientas Yato

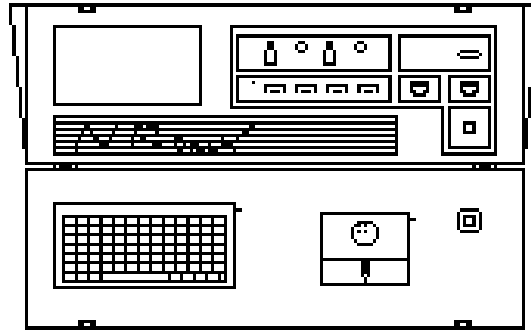
★★★★★ 15

Ningún chasis me convencía, pase días enteros pensando en la carcasa perfecta para mi dispositivo de ciberseguridad futurista. Hasta que finalmente abandone la búsqueda y me limite a programar el servicio en cuestión.

Un día, mi padre me sugirió la idea y me motivo a llevarla a cabo. Recuerdo ese día como ayer, pase dos días enteros haciendo bocetos y diseñando lo que sería el *primer prototipo del ND*.



SQUID



Este diseño surgió hace poco menos de un año, y se ha mantenido en mi cabeza todo este tiempo, **variando lo menos posible.**

Ya contaba con una Rasberri Pi del año anterior, y ya tenía claro que necesitaba mi proyecto así que invertir en **productos que encontré en amazon** con la esperanza de que este puzzle tan bien formado en mi cabeza encajara.

2.2. Costes de Desarrollo.

Hice un total de dos compras. Primero el hardware de cara a mi rbPI y luego el que sería el chasis que formaría el NacreDECK

Primero, me aseguré de tener un **teclado y pantalla** de calidad. Así como los **extensores** que en algún momento colocaría en el frontal de mi dispositivo, fuera como fuera cuando llegara el momento.



para Pantalla Raspberry Pi 4,
Monitor táctil de 7 Pulgadas con
Teclado USB Funda de Cuero
Pantalla táctil capacitiva IPS...

64,99€



TP-Link UE300 -Adaptador USB 3.0
A Gigabit Ethernet 10/100/1000, PC
O Portátiles , Blanco

★★★★☆ ~ 6.124

11,50€ ~~29,99€~~



Patrocinado ⓘ

Perixx PERIPRO-506 - Ratón con
USB Trackball (ratón – 100 x 80 x 42
mm – 25 mm – Trackball Brillante –
reposa Palmas de Gel extraíble –...

★★★★☆ ~ 213

31,99€



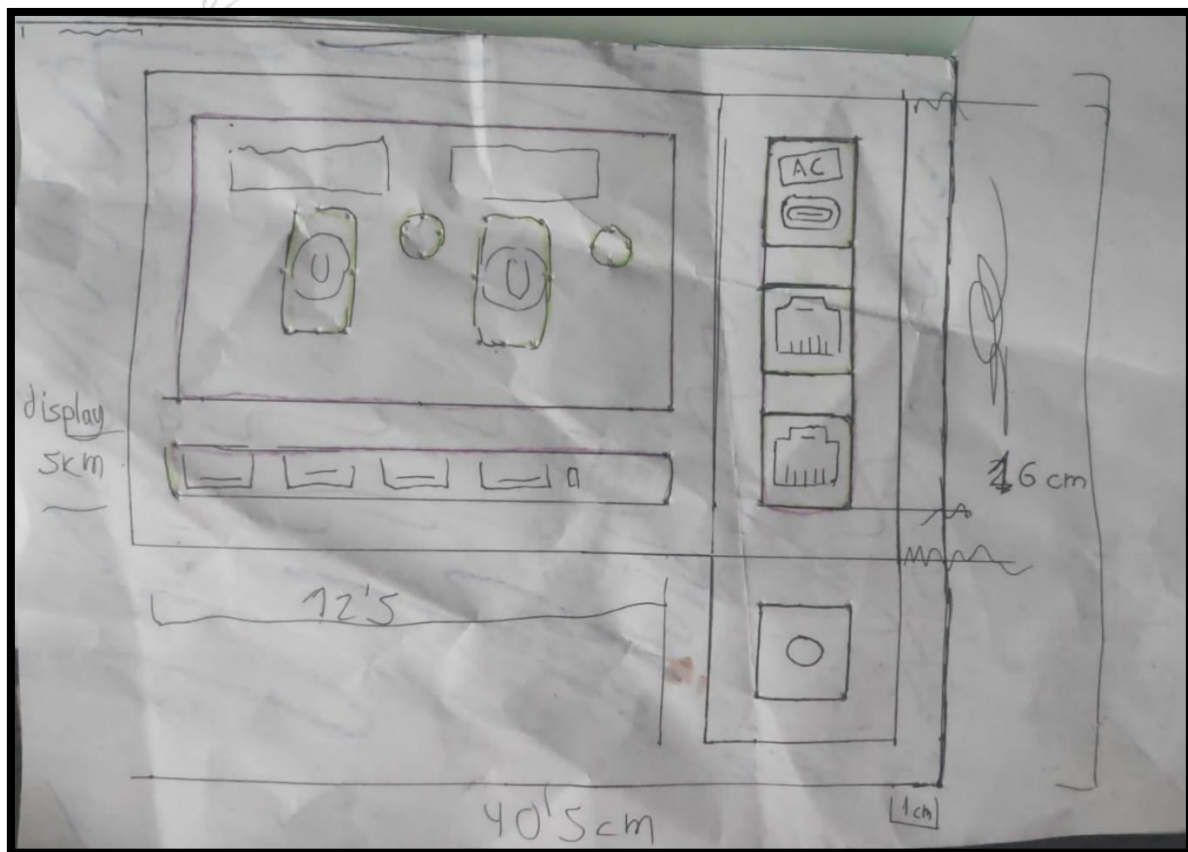
iVANKY Cable Alargador USB C a
USB C, Cable Extensión Tipo C
Macho a Hembra, USB 3.1 Gen 2 4K
@60Hz 10Gbps Compatible con...

★★★★☆ ~ 1.164

12,99€

Tras recibir los elementos principales, **ya podía armar un frontal con referencias y medidas mas realistas**

Esos días comencé el proceso creativo, Realicé sobre el papel muchos diseños posibles a escala final. Siempre usando la unidad de centímetro como medida referencial. **Este es el diseño final sobre el que construir todo el chasis después.**



Seguidamente, hice los primeros prototipos sobre cartón. Mi prioridad era **jugar con el concepto de las capas**. Sabía que **usar diferentes profundidades daría a mi proyecto el toque elegante y profesional que buscaba**

3. Diseño Estructural.

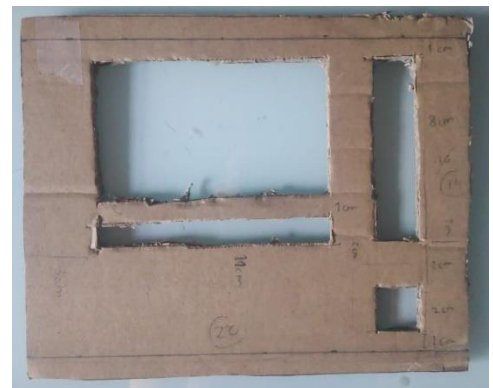
3.1. Diseño Arquitectónico.

Capas 1, 2 y 3;

- 1) Superficie metálica, **marco de pantalla y zócalo de puertos**, Mismo tamaño y proporción aurea.



- 2) **Mitad de tamaño, marcos individuales** para interruptores, Hub Usb y puertos

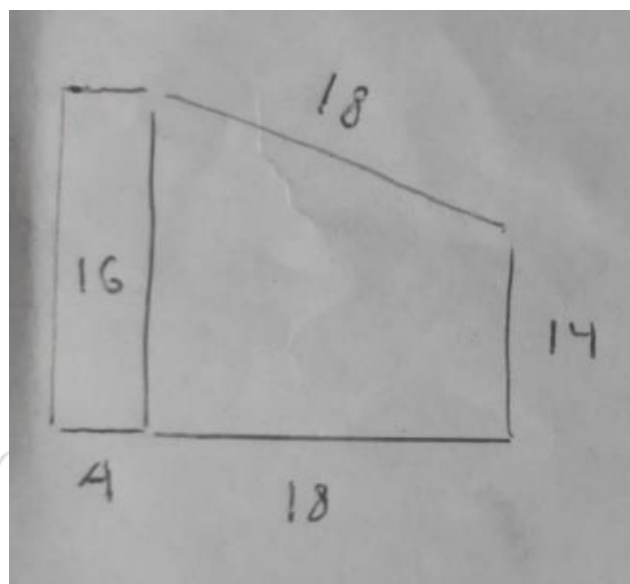
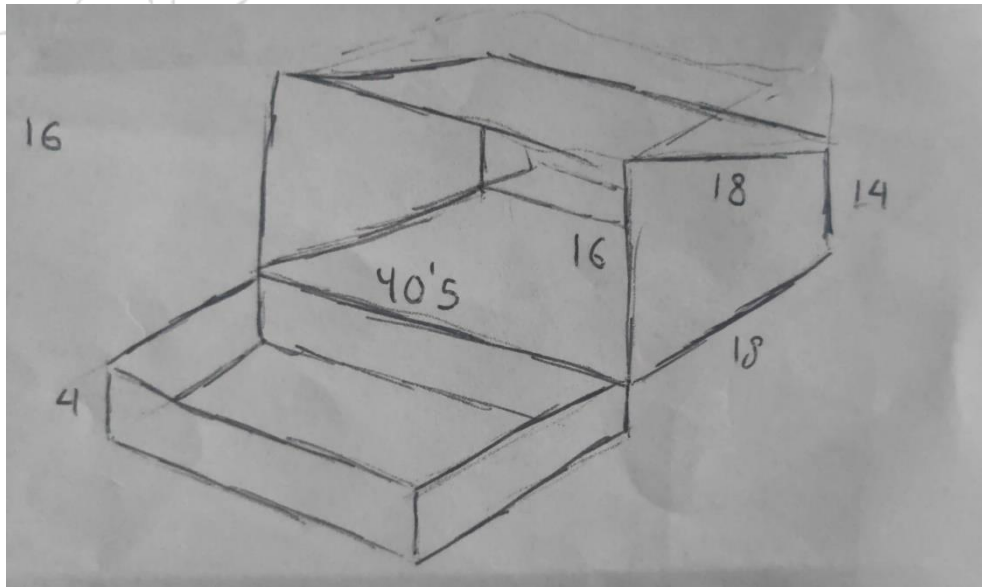


- 3) Justo detrás de la capa 2, **Ranuras individuales para cada puerto**



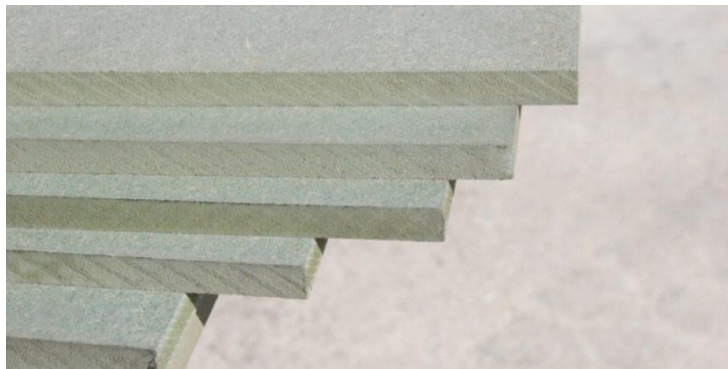
Teniendo estas medidas como referencia, era hora de hacer lo mas difícil, **la caja de madera.**

En mi opinión, **el paso mas delicado.** Aquí pondría a prueba mis medidas sobre el cartón, todo tenia que encajar. Diseñé el armazón teniendo en mente sobre todas las cosas el **frontal de carton**



Con las medidas completamente claras. Elegi un material conocido como **DM**. El cual consiste en madera prensada y endurecida, tiene un color verdoso y es hidrofuga y ultrarresistente

Ref inmediata 'http://www.mallarach.net/es/productos-2-madera-transformada-2-3-tableros-y-paneles-dm-mdf-dm-mdf-hidrofugo/dm-mdf-hidrofugo'



Con la madera en nuestro poder, junto con mi padre realicé el trabajo de ebanistería.

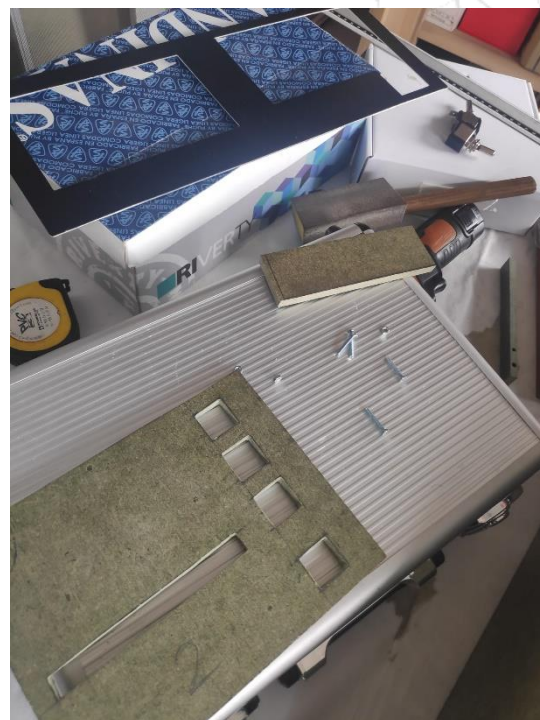
Cortando con segueta, **marcando** con grillete y **agujereando y limando** con taladradora y lima.

Pegando con soldador en frio y clavos.

Un trabajo muy duro.



Conseguí una **plancha metálica de chapa** por ahí. **(1)** Tenía una cara pintada de negro y venía perfecta para mi concepto, junto con mi padre, la corté, la limé y la convertí en la primera capa.



Use restos de madera para dar **profundidad a la primera capa** (chapa). Pegué todo y me cercioré de que estuviera bien seco **(2)**.



A la hora de pensar en el color. Pensé en pintarlo en **color cereza**, siguiendo el patron de **colores negro y rojizo**, sin embargo, las pruebas realizadas **no me convencieron en lo absoluto**

Pase tiempo pensando en colores, barnices y texturas. Hasta que me decanté finalmente por una pintura efecto madera, **Titanlak**, de tono marrón sapeli el cual imita la textura y beta de la madera refinada.

El resultado en las pruebas me sorprendió. Fue a partir de aquí cuando empecé a ver que el proyecto tomaba forma. Comenzamos a pintar la superficie del NacreDECK con cuidado, usando una brocha de cedras gruesas y en **una sola dirección** logramos el efecto deseado.





Pegué interruptores a placas de madera, y estas a la superficie de chapa. Comencé a incorporar el *HUB* y los alargadores de *RJ-45* y *USB* de alimentación.

Para pegar la **chapa a la caja de madera** recién pintada, **usé tornillos**. Realicé un **avellanado sencillo** sobre el frontal usando una taladradora y una broca gruesa. De este modo el tornillo entrará sin sobresalir de ninguna forma.

Para que el tornillo perfora la caja de madera y agarre a la misma sin dañarla **incrusté tuercas hexagonales** con pegamento rápido. **El tornillo gira dentro de la tuerca y asegura la fijación** del frontal en el dispositivo.

3.1.1. Hardware interno

Los elementos internos de NacreDECK constan de conexiones USB al chasis de la raspberry PI y de dos **circuitos aislados**, definidos por **dos interruptores**:



a) Pantalla 1:

Delimita la **continuidad de la alimentación del monitor.**

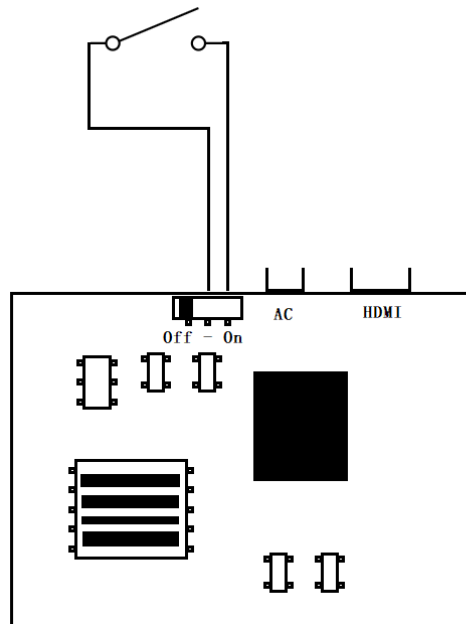
Apaga y enciende la pantalla

b) Leds 2:

Alimentado con una pila de petaca, crea una conexión en paralelo con dos leds rojos

a) Pantalla 1:

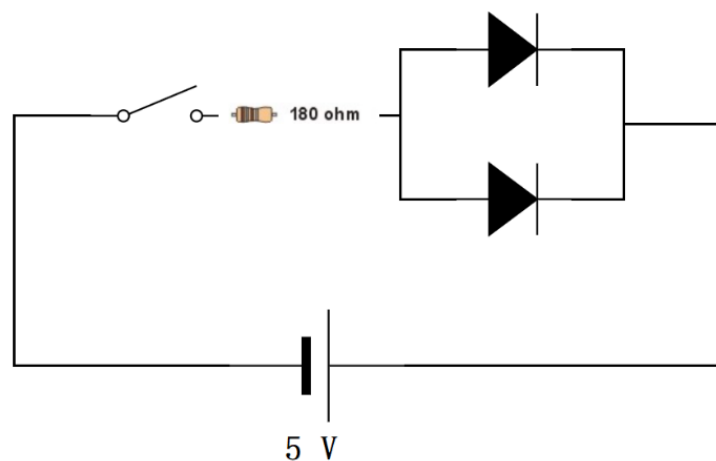
El interruptor integrado en el monitor esta **desconectado**. Doy continuidad a los dos pines por medio del interruptor del NacreDECK



b) Leds 2:

Interruptor del ND en un circuito de pila, resistencia y leds.

Siguiendo la *ley de Ohm*. Uso una resistencia de 180 ohmios antes de ambos leds en paralelo para compensar la corriente de los 5 voltios.

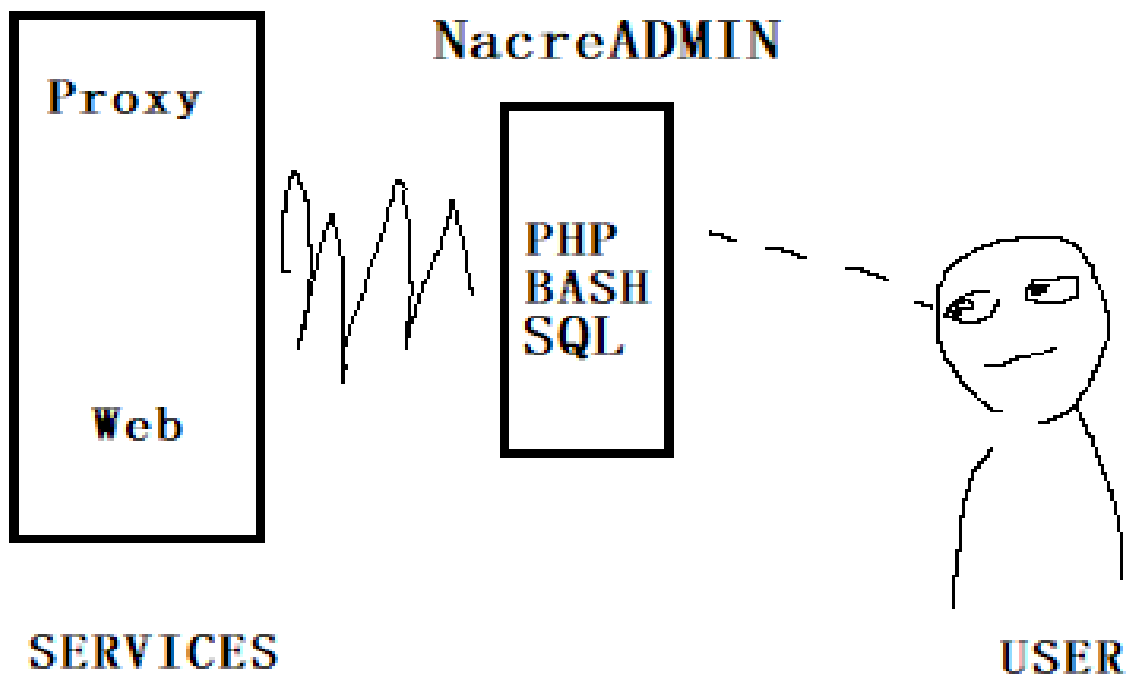


4. Diseño de Datos

4.1. Servicios del NacreDECK

El sistema esta compuesto de dos servicios troncales; **SQUID y APACHE**, Los cuales permiten hospedar de forma local la administración web y gestionar el proxy respectivamente.

Ambos han sido modificados y unificados con lenguaje PHP y Bash, Y son interpretados por el usuario a través de NacreADMIN.



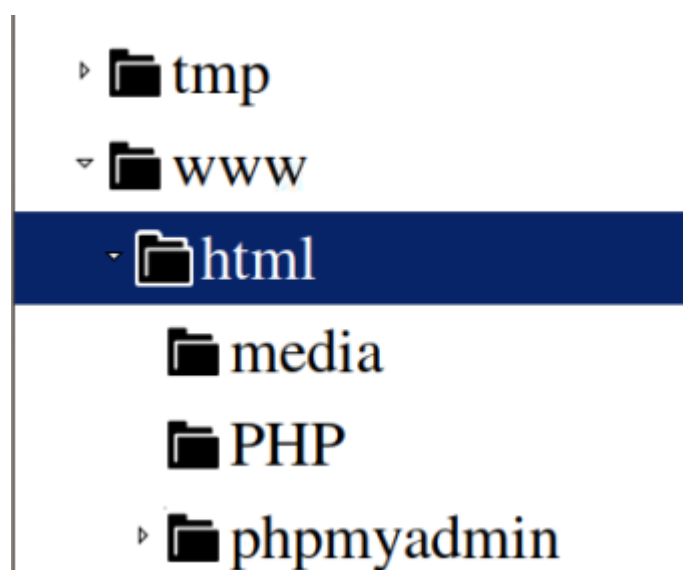
A continuación, El core de dichos servicios explicado a fondo, Mostraré que hay detrás de dicho interprete:

Junto a la presente memoria, se adjuntarán todos los ficheros implicados en estos servicios. Asi como el código explicado.

4.1.1. Apache, Core web. PHP

Apache aporta el rol de **servidor web HTTP y sitio virtual** al NacreDECK. Permite alojar por medio de un dominio local una pagina web jerarquizada y completamente funcional.

Al instalarse, de forma nativa asocia el *'localhost'* o *127.0.0.1* del sistema a la página index ubicada en *var/www/html/*



Aquí es donde se hospeda toda la red de paginas que componen **NacreADMIN**.
Entendiéndose fichero/s:

- PHP:
 - o Paginas de hipertexto web, cada fichero es una pagina web.
- CSS
 - o Pagina de estilo CSS. Encargada de dar apariencia a la administración

4.1.2. MariaDB, Base de Datos SQL

El sistema gestor de bases de datos empleado por el ND es MariaDB.

Es muy fácil de usar y de implementar, PHPmyadmin es un brillante asistente de uso de esta herramienta. Podremos acceder a el con la ruta;

<https://IP/phpmyadmin>

La base de datos de NacreADMIN es muy sencilla, consta únicamente de **una tabla**. La cual aloja el **id autoincremental**, **nombre**, **contraseña encriptada** y **nivel de usuario**.

U S E R
ID : int(11), A_I
NA : varchar(50)
PA : varchar(80)
TY : tinyint(1)

El código empleado para la creación de dicha tabla fue:

```
CREATE TABLE `user` (  
  `id` int(11) NOT NULL,  
  `na` varchar(50) NOT NULL,  
  `pa` varchar(80) NOT NULL,  
  `ty` tinyint(1) NOT NULL  
) ENGINE=InnoDB DEFAULT CHARSET=utf8mb4;  
  
ALTER TABLE `user`  
  ADD PRIMARY KEY (`id`);  
  
ALTER TABLE `user`  
  MODIFY `id` int(11) NOT NULL AUTO_INCREMENT, AUTO_INCREMENT=16;  
/*!40101 SET CHARACTER_SET_CLIENT=@OLD_CHARACTER_SET_CLIENT */;  
/*!40101 SET CHARACTER_SET_RESULTS=@OLD_CHARACTER_SET_RESULTS */;  
/*!40101 SET COLLATION_CONNECTION=@OLD_COLLATION_CONNECTION */;
```

4.1.3. SQUID

SQUID es en palabras honestas, una bestia. Es un servidor-proxy cache de código abierto, capaz de ser programado casi sin limites.

Una vez instalado, el fichero a modificar será el:

/etc/squid/squid.conf

Aquí se plantearán, de forma **secuencial**, los pasos de **actuación del proxy**, todos **automatizados por la programación PHP+BASH**

```
# WELCOME TO SQUID 4.6 FOR NACRE DECK 1.0
# -----

#NACREDECK ACL DET.

acl denegados url_regex "/etc/squid/denegados" (1)
acl permitidos src "/etc/squid/permitidos" (2)
acl borrar url_regex Borrar2.php (3)

http_access allow borrar (3)
http_access deny denegados (1)
http_access allow permitidos (2)
```

(1) La ACL DENEGADOS recoge mediante el parámetro `url_regex` el texto del fichero `/etc/squid/denegados` y lo **compara con** lo que exista en el **dominio** de las paginas web que hagan petición a los equipos locales, si coinciden son **denegadas**.

(2) La ACL PERMITIDOS usa el parámetro simple `src`, el cual **recoge lo que hay** justamente después (el contenido del **fichero permitidos**) y lo compara con **la IP que desee conectarse a la red**.

(3) La ACL BORRAR surge tras la complicación resultante al crear un formulario HTML de tipo get por URL para la eliminación de las expresiones de la lista “denegados” (**Ver 4.1. Depuracion y scripts**).

Esta ACL crea una excepción a la negación de la ACL DENEGADOS, utilizando el nombre de `Borrar2.php` como expresión, siendo esta la pagina que tramita dicha gestión en cosa de un segundo.

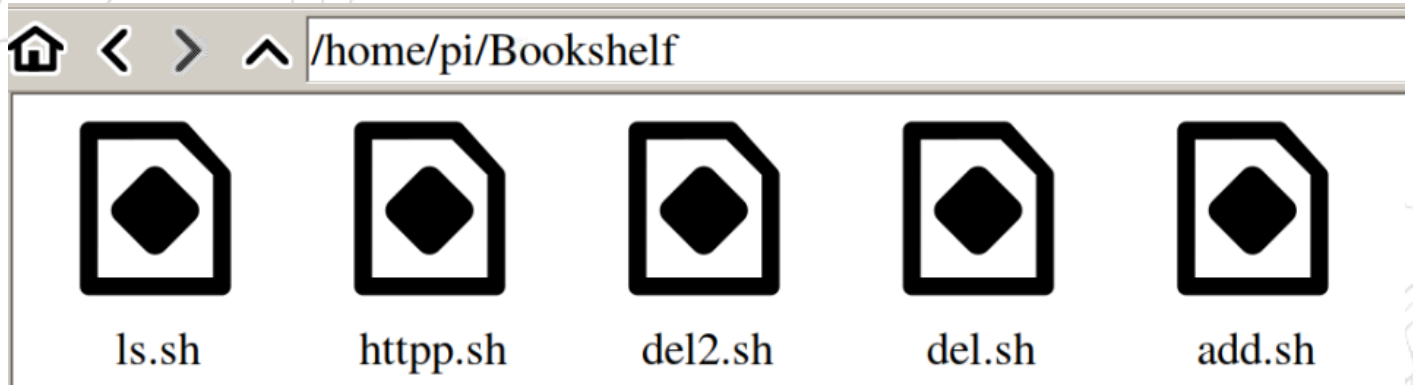
4.1.4. BASH

He programado una serie de ficheros bash con scripts de acción sobre el sistema Linux del NacreDECK. Estos son ejecutados y sentenciados a través de la web por medio de la función de PHP: **`Shell_exec()`**; Con esta función, podemos inyectar cualquier comando Shell en Linux desde páginas web. No obstante, dicha función posee ciertas limitantes a la hora de formar comandos compuestos. Es por ello que decidí emplear scripts `.sh` y sus capacidades de inserción de **argumentos posicionales** (`$1`, `$2` ...)

```
$comando=shell_exec("/script.sh ". $variable . " 2>&1 ");
```

De esta forma, podemos trabajar con el núcleo del sistema con privilegios administrativos con cualquier posibilidad que se me ocurra.

Ej) NacreADMIN funciona con 5 scripts principales. Los cuales se alojan en el directorio Bookshelf.



El siguiente fichero es **http.sh**. el cual permite desde NA, modificar el puerto web de apache.

```
#!/bin/bash
# filtramos el puerto de esucha http. lo almacenamos en $a
a=$(sudo head -n5 /etc/apache2/ports.conf | grep Listen | awk -F 'Listen ' '{print $2}')
# Sustituimos $a por $1, por medio de sed
sudo sed -i "s/$a/$1/g" /etc/apache2/ports.conf
```

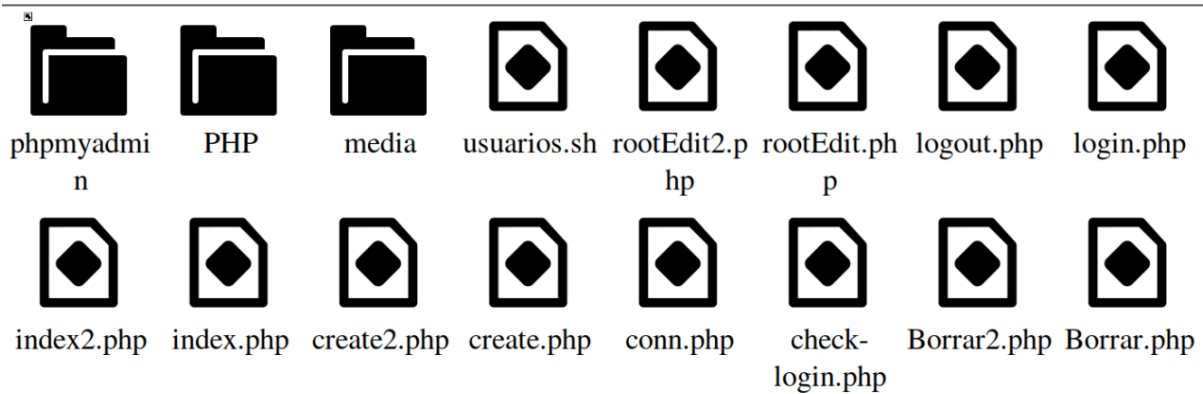
En el fichero web .php, debemos hacer que \$1 sea la variable obtenida a través del formulario, osease. El numero indicado por el usuario.

```
$outputHP=shell_exec("/home/pi/Bookshelf/http.sh ". $http . " 2>&1");
print_r($outputHP);
```

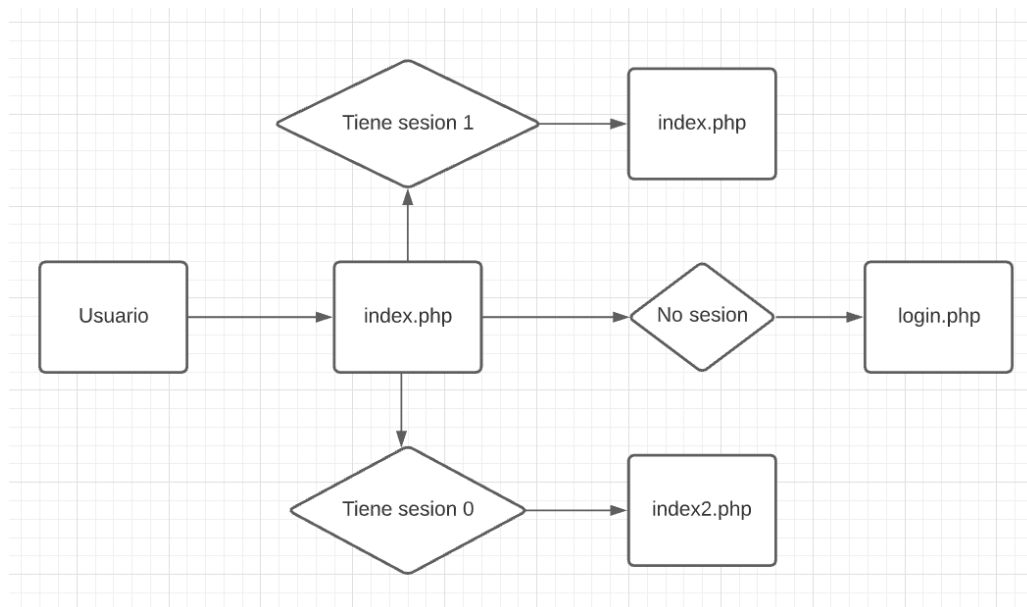
5. Pruebas de Control

5.1. Esquematización

En esta sección mostraré y explicaré los elementos de código PHP principales.



La administración funciona por medio de sesiones de PHP. Si detecta una sesión, el usuario será llevado automáticamente a **index.php** o **index2.php** en función de su nivel. En caso contrario, tendrá que iniciar una sesión desde **login.php**, comprueba con **check-login.php**



Los ficheros son concisos, realizan funciones aisladas y bien determinadas entre si.

- **Index.php**
 - **Pagina índice** central, valida al usuario y solo le permite quedarse si su tipo es **0**. Posee subvariables que, al adjuntarse con valor de true en la url del navegador, permiten mostrar cada una de las opciones que posee.
- **Index2.php**
 - Identido al anterior, pero con funciones capadas, solo permite al usuario permanecer si su tipo es **1**.
- **rootEdit.php / rootEdit2.php**
 - Permite **modificar los parámetros del usuario root** en la base de datos SQL.
- **Logout.php**
 - **Cierra las conexiones** con la base de datos y **elimina las sesiones** existentes con el navegador.
- **Login.php**
 - Permite al usuario **crear variables** con parámetros que serán **comparados con los de la base de datos**.
- **Checklogin.php**
 - **Valida la información** heredada de login.php con la base de datos SQL
- **Create.php / Create2.php**
 - **Inserta** nuevas filas en la base de datos de **usuarios**, el tipo siempre es **1**.
- **Borrar.php / Borrar2.php**
 - Borra las **IP permitidas** y las **expresiones regulares denegadas** en el proxy respectivamente. Ambas recogen la información de **index.php** por medio de **\$request** y la aplican a la función **Shell_exec** como segundo parámetro de el script de bash **del.sh**

5.2. Depuración y scripts

Index.php

```
<?php
```

```
    session_start();
```

Si hay una personalización de estilo aplicada asocia el estilo a la variable \$col, si no, la deja de color blanco

```
    if (isset($_SESSION['col'])) {
        $col=$_SESSION['col'];
    }
    else {
        $col='white';
    }
```

Variables de sesion

```
$n=$_SESSION['na'];
$colF=$_SESSION['colF'];
$list=$_SESSION['list'];
```

```
>>
<!doctype html>
<html>
    <head>
        <head>

        <title>NacreADMIN</title>
        <meta charset="utf-8">
        <link rel="stylesheet" href="/class.css?v=<?php echo(rand()); ?>" />
```

Asocia las variable de color a la hoja de estilo

```
        <style> <?PHP echo '
body {background-color:' . $colF . '};
td {background-color:' . $col . '};

fieldset {background-color:' . $col . ';
          z-index:1;}
.sel {background-color:' . $col . '};
'; ?></style>

        <script type="text/javascript">
            function ver(n) {

                document.getElementById("subseccion"+n).style.display="block"
            }
            function ocultar(n) {

                document.getElementById("subseccion"+n).style.display="none"
            }
        }
    </script>

</head>
<body>

    <div class="menu">

        <img src='b.png' class='sm'>
        <h1>NacreADMIN.</h1>
        <h3>Administrative Service. &nbsp; &nbsp; &nbsp; <span> &nbsp; &nbsp; ROOT &nbsp; &nbsp;

<span></h3><br><br>
```


Menu de configuración.

```
// SHOW INFO FROM MENU

if (isset($_GET['sys']) ) {
    ?><table class="greyGridTable">
        <thead>
        <tr>

            <th>System Settings</th>
        <th></th>

        </tr>
        </thead>
        <tbody>

        <tr>

            <td>
            </td>
            </tr>
            <tr>
            <td>Hostname</td>

            <td>
                <?php

                $output=shell_exec("hostname 2>&1");
                echo '<b>'.$output. '</b>';

                ?>

            </td>
            </tr>
        </tbody>
        </tr>

    </table>
    <?php
```

En función de que puerto esté habilitado para el proxy, la administración mostrará uno u otro.

```
        $outputeth0=shell_exec("ifconfig eth0 | grep 'inet' |awk -F 'inet '
        '{print $2}' | awk -F 'netmask' '{print $1}' | head -nl 2>&1");
        $outputeth1=shell_exec("ifconfig eth1 | grep 'inet' |awk -F 'inet '
        '{print $2}' | awk -F 'netmask' '{print $1}' | head -nl 2>&1");
        if (empty($outputeth0)) {
            echo '<td>Ethernet(1)</td>';
        }
        elseif (empty($outputeth1)) {
            echo '<td>Ethernet(0)</td>';
        }
        else {
            echo '<td>Ethernet(0)</td>';
            echo '<td>Ethernet(1)</td>';
        }
    }
}
```

```

        <?php
        (empty($outputeth0)) {
            $outputeth1.'</td>';
        }
        elseif (empty($outputeth1)) {
            $outputeth0.'</td>';
        }
        else {
            echo '<td>'. $outputeth1.'</td>';
            echo '<td>'. $outputeth0.'</td>';
        }
    }
}
?>
<td>Proxy Port</td>
</tr>
<tr>

```

Puerto proxy

Filtra el comando netstat por el servicio squid, mostrando únicamente la columna del puerto

```

<?php
    $output=shell_exec("sudo netstat -apn | grep squid | awk -F 'tcp6    0    0 :::'
    '{print $2}' | awk -F '::::*' '{print $1}' | sort | tail -n1 2>&1");
    echo $output;
}
?>
</td>
</tr>
</tr>
<tr>
    <td>Server
    <td>
    <?php
    Status</td>

```

Status del servicio, con hora y fecha de ultima activación

```

$output=shell_exec("systemctl status apache2 | grep active | awk -F 'Active: ' '{print $2}' | head -n1 |
sed -r 's/\\<.7\\U&/g' 2>&1");
print_r($output);
?>
<tr>
    <td><hr></td>

```

```
<td><hr></td>
</tr>
```

Hard reset manual de servicios proxy y web

Aplica un service squid/apache2 reload. Útil para forzar la aplicación de acl o la depuración general de la administración

```
<td>Reload Services</td>
```

```
action="index.php?sys=true" >
name='squidrst' type="submit" >PROXY</button>
name='apacherst' type="submit" >WEB</button>
```

```
if (isset($_POST['squidrst'])){
```

```
    echo "    Reloading Squid Daemon...";
    $outputT=shell_exec("sudo service squid reload 2>&1");
    print_r($outputT);
    echo "<META HTTP-EQUIV='refresh' CONTENT='1;URL=index.php?sys=true'>";
}
```

```
(isset($_POST['apacherst'])){
```

```
    echo "    Reloading Apache2 Daemon...";
    $outputT=shell_exec("sudo service apache2 reload 2>&1");
    print_r($outputT);
    echo "<META HTTP-EQUIV='refresh' CONTENT='1;URL=index.php?sys=true'>";
}
```

```
?>
```

```
<td>
<form method="post"
<button
<button
<?php
```

```
if
```

```
</form>
```

```
<td><hr></td>
```

```
</tr>
<tr>
```

Cambio de hostname

Usa el comando hostname junto con el valor introducido

```
action="index.php?sys=true" >
name="hostname">
type="submit">Change</button>
```

```
<td>
```

```
<td>Hostname</td>
```

```
<form method="post"
<input type='text'
<button
```

```

<?php
(isset($_POST['hostname'])) {
    $http=$_POST['hostname'];
    $output=shell_exec("sudo hostname ". $http . " 2>&1");
    print_r($output);
}
?>
</form>
</td>
</tr>
</tbody>
</tr>
<tr>
</tr>
</thead>
<thead>
<tr>
<th>System Time</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>

```

NTP. Formulario de gestión

Usa `timedatectl` para variar el reloj interno del sistema, permite desincronizar y sincronizar el reloj con dos botones

```

<td>Current System Time</td>
</td>
<form method="post" action="index.php?sys=true" >
<?PHP
$outputT=shell_exec("date 2>&1");
    print_r($outputT);
?>
<button name='sync' type="submit">NTP ON</button>
<button name='sync0'>NTP OFF</button>
<input type='time' name="time">
>button type="submit">Change</button>
</td>
</tr>
</tbody>
</tr>
</thead>
<thead>
<tr>
<th>System Time</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>

```

```

unset($_POST['sync0']);
$time=$_POST['time'];
$outputT=shell_exec("sudo timedatectl set-ntp 1 2>&1");
print_r($outputT);
echo "<META HTTP-EQUIV='refresh' CONTENT='0.5;URL=index.php?sys=true'>";
}

(isset($_POST['sync0'])) {
unset($_POST['sync']);
$time=$_POST['time'];
$outputT=shell_exec("sudo timedatectl set-ntp 0 2>&1");
print_r($outputT);
echo "<META HTTP-EQUIV='refresh' CONTENT='0.5;URL=index.php?sys=true'>";
}

?>
</form>
</td>
</tr>
</tbody>
</tr>
</thead>
<thead>
<tr>
<th>Listen Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP Port</td>
<td>
<form method="post"
<input type='number'
<button
action="index.php?sys=true" >
name="http" required>
type="submit">Change</button>

```

Cambio de puertos de escucha

Usa el script `http.sh` para modificar puertos en función del carácter indicado

```

<?php
(isset($_POST['http'])) ) {
if
    $http=$_POST['http'];
    $outputHP=shell_exec("/home/pi/Bookshelf/http.sh ". $http . " 2>&1");
    print_r($outputHP);
}

```



```

action="index.php?sys=true" >
name="httpsp" required>
type="submit">Change</button>

```

```

}
?>
</form></tr>
<tr>
<td>HTTPS Port</td>
<td>
<form method="post"
<input type='number'
<button
?>
</form></tr></tr>
</tbody>
</tr>
</thead>
<thead>
<tr>
<th>NacreADMIN Appearance</th>
<th></th>
</tr>
</thead>
</tbody>

```

```

<?php
(isset($_POST['httpsp'])) {
    $https=$_POST['httpsp'];
    $outputHP=shell_exec("/home/pi/Bookshelf/http.sh ". $http . " 2>&1");
    print_r($outputHP);
}
?>

```

Menu de personalización; fondo y menú.

Modifica el css de la pagina localizado al inicio de la misma, almacena un codigo hexadecimal en una variable de sesión y actualiza index.php para aplicar cambios

```
Color</td>
```

```

action="index.php?sys=true" >
name="col" value="#FFFFFF">
type="submit">Change</button>

```

```
(isset($_POST['col'])) {
```

```

<tr>
<td>Display
<td>
<form method="post"
<input type='color'
<button
<?php
if

```

```

    $col=$_POST['col'];
    echo 'Wait...';
    $_SESSION['col']=$col;
    echo "<META HTTP-EQUIV='refresh' CONTENT='0.5;URL=index.php?sys=true'>";

```

```

}

```

```

?>

```

```

</form></tr>

```

```

</tbody>
</tr>
</thead>

```

```

<tbody>
<tr>

```

```

<td>Background

```

```

<td>

```

```

<form method="post"

```

```

<input type='color'

```

```

<button

```

```

Color</td>

```

```

action="index.php?sys=true" >

```

```

name="colF" value="#FFFFFF">

```

```

type="submit">Change</button>

```

```

<?php

```

```

if

```

```

(isset($_POST['colF'])) {

```

```

    $colF=$_POST['colF'];

```

```

    echo 'Wait...';

```

```

    $_SESSION['colF']=$colF;

```

```

    echo "<META HTTP-EQUIV='refresh' CONTENT='0.5;URL=index.php?sys=true'>";

```

```

}

```

```

?>

```

```

</form></tr>

```

```

</tbody>
</tr>
</thead>

```

```

</thead>

```

```

<thead>

```

```

<tr><br>

```

```

<th>NacreADMIN Miscellany</th>

```

```

<th></th>

```

```

</tr>

```

```

</thead>

```

```

<tbody>

```

```

<tr>

```

```

<td><b>Reboot</b> the

```

```

NacreDECK.</td>

```

```
action="index.php?sys=true" >
type="submit">Reboot</button>
```

```
<?php
```

Reinicio y apagado del NacreDECK

Aplica un reboot o un shutdown

```
unset($_POST['reb']);
$output=shell_exec("sudo reboot 2>&1");
print_r($output);
```

```
the NacreDECK.</td>
```

```
action="index.php?sys=true" >
type="submit">Shutdown</button>
```

```
<?php
```

```
(isset($_POST['sh'])) {
```

```
unset($_POST['sh']);
$output=shell_exec("sudo shutdown -r now 2>&1");
print_r($output);
```

```
<td>
<form method="post"
<button name='reb'
```

```
if (isset($_POST['reb'])) {
```

```
}
```

```
?>
```

```
</form>
```

```
</tr>
```

```
<td><b>Turn Off</b>
```

```
<td>
```

```
<form method="post"
```

```
<button name='sh'
```

```
if
```

```
}
```

```
?>
```

```
</form>
```

```
</tr>
```

```
</tbody>
```

```
</tr>
```

```
</thead>
```

```
Entries.</h1>
general users.<h3>
```

```
        }
    }
}

if (isset($_GET['passwd']) ) {

    echo '<table class="greyGridTable">

        <h1>NacreDECK User OS

        <h3>Logger of NacreDECK system

        <br>
        <thead>

            <tr>
            <th>Name</th>
            <th>Folder</th>
            <th>UID</th>
            <th>GUID</th>
            </tr>

            <tbody>
```

USUARIOS LINUX

Consulta el fichero passwd del sistema Linux, extrae de el la información mas importante con awk y la filtra por líneas

```
awk -F ':' '{print $1}' 2>&1";

awk -F ':' '{print $6}' 2>&1";

awk -F ':' '{print $3}' 2>&1";

awk -F ':' '{print $4}' 2>&1";

';
echo "<td><b>";
$outputHP=shell_exec("cat /etc/passwd |
echo "<pre>$outputHP</pre>";
echo "<td><b>";
$outputHP=shell_exec(" cat /etc/passwd |
echo "<pre>$outputHP</pre>";
echo "</td>";
echo "<td><b>";
$outputHP=shell_exec("cat /etc/passwd |
echo "<pre>$outputHP</pre>";
echo "</td>";
echo "<td><b>";
$outputHP=shell_exec("cat /etc/passwd |
echo "<pre>$outputHP</pre>";
echo "</td>";
echo "<td><b>";
}
```

USUARIOS BDD

Consulta línea por línea gracias al fichero con.php la base de datos, segmenta por columnas la información

```
#Usuarios
if (isset($_GET['users']) ) {
```

```

// query almacenado en variable

conn.php
$dbpass, $dbname);

fallida. llama al administrador y dile que el error ha sido: " . mysqli_connect_error());

"SELECT * FROM user");

```

```

include 'conn.php';
// Connection variables. importadas de
$conn = mysqli_connect($dbhost, $dbuser,

// Check connection
if (!$conn) {
    die("oops. conexion con la BBDD
}
else {

```

```

Entries.</h1>
database general users.<h3>

```

```

mysqli_fetch_assoc ($result)) {

.</b></td>";

```

```

$result = mysqli_query($conn,
if (!$result){
    echo "error";
}

```

```

echo "

```

```

<table class='greyGridTable'>
<h1>NacreADMIN User Database

```

```

<h3>Logger of NacreADMIN

```

```

<br>
<thead>
<tr>
<th>User</th>
<th>Hash</th>
<th>Role</th>
</tr>
</thead>
<tbody>

```

```

<tr>

```

```

<td>
</td>
</tr>
<tr>

```

```

";
while ($row =

```

```

echo "<td><b>";
echo $row['na'];

```

```

echo "<td>";
echo $row['pa'];
echo "<td>";

```

Tipo de usuario y link a cambio de parámetros de administrador.

Se muestra el tipo de usuario y lo asocia a un color; verde es admin y rojo es usuario limitado. El verde contiene el acceso a rootEdit.php

```

$row['ty'] == 1 ) {
    echo "<u><b style='color:green'><a href='rootEdit.php' style=
        'color: Green;
        padding-top:0px;
        padding-bottom:0px;
        padding-left:0px;
    '>
    Administrator</a></b></u>";
}
if (
$row['ty'] == 0 ) {
    echo "<b style='color:red'>User</b>";
}

```

```

    }
    echo "</td></tr>";
    echo "</td></tr>";

```

```

}
mysql_free_result($result);
echo "</tbody></table>";

```

ACL

Implementacion de Ips

Imprime línea por línea el contenido de PERMITIDOS, usando \$numlinea como contador hasta llegar al final. Al margen de cada entrada hay un botón de eliminar, el cual exporta la id de cada expresión via URL y la elimina del documento con del y add

```

if (isset($_GET['Acl'])) {
    echo '
<table class="greyGridTable">
    <h1>Permitted IPs</h1>
    <hr>
    <h3>This is the list of
addresses which will be <b>allowed</b> from the ND network.<br> <br>

```

```

<br>
<thead>
<tr>
<th>IPs</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>
</td>
</tr>
<tr>

```

```

';
    $f =
fopen("/etc/squid/permitidos", "r");
while
($linea = fgets($f)) {
    echo "<td><b>";
    echo '<b>' . $linea . "</b></td>" ;
    $aux[] = $linea;
    $numlinea++;
    echo "<td>";

```

```

        echo "
href='Borrar.php?Del=$linea'><img src='/media/Del.png' width='30'></a>
</td></tr>";

href='index.php?Add=true'><img src='/media/Add.png' width='30'></a>";

```

```

        <a
        <br />
    }
    echo "<td></td><td>";
    echo "<a

```

Denegacion de expresiones

Imprime línea por línea el contenido de DENEGADOS, usando \$numlinea como contador hasta llegar al final. Al margen de cada entrada hay un botón de eliminar y añadir, el cual exporta la id de cada expresión via URL y la elimina del documento con del2 y Add2

```
/*DENEGADAS*/
```

```
class='greyGridTable'>
```

```
which words has to exclude from it's network.</h3>
```

```
fopen("/etc/squid/denegados", "r");
```

```
($linea = fgets($f)) {
```

```

    echo "<td><b>";
    echo '<b>' . $linea;
    $TLinea = "$linea";

```

```

    echo "</b></td>" ;
    $aux[] = $linea;

```

```

    $numlinea++;
    echo "<td>";

```

```

    echo "
href='Borrar2.php?Del2=$linea'><img src='/media/Del.png' width='30'></a>
</td></tr>";

```

```

        echo "
        </td>
        </tbody>
        </table>
        <table
        <thead>
        <tr>
        <h1>Denied Expressions </h1>
        <hr>
        <h3>The next list tells ND
        <br>
        <th>Expression</th>
        <th></th>
        </tr>
        </thead>
        <tbody>
        <tr>
        <td>
        </td>
        </tr>
        <tr>";

```

```
$f =
```

```
while
```

```

        <a
        <br />

```



```

        }
        echo "<td></td><td>";
        echo "<a
href='index.php?Add2=true'><img src='/media/Add.png' width='30'></a>";

/* AÑADIR PERMITIDA*/

if (isset($_GET['Add'])) {
    echo '

<table class="greyGridTable">
    <thead>
    <tr>
    <th>IP</th>
    <th></th>
    </tr>
    </thead>
    <tbody>

    <tr>

    <td>
    </td>
    </tr>
    <tr>

    <td><b>";
    ?>
}

```

Nueva IP

Toma los valores de los cuatro cuadros, los convierte en una única cadena de caracteres separados por puntos y los añade al final del documento permitidos

```

action="index.php?Perm_add=true" >
name="1" maxlength='3' min="0" max="255" required style="width : 50px; height : 1px">
name="2" maxlength='3' min="0" max="255" required style="width : 50px; height : 1px">
name="3" maxlength='3' min="0" max="255" required style="width : 50px; height : 1px">
name="4" maxlength='3' min="0" max="255" required style="width : 50px; height : 1px">
type="submit">Add Ip</button>

<form method="post"
<input type='number'
<input type='number'
<input type='number'
<input type='number'
<br><button
</form>
<?php
}
if (isset($_GET['Perm_add'])) {
    $FULLIP=$_POST['1'].".".$_POST['2'].".".$_POST['3'].".".$_POST['4'];
    echo "Wait a few... <br>";
    $outputHP=shell_exec("echo $FULLIP >> /etc/squid/permitidos 2>&1");
    print_r($outputHP);
}

```

```
EQUIV='refresh' CONTENT='0.5;URL=index.php?Acl=true'>";
$outputT=shell_exec("sudo service squid reload 2>&1");
```

```
echo "<META HTTP-
print_r($outputT);
}
```

Nueva Expresion

Al igual que en el caso anterior, añade el texto almacenado en variable del formulario `name='1'`

```
/* AÑADIR DENEGADA */
echo '
if (isset($_GET['Add2']) ) {
<table class="greyGridTable">
</table>
</h1>
<h2></h2>
<thead>
<tr>
<th>Denied Expressions | New
</th></tr>
</thead>
<tbody>
<tr>
<td>
</td>
</tr>
<tr>
echo "<td><b>";
?>
<form method="post"
<input type='text'
<br><button
type="submit">Add</button>
</form>
<?php
}
if (isset($_GET['Den_add']) ) {
$FULLIP=$_POST['1'];
echo "Wait a few... <br>";
$outputHP=shell_exec("echo $FULLIP >> /etc/squid/denegados 2>&1");
print_r($outputHP);
$outputT=shell_exec("sudo service squid reload 2>&1");
print_r($outputT);
echo "<META HTTP-
}
EQUIV='refresh' CONTENT='0.5;URL=index.php?Acl=true'>";
```

REGISTRO DE ACTIVIDAD

Permite filtrar por numero de salidas de comando tail al log de accesos de squid.

```
if (isset($_GET['Acl_log']) ) {  
    echo '  
        <table class="greyGridTable">  
            <h1>Network Log </h1>  
  
            <h3><b>Last</b> activity  
  
            <hr>  
                <form method="post"  
                    <input type="number"  
  
                    <button class="X"  
  
                    <hr>  
                <thead>  
                    <br>  
                    <tr>  
                        <th>IP</th>  
                        <th>Address</th>  
                        <th>Status</th>  
                    </tr>  
                </thead>  
                <tbody>  
  
                <tr>  
  
                <td>  
                </td>  
            </tr>  
  
            </tbody>  
        </table>  
    </pre>';  
    echo "<td><b>";  
  
    $outputHP=shell_exec("sudo tail -  
n" . $list . " /var/log/squid/access.log | awk '{print $3}' | tac 2>&1 2>&1");  
    echo "<pre>$outputHP</pre>";  
    echo "</td>";  
    echo "<td><b>";  
  
    $outputHP=shell_exec("sudo tail -  
n" . $list . " /var/log/squid/access.log | awk '{print $7}' | tac 2>&1");  
    echo "<pre>$outputHP</pre>";  
    echo "</td>";  
    echo "<td><b>";  
  
    $outputHP=shell_exec("sudo tail -  
n" . $list . " /var/log/squid/access.log | awk '{print $4}' | awk -F 'TCP_' '{print $2}' | awk -F '/' '{print  
$1}' | tac 2>&1");  
    echo "<pre>$outputHP</pre>";  
    echo "</td>";  
    echo "<td><b>";  
  
    if  
  
    (isset($_POST['list']) ) {
```

Para poder mostrar la hora de cada registro del proxy, he empleado el comando perl -pe para adjuntar la hora y fecha local y asociarla a cada entrada del fichero

```
$outputHP=shell_exec("perl -pe 's/[\\d\\.]+/localtime($&)/e' /var/log/squid/access.log | awk -F '202'  
'{print $1}' | tail -n" . $list . " | tac 2>&1" );  
    echo "<pre>$outputHP</pre>";  
    echo "</td>";  
  
    if
```

```

$list=$_POST['list'];
$_SESSION['list']= $list;

echo "<META HTTP-EQUIV='refresh' CONTENT='0.01';URL=index.php?Acl=true>";
}
}

```

```
fclose($f);
```

Usuario no root, else de la primera comprobación.

```

} else {
    echo '<b>Unregistred user</b>';
    </div>
    <div class="disp" style="background-color:' . $col
    echo '<h1>Welcome to NA Administrative service</h1>';
    echo '<h2>wait a few seconds...</h2>';
    echo '';
    echo "<META HTTP-EQUIV='refresh'
CONTENT='3;URL=login.php'>";
}
?>
</div>
</body>

```

6. Bibliografía

6.1. Direcciones web / Referencias

NacreREPO en bandcamp

<https://nacrerepo.bandcamp.com>

La pagina donde subo mi música y mis creaciones. Inspiración directa para este proyecto

Software

<https://www.raspberrypi.org/software/operating-systems/>

<http://www.squid-cache.org>

<https://www.apache.org>

<https://nmap.org>

<https://www.maltego.com/downloads/>

<https://mariadb.com/>

Software de terceros empleado en la realización del NacreDECK y el NacreADMIN

Referencias de estudio SQUID

<https://www.alcancelibre.org/staticpages/index.php?page=19-0-como-squid-general>

pagina de estudio y apuntes de SQUID. De mucha ayuda.

Paginas de venta

<https://www.amazon.es>

Dalpes Illescas, Yuncos. 925 53 22 13

Compra de materiales, los materiales no citados fueros reciclados o encontrados en la calle

Gif de Esqueleto.

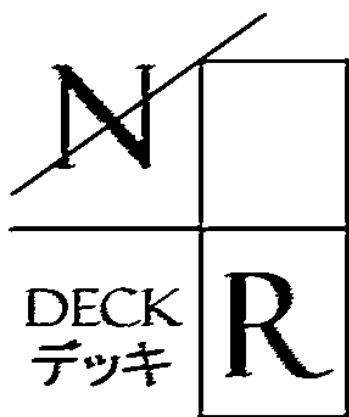
<https://media4.giphy.com/media/3oEjI6SIIHBdRxXI40/giphy.gif>

Gif que aparece cuando el usuario no es identificado, completamente necesario!.

6.2. Comentarios finales

Deseo agradecer de corazón al equipo de profesores de los ciclos formativos de Salesianos de Atocha, Gracias por haber guiado el viaje de mi vida y haberme ayudado a llegar donde estoy ahora. Agradecer a mis compañeros de clase por contar conmigo en las buenas y en las malas.

Pero en sobre todas las cosas agradezco a mi padre, por ayudarme siempre que le necesité, por ofrecerme toda ayuda que fuera capaz de darme, nunca olvidaré lo que he creado gracias a tu motivación y esfuerzo. Dedico este proyecto a nosotros, te quiero.



see ya!
:)