

CENTRE INTEGRAL FP ILERNA-SISTEMAS MICROINFORMÁTICOS Y REDES

PROMOCIÓN 2019-2021

ILERNA



OSIX
ENTERPRISE

- ALEJANDRO
- EDUARD
- FERNANDO
- SERGI



**NEW
NORMAL LIFE**

**PROPUESTA
EMPRESARIAL**

MAYO • 2021

**MEMÓRIA DE
SÍSTESIS**



Índice

Plan de New Normal Life	1
Índice	1
Introducción	5
Empresa propia, Osix Enterprise	8
Elección del nombre de la empresa	9
Elección y creación de marca corporativa	10
Elección de servicios	11
Construcción	12
Diseño	12
Seguridad y Regulaciones	12
Pack de servicios	13
Elección de objetivos	14
Elección de empleados y funciones	14
Creación del plan financiero	17
Gasto total en trabajadores	17
Gastos variables de los trabajadores	17
Aumento o reducción de personal	18
Elección y propuesta de sucursales	18
Informe técnico	18
Lleida	18
Cisco packet tracer	20
Tarragona	21
Barcelona	22
Girona	22
Cisco packet tracer general	24
Programas Utilizados	28
Cisco Packet Tracer	28
Diagrams.net	28



Creación de la página web	28
Inicio	29
Teoría del NavBar	30
Título	32
Sección Servicios	33
Equipo	36
Sobre Nosotros	39
Footer	41
Proyecto New Normal Life	44
Elección y creación de marca corporativa	45
Elección sistemas informáticos	46
Maquetación y estructuración de la base de datos Access	48
Inicio de la base de datos	49
Aplicación teórica de la seguridad de la empresa	56
Control de acceso	57
Registro de acceso	58
Acceso a datos	58
Copias de seguridad e imágenes del sistema	59
Sistema de redundancia	59
Discos duros	60
Personal y seguridad	60
Personal de seguridad	61
Plan de personal de seguridad extremo	61
Plan de personal de seguridad intermedio	62
Plan de personal de seguridad bajo	62
Política de seguridad	62
Plan de contingencia	63
Protección de datos	65
Copias de seguridad e imágenes del sistema	65
CPD y DRS	65



Seguridad física	66
Seguridad lógica	66
Seguridad en las redes	66
Seguridad en la red	66
Itinerario New Normal Life	67
Los enemigos de la empresa	68
Plan Director de Seguridad	68
Puesto de trabajo	69
Fuera de la oficina	69
Emails sospechosos	69
Cultura de seguridad	70
Recursos Humanos	71
Información y su destino	71
Subcontratación TIC	72
Confianza en subcontrataciones TIC	72
Nuestra web	73
Super contraseñas	73
Trabajo desde el móvil	73
Los datos y la ley	74
Pérdida de archivos	74
Aplicaciones Seguras	74
Las redes sociales	75
Engaños	75
Plan de contingencia	75
Información portátil	76
Información en el aire	76
Clasifica, Utiliza y Destruye	76
Todos somos seguridad	77
Concienciación para fomentar los buenos hábitos de seguridad	77
Incidentes de seguridad	77



Los tres pilares de la seguridad	77
Clasificación de la información	78
Tratamiento de la información	79
Copias de seguridad	80
Tipos de copias de seguridad	80
Borrado seguro de la información	81
Correos fraudulentos	81
Contraseñas	82
Puesto de trabajo	82
Mesas limpias	83
Contrato de confidencialidad	83
BYOD Teletrabajo	84
El valor de las redes sociales	87
Políticas de empresario	88
Gestión de recursos humanos	88
Almacenamiento en la red corporativa	89
Almacenamiento en los equipo de trabajo	90
Almacenamiento en la nube	91
Aplicaciones permitidas	92
Clasificación de la información	92
Concienciación y formación	93
Continuidad de negocio	94
Cumplimiento legal	95
Plan de director de seguridad	96
Relación con proveedores	97
Políticas para el personal técnico	98
Teletrabajo seguro	98
Borrado seguro y gestión de soportes	99
Uso de dispositivos móviles corporativos	100
Almacenamiento en la nube	101



Auditoria de sistemas	101
Comercio electrónico	102
Control de acceso	103
Copias de seguridad	104
Gestión de logs	105
Protección de la página web	106
Respuesta a incidentes	107
Uso de técnicas criptográficas	107
Actualización de software	108
Almacenamiento en los dispositivos extraíbles	109
Políticas para el empleado	110
Contraseñas	110
Uso de dispositivos móviles no corporativos	111
Uso del correo electrónico	112
Uso de wifi y redes externas	113
Protección del puesto de trabajo	114
Conclusiones	115
Presupuesto	116
Políticas de seguridad para el empleado	116
Políticas para el empresario	116
Estos puntos son los tratados en este plan de seguridad	117
Precio e indicaciones	117
Políticas de seguridad para el servicio técnico	117
Estos puntos son los tratados en este plan de seguridad	118
Precio e indicaciones	118
Referencias	118
Incibe	118
Implementación de los servicios de red	119
Servicios: Windows Server	119
Instalación de webmin	120



Cliente	126
Servidor ftp	127
Cliente	131
Servidor de correo Thunderbird	132
Creación del gestor Joomla	136
Creación de cursos en Moodle	140
Creación de la página web	142
Inicio	142
Teoría del NavBar	144
Sección Servicios	146
Equipo	148
Sobre Nosotros	152
Footer	154



Introducción

Este proyecto consiste en simular un acontecimiento real, el cual requiere la creación y ejecución teórica de varios proyectos para conseguir crear nuestra propia empresa, desde esa misma empresa deberemos crear nuestro primer encargo, que consiste en crear desde 0 una empresa de domótica la cual se llama New Normal Life, esta solamente tiene el nombre de la empresa, y delega a nuestra empresa la creación de todas las necesidades para crear una empresa de domótica funcional.

Dentro del proyecto de síntesis hemos creado varios documentos necesarios para la funcionalidad de nuestra propia empresa, catalogando estos desde:

- Elección del nombre de empresa
- Elección y creación de marca corporativa
- Elección de servicios
- Elección de objetivos
- Elección de empleados y funciones
- Creación del plan financiero
- Creación de la página web

Una vez creada y verificada esta información de nuestra empresa, New Normal Life nos contrata para pedirnos la creación de toda su estructura empresarial, esta documentación ha consistido en crear varios documentos:

- Elección y creación de marca corporativa
- Elección sistemas informáticos
- Creación de la base de datos
- Aplicación teoría de la seguridad de la empresa
- Implementación de los servicios de red
- Creación del gestor Joomla
- Creación de cursos en Moodle
- Creación de la página web

Durante la creación de estos documentos hemos utilizado e implementado diferentes aplicaciones y páginas web que han sido fundamentales para el objetivo final del trabajo, mencionando en primera parte:

- Canva
- Figma
- Visual Studio Code
- VMware
- Microsoft Access
- Adobe Photoshop
- Github
- Gitbook
- Visme
- Tolteck
- Google Drive
- Microsoft Excel
- Incibe
- Cisco Packet Tracer
- Diagrams.net

Estos serán mencionados posteriormente cada vez que han sido utilizados y la funcionalidad que nos han aportado.

Toda la documentación ha sido realizada en un interlineado 1.5, en letra Montserrat y con el texto Justificado.

- El título 1, tiene un tamaño de 16 con estilo de negrita
- El título 2, tiene un tamaño de 14 en gris oscuro 4
- El título 3, tiene un tamaño de 12 en gris oscuro 4
- El texto, tiene un tamaño de 11 en negro



OSIX ENTERPRISE

PLAN DE EMPRESA

PROUESTA DIRECTIVA

DATE

02 FEBRERO 2021

PROUESTA DE
EDUARD CASTELLÓ
CEO, OSIX ENTERPRISE

Elección del nombre de la empresa

El logo lo escogimos para retransmitir la fluidez y la continuidad de un río, ya que como empresa nuestro objetivo es llevar a nuestros usuarios a la mayor comodidad y bienestar posible.

Por ende quisimos transmitir unos valores de paz y armonía que es lo que nuestros usuarios andan buscando , así que nuestros colores fueron escogidos a conciencia , que hay más natural y tranquilo que el verde y el azul , dos colores que puedes observar en un río, (azul del agua que lleva consigo el río y que no frena nunca hasta llegar a su destino y verde de la vegetación que deja el río al transportar el agua , esas plantas tan vivas y fuertes.)

También el verde lo asociamos al color del dinero o a el crecimiento de la empresa que nos contacta.

La creación de Osix fue decidida entre los cuatro fundadores de la empresa, los cuales aportaron varios nombres y logos para la misma, con un pequeño texto explicativo de la elección de cada uno



Como primera opción tenemos Make It Clear expuesto por Alejandro Beregona:

Este logo lo cree porque la función de la empresa es solucionar problemas de otra en este caso páginas web y problemas varios.

Debido a esto surgió MAKE IT CLEAR: Que traducido no es más que aclararlo. En este caso el nombre sería una asimilación de lo que haría la empresa (aclarar y solucionar tus problemas)



El logo es una especie de río de color verde y azul .

Uso la imagen de un “río” porque quiero como empresa solucionar tus problemas igual que el río lleva agua (con un buen recorrido , claro y tranquilo) igual que los colores que seleccione , son tranquilos y calmados que desde la empresa de MAKE IT CLEAR quiere transmitir.

Como segunda opción tenemos Osix expuesto por Eduard Castelló:

Quería un logo sencillo y un nombre fácil de recordar, simplemente Osix básicamente está formado de las primeras letras de palabras relacionadas con la informática.

Como tercera opción tenemos Funcional Technology expuesto por Sergi Palacios:

Básicamente , he elegido el nombre de “Funcional Technology” porque el nombre significa tecnología funcional y hace referencia a utilizar o reparar tecnología que nos pueda ayudar en nuestras vidas , lo cual ampara desde ordenadores hasta algún cierto punto de la robótica.

Finalmente se decidió en común hacer una mezcla de elecciones entre el propio logo de MAKE IT CLEAR junto con el nombre empresarial de Osix al cual se le añadió el término Enterprise y dando un rediseño al logo junto el nombre.



Elección y creación de marca corporativa

Una vez elegido el logo y el nombre de la empresa, tuvimos un proceso de creación de nuestra marca corporativa,

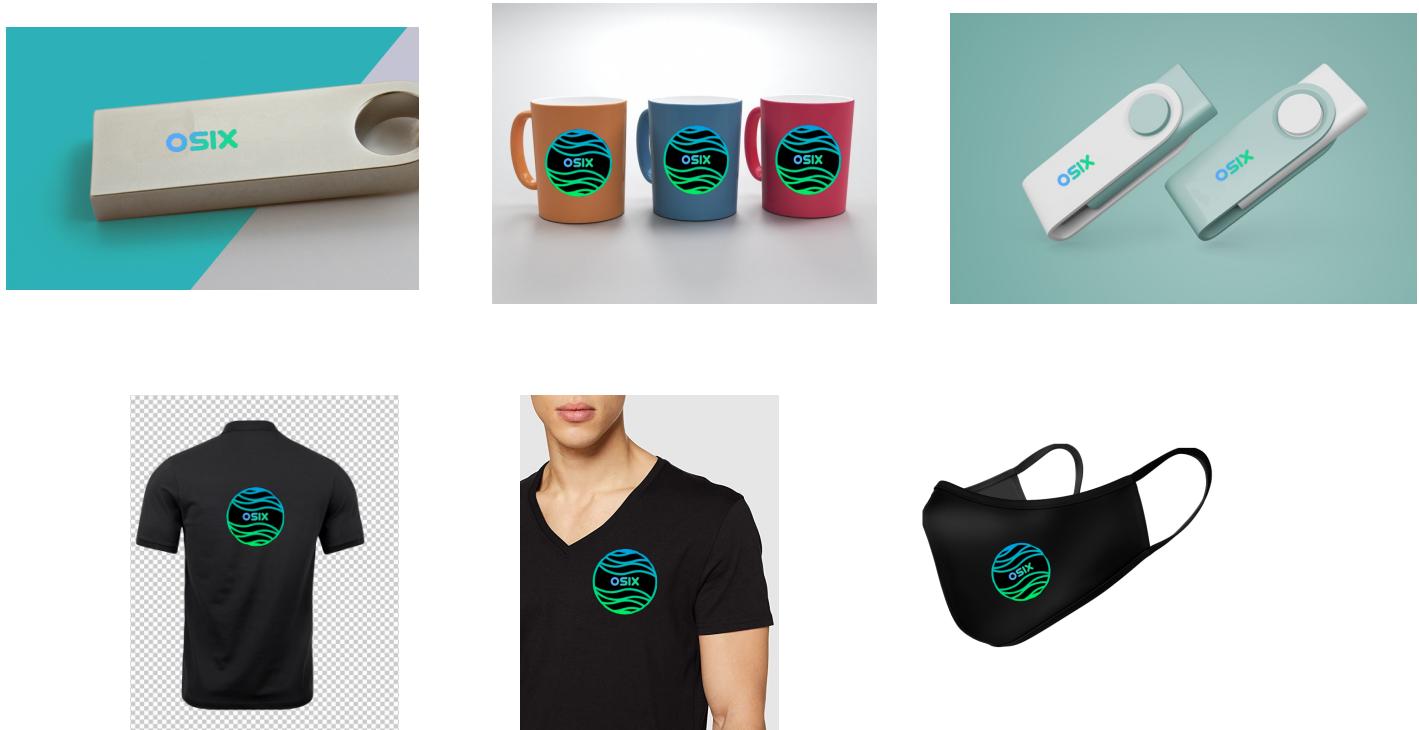


eliendo los colores de la empresa y diseñando diferentes logos para las varias necesidades.

Los colores elegidos de Osix van desde un gradiente del #27920c hasta #00f7ff



También creamos una pequeña beta de un merchandising propio



Elección de servicios

Osix esta creado para ofrecer diferentes servicios a empresas recién creadas y para emprendedores que no tienen muchos contactos ni ideas para empezar su proyecto, en esos casos, Osix tiene toda una lista de complementos y servicios completos que pueden ayudar a cualquier emprendedor:



Construcción

- Construcción e instalación de los muebles de tu empresa
- Construcción e instalación del hardware de tu empresa
- Instalación del software de tu empresa
- Configuración y adaptación del software de tu empresa
- Implementación de la seguridad física de tu empresa
- Configuración de la seguridad física de tu empresa
- Implementación de la ciberseguridad de tu empresa
- Creación de los servicios web de tu empresa
- Instalación de los servidores de tu empresa
- Configuración de los servidores de tu empresa

Diseño

- Planificación y creación del back-end de la página web de tu empresa
- Planificación y creación del front-end de la página web de tu empresa
- Planificación y creación de los planos físicos de las sucursales de tu empresa
- Planificación y creación de los planos lógicos de las sucursales de tu empresa
- Planificación y creación de tu marca personal de empresa
- Planificación y creación del marketing de tu empresa
- Planificación de los servidores necesarios para tu empresa

Seguridad y Regulaciones

- Implementación de la gestión de recursos humanos
- Implementación del almacenamiento en la red corporativa
- Implementación del almacenamiento en los equipos de trabajo
- Implementación del almacenamiento en la nube
- Implementación de las aplicaciones permitidas
- Implementación de la clasificación de la información
- Implementación de la concienciación y la formación
- Implementación de la continuidad de negocio



- Implementación del cumplimiento legal
- Implementación del plan del director de seguridad
- Implementación de la relación con los proveedores
- Implementación del teletrabajo seguro
- Implementación del borrado seguro y la gestión de soportes
- Implementación del uso de dispositivos móviles corporativos
- Implementación del antimalware
- Implementación de la auditoría de sistemas
- Implementación del comercio electrónico
- Implementación del control de acceso
- Implementación de las copias de seguridad
- Implementación de la gestión de logs
- Implementación de la protección de la página web
- Implementación de la respuesta a los incidentes
- Implementación del uso de técnicas criptográficas
- Implementación de las actualizaciones de software
- Implementación del almacenamiento en dispositivos extraíbles
- Implementación de la protección del puesto de trabajo
- Implementación del uso de wifi y las redes externas
- Implementación del uso de correo electrónico
- Implementación del uso de dispositivos móviles no corporativos
- Implementación de las contraseñas

Pack de servicios

- Construcción de tus sucursales
- Diseño de tu empresa
- Seguridad y regulación de tu empresa
- Políticas para el empresario
- Políticas para el personal técnico
- Políticas para el empleado
- Confía en nosotros

Elección de objetivos

La empresa de Osix ha sido creada con la finalidad de dar servicio a los nuevos emprendedores, teniendo como objetivo el crecimiento de la empresa para otros proyectos de la misma y el aumento de la popularidad entre las diferentes empresas.

Como objetivo de crecimiento, tenemos en mente aumentar las opciones de nuestros servicios, con nuevos empleados que sean profesionales en los mismos servicios, aparte de un aumento de plantilla cada vez mayor, así poder ofrecer los mismos servicios a muchas más empresas al mismo tiempo.

Elección de empleados y funciones

Los cuatro cofundadores de Osix Enterprise, son actualmente los propios empleados de la misma, acaparando muchos puestos de trabajo que van a estar ocupados por nuevos profesionales durante Osix esté en aumento.



Eduard Castelló como presidente de la empresa y encargado de todas las delegaciones de la misma, a parte de dirigir los temas jurídicos de la empresa siendo el propio asesor jurídico.



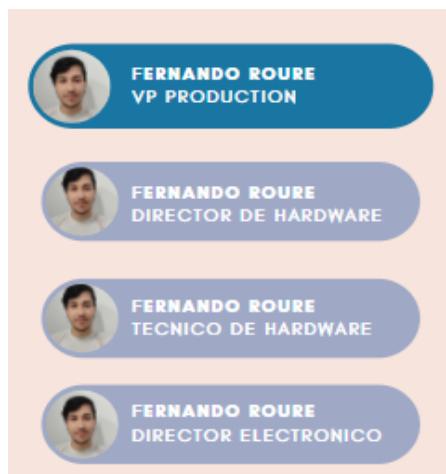
Alejandro Berengena es el director de ventas y marketing de la empresa, ocupándose de todas las partes de las ventas de Osix Enterprise, las relaciones públicas, los envíos y los contactos con las diferentes empresas.



Sergi Palacios es el director financiero y el diseñador de la empresa, es el encargado de poner los precios a los diferentes servicios para obtener un beneficio suficiente para el crecimiento de la empresa, y procurar que nuestro público sea consciente de nuestra existencia y incentivar el uso de nuestros servicios, se encarga de la contabilidad de toda la empresa y del diseño de cada publicidad, producto o servicio técnico.



Fernando Roure es el director de producción de Osix Enterprise, encargado de los materiales que pueden usarse y en qué caso es más óptimo usarlos, se encarga de la contratación de los obreros necesarios y del material a utilizar en cada situación.



Creación del plan financiero

El plan económico está relacionado con el total de gasto posible a asumir para el pago de todos los empleados, los gastos variables de la empresa respecto a los empleados y la posibilidad y opción de aumentar o la necesidad de reducir gastos relacionados con los empleados.

Gasto total en trabajadores

En Osix se ha decidido hacer una previsión del gasto total en cada trabajador, para ello se tiene en cuenta el gasto económico total para la empresa, que consta de el sueldo del trabajador más los impuestos pagados por la empresa por tener el mismo, en los gastos también se tiene en cuenta un aporte económico mensual para los gastos del trabajador que estén relacionados con su trabajo, y otro margen por si surgen problemas con el mismo trabajador, siempre que el trabajador no tenga una estricta culpa sobre el problema, en los gastos, también se cuentan las pagas extras y un cierto número de horas extra a pagar para tener otro margen de las mismas.

Gastos variables de los trabajadores

Los gastos variables de osix tienen en cuenta un número mínimo horas extra mensuales trabajadas y un cierto número máximo que se debe evitar, siempre existe la posibilidad de una mala época de desgracias, para ello Osix tiene un margen bastante amplio para los mismos, si un empleado es dado de baja o es despedido, Osix cuenta con un límite máximo de gasto permitido para contratar a otro trabajador en su lugar.

Osix tiene en cuenta gastos como las comidas de empresa o el transporte necesario para ir a un cierto lugar siempre que sea posible para alguna celebración, dado que todas estas “fiestas de trabajo” corren a total cuenta de Osix Enterprise.

Aumento o reducción de personal

Osix Enterprise tiene en mente y como objetivo, poder crecer lo suficiente como para competir con las actuales empresas más reconocidas, con lo cual el objetivo es poder contratar a los máximos empleados posibles, para ello si el beneficio trimestral de la empresa supera el 30% Osix tiene un plan de aumento de sucursal, al finalizarlo se planeará en la contratación de 5 nuevos empleados para el aumento de personal.

Elección y propuesta de sucursales

Informe técnico

En nuestra empresa decidimos crear una sede principal, la cual sirva también de zona de testeo de nuevos productos.

Luego por otra parte tenemos nuestras sedes que tienen estructuración, pero aún son ideas candentes e ilusiones de nuestra empresa ya que estamos empezando y sería lo que nos gustaría hacer.

Cada pc tiene dos rosetas y un sai, que les permiten tener conexión y si ocurriera cualquier apagón estarían seguros durante una hora más o menos.

Los equipos móviles tienen debajo de la mesa un alargador con cada cargador móvil correspondiente, para que mientras los clientes los prueben se sigan cargando así siempre están disponibles para probar.

Y cada estructuración tiene una subestructuración de cámaras para tener la tienda totalmente vigilada.

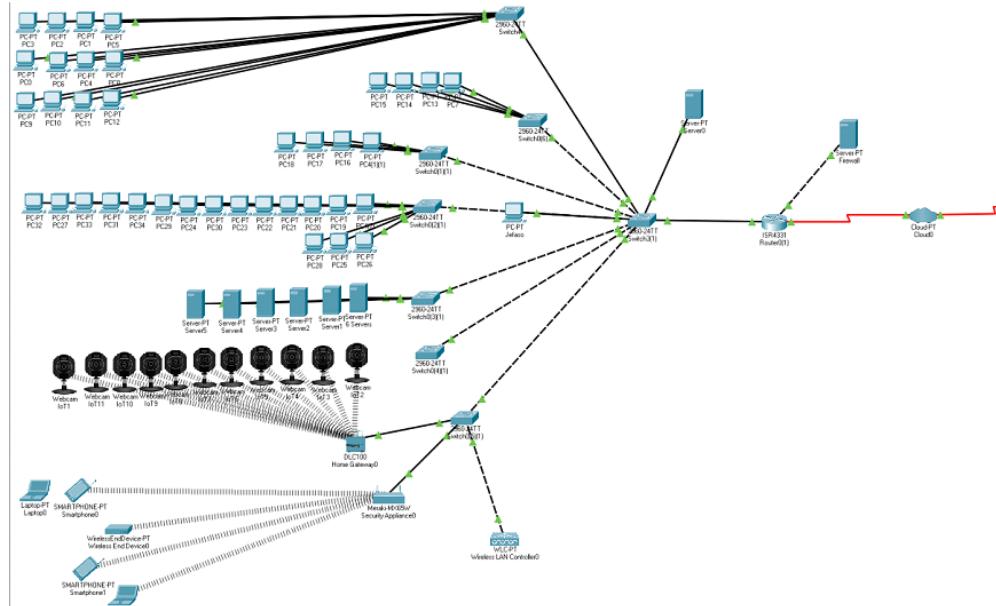


Lleida



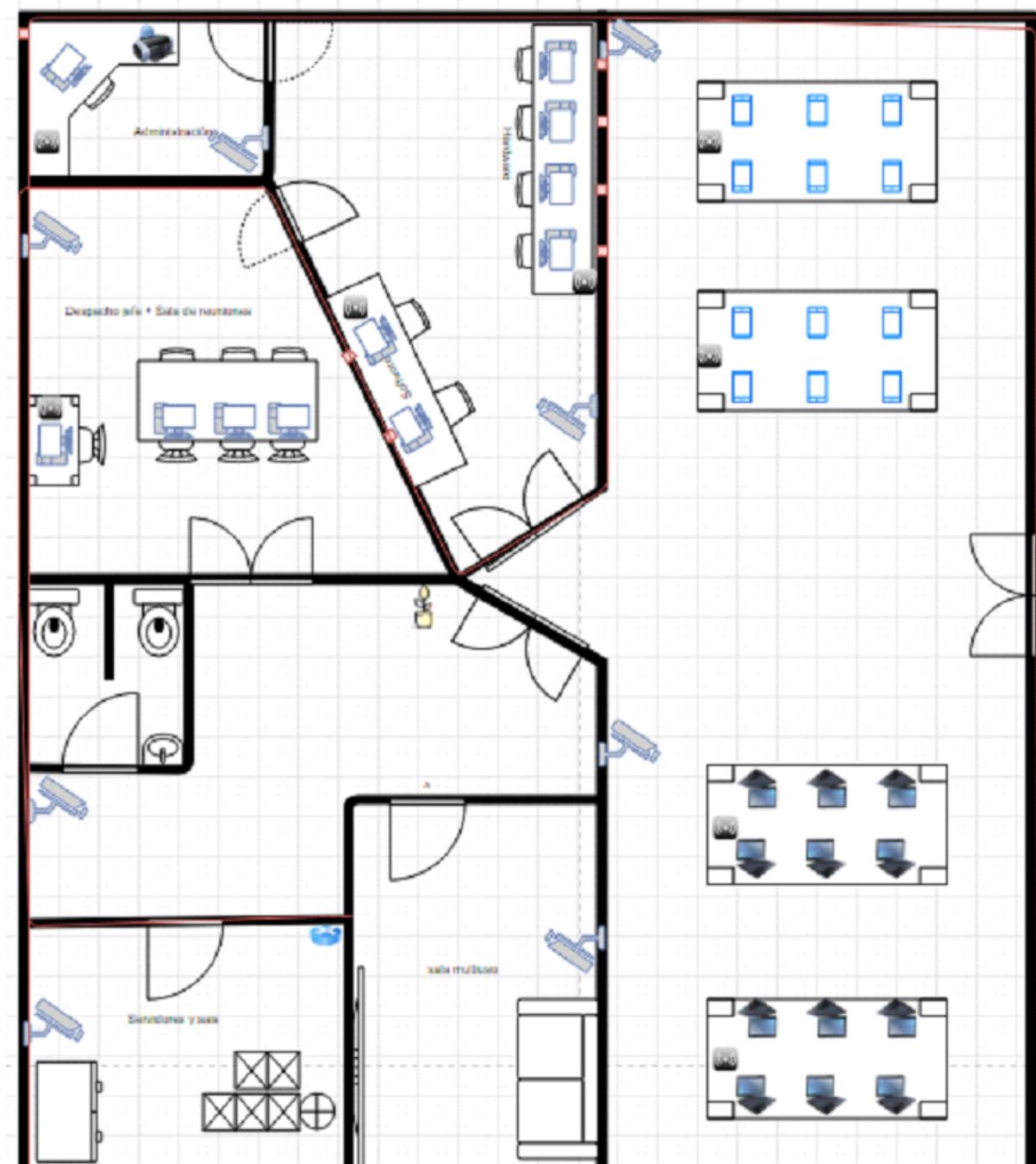
Esta sería nuestra sede principal en Lleida, la cual como explicamos antes tenemos la zona de testo en la parte inferior del sce, también hacemos clases para enseñar a los clientes que lo deseen.

Cisco packet tracer



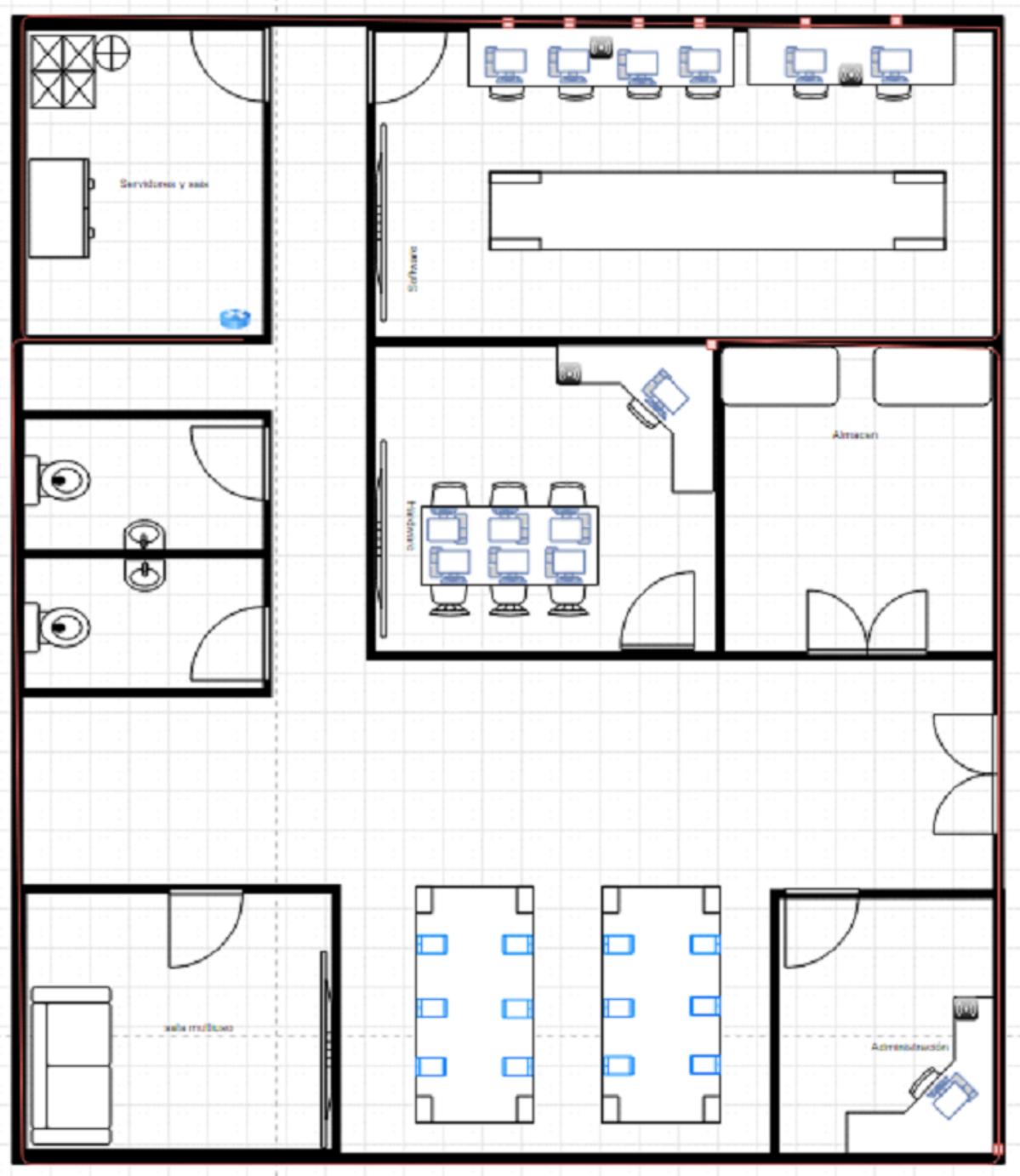
Este es nuestro cisco packet tracer, es nuestro cableado principal, se basa en un sistema dhcp, así cada pc tiene una ip asignada, cada switch sirve de bloqueo, así cada red es privada y tenemos una red a parte de todo para las cámaras. Tenemos un servidor privado para la seguridad.

Tarragona



Aquí en Tarragona quisimos innovar con la estructura de la tienda ya que era una estructuración de pared lateral y quisimos adaptarnos e ella lo mejor posible ya que la localización de la tienda merece la pena

Barcelona

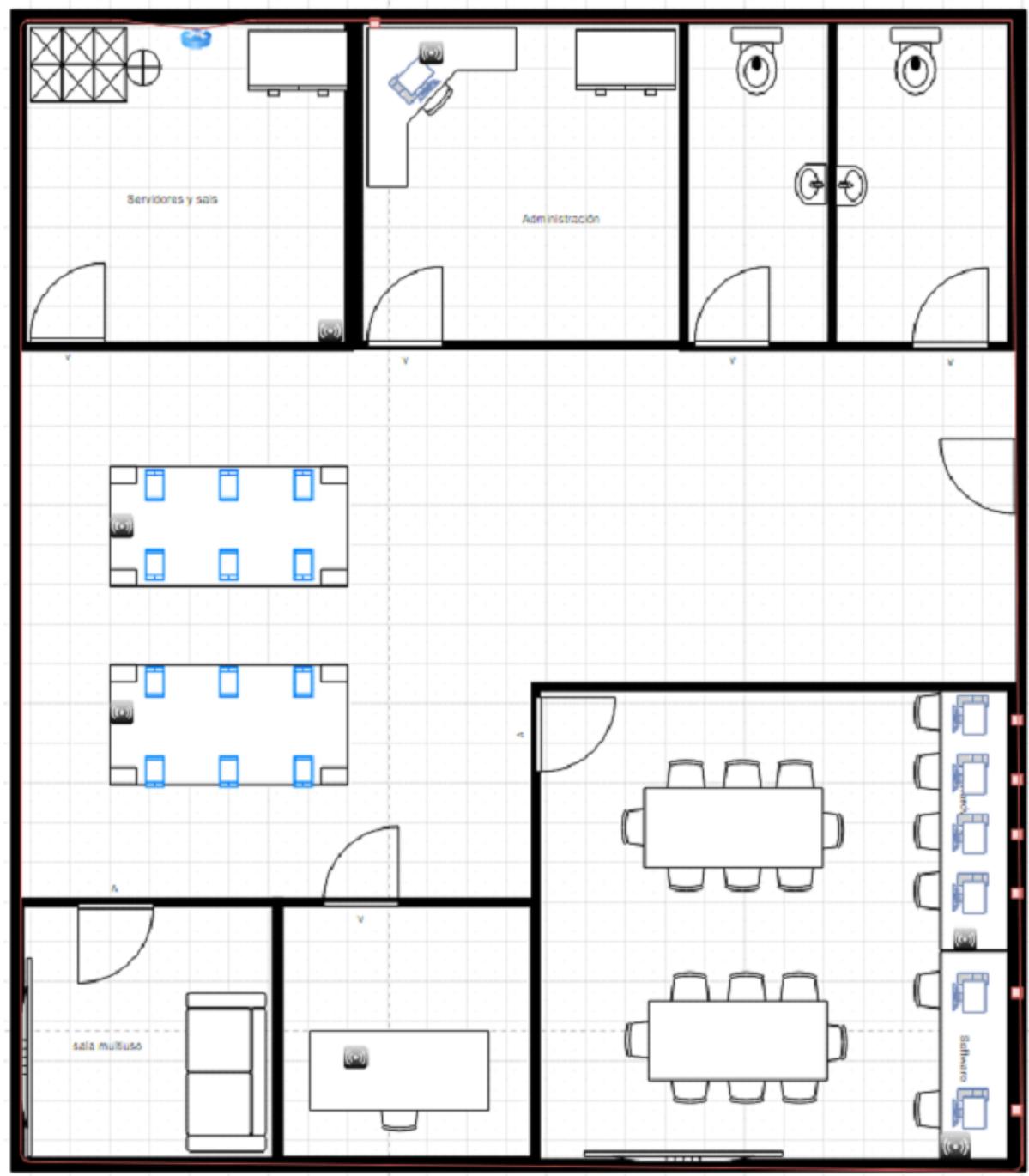


En Barcelona optamos por una tienda más amplia y con más espacio, ya que es la ciudad con más población.

Y para que no se aglomere la gente dijimos de hacerla espaciosa.

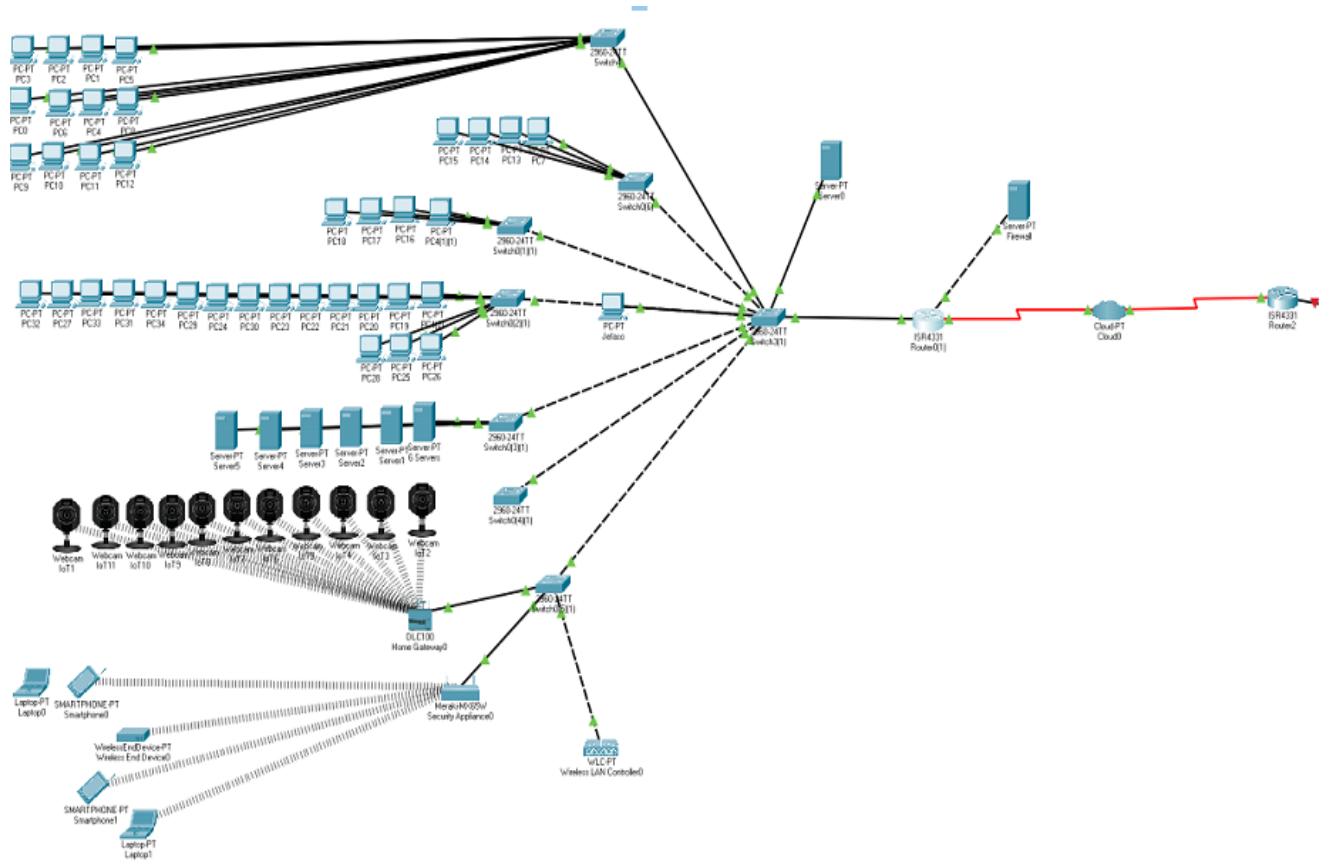
Sobre todo el pasillo principal.

Girona

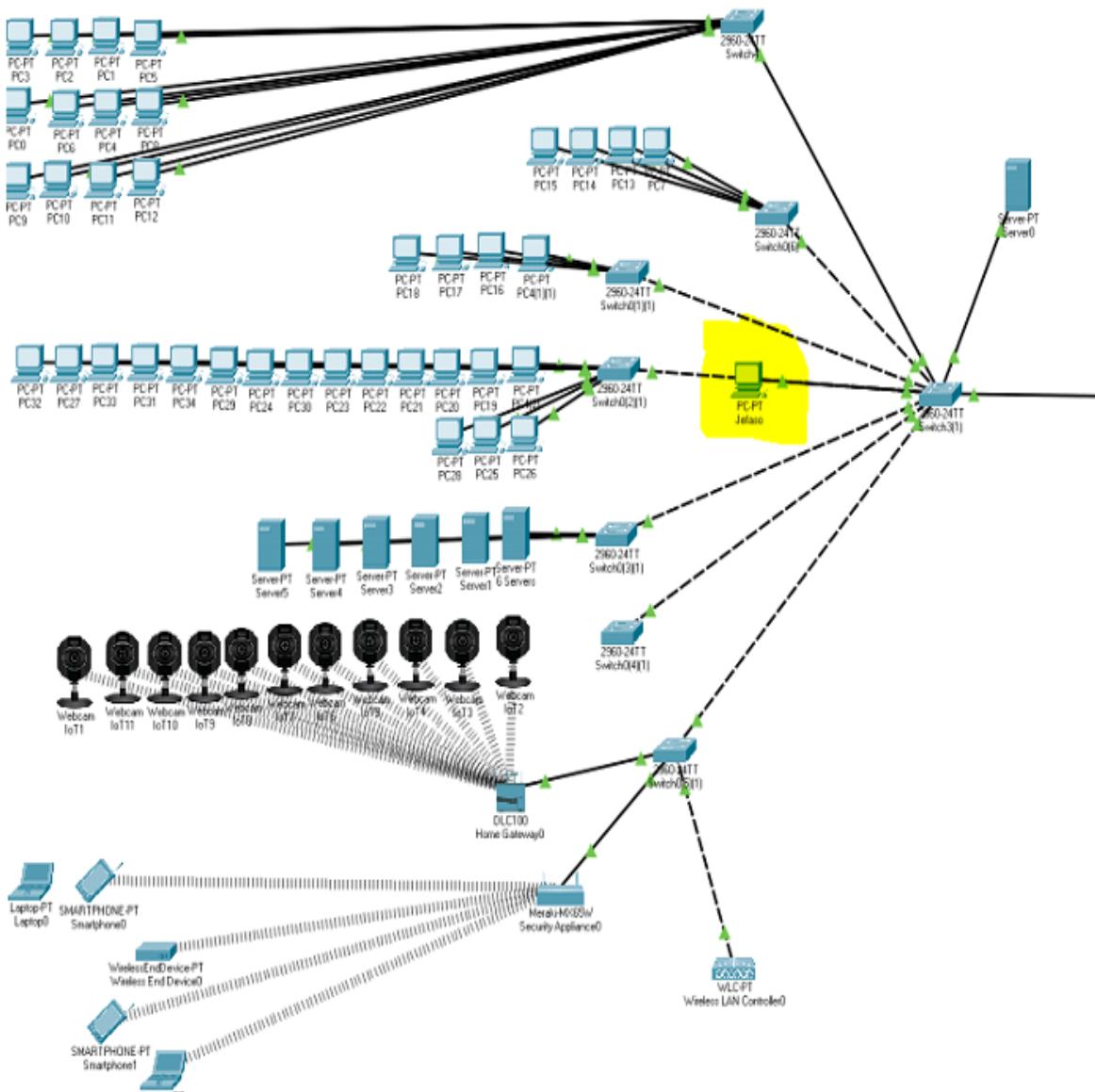


En Girona dijimos de hacer una sala grande central y de ahí partir a todas las demás, de momento es la tienda que más nos gusta en comparación con las sedes, ya que nuestra mejor tienda siempre sera nuestra tienda principal de Lleida

Cisco packet tracer general



Esta sería nuestra organización en el cisco, tenemos un router principal del cual semana 1 switch principal para dividir la red en 7, las cuales tienen un switch principal cada uno.



A destacar estaría el pc del Jefe el cual estaría situado antes de los switch de cada red, mejor dicho con los switch de cada rez, ya que así puede acceder a todas las redes y a su vez puede tener una red privada.

Router0(1)

- [Physical](#)
- [Config](#) **Config**
- [CLI](#)
- [Attributes](#)

Algorithm Settings	GigabitEthernet0/0/1
ROUTING	
Static	<input checked="" type="checkbox"/> On
RIP	<input type="radio"/> 1000 Mbps <input checked="" type="radio"/> 100 Mbps <input type="radio"/> 10 Mbps <input checked="" type="checkbox"/> Auto
SWITCHING	<input type="radio"/> Half Duplex <input checked="" type="radio"/> Full Duplex <input checked="" type="checkbox"/> Auto
VLAN Database	MAC Address
INTERFACE	00E0.B08B.4452
GigabitEthernet0/0/0	
GigabitEthernet0/0/1	IP Configuration
GigabitEthernet0/0/2	IPv4 Address
Serial0/1/0	192.168.1.2
Serial0/1/1	Subnet Mask
GigabitEthernet0/2/0	255.255.255.0
GigabitEthernet0/2/1	
GigabitEthernet0/2/2	Tx Ring Limit
GigabitEthernet0/2/3	10

Equivalent IOS Commands

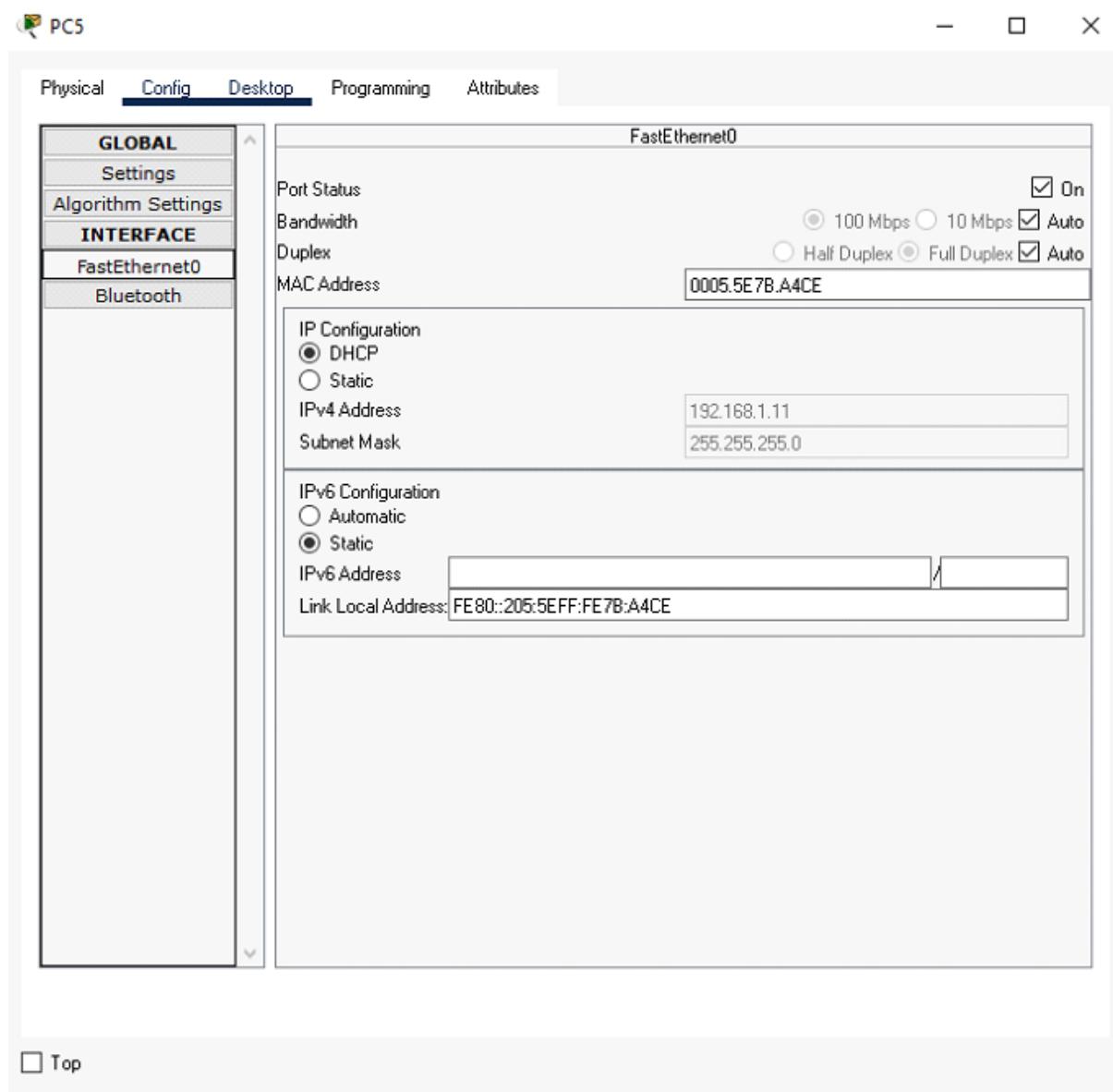
```

Router(config)#interface GigabitEthernet0/2/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/2/2
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/2
Router(config-if)#
Router(config-if)#exit
Router(config)#interface GigabitEthernet0/0/1
Router(config-if)#

```

Top

El router estará configurado así, le indicamos la máscara y la ipv 4
y indicariamos que queremos dhcp y marcariamos la franja de ip deseadas



Top

Los pc estarían configurados así, les indicaremos que deben usar el dhcp antes puesto en el router y automáticamente se les asignará una ip de las que fueron puestas en el router.

En nuestro caso sería de la 1 a la 255

Programas Utilizados

Cisco Packet Tracer

El cisco packet tracer fue de muy buena ayuda, ya que es un programa que se caracteriza por la realización de redes y estructuraciones red, puedes configurar cada dispositivo de manera particular, le puedes añadir o quitar partes del dispositivo para adaptarlo de una forma más específica y única, nos permite crear y editar las conexiones que indiquemos y subdividir las redes que veamos.

También nos permite editar servidores para especializarse en firewalls.

Diagrams.net

Es una herramienta muy útil a la hora de la creación de estructuras, desde casas domotizadas a edificios enteros, en nuestro caso realizamos 4 estructuras de tienda totalmente cableadas y montadas, con sus respectivos servidores, pc, cámaras etc...

Es muy específica y certera, ya que tienes los pixeles de tamaño los cuales puedes modificar a tu gusto y te permite crear estructuras muy certeras.

Creación de la página web

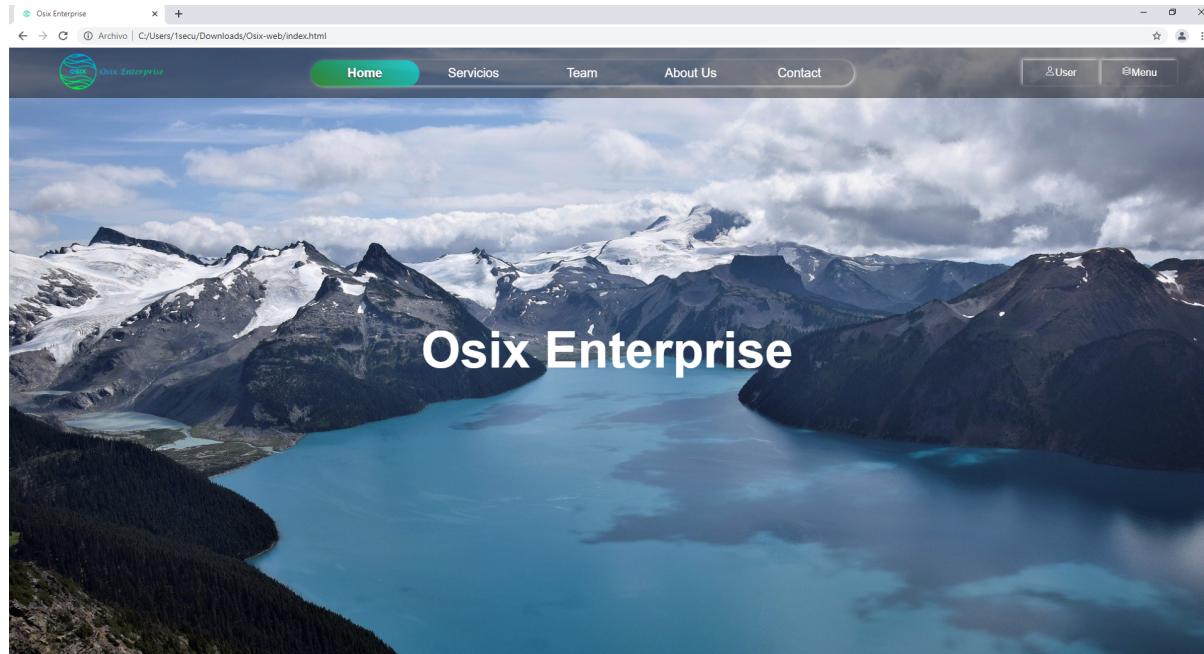
Como página web principal de Osix Enterprise, tenemos creada y establecida una beta de la misma, la cual solo consta del front-end de la propia web, este front end queríamos hacerlo solamente en lenguaje puro, tanto html puro, como css puro, no hemos querido integrar ningún tipo de programación de javascript ya que pensabamos que sería demasiado avanzado para el proyecto.

Dentro de toda la estructura de nuestro front-end, podemos encontrar un indice.html principal con sus propio estilo.css, como páginas secundarias, tenemos la página de login de la empresa y la página de registro, que comparten el mismo código de css, a parte tenemos una plantilla preparada para hacer un menú para los usuarios en una página aparte con su propio estilo.css, finalmente, tenemos un que nos lleva a cuatro diferentes páginas web con la información de cada uno de los fundadores de Osix Enterprise.



La web de Osix Enterprise está en un apartado Alpha, el cual no dispone aún de una web funcional y bien diseñada para móviles ni tabletas, tampoco tiene ninguna base de datos acoplada a ella.

Inicio



Al entrar a la página vemos un header que ocupa todo el amplio de la pantalla, está basado en que puedas moverte por toda la página web, que es One-Page. Con el menú central podemos bajar y subir por toda la web y podemos volver arriba de la misma con el propio botón de home o clicando en el logo de Osix, también podemos acceder al login de la web con el botón de "User" o acceder al menú con el botón de "Menú". Tenemos un background con una foto tranquila intentando hacerte sentir tranquilo y el nombre de nuestra empresa en un blanco básico en medio de la pantalla.

Teoría del NavBar

```
<!--navegacion principal-->
<header>
    <a href="#" class="logo">
        
    </a>
    <div class="wrapper">
        <nav>
            <input type="radio" name="tab" id="Home" checked>
            <input type="radio" name="tab" id="About">
            <input type="radio" name="tab" id="Services">
            <input type="radio" name="tab" id="ContactUs">
            <input type="radio" name="tab" id="Team">
            <label for="Home" class="Home"><a href="#home">Home</a></label>
            <label for="About" class="About"><a href="#servicio">Servicios</a></label>
            <label for="Services" class="Services"><a href="#team">Team</a></label>
            <label for="ContactUs" class="ContactUs"><a href="#about">About Us</a></label>
            <label for="Team" class="Team"><a href="#footer">Contact</a></label>
            <div class="tab"></div>
        </nav>
    </div>
    <div class="user">
        <nav>
            <div class="nav left">
                <div class="btn left" id="left">
                    <a href="Login/login.html">
                        <ion-icon name="person-outline"></ion-icon>User
                    </a>
                    <div class="d1"></div>
                    <div class="d2"></div>
                    <div class="d3"></div>
                    <div class="d4"></div>
                </div>
            </div>
            <div class="nav left">
                <div class="btn left" id="right">
                    <a href="Menu/Menu.html">
                        <ion-icon name="layers-outline"></ion-icon>Menu
                    </a>
                    <div class="d1"></div>
                    <div class="d2"></div>
                    <div class="d3"></div>
                    <div class="d4"></div>
                </div>
            </div>
        </nav>
    </div>
</header>
```

En el html, para hacer la animación de la navegación principal sin usar javascript, hemos necesitado crear por cada label, un input que nos ayuda junto a el css a hacer la propia animación, estos labels los relacionamos entre los inputs para que detecten cuando clicas en ellos, al final de la navegación tenemos un div llamado tab que es la propia forma del fondo del menú.

En la derecha del header, los botones de user y menú, son varios divisores donde dentro esta el link para ir a los diferentes sitios, esto esta hecho asi porque



tenemos cuatro animaciones que rodean el botón principal, los cuales son los 4 divs que tiene cada botón, podríamos haber puesto un botón pero no pensamos en ello en el momento y no funcionaban varios intentos.

```
/*navegacion principal*/

header {
    position: fixed;
    top: 0;
    left: 0;
    width: 100%;
    height: 20px;
    display: flex;
    justify-content: space-between;
    align-items: center;
    place-items: center;
    text-align: center;
    transition: 0.6s;
    padding: 40px;
    z-index: 100000;
    background-color: #rgba(0, 0, 0, 0.432);
}

header .logo {
    position: relative;
    margin-left: 40px;
    transition: 0.6s;
    width: 170px;
}

.wrapper {
    height: 40px;
    width: 45vw;
    line-height: 40px;
    border-radius: 50px;
    box-shadow: 2px 2px 5px #rgba(255, 255, 255, 0.603), -3px -3px 7px #rgba(255, 255, 255, 0.05);
    margin-right: 40px;
}

header .wrapper nav {
    position: relative;
    display: flex;
}

header .wrapper nav label {
    flex: 1;
    width: 100%;
    z-index: 1;
    position: relative;
    cursor: pointer;
}
```

en el css simplemente ponemos que el header sea fijo para que pueda moverse por la pantalla y distribuimos el espacio con la opción de flex, también lo ponemos delante de cualquier cosa de la web con z-index y vemos que tamaños y algunas otras opciones del logo y la navegación principal.

Título

```
<!--titulo-->
<section class="titulo" id="home">
|   <h1>Osix Enterprise</h1>
</section>
<!--fin del titulo-->
```

El título de Osix Enterprise es solamente una sección con un h1,

```
/*titulo*/
.titulo {
    width: 100%;
    height: 100vh;
    background-image: url(imagenes/lake-6003746_1920.jpg);
    background-size: cover;
    background-position: center;
    background-repeat: no-repeat;
    display: flex;
    flex-direction: column;
    justify-content: center;
    position: relative;
    animation: changeColor 5s linear infinite;
}

.titulo h1 {
    margin: auto;
    font-size: 58px;
    position: absolute;
    top: 45%;
    width: 100%;
    text-align: center;
    font-size: 5em;
    color: ■white;
}

.titulo .borde .dot {
    color: ■white;
}

/*fin del titulo*/
```

El css del título, solo centramos el propio h1 con flex y centramos todo el contenido y le añadimos color.



Sección Servicios

Servicios tanto a particulares como a empresas recien creadas

Construcción	Diseño	Seguridad
2500€	2000€	1500€
Instalación	10GB space	10GB space
Configuración	10GB space	10GB space
Implementación	10GB space	10GB space
Creación	10GB space	10GB space
Información	Información	Información

Pack 1	Pack 2	Pack 3
3000€	4000€	5000€
Instalación	10GB space	10GB space
Configuración	10GB space	10GB space
Implementación	10GB space	10GB space
Creación	10GB space	10GB space
Información	Información	Información

Tenemos unas tarjetas modificadas con el título del paquete del servicio, el precio del mismo, y los servicios que incluye, esta sección también tiene varias animaciones sin javascript.

```

<!--tarjetas productos-->
<section class="servicios">
    <h1>Servicios tanto a particulares como a empresas recien creadas
    </h1>
    <div class="contenedor">
        <div class="linea">
            <div class="columna">
                <div class="box">
                    <div class="titulo1"><i class="fa fa-paper-plane"></i>
                        <h2>Construcción</h2>
                    </div>
                    <div class="precio">
                        <h4>2500<sup>€</sup></h4>
                    </div>
                    <div class="opciones">
                        <ul>
                            <li><i class="fa fa-check"></i>Instalación</li>
                            <li><i class="fa fa-check"></i>Configuración</li>
                            <li><i class="fa fa-check"></i>Implementación</li>
                            <li><i class="fa fa-check"></i>Creación</li>
                        </ul>
                    </div>
                    <a href="#">Información</a>
                </div>
            </div>
            <div class="columna">
                <div class="box">
                    <div class="titulo1"><i class="fa fa-paper-plane"></i>
                        <h2>Diseño</h2>
                    </div>
                    <div class="precio">
                        <h4>2000<sup>€</sup></h4>
                    </div>
                    <div class="opciones">
                        <ul>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                        </ul>
                    </div>
                    <a href="#">Información</a>
                </div>
            </div>
            <div class="columna">
                <div class="box">
                    <div class="titulo1"><i class="fa fa-paper-plane"></i>
                        <h2>Seguridad </h2>
                    </div>
                    <div class="precio">
                        <h4>1500<sup>€</sup></h4>
                    </div>
                    <div class="opciones">
                        <ul>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                        </ul>
                    </div>
                    <a href="#">Información</a>
                </div>
            </div>
        </div>
    </div>

```

Para los servicios tenemos cada tarjeta en su propio div, y estas están en otro div en grupos de tres, las siguientes tres están en otro div diferente.

```

.container {
  width: 100%;
}

.container h1 {
  text-align: center;
  margin-bottom: 50px;
  font-size: 38px;
  text-shadow: 0px 5px 10px rgba(168, 168, 168, 0.685);
  background: -webkit-linear-gradient(#c57242, #eff000);
  -webkit-background-clip: text;
  -webkit-text-fill-color: transparent;
}

/*Servicios tarjetas*/

.servicios {
  padding: 100px 0px;
  box-sizing: border-box;
  background: linear-gradient(30deg, #2fb30e, #159ba0);
}

.contenedor {
  width: 1200px;
  height: 520px;
  margin: 0 auto;
}

.contenedor .columna {
  position: relative;
  width: 400px;
  float: left;
  transition: 0.5s;
}

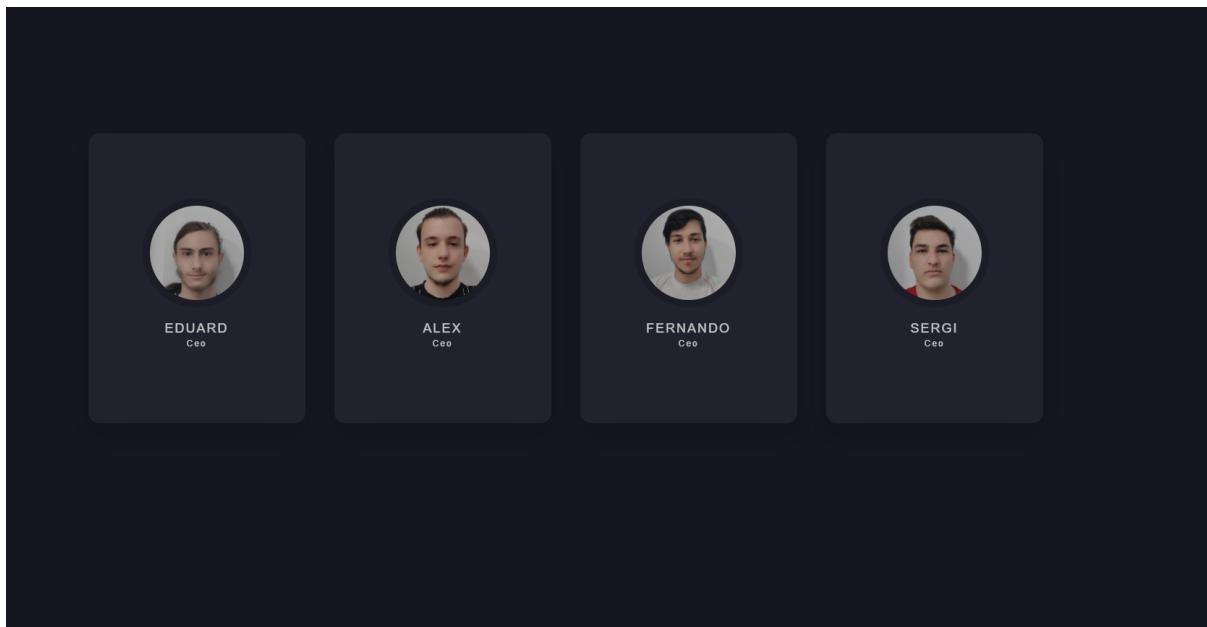
.contenedor .columna .box {
  position: relative;
  width: 320px;
  min-height: 550px;
  margin: 0 auto;
  padding: 20px;
  box-sizing: border-box;
  text-align: center;
  border-bottom-left-radius: 150px;
  border-bottom-right-radius: 150px;
  border: 1px solid rgba(255, 255, 255, 0.04);
  border-right: 1px solid rgba(255, 255, 255, 0.02);
  border-bottom: 1px solid rgba(255, 255, 255, 0.02);
  box-shadow: 0 5px 45px rgba(0, 0, 0, 0.1);
  overflow: hidden;
  transition: 0.5s;
}

.contenedor .columna .box:hover {
  transform: translateY(-20px);
}

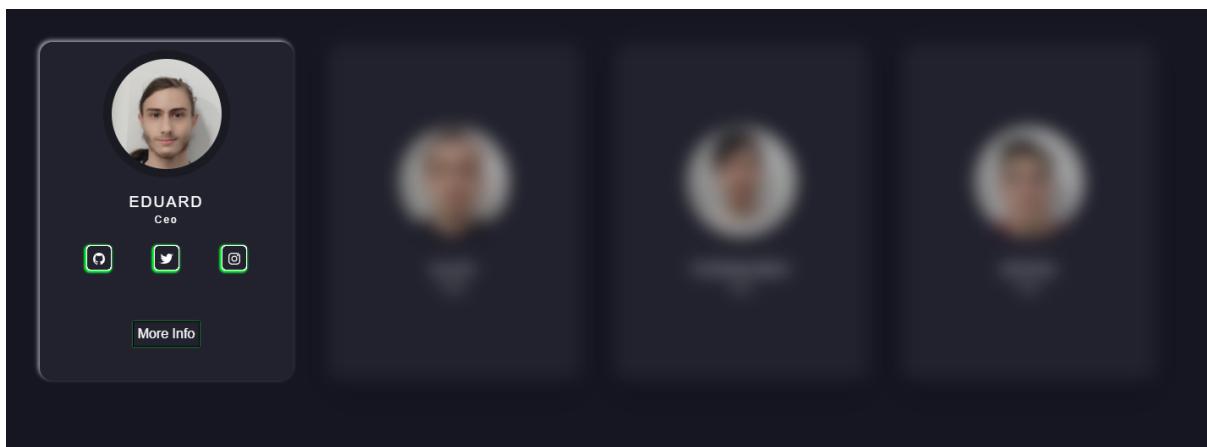
```

El css es un poco más complicado en este caso porque hemos de hacer la forma de la tarjeta modificando el radio de los lados, le añadimos el tiempo de la transición y el movimiento y el degradado de verde a azul del fondo.

Equipo



Queríamos diseñar algo minimalista para este trozo de la web, diseñando así una tarjeta con una portada base para cada miembro de Osix.



Al poner el ratón sobre uno de los miembros, los demás miembros se difuminan y aparece desde abajo varias redes sociales del miembro y un botón que lleva a otra pagina donde hay más información.

```

<!--cartas-->


<section class="workers">
        <div class="contenedorcarta">
            <div class="cartas">
                <div class="contenido">
                    <div class="imagen">
                        
                    </div>
                    <div class="contenidotext">
                        <h3>Eduard<br><span>Ceo</span></h3>
                    </div>
                </div>
                <ul class="cli">
                    <li style="--i:1">
                        <div class="iconos"><a href="https://github.com/kutedo2001">
                            <div class="layer">
                                <span></span>
                                <span></span>
                                <span></span>
                                <span></span>
                                <span class="fab">
                                    <ion-icon name="logo-github"></ion-icon>
                                </span>
                            </div>
                            <div class="textito" id="face">Github</div>
                        </a>
                    </div>
                    <li style="--i:1">
                        <div class="iconos"><a href="https://twitter.com/kutedo19">
                            <div class="layer">
                                <span></span>
                                <span></span>
                                <span></span>
                                <span></span>
                                <span class="fab">
                                    <ion-icon name="logo-twitter"></ion-icon>
                                </span>
                            </div>
                            <div class="textito" id="twitt">Twitter</div>
                        </a>
                    </div>
                    <li style="--i:1">
                        <div class="iconos"><a href="https://www.instagram.com/eduard_castello/">
                            <div class="layer">
                                <span></span>
                                <span></span>
                                <span></span>
                                <span></span>
                                <span class="fab">
                                    <ion-icon name="logo-instagram"></ion-icon>
                                </span>
                            </div>
                            <div class="textito">Instagram</div>
                        </a>
                    </div>
                </ul>
                <div class="more">


```

Para el html creamos un div donde están varios divs que son los diferentes contenidos de cada carta,

```

/*cartas*/
.cartitas {
  display: flex;
  justify-content: center;
  align-items: center;
  flex-wrap: wrap;
  min-height: 100vh;
  background: #161623;
}

.workers {
  position: relative;
}

.contenedorcarta {
  position: relative;
  z-index: 1;
  display: flex;
  justify-content: center;
  flex-wrap: wrap;
  margin: 40px 0;
}

.contenedorcarta .cartas {
  position: relative;
  width: 300px;
  height: 400px;
  background: rgba(255, 255, 255, 0.05);
  margin: 20px;
  box-shadow: 0 15px 35px rgba(0, 0, 0, 0.2);
  border-radius: 15px;
  display: flex;
  justify-content: center;
  filter: blur(0px);
}

.contenedorcarta .cartas .more {
  position: absolute;
  bottom: -60px;
  display: flex;
  transform: translateY(100px);
  transition: 0s;
  opacity: 0;
  text-decoration: none;
}

.contenedorcarta .cartas:hover .more {
  transform: translateY(-100px);
  transition: 0.5s;
  opacity: 1;
  box-shadow: 0px 0px 2px #14f339;
}

.contenedorcarta .cartas:hover .more a {
  text-decoration: none;
  color: #fff;
  background: transparent;
  border: 1px solid black;
  padding: 5px;
}

.contenedorcarta .cartas .more a:hover {
  background-color: #14f339;
  color: black;
}

```

El css define primero los márgenes entre las cartas de los miembros, añade el color del fondo de la sección y añade una animación al botón de más información de cada carta.

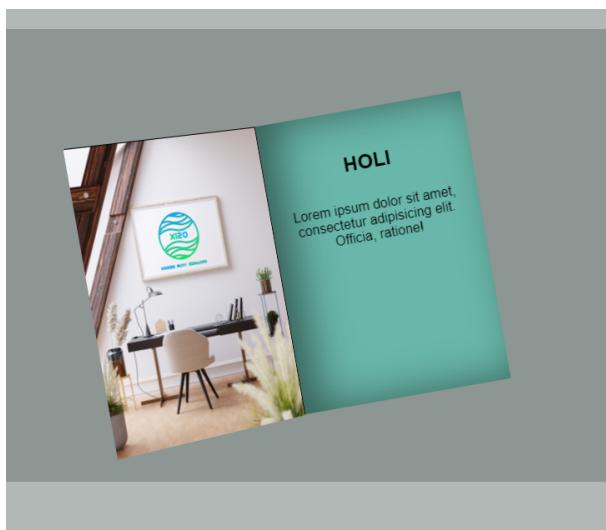


Después definimos la animación y por donde queremos que lleguen las redes sociales, y metemos blur en el div donde están las cuatro cartas para quitarlo después de la carta en la que está el ratón, añadimos que el div de la foto tenga esa circunferencia y que tenga una animación que le suba arriba de la carta.

Sobre Nosotros

The screenshot shows the 'About Us' section of a website. At the top center is the heading 'About Us'. Below it is a large image of an office interior with a desk, chair, and a framed logo on the wall. To the right of the image, the company name 'OSIX ENTERPRISE' is displayed in bold capital letters. A small paragraph of text follows, describing the company's mission to help entrepreneurs turn their ideas into reality. Below this text are three social media icons: Instagram (blue), Twitter (red), and GitHub (blue).

Esta sección tiene un pequeño texto a la izquierda donde nos presentamos, con las redes sociales de la empresa debajo de ese div y a la izquierda tenemos la portada de un libro que al ponernos en ella se abre mostrando otro texto.



La propia carta tiene una animación de 360 grados para abrirse y al abrirse tenemos un borde o contorno difuminado en negro para darle contorno al libro.

```

<!--Conocenos-->


<div class="containerAU">
        <div class="lin">
            <div class="section-title">
                <h1>About Us</h1>
            </div>
        </div>
        <div class="lin">
            <div class="inner-container">
                <div class="inner-box">
                    <div class="izqui">
                        <div class="cartAU">
                            <div class="imgca">
                                
                            </div>
                            <div class="detalles">
                                <h2>HOLI</h2>
                                <p>Lorem ipsum dolor sit amet, consectetur adipisicing elit. Officia, ratione!</p>
                            </div>
                        </div>
                    </div>
                    <div class="dere">
                        <h1>Osix Enterprise</h1>
                        <p class="tt">Osix Enterprise es una empresa dedicada a proporcionar diversos servicios a emprendedores con ganas de hacer sus ideas d negocio realidad, ayudamos en todo lo que podamos a estos emprendedores y les acompañamos en su primer año, Osix Enterprise tambien esta dedicada a la creacion y mejora de software privado para empresas que deseen adquirirlo.
                    </p>
                    <div class="rede">
                        <span>Instagram</span>
                        <span>Twitter</span>
                        <span>Github</span>
                    </div>
                    <div class="soci">
                        <a href="https://www.instagram.com/osix.es/">
                            <ion-icon class="ico insta" name="logo-instagram"></ion-icon>
                        </a>
                        <a href="https://twitter.com/kutedo19">
                            <ion-icon class="ico twi" name="logo-twitter"></ion-icon>
                        </a>
                        <a href="https://github.com/Osix-Enterprise">
                            <ion-icon class="ico fac" name="logo-github"></ion-icon>
                        </a>
                    </div>
                </div>
            </div>
        </div>
    </div>
<!--Fin de conocenos-->


```

Tenemos un div donde tenemos el h1 del título de la sección y después un div que es para la carta de la izquierda y otro div que contiene el resumen de la empresa y otro con las redes sociales.



```

/*Conocenos*/
.about-section {
  padding: 10px;
  background: #rgba(108, 119, 117, 0.527);
}

.section-title h1 {
  justify-content: center;
  align-items: center;
  text-align: center;
  padding: 25px;
  font-size: 48px;
  text-shadow: 0px 5px 10px #rgba(168, 168, 168, 0.685);
  background: -webkit-linear-gradient(120deg, ##045891e3, ##1a352fef);
  -webkit-background-clip: text;
  -webkit-text-fill-color: transparent;
}

.inner-container {
  display: flex;
  justify-content: center;
  align-items: flex-end;
  padding: 20px 50px;
  flex-wrap: 0 0 80%;
  z-index: 1;
  position: relative;
}

.izqui {
  display: flex;
  background-size: cover;
  height: 100%;
  border-radius: 2%;
  margin-left: 200px;
  margin-bottom: 20px;
  justify-content: center;
  align-items: center;
  text-align: center;
}

.cartAU {
  position: relative;
  margin-left: 50px;
  width: 250px;
  height: 350px;
  background: #rgba(89, 199, 179, 0.692);
  transform-style: preserve-3d;
  transform: perspective(2000px);
  transition: 1s;
  box-shadow: inset 30px 0 50px #rgba(0, 0, 0, 0.5);
  cursor: pointer;
}

.cartAU:hover {
  z-index: 1000px;
  transform: perspective(2000px) rotate(-370deg);
  box-shadow: inset 20px 0 50px #rgba(0, 0, 0, 0.5);
}

.cartAU .imgca {
  position: relative;
}

```

Alineamos el título de la sección y utilizamos flex para dividir las dos partes, agregamos la animación del libro dándole la rotación y el tiempo para ello en los ejes correspondientes y las animaciones de los hover de cada red social.



Footer

The screenshot shows a footer with three main sections. The first section, 'Esta web', contains a paragraph of text about the website and four social media icons (Instagram, Twitter, GitHub, LinkedIn). The second section, 'Enlaces', lists links to 'Nosotros', 'Ayuda', 'Política de privacidad', 'Términos y condiciones', and 'Contactar'. The third section, 'Información de contacto', provides an address ('Lleida Cronista Muntaner 25001'), a phone number ('+34 644166918'), and an email ('1secuncala@gmail.com').

Debajo de la pagina principal añadimos un Footer con un fondo negro y los titulos en blanco, el texto esta en un gris claro y tenemos las redes sociales y algunos links con unas pequeñas animaciones al ponernos encima de ellas.

```
<!--footer-->
<footer>
  <div class="foot" id="footer">
    <div class="sect uno">
      <h2>Esta web</h2>
      <p>La web de Osix Enterprise, es un proyecto educativo y personal a partes iguales, esta, está diseñada y programada por Eduard Castelló, el CEO de la propia empresa, tambien ficticia, cada linea de codigo a sido escrita a mano, tanto de HTML como de CSS y sin utilizar ningun codigo de JavaScript, esto a sido posible gracias a el estudio y la repeticioes de muchas lineas de programacion encontrada por internet. No obstante Osix Enterprise es una web totalmente legitima y no vulnera ningun derecho, ni la web, ni Osix Enterprise como empresa dueña de la misma.</p>
      <ul class="lis">
        <li><a href="https://www.instagram.com/eduard_castello/">
          <ion-icon class="dec" name="logo-instagram"></ion-icon>
        </a></li>
        <li><a href="https://twitter.com/kutedo19">
          <ion-icon class="dec" name="logo-twitter"></ion-icon>
        </a></li>
        <li><a href="https://github.com/kutedo2001">
          <ion-icon class="dec" name="logo-github"></ion-icon>
        </a></li>
        <li><a href="https://www.linkedin.com/in/eduard-castelló-55a62614b">
          <ion-icon class="dec" name="logo-linkedin"></ion-icon>
        </a></li>
      </ul>
    </div>
    <div class="sect dos">
      <h2>Enlaces</h2>
      <ul>
        <li><a href="">Nosotros</a></li>
        <li><a href="">Ayuda</a></li>
        <li><a href="">Política de privacidad</a></li>
        <li><a href="">Términos y condiciones</a></li>
        <li><a href="">Contactar</a></li>
      </ul>
    </div>
    <div class="sect tres">
      <h2>Información de contacto</h2>
      <ul class="inf">
        <li><span>
          <ion-icon class="dec" name="locate-outline"></ion-icon>
          </span><span>Lleida<br>Cronista Muntaner<br>25001</span>
        </li>
        <li><span>
          <ion-icon class="dec" name="call-outline"></ion-icon>
          </span>
          <p><a href="">+34 644166918</a><br><a href="">973 21 04</a></p>
        </li>
        <li><span>
          <ion-icon class="dec" name="mail-outline"></ion-icon>
          </span>
          <p><a href="">1secuncala@gmail.com</a></p>
        </li>
      </ul>
    </div>
  </div>
</footer>
```

El html tiene un div principal que contiene las tres columnas del footer, con varios spans para editar esas partes en concreto de una manera específica.



```

/*Footer*/
footer {
    position: relative;
    width: 100%;
    height: auto;
    padding: 50px 100px;
    background: #111;
    display: flex;
    justify-content: space-between;
    flex-wrap: wrap;
    flex-direction: row;
}

footer .foot {
    display: flex;
    justify-content: space-between;
    flex-wrap: wrap;
    flex-direction: row;
}

footer .foot .sect {
    margin-right: 30px;
}

footer .foot .sect.uno {
    width: 40%;
}

footer .foot h2 {
    position: relative;
    color: #fff;
    font-weight: 500;
    margin-bottom: 15px;
    text-shadow: 2px -2px 4px rgba(223, 99, 99, 0.344);
}

footer .foot h2:before {
    content: '';
    position: absolute;
    bottom: -5px;
    left: 0;
    width: 50px;
    height: 2px;
    background: #f00;
}

footer p {
    color: #999;
}

.lis {
    margin-top: 20px;
    display: flex;
}

.lis li {
    list-style: none;
}

.lis li a {
    display: inline-block;
    width: 40px;
}

```

El css del footer también está dividido con flex, dividiendo cada columna con el mismo espacio entre ellas y dándole a los h2 un subrayado rojo al ponernos encima de ellos.



Plan de empresa



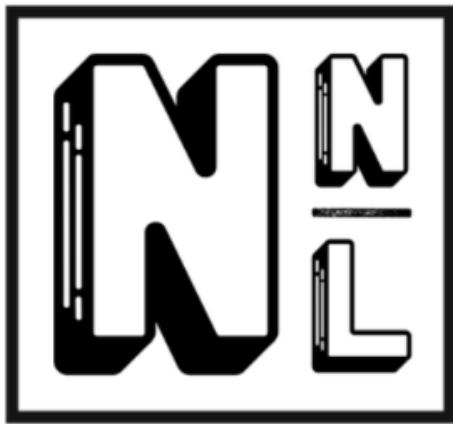
New Normal Life

Domótica

Proyecto directivo



Elección y creación de marca corporativa



A la hora de decidir que logo crear para NNL decidimos continuar con el ejemplo que ellos nos dieron pero modificando algunas cosas y dándole color.

Queríamos un diseño minimalista, y que no distara mucho del logo que nos dió la empresa, así que escogimos mantener su forma original, usando el blanco y el negro como tonos principales, que inspiran seriedad y profesionalidad y le pusimos un relleno y contorno azules (html:#012674) ya que es un color que inspira al progreso y la tecnología.



Decidimos ponerle las palabras que conforman la empresa para no crear un logo rígido y estático para darle un poco más de "movimiento" .

Elección sistemas informáticos



Este es el sce de NNL , el cual está estructurado de esta forma:

En la parte superior izquierda encontramos la sala de servidores , la cual está algo aislada para que no haya problemas con los servidores y el router principal además se encuentra toda la zona de cables principal, ya que tenemos 8 redes de las cuales 7 son cableadas y todas empiezan en la sala de servidores.

- Red general
- Red Hardware
- Red de servidores
- Red Software
- Red administración
- Red tienda
- Red cámaras
- Red Wi-fi

La sala a su derecha es el baño, donde nuestros empleados pueden ir a hacer sus servicios.

Justo después y ya en medio de la tienda en el apartado superior se encuentra la sala de hardware, donde nuestros trabajadores se dedican a tiempo completo a fabricar el hardware de domótica.

Debajo de la misma se encuentra la de software para poder comunicarse con la de hardware con facilidad y a su vez con el jefe ya que se encuentra a su izquierda, estos trabajadores se dedican a configurar el software de todo el hardware.

A su izquierda como hemos explicado antes se encuentra el jefe el cual está situado en una posición específica para controlar y hablar con los trabajadores, para facilitar la comunicación y ver que tal trabajan los trabajadores.

Debajo se sitúa la sala de administración para poder administrar de forma rápida todo lo que suceda ya que está al lado del jefe y todo lo que se necesite se le comunicará de forma rápida y eficaz .

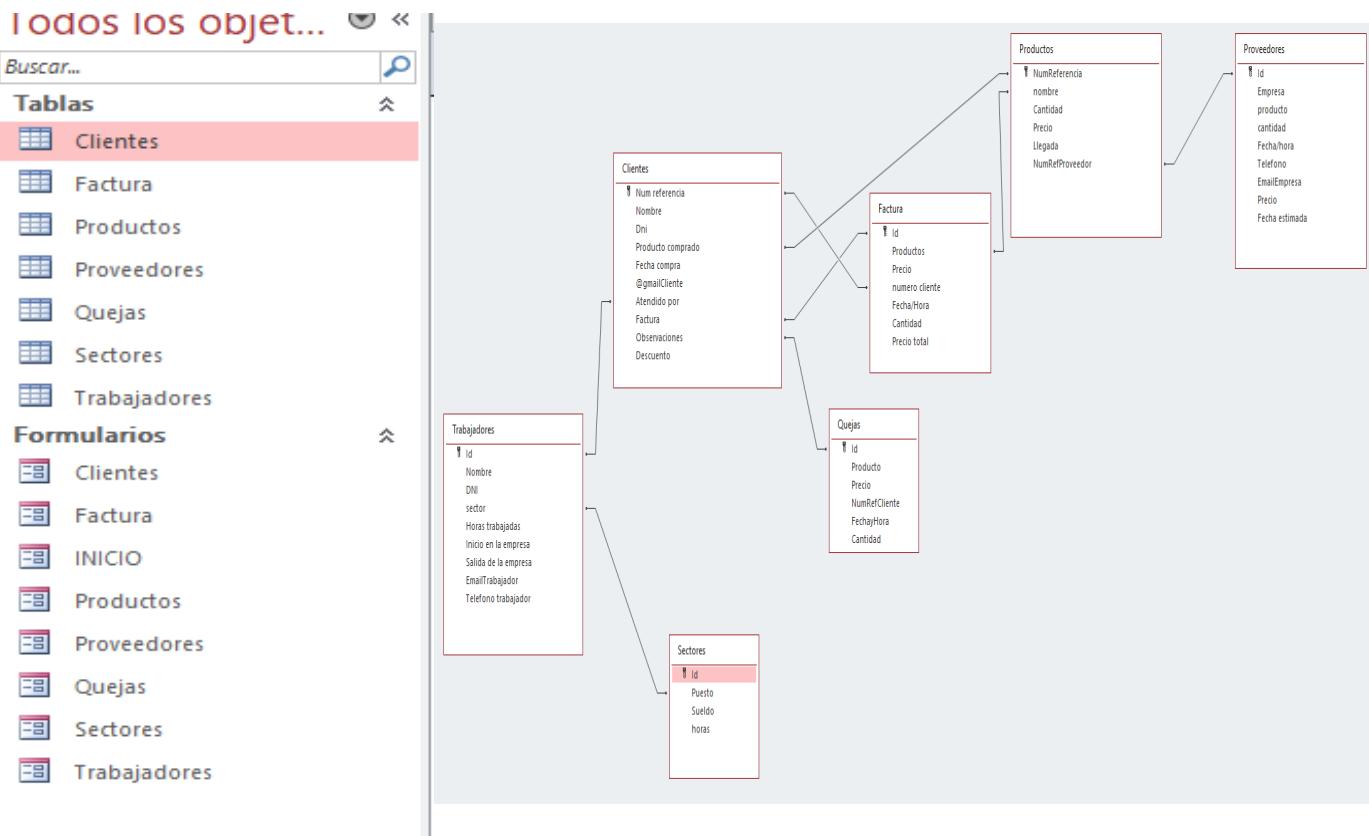
A la derecha encontramos la sala de reuniones y de descanso, está situada en la misma ya que el mobiliario para esta sala es específico para que un grupo de gente esté reunida además es un mobiliario que permite descansar a su vez.

Debajo tendríamos la sala de testeo/almacén para probar y guardar todos los productos que elaboremos además tenemos conexión directa con la tienda para poder llevar productos cuando falten.

A la derecha de todo esto se encuentra la tienda, que ocupa prácticamente el mismo espacio que todas las salas previamente nombradas, ya que es una tienda estilo apple, donde los clientes pueden ir andando y probando los productos, además en la parte inferior encontramos la mesa donde se realiza los cursos específicos para los clientes que lo deseen.

Maquetación y estructuración de la base de datos Access

Para la creación de esta base de datos hicimos lo siguiente, creamos 7 tablas con 8 formularios, las tablas para añadir la información a la base de datos y así poder crear relaciones entre sí y los formularios para que tenga una mejor lectura y en un futuro que se pueda añadir desde ahí directamente y sea más sencillo.



Las relaciones están pensadas para que de una forma u otra haya una relación siempre desde el cliente ya que así si ocurre alguna cosa todo nos llegue al cliente y lo podamos solucionar con rapidez y seguridad.

Inicio de la base de datos



En el inicio de la base de datos podemos ver el logo de nuestra empresa seguido de los botones que te llevan a cada apartado de la misma, desde los clientes hasta los trabajadores, a parte tenemos un botón para cerrar completamente la base de datos y otra para pasar páginas.

Si le das al botón de clientes te aparecerá esto

A screenshot of a client data entry form titled "Clientes". The form contains the following fields and their values:

Numero Referencia	3
Nombre	Susana
Dni	75489854V
Producto comprado	Plan de seguridad
Fecha compra	08/02/2021
Correo Cliente	sus@gmail.com
Atendido por	Eduard Castello
Factura	3
Observaciones	A2
Descuento	Ninguno

At the bottom of the form are three blue navigation buttons: a left arrow, a right arrow, and a red X.

Te aparecerán estos apartados:

- Número de referencia del cliente
- Nombre del cliente
- Dni del cliente
- Producto comprado
- Fecha en la que se hizo la compra
- Correo del cliente
- El trabajador que atendió al cliente
- El número de factura
- Las observaciones
- Descuento

Todo esto es lo que muestra el apartado de clientes con su correspondiente respuesta al apartado.

También tendrás los botones para ir hacia delante y hacia atrás con los otros botones de salir del access y salir del apartado de clientes

El siguiente apartado es el de la factura del cliente:

The screenshot shows a Microsoft Access form titled "Factura". The form contains the following data:

Id	3
Productos	Plan de seguridad
Precio	1.100,00 €
numero cliente	3
Fecha/Hora	08/02/2021
Cantidad	1
Precio total	1.100,00 €

Below the table are four buttons: a left arrow, a right arrow, a plus sign, and a minus sign.

En el apartado de Factura tendrás

- La id
- Los productos comprados
- El precio del producto
- El número del cliente
- Fecha/Hora
- La cantidad comprada
- El precio total

Con sus correspondientes botones como todos los apartados

El siguiente apartado es el de Productos

Productos

Numero Referencia	3
Nombre	Plan de seguridad
Cantidad	15
Precio	1.100,00 €
Llegada	20/12/2020
Numero Referencia Proveedor	3

Este formulario tiene

- Número de referencia
- Nombre del producto
- Cantidad del producto para vender
- Precio del producto

- El dia que llego el ultimo pedido del producto
- Número de referencia de Proveedores

A parte tenemos un apartado para escribir las características principales de los productos y su fecha de expiración o de venta.

También tiene los botones de cada formulario los de ir para delante y atrás más los de salida

El siguiente formulario es el de Proveedores

	NumReferencia	nombre	Cantidad	Precio	Llegada
*	1	Camara	90	83,84 €	20/11/2020
*	(Nuevo)		0	0,00 €	

Este formulario nos ofrece

- La id
- La empresa proveedora
- EL producto
- Cantidad

- Fecha/Hora
- Teléfono
- Correo Empresa
- Precio
- Fecha estimada

A parte ofrece la posibilidad de que veas todo lo que los proveedores nos han traído ya.

El siguiente es el de Quejas

Id	1
Producto	camara
Precio	83,84 €
Numero Referencia Cliente	1
Fecha y Hora	08/12/2020
Cantidad	3

- Id
- Producto
- Precio
- Numero de referencia del cliente
- Fecha/Hora
- Cantidad

Deabajo de todo esto tenemos un espacio para que el cliente escriba la queja y diga todo lo que le ocurre con el producto o el trabajador.

También tenemos los botones para ir pasando las quejas por si tenemos que atender varias quejas a la vez o las queremos archivar.

Seguimos manteniendo ambos botones de salida.

A Continuación veremos el de Sectores

Id	2
Puesto	Reparación productos
Sueldo	1.250,00 €
Horas	125

Below the form are four buttons: a left arrow, a right arrow, a magnifying glass icon, and a red X icon.

- Id
- Puesto
- Sueldo
- Horas

todo esto nos ayuda a saber cuánto cobran los diferentes sectores de la empresa y cuantas horas hacen al mes.

A parte tenemos los botones que nos permiten cambiar de página para ver todos los sectores y acordarnos de cosas que a lo mejor necesitamos.

Continuamos manteniendo los botones de salida.

Por último tenemos el de trabajadores:

Trabajadores

Id	4
Nombre	Fernando Roure
DNI	24897596F
sector	
Horas trabajadas	0
Inicio en la empresa	23/11/2020
Salida de la empresa	18/12/2020
Correo Trabajador	fernandoroure@gmail.com
Teléfono Trabajador	635168759

◀ ▶ ⏪ ⏹

- Id
- Nombre del trabajador
- Dni
- Sector
- Horas trabajadas
- Inicio en la empresa
- Salida de la misma
- Correo electronico del trabajador
- Teléfono del trabajador

A parte tenemos un pequeño apartado para apuntar cosas concretas de cada empleado.

Tenemos los botones para cambiar de trabajador y para salir del acceso y el formulario

Aplicación teórica de la seguridad de la empresa

Osix ha diseñado un plan de seguridad para la correcta funcionalidad de la empresa de New Normal Life, hemos tenido en cuenta tanto la identificación de los empleados, los accesos de seguridad físicos y lógicos de cada uno de los empleados según su nivel de importancia en la empresa, diferenciando entre los empleados que no necesitan mucha información relevante, hasta el director de la propia empresa que tendrá acceso a todos los datos de la misma.

Desde Osix, indicamos los pasos a seguir para tener un buen registro de acceso, eficaz y seguro controlando las contraseñas de los empleados, y el acceso a la base de datos y la monitorización de la misma, también indicamos a NNL como realizar las copias de seguridad y cuando hacerlo, recomendando también un sistema de redundancia para no obtener ningún tipo de pérdida de datos.

En estos apartados también tenemos en cuenta que almacenamiento es el idóneo para los servidores de NNL , cuanto espacio mínimo se requiere y que discos de almacenaje son los más recomendables.

En el apartado de la seguridad física de las propias tiendas de NNL tenemos creadas tres propuestas dependiendo del presupuesto que se quiera desear a la propia seguridad.

Hemos diseñado las políticas de seguridad, los planes de contingencia y la protección de datos, tanto de los empleados como de los empresarios y de los propios técnicos que colaboren con New Normal LIfe.

Identificación

Tarjeta de identificación



Formato de identificación de empresas	
INFORMACIÓN DEL TRABAJADOR:	
Nombre y Apellidos:	
Código:	Puesto:

Control de acceso

Se tendrá en cuenta un riguroso plan de control de acceso, el cual funcionará de manera escalonada, cuanto más peso tienen en la empresa más acceso tienen a esta misma.

Lo único que no seguirá esta norma es el acceso a empleados que requieran un acceso especial para realizar su trabajo o requiera de ello por una orden o necesidad. (se le otorgará la tarjeta necesaria durante un periodo de tiempo)

Todo esto con unas cerraduras electrónicas y unas tarjetas para abrir las puertas y controlar el acceso de la empresa.

Registro de acceso

El registro de acceso se basará en un riguroso documento el cual se basará en:

Nombre: Eduarda

Apellidos: Castellana Lana

DNI: 48297815A

Puesto de trabajo: “”

Dia de inicio: 12/02/2021

Dia de hoy: 12/02/2021

Número de trabajador: “1”

Acceso a datos

El acceso a datos funcionaría de forma similar que el control de acceso, ya que se tendrá muy en cuenta quién tiene acceso a según qué datos, y se seguirá una jerarquía de importancia empresarial para la obtención de datos de la empresa.

De todas formas también se requerirá de una supervisión mensual de los datos que hayan sido supervisados y sobretodo por quien.

Esto se logra gracias a controles de acceso en todos los informes y diferentes niveles de seguridad en estos mismos.

Como clave final también se deberá avisar a su supervisor antes de acceder a esos datos, sobretodo si tienes permisos limitados.

En cada puesto donde se sitúa un ordenador abra una cámara insertada en la zona la cual se asegure de registrar quien entra en ese ordenador y a que hora

Copias de seguridad e imágenes del sistema

En este tema de las copias de seguridad e imágenes del sistema podríamos tener a una empresa subcontratada para hacer el mantenimiento de los ordenadores y también para hacer las copias de seguridad , o sino con los servidores podríamos crear una base de datos para ir haciendo las copias de seguridad en la nube.

Sistema de redundancia

Este respaldo es básicamente para la red que utiliza tu proveedor de Web Hosting para mantener tu información en línea. Las compañías fiables tienen más de un operador de internet para el funcionamiento de sus servidores de modo de garantizar que tu sitio web nunca estará abajo por la interrupción de un enlace de red.

Mantener esto significa tener una inversión para mantener los servidores y tener varias líneas de internet para no tener nunca una caída de los servidores.

También hay una parte de la redundancia que se refiere a las piezas físicas de hardware del servidor. Por ejemplo, una capa de redundancia es para los discos duros. La idea es, si llegara a fallar un disco duro en un servidor, este se mantenga en funcionamiento y tu sitio no deje de estar en línea, a través de arreglos RAID en el servidor, se cuenta con repuestos de emergencia que permiten la continuidad de funcionamiento.

En esta parte anteriormente explicada hace falta hacer una inversión de manera previa antes de crear nada en la parte de hardware para no tener componentes que hagan que el servidor se pueda caer o que al llevar 40h encendido haga que se rompa o cualquier otra cosa , ya que esto haría que a la empresa le crearía pérdidas de dinero importantes y esto no le tendría que interesar.

A el sistema de redundancia le tendríamos que dedicar unos 300€/mes o tener algún trabajador especializado en realizar estas tareas.

Discos duros

Este es un apartado importante para la empresa ya que será donde se almacenará toda la información de la empresa.

Primeramente tendremos el guardado en la nube de toda la información que manejan nuestros trabajadores también para tenerlo todo protegido , pero también tendríamos una red local de almacenamiento en local con centros de almacenamiento como el siguiente de 20 TB cada uno, aumentables a 24 y/o 28 si en algún momento se necesitará.

https://shop.westerndigital.com/es-es/products/external-drives/wd-my-book-duo-usb-3-1-hdd?utm_medium=pdsh2&utm_source=gads&utm_campaign=WD-EU-ES-PLA&utm_content=895040615489&utm_term=WDBFBE0200JBK-EESN#WDBFBE0200JBK-EESN

En total para almacenar toda la información en local y tener una copia física de los documentos y tenerlos controlados hemos calculado que podría ascender a unos 3.360€. incluyendo únicamente el guardado en local , el guardado en la nube tendría otro precio juntamente con el presupuesto de seguridad y el precio de los servidores y su montaje y mantenimiento.

Personal y seguridad

Como personal de seguridad y la propia seguridad de la empresa, New Normal Life contará con tres distintas catalogaciones para tener mayor efectividad y seguridad.

Tendremos planteadas 3 diferentes políticas y planes para poder ocupar todos los sectores referentes NNL y sus empresas importadoras y exportadoras, tendremos además la facilidad de contentar a nuestros clientes con unas políticas firmes, claras, fáciles y seguras, que les podremos demostrar en todo momento.

Estos documentos serán divididos y catalogados por puntos para la clara interpretación y la facil sustitucion y reparacion de los diferentes fallos que puedan surgir.

En este documento también se tiene en cuenta la seguridad del propio establecimiento de compra, de los clientes dentro de la misma y de los

productos a la venta, dando diversas opciones para la vigilancia y seguridad del local de ventas.

Personal de seguridad

El personal de seguridad será el encargado de garantizar la seguridad de todo lo referido a las sucursales de venta que tenga New Normal Life, por lo tanto deberán tener la suficiente habilidad como para

- Identificar posibles amenazas en horas de apertura
- Ser capaz de prever clientes que tengan como objetivo el posible hurto
- Poder expulsar a los clientes conflictivos de la tienda, sin causar muchos revuelos.
- Poder tener la capacidad de solucionar conflictos sin que suponga un peligro para todas las personas
- Poder controlar un número elevado de clientes sin que ninguno suponga un problema
- Acudir rápida y efectivamente a cualquier disputa

En este punto se ha decidido proponer varios presupuestos más o menos económicos, dependiendo de las seguridad que desee, estas propuestas están detalladas en el documento excel llamado “Presupuesto de personal”.

Plan de personal de seguridad extremo

Pablo García, 39 años, ex-policía retirado con 13 años de experiencia, capaz de realizar todas las habilidades pertinentes en este sector.

Sergio Pérez, 26 años, personal de seguridad privado con 4 años de experiencia, capaz de realizar todas las habilidades pertinentes en este sector.

Marc Ramón, 46 años, ex-militar retirado con 8 años de experiencia, ex-personal de seguridad durante 3 años, capaz de realizar todas las habilidades pertinentes en este sector.

Julian Sans, 23 años, guardaespaldas desde hace 4 años, capaz de realizar todas las habilidades pertinentes en este sector.

Plan de personal de seguridad intermedio

Will Sanchez, 28 años, Guardaespalda privado con 2 años de experiencia, capaz de realizar varias habilidades pertinentes en este sector.

Petrov Kirat, 31 años, ex-militante de la Unión Soviética, capaz de realizar todas las habilidades pertinentes en este sector pero no entiende muy bien el español.

Plan de personal de seguridad bajo

Eduarda Castellana, 20 años, tiene el bachillerato de artes y quiere un trabajo en el que ganar dinero fácil, puede realizar algunas habilidades de las que se requieren.

Política de seguridad

Como seguridad establecida en la empresa, hemos formalizado un extenso documento detallando cada apartado y acción a seguir para tener una seguridad eficiente para la compañía, incluida la empresa, los empleados, los proveedores e incluso los clientes.

se detallan las acciones, las medidas necesarias y los documentos que son necesarios.

Los objetos estarán adjuntos en la carpeta “presupuesto política de seguridad” con varios archivos pdf para tener en cuenta el precio de cada implementación y el total de los mismos.

En este apartado de personal y seguridad solamente se presentará un documento final y no varios tipos de presupuestos, ya que pensamos que es muy necesario tener la seguridad mínima en políticas de seguridad, y eso será lo que ofreceremos.

El documento general de las políticas necesarias está formalizado en el archivo “políticas de seguridad” adjuntado también a estos documentos.

Plan de contingencia

Para poder realizar el plan de contingencia correctamente, primero deberemos saber qué recursos tiene NNL y organizarlos según la prioridad que deseemos.

Para ese documento se tendrá en cuenta que el recurso principal y más prioritario de NNL, son las opiniones y los datos de los clientes y proveedores.

Se deberán identificar los riesgos clave de la empresa, para ello los empleados son una parte fundamental, es necesario que sean conscientes de los riesgos que corren al realizar cada acción y como arremeter contra los problemas para solucionarlos eficazmente. Estos riesgos también deben de ser organizados según su prioridad.

El plan de contingencia empieza catalogando los recursos de NNL según su prioridad:

- Datos de NNL
- Datos de los clientes y proveedores
- Datos del personal contratado
- Datos de los productos de NNL
- Personal contratado
- Clientes



- Hardware de la sucursal de NNL

Seguidamente tendremos una lista de los riesgos organizados según su prioridad:

- Robo de información confidencial de NNL
- Robo de información privada de NNL
- Robo de información de clientes y empleados
- Agresiones físicas de clientes a empleados o de empleados a clientes
- Agresiones a la tienda física de NNL
- Rotura de material de hardware propiedad de NNL

Una vez obtenido los puntos clave de los recursos y riesgos de NNL, las contingencias a seguir para cada problema están detallados a continuación:

Una vez la empresa ha recibido un ataque de robo de información de cualquier tipo, se procederá a verificar y diagnosticar cuando y como a podido suceder ese error, una vez hecho el diagnóstico, se procederá a establecer los parques necesarios para no ir perdiendo más datos, establecido el parche, detectaremos al culpable del robo y se procederá de la forma mas beneficiante para NNL, ya sea contactando con las autoridades y denunciando o hablando directamente con el culpable y después de ello, probaremos y mejoramos el parche establecido para asegurarnos de que no volviera a pasar.

Conforme el punto de contingencia para las agresiones físicas, la única opción racional a seguir, sería:

- Si un empleado es agredido se procede a sacar al agresor fuera de la tienda gracias a la seguridad de NNL y llamar a las autoridades para denunciar la agresión. Exactamente, se seguirá el mismo proceso si un cliente rompe intencionadamente algún producto de la tienda.
- Si un empleado agrede a un cliente, se procederá al despido del mismo, también se le darán las facilidades que el cliente necesite si este desea denunciar al empleado.

Protección de datos

La protección de datos de NNL contendrá un sistema de cifrado para cada uno de los envíos de información, ya sea entre empleados en la empresa o modificaciones en las bases de datos o servidores, todos los dispositivos empresariales contará con el sistema de cifrado WPA2 para maximizar la protección de absolutamente todos los datos.

Contaremos también con un sistema de seguridad con nuestros proveedores, teniendo así documentos con nuestros requerimientos según la seguridad que queramos establecer con los proveedores, a parte de varios contratos de confidencialidad para asegurar que nuestros datos no son difundidos.

Respecto a un tema de ciberseguridad, nuestros expertos configuraron una red segura con varios firewalls y niveles de seguridad para evitar ciberataques y robos de datos.

Para evitar los robos de información todos los empleados recibirán un curso sobre la seguridad que deben tener al trabajar con NNL, al no cumplir las normas enseñadas se podría proceder al despido inmediato del trabajador.

Copias de seguridad e imágenes del sistema

CPD y DRS

Proporcionamos un CPD, también denominado como Centro de Procesamiento de Datos, que es un espacio donde se concentran los recursos necesarios para el procesamiento de la información de una organización, para asegurar la continuación de sus funcionalidades y un DRS o plan de contingencia que es un instrumento de gestión para el manejo de las TIC, contiene las medidas técnicas humanas y organizativas necesarias para una organización, elaborado por nuestra empresa, para garantizar la máxima seguridad de la información.

Seguridad física

La seguridad física es un conjunto de mecanismos concebidos para detectar amenazas físicas al hardware. Nuestra empresa aporta uso de cámaras de videovigilancia, sistemas SAI para evitar que un apagón impida la realización de las funciones de la empresa, contratación de una segunda empresa conexión para garantizar absoluta disponibilidad de la red y de los equipos, subcontratación de una empresa de seguridad privada para la vigilancia del uso de los equipos y espacio de trabajo. Además ventanas de espejo de seguridad laminado, para evitar que la gente pueda espiar desde el exterior.

Seguridad lógica

La seguridad lógica la conforman todas aquellas barreras que evitan, virus, programas no testeados y accesos no autorizados entre otros, Osix aportaría cámaras de videovigilancia para comprobar que haya un correcto uso de los equipos, antivirus con eficacia testada y asegurada por nuestra empresa, un documento de concienciación para la seguridad de la empresa.

Seguridad en las redes

La seguridad en las redes consiste en las políticas y prácticas adoptadas para prevenir y supervisar el acceso no autorizado, el uso indebido, la modificación o la denegación de una red informática y sus recursos accesibles. Para ello el uso de programario de control de paquetes de red para evitar conexiones a sitios no deseados en la empresa, uso de vpn local para garantizar máxima velocidad en comunicaciones internas de la empresa.

Seguridad en la red

Osix ha realizado un esquema de todo lo necesario en torno a la seguridad, que New Normal Life debe seguir para ser una empresa segura y eficaz, este contiene



toda la información necesaria tanto para la ciberseguridad de la empresa como para la de sus empleados, distribuidores y clientes, de esta forma, podremos ver qué directrices va a seguir la empresa para hacer posible la mejor seguridad actual, disponiendo de un itinerario donde vamos a ver los pasos que seguirá nuestra empresa, continuando con las descripciones de los trípticos y demás informaciones y finalmente detallando los protocolos que seguirá NNL, detallados y con la información concisa para que todo empleado o cliente pueda entender porque es segura nuestra empresa y que hacemos dia a dia para que lo siga siendo.

Itinerario New Normal Life

En nuestro itinerario lo principal que tenemos en cuenta es la seguridad de los datos que manejamos, ya que nuestra empresa controla datos tanto personales como bancarios y/o influyentes para a nuestros clientes, tal es así que una pérdida ínfima de estos podría causar el cierre de nuestra empresa.

Una vez esta idea está clara empezamos a explicar los puntos de dicho itinerario y todo aquello que seguimos para llegar a lo recién explicado.

Riesgos del sector:

- Pérdida de datos personales y bancarios
- Fraude online
- Sistemas desactualizados y vulnerables
- Cese de actividad
- Sanción por incumplimiento legal

Estos 5 apartados son los riesgos de nuestra empresa todos ellos supondría una misma cosa pérdidas para nuestra empresa y de un modo u otro un peligro para la continuidad de la misma.

La mayoría de estos riesgos se basan en los datos y la usurpación de estos, por eso explicamos su importancia previamente por que en un sistema como el nuestro es lo que más se valora, ya que, si robas una cuenta bancaria que estaría situada en el primer punto también se verían involucrados el punto 2, 4 y 5 podría ser el 3 también, pero nos tendríamos que cerciorarse por que el fallo de seguridad

podría deberse a sistema desactualizado o no simplemente que un ciberdelincuente haya sobrepasado el sistema.

Los enemigos de la empresa

Muchas veces los enemigos de nuestra empresa son de esta misma, sean directos o no muchas veces los propios empleados causan estragos en la empresa, ya sea tocando algo que no deben y eliminando datos existenciales de la misma o ex empleados que aún conserven acceso a la empresa y maliciosamente extraigan información de esta para venderla y perjudicar a la empresa.

Por otra parte, también es evidente que hay ciberdelincuentes que buscan robar a la empresa para su beneficio propio y hay que tenerlos en cuenta.

Otro apartado sería nuestra propia seguridad nos podría dar una falsa seguridad ya sea por fallos del sistema o por su falta de configuración.

Por otra parte, podría haber intervenido un virus y facilitar así la entrada de un ciberdelincuente.

Como otro enemigo clave encontramos a la competencia del sector en el que trabajamos, que para facilitar su propio crecimiento hunde otras empresas de sus alrededores.

Plan Director de Seguridad

Debemos analizar con claridad nuestra empresa y llevar a cabo un determinado análisis de seguridad para determinar qué nivel de seguridad queremos y necesitamos en nuestra empresa.

Deberemos también definir los proyectos de la empresa para saber cómo estructuran el plan.

Hacer una clasificación y priorización de datos más valiosos y los cuales deben estar más o menos seguros. Lo pasamos a dirección para que sea aprobado y lo aplicamos para estructurar toda la información.

De todas formas, nunca se puede estar tranquilo antes estos ataques, pero todo esto es un ejemplo de mejora continua así que avanzaremos progresivamente y podremos estar algo más aliviados.

Puesto de trabajo

Hay que cuidar siempre nuestro puesto de trabajo, esto significa nada de contraseñas en post-its, papeles confidenciales bien guardados y si es bajo llave mejor, papeles confidenciales que ya no sean importantes destruirlos en la trituradora siempre ya que esa información sigue siendo confidencial.

Todo esto es muy importante ya que un pequeño fallo en nuestro puesto de trabajo supondría una falla grande de seguridad en nuestra empresa.

Fuera de la oficina

Fuera de la oficina tampoco debemos bajar la guardia, ya que nos rodea mucha gente y nunca podemos saber lo que esa gente piensa así que, si nos descuidamos de nuestro ordenador o tenemos una conversación confidencial podría haber gente husmeando la cual podría intervenir en la seguridad de la empresa, así que nunca bajéis la guarda ya que podría suponer un error muy grande.

Emails sospechosos

Al trabajar con correos es fácil recibir correos engañosos los cuales se utilizan para el robo de contraseñas para poder acceder dentro de la empresa.

Para esto existen diferentes modos uno por ejemplo es el phishing que en lo que se basa es en hacerse pasar por otra persona para realizar un engaño y así conseguir información valiosa.

Otra herramienta sería el spam el cual es un cúmulo de correos no deseados que la mayoría de veces se basan en publicidad no solicitada, pero un pequeño porcentaje es publicidad engañosa la cual solicita nuestra atención para engañarnos y recaudar dinero.

Por ello es muy importante saber distinguir los correos y aprender a desechar los correos como estos. Por último, pero no menos importante encontramos los correos con archivos adjuntos, estos pueden contener malware que puede afectar seriamente a tu ordenador haciéndole perder información valiosa y haciendo gastar un dinero a la empresa para solucionar este virus.

Estos correos suelen ser fáciles de detectar y se suelen asociar al spam así que como dijimos hay que saberlos distinguir bien, por lo tanto, no te descargues nunca un archivo sin antes cerciorarte bien de que es seguro.

Cultura de seguridad

Como vengo explicando la ciberseguridad lo es todo en nuestra empresa, así que culturizarse en seguridad nunca está de más, por lo tanto, hay que tomar conciencia de que la información que almacena la empresa es esencial protegerla.

Además, si seguimos todos los pasos bien y si encontramos problemas los reportamos debidamente con el paso del tiempo crearemos una buena cultura de ciberseguridad.

Pero eso sí para crear una buena cultura de ciberseguridad tenemos que colaborar todos, no penséis que es cosa solo de informáticos, todos aquellos que estemos en la empresa debemos colaborar y aportar nuestro grano de arena.

Recursos Humanos

Para todos aquellos que entren en nuestra empresa les debemos garantizar la información necesaria para que se percaten de la ciberseguridad sea cual sea su sector de trabajo ya que todos importamos por igual cuando hablamos de la ciberseguridad.

Después de esto les debemos asignar los permisos suficientes para la buena realización del trabajo. Pero solo para eso otra información de rango superior no se le otorgara.

También contamos con el proceso de contratación que suele ser el mejor para dotar de conocimientos de ciberseguridad y saber el nivel de recepción que tiene nuestro futuro empleado para ello.

También debemos garantizar una seriedad y firmeza ante esto, ya que es muy importante la sensación que le otorgamos al nuevo empleado para que vea el nivel de importancia de las cosas.

Por último, pero no menos importante es necesario firmar un acuerdo de confidencialidad para que todo lo que le enseñemos no sea filtrado.

En caso de la finalización de un empleado debemos controlar la información que puede llegar a filtrar o en casos extremos la difamación que podría hacer de nuestra empresa.

Para ello debemos despojarle de todos sus accesos a nuestra empresa.

Aunque dudamos que nuestros empleados puedan hacer tales cosas ya que se les instruirá en base del compañerismo. Por lo tanto, serán bien tratados.

Información y su destino

Todo personal nuevo que no sepa dónde ni cómo nos organizamos merece una explicación así que les comunicaremos nuestro PDS para que sepa cómo funcionamos donde almacenamos nuestra información y la gran seguridad que

tiene que tener con todos nuestros datos, ya que le debemos transmitir nuestra preocupación por la seguridad.

Con ello le explicaremos a qué información puede acceder y a cuál no ya que dependiendo de su rango de trabajo tendrá una u otra información así también comprenda mejor la importancia de todo esto.

Subcontratación TIC

Dejando a un lado a que compañía subcontratamos tenemos que tener en cuenta que programas y que equipos se nos da, ya que pueden ser correctos o no.

Además, debemos cerciorarnos que nuestra información está siendo almacenada y administrada de la mejor manera posible ya que a parte de la seguridad que tengamos nosotros en nuestra propia empresa debemos intentar controlar que la información que por subcontratación se protege esté bien protegida y segura.

Todo esto debe estar en el contrato de subcontratación para que esté correcto.

Gracias a esto debemos analizar con certeza todo lo que nos ofrecen y realizar un contrato con demandas por fallas y firmar acuerdos de confidencialidad.

Confianza en subcontrataciones TIC

Al fin y al cabo, lo más importante es la confianza que te transmiten ya que si no te transmiten confianza a ti los ciberdelincuentes no tendrán miedo de asaltar tu compañía porque ellos notarán que esa compañía no transmite seguridad y aunque sea más segura tendrán más intentos de asaltos simplemente por ese sentimiento.

Ya que si tú no te sientes seguro es por algo, aparte puedes llegar a acuerdos con la misma compañía y modificar cosas del contrato para sentirte mejor.

Incluso una mejora de productos o un incremento de programas de seguridad.

Nuestra web

¿Nuestra propia web transmite la confianza tan anhelada por nosotros mismos?

Si no es así no esperemos que nadie confié en nosotros ya que si nosotros no confiamos en compañías que no demuestren su seguridad no podemos pretender que los demás lo hagan con nosotros, así que una cosa primordial es transmitir esa confianza que sabemos que tenemos, con una buena página web y comunicando en esta misma toda la seguridad que garantizamos y tenemos para otorgar.

Super contraseñas

Uno de los factores clave para la protección de datos es nuestras contraseñas y qué mejor que aplicar super contraseñas, contraseñas que sean super seguras, así podremos evitar muchos problemas de seguridad en un futuro y nivelar el nivel de seguridad de nuestros datos, aunque lo que también se puede hacer y es incluso mejor es utilizar siempre super contraseñas para que sea incluso más difícil acceder a cualquier dato de nuestra empresa eso sí tendríamos que tener una gran precaución con todos aquellos que obtengan estas super contraseñas ya que podrías dejar de ser super contraseñas.

Trabajo desde el móvil

Si emprendemos nuestro trabajo desde nuestro móvil debemos saber que es lo mismo que un ordenador, debemos estar atentos, ante todo.

Ya que cualquier cosa que instalemos puede ser dañina para el móvil o pedir demasiados permisos para el móvil para así robarnos información, trabajes por donde trabajes nunca debes descuidar tu información confidencial ya que te puede afectar directamente o incluso a la empresa presta atención a los mensajes y a las instalaciones.

Los datos y la ley

Todos debemos saber que nuestros datos están amparados por la ley, así que si recibimos correos los cuales no queremos o publicidad engañosa siempre podremos denunciar al remitente de dicho correo ya que la LOPD ampara nuestra privacidad y los datos que le acompañan por eso es muy importante estar informado de nuestros derechos ante estos mensajes, además si aún y habiendo solicitado la denegación de dichos mensajes.

Pérdida de archivos

Cuando se pierde un archivo se puede intentar recuperar ya que hay aplicaciones para ello, pero hay una falla de seguridad porque hay un archivo que puede interferir en el bienestar de la empresa, ya que puede utilizarse para dañar a la empresa o vender su información.

De todas formas, puedes tener una empresa contratada de soporte informático para facilitar todos estos problemas.

Así puedes tener mayor seguridad y solucionar los problemas de manera más eficiente y segura, así también transmitiremos mayor seguridad.

Aplicaciones Seguras

Para la utilización de aplicaciones seguras siempre nos podemos cerciorar de su seguridad buscando información o contratando a profesionales del tema para que no guíen para la utilización de diferentes aplicaciones, ya que cada aplicación es un mundo, el cual tiene sus pros y sus contras ya que la mayoría de aplicaciones gratuitas suelen cobrarte con tu información y eso es lo primero que no queremos así que más vale contratar aplicaciones aunque nos cueste dinero antes que dejar nuestros datos en manos ajenas.

Las redes sociales

Las redes sociales son un arma de doble filo, ya que son muy útiles para expandirse y darse a conocer, pero esto hace que sea más fácil la denigración de nuestra empresa y la malversación de la información que publicamos por nuestras redes, ya que vivimos en la época en la cual todo se puede manipular y malinterpretar.

Así que hay que tener mucha precaución porque puede ser muy buen instrumento para la expansión, pero si cometemos un error es el doble de importante que un error normal ya que es mucho más mediático e impactante ya que las redes sociales abren la puerta a convertirte en una empresa mundana sin serlo realmente así que es un adminículo muy útil, pero a la vez muy peligroso.

Hay que cerciorarse si es rentable tener o no, aunque cada vez más es difícil crecer sin redes en este mundo.

También hay que tener en cuenta en las redes sociales de los empleados ya que puedes dar información sin que ellos se den cuenta así que por ética y seguridad habría que poner normas sobre las redes sociales en nuestra empresa, pero eso ya dependerá de la utilización de ellas.

Engaños

Igual que con los correos es necesario cerciorarse con quien estamos hablando ya que pueden hacer suplantación de identidad para conseguir lo mismo de siempre por eso antes de decir nada confidencial asegúrate con quien hablas.

Porque no solo intentan robar información vía pc, sino que todos los métodos de comunicación son los que atacan así que infórmate y asegúrate.

Plan de contingencia

El plan de contingencia es siempre esencial para que toda empresa siga funcionando y es que sin él todo sería un desastre.

Cuando un error aparece debemos tener claro lo que seguir por eso el plan de contingencia siempre tiene que estar actualizado y a la mano de los trabajadores porque nunca se sabe cuándo puede fallar algo.

Para ello debemos conocer muy bien nuestra empresa y saber cómo actuar, ya tenemos cosas que nos pueden ayudar como el PDS que nos puede ayudar a identificar donde están las cosas y qué cosas son más importantes que otras para continuar su funcionamiento.

Información portátil

Tienes que saber que la información que almacenes en pendrives o discos duros es la más sensible ya que a no ser que pongas clave a dicho aparato si pierdes el aparato pierdes toda su información así que estamos hablando de una información muy sensible que nunca está de más hacer copias y suministrar lo mejor posible también es muy recomendable que crees una contraseña para acceder a dicho aparato.

Información en el aire

Toda la información que compartes vía internet está en el aire por ondas las cuales se pueden detectar y interferir así construyendo una red falsa para robar información muy útil, esto puede pasar conectándose en una wifi que no conoces o directamente en la tuya propia que no sea suficientemente segura así que estás atento a donde te conectas y de quien te fías.

Clasifica, Utiliza y Destruye

Una buena forma de no tener problemas es estar bien organizado, así que clasifica tu información, para saber lo más primordial y de qué ámbito es cada cosa.

Utiliza hasta que te sirva la información y una vez te deje de servir destrúyela para que no se filtre y así conseguirás una buena organización y seguridad.

Todos somos seguridad

Por último, conciénciate con todo lo que leíste en que la seguridad de la información es la clave de nuestra era.

Ya que todos nuestros actos en la empresa y fuera de ella pueden afectar directa o indirectamente a esta misma, así que todos somos la seguridad de todos y la de nosotros mismos.

Concienciación para fomentar los buenos hábitos de seguridad

Incidentes de seguridad

Es importante mantener la información a buen recaudo, puesto que la falta de disponibilidad, difusión o alteración de esta puede acarrear problemas con el desarrollo de la empresa.

Existen tres tipos de incidentes de seguridad que afectan a la información de nuestra empresa

- Accidentales: no intencionados. Borrar accidentalmente un archivo, averías, incendios, etc.
- Intencionados por insiders: Los insiders son empleados que en ocasiones deciden llevarse información de la empresa
- Causados por ciberdelincuentes: estos individuos utilizan malware que introducen aprovechando debilidades en nuestros sistemas

Los tres pilares de la seguridad

En cuanto a la seguridad de la información de nuestra empresa, es importante mantener tres propiedades básicas:

disponibilidad, integridad y confidencialidad, eso significa que la información debe estar lista para su uso en cualquier momento, debe estar limpia de fallos y errores y no debe revelarse a individuos o entidades no autorizadas.

Así mismo, es importante la protección de los datos personales, que son todos aquellos datos que contengan información concerniente a personas físicas identificadas o identificables, en otras palabras, debe estar protegida toda aquella información que pueda llevar a conocer a una persona.

Debe saberse que llevar a cabo una mala gestión de la información en una empresa que trata con información personal puede suponer graves consecuencias para una empresa así como con su continuidad, para evitarlo, deberemos identificar si se trata con datos especialmente protegidos o a gran escala, y en caso contrario justificarlo debidamente.

También debemos garantizar la absoluta confidencialidad, integridad y disponibilidad de los datos personales, garantizar los derechos y libertades a aquellas personas cuya información está bajo custodia de la empresa, para ello, deberán estar informadas de forma visible, accesible, sencilla y transparente, es decir, no se realizará ninguna gestión ni cambio con su información sin que ellos sean notificados, se debe obtener el consentimiento inequívoco para el uso de sus datos, permite que puedan ejercer sus derechos de acceso, rectificación, supresión, limitación, portabilidad, oposición y derecho a no ser objeto de decisiones individualizadas e informarles en caso de violaciones de seguridad, y por último permitir que las autoridades verifiquen que el trato de información se realiza correctamente.

Clasificación de la información

Se debe mantener siempre una correcta organización de la información, tanto en formato físico como digital, además es recomendable catalogar otras características como los departamentos que intervienen o ubicación por ejemplo.

Cada empresa debe tener una jerarquía de niveles en función de cuán importante es la confidencialidad de estos, como orientación podríamos tener los siguientes niveles

- *Confidencial:* La confidencialidad de esta información es de vital importancia para el futuro de la empresa.
- *Restringida:* Uso exclusivo para aquellos miembros de la empresa cuyo trabajo no pueda llevarse a cabo sin esa información.
- *De uso interno:* Uso exclusivo para el personal de la empresa
- *Pública:* Información que puede ser difundida sin ningún tipo de reparo(contenido publicitario).

Tratamiento de la información

Para proteger la información se llevarán a cabo una serie de controles de seguridad: acceso limitado, cifrado, copias de seguridad, y tratamientos específicos según lo dictado por ley y aquellos sujetos a acuerdos de confidencialidad.

En el cifrado debe escogerse una clave lo más robusta posible, junto con un algoritmo criptográfico fuerte(es preferible que sea de dominio público) deben realizarse comprobaciones periódicas para verificar que el algoritmo no es vulnerable, la pérdida de la clave de descifrado imposibilita el acceso a la información, que debe estar almacenada a buen recaudo, y la herramienta de cifrado debe estar siempre actualizada.

También hay que saber eliminar los metadatos antes de publicar o enviar cualquier archivo, ya que pueden contener información valiosa para los ciberdelincuentes.

Aunque la mayoría de aplicaciones ofimáticas contienen herramientas para este fin, a través de windows también podemos hacerlo.

Copias de seguridad

Otra tarea a llevar a cabo es realizar copias de seguridad de nuestra información, ya que de no hacerlo, podrían sufrirse graves consecuencias, para evitarlo, debemos volver a la clasificación de antes, en función de ella se identificarán y copiaran aquellos datos cruciales para que la empresa pueda seguir con su actividad diaria.

Es importante definir una adecuada frecuencia de la realización de estas copias, de manera que no suponga una gran pérdida, ni afecte negativamente en la actividad laboral.

Existen diferentes tipos de copias de seguridad:

El Raid 1 mediante el cual se crea una copia exacta en tiempo real con la que se evita guardar datos obsoletos, la principal desventaja es que si este sistema sufre un fallo, hackeo o modificación.

Tipos de copias de seguridad

- *Completa*: consiste en hacer una copia de todos los datos de nuestro sistema en otro soporte haciendo que la recuperación, en caso de incidente, sea mucho más rápida. Pero requiere de un mayor tiempo para realizar la copia y mayor coste económico.
- *Diferencial*: únicamente se copian los archivos y directorios que han sido creados o modificados desde la última copia completa. No es lo más óptimo en cuanto a tiempo y espacio utilizado, pero requiere menos tiempo que la completa y es un proceso más sencillo .
- *Incremental*: sólo se copian los datos que hayan variado desde la última copia, el espacio y el tiempo utilizados son menores, pero hace la recuperación de datos más compleja se utiliza el método 3-2-1 para llegar a la mayor seguridad posible de los datos:

3: mantener 3 copias de cualquier fichero importante,el archivo original y 2 copias de seguridad.

2: almacenar las copias en dos soportes distintos de almacenamiento para protegerlas ante distintos riesgos.

1: almacenar UNA copia de seguridad fuera de nuestra empresa, lo que también se conoce como backup offsite. Como la copia en la nube.

Borrado seguro de la información

Además se debe conseguir un borrado seguro de la información, es decir, destruirla de forma segura para que no vuelva a ser accesible, el primer paso es realizar un inventario de activos para que ninguno se pierda, después para eliminar la información, deberán triturarse todos los medios de almacenamiento no electrónicos, los dispositivos que permitan su reutilización, deberán ser sobreescritos múltiples veces, los teléfonos móviles, se cifran antes de ser borrados y se restaurarán a formato de fábrica, los soportes que no funcionen, deberán ser destruidos o desmagnetizados.

Correos fraudulentos

Para defendernos de los ataques por correos fraudulentos deberemos conocer los tipos que existen:

- Phishing: suplantación de una entidad fiable para hacerse con claves de acceso o información sensible.
- Scam: se basa en perpetrar engaños y estafas.
- Sextorsión: extorsionar al receptor con un supuesto video de contenido privado o comprometedor, que probablemente no exista, y amenazar con difundirlo.
- Malware: se trata de código malicioso oculto, que podría infectar dispositivos.

A menudo este tipo de correos muestran un patrón que les relaciona entre sí, suelen ser de remitente desconocido, que a pesar de que no lo sean, existen herramientas que pueden detectar el email spoofing (remitente y firma falsos) o la ausencia o cambio de firma.

El objetivo de estos correos es instar al usuario a que realice una determinada acción mediante el uso de ingeniería social en el cuerpo y asunto del mensaje. Las comunicaciones impersonales, documentos adjuntos, faltas de ortografía y mala redacción deben ser signos de alerta, así como el uso de enlaces, cuyo destino debe ser comprobado antes de abrir, para mayor facilidad la mayoría de clientes de correo cuentan con herramientas para ese fin.

Aun así, los ciberdelincuentes pueden no ser siempre el problema, los errores de los empleados como el uso de la función de autocompletado, que podría resultar en el envío de un correo a un destinatario erróneo o la descarga automática de archivos pueden suponer un problema.

Contraseñas

Algo que sabes: contraseñas, preguntas personales, etc.

Algo que eres: huellas digitales, iris o retina, voz, etc.

Algo que tienes: tokens criptográficos, tarjeta de coordenadas, etc.

Longitud mínima de 8 caracteres, ya que cuanto más larga sea esta, más tiempo se tardará en descubrirla.

Utilizar combinaciones de letras mayúsculas, minúsculas, números y símbolos.

Una forma de conseguir contraseñas robustas es utilizar reglas mnemotécnicas aplicadas a una frase:

- Seleccionamos una frase: «en un lugar de la mancha»;
- Hacemos uso de mayúsculas: «En un lugar de la Mancha»;
- Incluimos el servicio: «En un lugar de la Mancha Correo»;
- Añadimos números: «En un lugar de la Mancha Correo de 2019»;
- Añadimos caracteres especiales: «En un lugar de la Mancha Correo de 2019!»;
- Podemos comprimirla para hacerla más fácil de recordar, utilizando, por ejemplo, la primera letra de cada palabra, de tal forma que quedara: «EuldlM d2019!».

Puesto de trabajo

Riesgos a los que se expone el puesto de trabajo:

- Información en papel al alcance de cualquiera.
- La falta de confidencialidad de los medios de comunicación tradicionales como el teléfono.
- Accesos no autorizados a los dispositivos. Infecciones por malware.
- Robo de información, etc...

Mesas limpias

Al acabar la jornada se debe guardar la documentación que se encuentre a la vista.

Se debe prestar especial atención a que:

- El puesto de trabajo está limpio y ordenado.
- La documentación que no se utilice en un momento determinado debe estar guardada correctamente, especialmente cuando se abandona el puesto de trabajo o se finaliza la jornada.
- No hay usuarios ni contraseñas apuntadas en post-it o similares.
- Bloqueo de sesión
 - ❖ Windows= Win + L
 - ❖ MacOS= control + opción + q
 - ❖ Linux= Ctrl + alt + L

Hace falta tener el software actualizado y el antivirus y Firewall son las herramientas de Seguridad que protegen al equipo del software malicioso.

Contrato de confidencialidad

- Indicar qué información se considera confidencial y por lo tanto está protegida por el acuerdo.
- Fijar la duración de la relación de confidencialidad, que generalmente será superior al tiempo de prestación del Servicio.
- En caso de ser necesario, se indicará la jurisdicción legal a la que se acoge cada una de las partes.
- Acceder a sitios de dudosa legitimidad como webs de descargas, juego, adultos, etc., no es un uso lícito de los recursos empresariales.
- Software legítimo.
- Programas pirata o adquiridos de forma fraudulenta podrían conllevar sanciones económicas y penales.

- Software ilegal que puede terminar en una infección por malware del equipo.
- Cómo y cuándo reportar un incidente de Seguridad.
- Acceso no autorizado a sistemas o información, como en el caso de robo de un dispositivo o de las credenciales de acceso.
- Denegaciones de servicio, en las cuales el incidente impide el correcto funcionamiento de un recurso, como por ejemplo la página web de la empresa. Infección por malware.
- Robo de información de la empresa.
- Uso seguro de dispositivos de almacenamiento extraíbles.

Tenemos que minimizar las situaciones de riesgo si su uso está permitido en la empresa y saber en qué situaciones se pueden utilizar y qué información se puede llevar en estos dispositivos, para ello se utilizarán métodos seguros de borrado y destrucción de soportes.

BYOD Teletrabajo

El robo o pérdida de los móviles, tabletas, portátiles y dispositivos de almacenamiento como discos duros externos y pendrives. Este puede ser el riesgo más importante al que se exponen estos dispositivos debido a su tamaño y en muchos casos, a su elevado coste.

La infección por malware siempre es un riesgo a tener en cuenta, pues el software malicioso puede robar información confidencial de la empresa y credenciales de acceso a diferentes recursos. A menudo descuidamos la protección antimalware en equipos pequeños.

Los sitios web fraudulentos, la publicidad agresiva o las páginas web de tipo phishing son las principales amenazas a las que se exponen. Navegar en dispositivos pequeños, particularmente en móviles, entraña riesgos al ser más difícil «librarse» de esta publicidad.

Utilizar redes wifi inseguras puede poner en riesgo la privacidad de las comunicaciones, ya que los ciberdelincuentes pueden estar «escuchando» todo lo que se envía y recibe. También podemos conectarnos a redes wifi que suplantan a redes wifi lícitas.

Instalar aplicaciones que necesitan acceder a determinados permisos del dispositivo, en ocasiones excesivos o innecesarios (como acceso a la cámara, los

contactos o los archivos), para poder funcionar con normalidad, pudiendo así verse la información empresarial comprometida.

Dispositivos que no cuentan con controles de acceso robustos que los protejan de un descuido, robo o pérdida. La ausencia de los mismos o el uso de algunos considerados débiles, como el patrón de bloqueo, son un riesgo para su seguridad. Tanto el sistema operativo, como las aplicaciones desactualizadas suponen un riesgo para la seguridad de toda la información que gestionan.

La modificación de los controles de seguridad impuestos por los fabricantes. Algunos usuarios deciden rootear o hacer jailbreak a sus dispositivos lo que puede suponer un grave riesgo, ya que los controles de seguridad impuestos por el desarrollador son eliminados.

Establecer que el dispositivo o la aplicación recuerde la contraseña. Si un tercero accede al dispositivo tendría acceso a todos los servicios en los que estuviera guardada la contraseña.

Utilización de servicios en la nube. La utilización de servicios en la nube o cloud puede suponer un riesgo, ya que la información de la empresa será almacenada en un tercero al que hemos de trasladar nuestros requisitos de confidencialidad, integridad y privacidad. Además, existe el riesgo de que si no fuera posible conectarse a Internet (problemas en la red como congestión o caída de la misma) la información almacenada en la nube no será accesible.

Contraseña de firmware, si el dispositivo lo permite, sobre todo en ordenadores portátiles. De esta forma, se evita que otros usuarios arranquen el equipo desde otro disco distinto del especificado.

Creación de cuentas de usuario y permisos.

En los sistemas operativos como Windows, MacOS o los basados en Linux, se permite la creación de distintos usuarios, otorgándoles una serie de privilegios acordes con su perfil. Es recomendable que cada usuario cuente con los privilegios mínimos y necesarios que le permitan desempeñar su trabajo. Además, deberán contar con una contraseña de acceso robusta.

Bloqueo de dispositivos. En los dispositivos basados en Android o iOS hay que establecer el bloqueo de pantalla en el menor tiempo posible y una contraseña de desbloqueo robusta. También pueden utilizarse métodos biométricos como la huella dactilar.

Activar el cifrado de la información en el dispositivo. Todos los sistemas operativos deberán contar con herramientas de cifrado que protegen la información en ellos

alojada. Los actuales sistemas operativos móviles como Android e iOS cuentan con cifrado de la información por defecto, pero los sistemas operativos para ordenador no, por lo que se debe activar.

Establecer cuál será el tratamiento aceptable de la información confidencial. Preferiblemente, se accederá a la misma por medio de Internet y se evitará siempre descargar en el dispositivo.

No se permitirán usos domésticos (juegos, descargas, etc.) por otros usuarios en el dispositivo utilizado como puesto de teletrabajo;

Se realizarán copias de seguridad de forma periódica; en caso de utilizar una conexión wifi doméstica que podamos configurar de forma segura [Ref. - 9].

Tendremos en cuenta:

- Utilizar cifrado WPA2 o WPA 3 en caso de estar disponible y que los dispositivos sean compatibles;
- Utilizar una clave robusta;
- Desactivar la función WPS en caso de estar activa.

Las distracciones de los empleados al utilizar un mismo dispositivo para tareas personales y laborales. La productividad puede disminuir al acceder a páginas web no relacionadas con su actividad profesional, redes sociales o la cuenta privada de correo electrónico.

Aumento de las posibilidades de accesos no autorizados a información empresarial, ya que el dispositivo se usa para trabajar y para uso personal. Por lo tanto, las posibilidades de pérdida o robo aumentan y por consiguiente, también aumentan los accesos no autorizados.

El dispositivo puede ser prestado a un amigo o familiar para realizar cualquier tarea, lo que puede poner en riesgo la seguridad de la información de la empresa. La relación contractual entre empleado y empleador puede llegar a su fin pudiendo ser un riesgo para ambas partes conservar información empresarial una vez ha terminado el contrato.

Ponerlo en conocimiento de la empresa para que se tomen todas las medidas necesarias que eviten el uso indebido del dispositivo y de la información que contiene o a la que tiene acceso.

Si el dispositivo ha sido robado, se deberá interponer una denuncia ante las Fuerzas y Cuerpos de Seguridad del Estado [Ref. - 7], aportando toda la información posible.

Bloquear el dispositivo de manera remota. La mayoría de sistemas operativos tanto para ordenador, como para móvil cuentan con herramientas que lo permiten, generalmente a través de un panel de administración web.

Geolocalizar el dispositivo. Actualmente, los dispositivos con sistema operativo Windows, MacOS, Android e iOS cuentan con herramientas que permiten conocer su posicionamiento aproximado. Siempre que sea necesario se debe tener habilitado en dispositivos empresariales que use el trabajador.

El empresario tiene que avisar a los empleados de forma clara, expresa e inequívoca, tal y como indica la LOPD GDD 3/2018.

En caso de no ser posible, recuperar el dispositivo se debe optar por realizar un borrado remoto del mismo, de tal manera que toda la información que contenga no pueda estar accesible. Para ello, tendremos habilitada esta opción.

El valor de las redes sociales

Mediante la analítica del uso de las redes sociales se pueden obtener datos sobre las características de los seguidores como género, edad o ubicación y sus preferencias de uso, que pueden ser útiles a la hora de lanzar una determinada campaña comercial, maximizando los beneficios de esta.

También son una buena herramienta para captar nuevos clientes y conocer lo que piensan sobre tus servicios o productos.

Permiten aumentar el tráfico web haciendo que la web de la empresa se posicione mejor en los buscadores y aumentando así su visibilidad.

Sirven para potenciar la marca con la colaboración de los propios usuarios de la red social.

Fraude por suplantación de clientes o proveedores. Los ciberdelincuentes pueden crear perfiles falsos suplantando a un cliente o proveedor para modificar datos en su beneficio. Podría modificar, por ejemplo, la cuenta de facturación, direcciones de envío, etc.

Campañas de malware. El envío de software malicioso por medio de los perfiles en redes sociales también es utilizado por los ciberdelincuentes para infectar los equipos de las víctimas. Para engañar a las víctimas utilizan diferentes técnicas como hacerse pasar por un cliente, un proveedor o incluso por alguien de la empresa. Terminan dirigiendo a la víctima a sitios web maliciosos donde descargaron el malware al hacer clic en un anuncio o simplemente para visitarla.

En otros casos, lo envían adjunto en mensajes privados dando como resultado, en ambos casos, la infección del equipo.

Campañas de phishing. Los ciberdelincuentes pueden hacerse pasar por una marca conocida y redirigir a la víctima a una página web fraudulenta donde robar información personal, bancaria y datos de la empresa, lanzar comentarios inoportunos, negativos o inapropiados, como quejas laborales; emitir juicios de valor, enfascarse en discusiones sin sentido, insultar, amenazar o acosar, propagar noticias falsas, dar información confidencial o sujeta a propiedad intelectual, etc.

Políticas de empresario

Gestión de recursos humanos

Debemos ser conscientes de que el error humano es la causa más frecuente de fallos de seguridad en una empresa, para solucionar esto se deben tomar medidas de seguridad en la gestión de contratos, firmas, realizar filtros y controles de ciberseguridad, concienciar a los trabajadores y formarlos en seguridad.

Los objetivos de este proceso es asegurarnos de que los trabajadores tienen sus derechos, deberes y responsabilidades así como tienen sus correspondientes sanciones si cometen cualquier infracción.

La gestión de recursos humanos tiene una serie de controles para seguir la medida de seguridad:

- *Cláusulas contractuales:* El empresario junto al departamento de recursos humanos deben establecer ciertos aspectos que serán relevantes en la seguridad de la empresa y serán reflejados en el contrato del trabajador, estos aspectos considerarán también la propiedad intelectual y los datos personales.
- *Acuerdos de confidencialidad:* Tanto los trabajadores como los colaboradores deberán firmar un acuerdo conforme a la información de la empresa, este deberá constar de las partes que intervienen, de la información confidencial, los compromisos de todas las partes y las sanciones y legislaciones.

- *Revisar las referencias de los candidatos:* En puestos con acceso a información muy confidencial, se detallaran las comprobaciones a realizar en el candidato, se determinarán las referencias revisadas y que datos deben verificarse, también indicaremos los puestos concretos libres de antecedentes penales.
- *Plan de formación y concienciación en ciberseguridad:* Estipular actividades para mantener informada a la plantilla sobre la seguridad.
- *Política de sanciones y expedientes:* Elaborar un procedimiento que establezca las sanciones en caso de negligencia en seguridad de la información, ha de ser accesible para los empleados en todo momento.
- *Finalización del contrato:* Comunicar a los empleados las obligaciones de confidencialidad una vez finalice su contrato.
- *Concesión autorizada de los permisos de acceso:* Dar de alta a cada empleado en su control de acceso correspondiente, para ello haremos lo siguiente: entregar las tarjetas de acceso físico, asignar cuentas de correo electrónico, conceder permisos de acceso a servicios, aplicativos y recursos compartidos y asignar el puesto de trabajo, los dispositivos y los equipos.
- *Revocación de permisos de acceso:* Al terminar un contrato se deberá recoger la tarjeta de acceso y los dispositivos, eliminar las cuentas de correo y eliminar los permisos de acceso al sistema.
- *Aceptación de cláusulas y políticas de seguridad de la información:* Cada empleado debe leer y firmar cada documento relacionado con la política de seguridad de la información.
- *Aprovechamiento de las sesiones formativas de concienciación:* Aprovechar las sesiones de formación a disposición de los empleados para comprender riesgos de ciberseguridad.

Almacenamiento en la red corporativa

La empresa dispone de servidores de almacenamiento en red donde almacenar el resultado de los trabajos, los controles de acceso a esta información son definidos por la dirección y el responsable de sistemas.

La información almacenada se determina a través de la política de clasificación de la información y se presta especial atención a información catalogada como crítica o si está sujeta a requisitos legales.

El objetivo es conseguir un buen uso de los servidores y concienciar a los empleados sobre la relevancia de la información y cómo almacenarla.

Controles a revisar de la política de seguridad:

- *Inventario de los servidores de almacenamiento:* Informar a los empleados sobre qué servidores hay y que se almacenan en ellos.
- *Criterios de almacenamiento:* Informar sobre el almacenamiento corporativo, quien puede acceder y cuando se elimina la información.
- *Clasificación de la información:* Informar sobre cumplir la política de clasificación de la información.
- *Control de acceso:* Establecer quién puede acceder a los discos y llevar un control de ello.
- *Copias de seguridad:* Hacer un plan de copias de seguridad donde detallar la información que se guarda, donde se guarda, cada cuando se guarda y cuanto tiempo se conserva.
- *Acceso limitado:* Permitir el acceso solo a las zonas necesarias para el trabajador.
- *Almacenamiento clasificado:* Crear las carpetas organizadamente según la política de la empresa y asignar los permisos imprescindibles a los empleados.
- *Auditoría de servidores:* Revisar el estado de los servidores.
- *Cifrado de la información:* Cifrar la información crítica.

Almacenamiento en los equipo de trabajo

Los trabajos guardados de manera local en los dispositivos de la empresa deben disponer de una política de regulación que determine el tratamiento de la información, que se ha de cifrar y cuando y quien controla esa información.

El objetivo es mantener la información local de forma segura y especificar los procedimientos a seguir a los empleados.

Los controles relativos en el almacenamiento en los equipos de trabajo son:

- *Que se puede almacenar en los equipos corporativos:* Crear una normativa que regule el almacenamiento personal.

- *Donde se guarda la información:* Informar de donde se debe guardar la información dentro de los directorios del equipo.
- *Conservación de la información en discos locales:* Determinar el tiempo que se conserva la información local antes de eliminarla o transferirla.
- *Permanencia de la información en discos locales una vez transferida a los servidores:* Determinar el tiempo de la información local en los servidores antes de ser eliminada.
- *Cifrado de información:* Cifrar información crítica antes de guardarla.
- *Conocimiento y aplicación de la normativa:* Conocer y aplicar la normativa.

Almacenamiento en la nube

La empresa ha de disponer de una política de clasificación de la información que indique que puede subirse a la nube y a de transmitirla en todo momento a los trabajadores para que estos hagan un buen uso de los recursos de almacenamiento disponibles.

El objetivo de esto es utilizar eficazmente el espacio en la nube y maximizar la seguridad de la información.

Los controles relativos en el almacenamiento en la nube son:

- *Uso de servicios de almacenamiento en cloud públicas:* Informar sobre las restricciones en clouds públicas a los trabajadores.
- *Lista de servicios cloud permitidos:* Elaborar una lista con los clouds permitidos para los trabajadores.
- *Proceso de borrado de la información en la nube:* Informar sobre los procesos de borrado adecuados para la información en la nube.
- *Tipo de información almacenada y tratamiento:* Informar de qué información puede ser almacenada en la nube y si ha de estar cifrada.
- *Copias de seguridad en la nube:* Valoración de ventajas o desventajas al almacenar las copias de seguridad en la nube.
- *Contratación de servicios de almacenamiento en la nube:* Contratar un servicio cloud que se acomode a los criterios de la empresa.
- *Política de seguridad del proveedor:* Conocer las políticas de almacenamiento en la nube del proveedor.

Aplicaciones permitidas

La empresa debe determinar y controlar el software utilizado por sus equipos para evitar riesgos de infecciones, fugas de información y sanciones penales.

El objetivo es controlar que todo el software utilizado sea legal y que sea el autorizado por la empresa.

Los controles relativos en las aplicaciones permitidas son:

- *Registro de licencias:* Mantener un registro de licencias de software actualizado.
- *Competencia para la instalación, actualización y borrado:* Nombrar personal técnico que se encargue del software de los equipos de la empresa.
- *Sanciones por usos no autorizados:* Informar al personal sobre las sanciones por usar software no autorizado.
- *Repositorio de software:* Tener un repositorio con todo el software autorizado y sus credenciales.
- *Auditoría de software instalado:* Analizar que el software instalado sea el autorizado y tenga licencia.
- *Autorización y licencia del software:* Utilizar el software autorizado en todos los dispositivos y disponer de sus licencias.
- *Política de copias de software:* No realizar copias de software sin consentimiento.

Clasificación de la información

La empresa debe realizar un inventario y clasificar cada activo de información dependiendo de su impacto respecto a la empresa aplicando para ello criterios de

confidencialidad, integridad y disponibilidad, también deberá establecer un tiempo un ciclo de vida dependiendo de la vigencia y de la vida útil del soporte.

El objetivo es garantizar una gestión eficaz de la seguridad de la información.

Los controles relativos en la clasificación de la información son:

- *Inventario de la información*: Elaborar un inventario detallado de la información de la empresa.
- *Criterios de clasificación de la información*: Determinar los criterios de seguridad para clasificar la información.
- *Clasificación de la información*: Etiquetar la información según los criterios de seguridad.
- *Tratamientos de seguridad disponibles*: Establecer una lista con los tratamientos de seguridad disponibles para la empresa.
- *Establecer y aplicar los tratamientos que corresponden a cada tipo de información*: Aplicar los tratamientos de seguridad correspondientes a cada información.
- *Auditorías*: Realizar auditorías de comprobación cada cierto tiempo.

Concienciación y formación

La dirección de la empresa debe poner total compromiso con la formación de los empleados, siendo consciente de la formación proporcionada y revisar periódicamente para prevenir incidentes y adaptarse a las nuevas tecnologías.

El objetivo es asegurarse de que los trabajadores conozcan, entiendan y cumplan las normas y las medidas de protección en ciberseguridad.

Los controles relativos en la concienciación y formación son:

- *Difusión de la política de seguridad*: Documentar y difundir las normas de ciberseguridad.
- *Concretar el plan de formación*: Elaborar y revisar los planes de formación en ciberseguridad de los trabajadores.
- *Programas de formación específicos*: Desarrollar programas de formación en ciberseguridad dependiendo de cada puesto de trabajo.
- *Periodicidad de la formación*: Cada cierto tiempo deben realizarse cursos o charlas para los empleados.

- *Evaluar el aprendizaje obtenido:* Comprobar el conocimiento asimilado por los empleados.
- *Promover una cultura de seguridad de la información:* Promover la seguridad de información en la cadena de suministros de la empresa y los clientes.

Continuidad de negocio

La empresa debe tener un plan de continuidad de negocio que debe tener en cuenta a las personas responsables de aplicarlo, a las operativas a seguir, a los activos implicados y las indicaciones.

Debe comprobarse que los servicios tecnológicos que se contraten tengan planes de contingencia que se adecuen a nuestra empresa.

El objetivo es diseñar y probar un plan que nos permita recuperar la operatividad habitual de la empresa en un tiempo razonable.

Los controles relativos en la continuidad del negocio son:

- *Determinar el alcance del PNC:* Analizar la continuidad de los activos y los procesos.
- *Concretar el flujo de responsabilidades:* Determinar las responsabilidades de las personas responsables del PCN en caso de desastres.
- *Realización del BIA(Análisis del impacto en el negocio):* Elaborar detalladamente el BIA.
- *Definir la política de comunicación y aviso a entidades externas:* Definir el tipo de mensajes que transmite la empresa si hay un desastre.
- *Caducidad del PCN:* Actualizar el PCN cada cierto tiempo.
- *Elegir la estrategia de continuidad:* Elegir una estrategia óptima de continuidad de la empresa.
- *Detallar la respuesta a la contingencia:* Detallar los controles y procedimientos a ejecutar en un desastre.
- *Desarrollar actividades para verificar, revisar y evaluar el plan de continuidad del negocio:* Probar y evaluar el PCN cada cierto tiempo.

Cumplimiento legal

La empresa debe conocer las responsabilidades del cumplimiento legal y que consecuencias puede tener su incumplimiento.

El objetivo es asegurar el conocimiento y cumplimiento de las obligaciones legales sobre seguridad de la información.

Los controles relativos en el cumplimiento legal son:

- *Definir y documentar la manera de cumplir con todos los requisitos legales:* Detallar los procedimientos a seguir para cumplir la legislación sobre ciberseguridad.
- *Garantizar el cumplimiento de los derechos de propiedad intelectual de terceros:* Controlar la compra y el uso de software de tu empresa para que este cumpla la ley de propiedad intelectual.
- *Garantizar el cumplimiento de los derechos de propiedad intelectual propios:* Revisar que se respeten los derechos sobre las obras de la empresa.
- *Comprobar si tu empresa realiza una actividad comercial en la UE o trata datos personales en la UE o sobre personas que se encuentren en la UE:* Comprobar si alguna actividad necesita una gestión de datos personal.
- *Determinar las responsabilidades para gestionar la protección de datos personales:* Designar un responsable del tratamiento de los datos y revisar los contratos con el.
- *Revisar el cumplimiento del deber de informar y que los interesados puedan ejercitar sus derechos según el RGPD:* El responsable informará sobre el tratamiento, obtener los consentimientos, permitir ejercer los derechos y notificar a las autoridades en caso de brechas.
- *Realizar una evaluación de impacto si haces tratamientos de alto riesgo para la privacidad:* Los tratamientos de alto riesgo tratan datos especiales o a gran escala.
- *Llevar un registro de actividades de tratamiento:* Con más de 250 trabajadores o si tienes tratamientos de alto riesgo, debes realizar el registro de actividades del RGPD.

- *Establecer un procedimiento para notificar en caso de brecha de seguridad:* Actualizar tus procedimientos para avisar de la brecha a las autoridades en un plazo de 72 horas.
- *Aplicar las medidas organizativas para adecuarse al RGPD:* Definir los procedimientos para cumplir el rgpd y ofrecer garantías a los interesados, proporcionar la información a los empleados si van a participar.
- *Aplicar las medidas técnicas de seguridad adecuadas según el análisis de riesgos para la privacidad:* Determinar dónde están los datos y clasificarlos por criticidad, monitorizar el uso, quien accede y cuando se eliminan o se cifran y garantizar confidencialidad integridad y disponibilidad.
- *Revisar si tu empresa realiza comunicaciones comerciales que obliguen al cumplimiento de la LSSI:* Cumplir con la LSSI garantizando la seguridad en comunicaciones comerciales.
- *Comprobar los requisitos de la LSSI y el RGPD si tu empresa dispone de comercio electrónico o realiza transacciones online:* Mostrar la información de la LSSI en la web. Informar de la política de cookies de la misma.
- *Garantizar el cumplimiento de los derechos de propiedad industrial y marcas propias y de terceros:* Revisar los derechos industriales, marcas y patentes.
- *Otras regulaciones:* Tener en cuenta la existencia de las limitaciones legales que afecten a la seguridad de tu información.

Plan de director de seguridad

La empresa deberá disponer de un PDS, partiendo de un buen análisis y este deberá estar alienado con los intereses de la empresa e incluirá obligaciones y prácticas a cumplir por todos los empleados.

El objetivo es planificar y organizar los proyectos para garantizar la protección de la seguridad de la información.

Los controles relativos en el plan director de seguridad son:

- *Analizar la situación actual de la empresa:* Analizar la situación de la empresa para acometer el PDS.
- *Alinear el PDS con la estrategia de la empresa:* Tener en cuenta la estrategia a la hora de diseñar el PDS.

- *Definir los proyectos a ejecutar:* Establecer acciones concretas para llegar al nivel de seguridad deseado.
- *Clasificar y priorizar los proyectos:* Clasificar las acciones a ejecutar para priorizar las que proporcionen mejor beneficio/coste.
- *Aprobar el PDS:* Aprobar y publicar el PDS.
- *Ejecución del PDS:* Poner en marcha los proyectos del PDS.
- *Certificación en seguridad:* Implantar un proceso que acredite el sistema de la gestión de seguridad de la empresa.

Relación con proveedores

La empresa deberá controlar y asegurar la seguridad de los proveedores y exigir la más favorable para la seguridad de ambas partes.

El objetivo es controlar la relación con los proveedores para controlar y proteger nuestra información en base a diversos acuerdos y contratos.

Los controles relativos en la relación con los proveedores son:

- *Requisitos de seguridad en productos y servicios:* Establecer los requisitos mínimos que deben cumplir los servicios que contrates.
- *Definir cláusulas contractuales en materia de seguridad de la información:* Ser riguroso elaborando las cláusulas contractuales.
- *Definir las responsabilidades concretas por ambas partes:* Delimitar las responsabilidades de todas las partes involucradas.
- *Definir los ANS:* Definir los ANS que sometes a los servicios contratados.
- *Controles de seguridad obligatorios:* Determinar que controles serán obligatorios en relación con los servicios de los proveedores.
- *Formar parte de los foros y organizaciones de usuarios de los productos/servicios software utilizados:* Controlar los productos que adquieres y la reputación de los proveedores.
- *Certificación de los servicios contratados:* Exigir a los proveedores los certificados contratados en sus productos.
- *Auditoría y control de los servicios contratados:* Supervisar que los productos correspondan al producto acordado.

- *Finalización de la relación contractual:* Garantizar la seguridad de la información tras finalizar un contrato.

Políticas para el personal técnico

Teletrabajo seguro

La empresa deberá contar con medidas de seguridad adecuadas para no poner en riesgo a la organización ni a los trabajadores teniendo en cuenta las necesidades de la empresa.

El objetivo es garantizar la seguridad de la información y gestionar correctamente los recursos disponibles, a parte de concienciar a los empleados.

Los controles relativos en el teletrabajo seguro son:

- *Normativa de protección del puesto de trabajo remoto:* Informar mediante auditorías, al personal sobre la normativa de protección.
- *Relación de usuarios que disponen de la opción de trabajar en remoto:* Llevar un control de las personas con opción a teletrabajar.
- *Procedimientos para la solicitud y autorización del teletrabajo:* Redactar un documento con todas las cuestiones de teletrabajo, ha de ser firmado por los teletrabajadores.
- *Periodo de implantación y pruebas:* Contemplar los riesgos de seguridad antes de habilitar el teletrabajo.
- *Realizar pruebas de carga en escenarios simulados:* Valorar la carga ocasionada en los sistemas internos por los teletrabajadores.
- *Aplicaciones y recursos a los que tiene acceso cada usuario:* Dar y detallar a los teletrabajadores los recursos y condiciones de uso permitidos.
- *Acceso seguro:* Gestionar las credenciales de acceso de los empleados con las normativas de la empresa.
- *Configuración de los dispositivos de teletrabajo:* Configurar los dispositivos utilizados por el teletrabajador.
- *Cifrado de los soportes de información:* Implantar tecnología de cifrado
- *Definición de la política de almacenamiento en los equipos de trabajo y en la red corporativa:* Elaborar políticas sobre el destino de la información.

- *Planificación de las copias de seguridad de todos los soportes:* Comprobar que se realizan y pueden restaurarse.
- *Uso de conexiones seguras a través de una red privada virtual o VPN:* Implementar una VPN extremo a extremo.
- *Aplicaciones de escritorio remoto siempre a través de una VPN:* Permitir el uso de aplicaciones de escritorio remoto solamente con una VPN.
- *Virtualización de entornos de trabajo:* Valorar la virtualización para cada empleado.
- *Priorizar el uso de dispositivos corporativos:* Elegir los dispositivos corporativos para teletrabajar.
- *Conexión a Internet:* Utilizar los datos móviles si no es posible utilizar la red doméstica.
- *Uso de dispositivos personales bajo una política BYOD:* Utilizar las configuraciones y conexiones permitidas para teletrabajar
- *Concienciar a los empleados antes de empezar a teletrabajar:* Formar a los empleados antes de empezar a teletrabajar.
- *Cumplimiento LOPD GDD:* Formar a los empleados para la protección de los datos personales durante el teletrabajo.
- *Aplicaciones de teleconferencia y colaborativas:* Configurar un uso seguro de las aplicaciones para respetar la privacidad y la propiedad intelectual.

Borrado seguro y gestión de soportes

La empresa debe cumplir con la ley de protección de datos destruyendo completamente la información que ya no sea necesaria

El objetivo es establecer las normas adecuadas para el borrado seguro de la información obsoleta.

Los controles relativos en el borrado seguro y la gestión de soporte son:

- *Inventario de activos:* Realizar un seguimiento de las personas responsables de los dispositivos, de los propios dispositivos y de la información que contienen.
- *Gestión de soportes:* Supervisar los dispositivos que almacenan información corporativa.

- *Eliminación de la información en soportes no electrónicos:* Destruir completamente la información de los soportes no electrónicos.
- *Eliminación de la información para la reutilización de soportes electrónicos:* Reescribir para reutilizar un soporte en buen estado.
- *Eliminación de la información antes de deshacernos de soportes electrónicos:* Desmagnetizar o destruir el soporte de almacenamiento antes de desechar.
- *Borrado de información en otros dispositivos:* Eliminar la información antes de deshacerse de los dispositivos.
- *Documentación de las operaciones de borrado realizadas:* Obtener un documento que verifique el borrado realizado con detalles.
- *Destrucción certificada:* Utilizar un servicio certificado para la destrucción de los datos confidenciales.

Uso de dispositivos móviles corporativos

La empresa debe tomar medidas de seguridad para no ser tan susceptible a los robos de información en caso de una pérdida de dispositivo.

El objetivo es establecer normas de seguridad para un correcto uso de los dispositivos corporativos.

Los controles relativos en el uso de dispositivos móviles corporativos son:

- *Asignación de dispositivos:* Elaborar un procedimiento de solicitud y asignación de los dispositivos.
- *Registro de equipos:* Registrar a quien y cuando se le da un dispositivo, y el software del mismo.
- *Mantenimiento de dispositivos:* Elaborar un formulario de solicitud de cambios en los dispositivos.
- *Protección de la BIOS:* Configurar la BIOS con contraseña.
- *Software de localización:* Comunicar al trabajador si el dispositivo tiene software de localización o si es necesario.
- *Almacenamiento de la información:* No almacenar información corporativa si no es necesaria.
- *Tratamiento de la información confidencial:* Cifrar y eliminar la información confidencial de forma segura.

- *Conexión a redes*: Conectar los dispositivos a redes conocidas o a los datos móviles solamente.
- *Notificación en caso de infección*: Notificar al personal técnico si se sospecha que hay alguna infección en el dispositivo.
- *Transporte y custodia*: Elaborar una serie de requisitos para la seguridad de los dispositivos al ser transportados fuera de un lugar de trabajo seguro.
- *Uso del puesto de trabajo*: Aplicar las políticas del puesto de trabajo relativas a usar un equipo informático.
- *Responsabilidades*: Conocer las responsabilidades y las normas al utilizar un dispositivo corporativo móvil.

Almacenamiento en la nube

La empresa debe establecer una política de control de malware.

El objetivo es proteger toda la información contra cualquier infección.

Los controles relativos en antimalware son:

- *Instalar o contratar una solución antimalware*: Analizar qué solución es la más adecuada para la empresa y aplicarla.
- *Configurar las herramientas de detección de malware*: Configurar correctamente las herramientas antimalware.
- *Actualizar las herramientas de detección de malware*: Actualizar cada cierto tiempo las herramientas antimalware instaladas.
- *Establecer el procedimiento de respuesta ante la infección por ejecución de malware*: Elaborar los procedimientos a seguir en caso de infección de malware.
- *Buenas prácticas para el control de malware*: Seguir las directrices de prevención de infecciones.

Auditoria de sistemas

La empresa debe determinar su nivel de seguridad actual y establecer el nivel a conseguir, para ello deberá realizar diferentes auditorias.

El objetivo es obtener las evidencias de que nuestros sistemas cumplen con los niveles de seguridad y avanzan en la mejora de seguridad.

Los controles relativos en la auditoría de sistemas son:

- *Detallar los elementos clave que queremos que sean auditados:* Identificar los activos más relevantes para ser auditados.
- *Mejora continua y modelos de madurez:* Enfocar las auditorías para una mejora continua.
- *Auditorías legales:* Verificar el cumplimiento de los requerimientos del RGPD.
- *Auditorías forenses:* Determinar lo ocurrido tras un incidente.
- *Procedimientos:* Definir procedimientos para auditar la seguridad de los sistemas de información.
- *Realización de auditorías periódicas:* Realizar auditorías de los sistemas de información cada cierto tiempo.
- *Ánalisis del resultado de la auditoría:* Buscar debilidades a corregir.

Comercio electrónico

La empresa debe contemplar la seguridad de los clientes y de la propia empresa a la hora de vender productos a través de la web.

El objetivo es verificar que las medidas que se aplican sean las correctas para evitar el fraude y garantizar la seguridad de los clientes.

Los controles relativos en el comercio electrónico son:

- *Cumplimiento de políticas relacionadas:* Cumplir la política de seguridad web y la política de relación con los proveedores.
- *Certificado web con validación extendida:* Adquirir un certificado con validación externa para la tienda online.
- *Sellos de confianza para el comercio electrónico:* Obtener sellos de confianza para garantizar la seguridad de la web.
- *Medidas de carácter legal:* Asegurarse de que la web cumple con las medidas legales.
- *Prevención de compras fraudulentas:* Elaborar listas blancas y negras de los clientes.
- *Pago virtual con tarjetas de crédito:* Cumplir con el estándar de seguridad de datos para la industria de tarjeta de pago.

- *Control de acceso:* Aplicar la política de control de acceso y de contraseñas para acceder al gestor de la web.
- *Detección de compra fraudulenta:* Comprobar los intentos de compra.
- *Prevención del fraude: comprobaciones a realizar para aceptar nuevos clientes:* Comprobar si los datos están en la lista negra o si tiene registros de fraude anteriores.
- *Prevención de fraude: comprobaciones a realizar para clientes registrados:* comprobar si los datos están en la lista blanca, si hay algún problema de pago y si los datos coinciden con pedidos anteriores.
- *Actuación ante la detección de compra fraudulenta:* No enviar el producto, contactar y comprobar la transacción y acudir a las FCSE para interponer una denuncia.

Control de acceso

La empresa debe controlar quien accede a la información de la misma y tener un registro de quien accede para analizar los posibles incidentes de seguridad.

El objetivo es establecer qué personal puede acceder a qué tipo de información y cuándo accede.

Los controles relativos en el control de acceso son:

- *Política de usuarios y grupos:* Definir a los trabajadores en función de la información a la que acceden.
- Asignación de permisos: Asignar los permisos necesarios a cada trabajador.
- *Creación/modificación/borrado de cuentas de usuario con permisos:* Definir un procedimiento para modificar las cuentas de usuario.
- *Cuentas de administración:* Gestionar las cuentas de administración teniendo en cuenta su criticidad.
- *Mecanismos de autentificación:* Implantar las técnicas de autenticación más adecuadas para el criterio de la empresa.
- *Registro de eventos:* Registrar todos los eventos relevantes en el manejo de la información de la empresa.
- *Revisión de permisos:* Revisar cada cierto tiempo que los permisos sean los correspondientes.

- *Revocación de permisos y eliminación de cuentas:* Desactivar los permisos y eliminar las cuentas una vez finalizada la relación contractual.

Copias de seguridad

La empresa debe realizar un inventario de activos de información y clasificarlos en base a su criticidad, la empresa ha de identificar a los responsables de los backups y ha de definir los procedimientos para las copias y restauraciones.

La empresa ha de llevar un control de los soportes utilizados y quién puede acceder a ellos.

El objetivo es verificar y garantizar la continuidad del negocio.

Los controles relativos en las copias de seguridad son:

- *Inventario de activos de información:* Mantener un inventario de los activos y clasificarlos según la criticidad.
- *Control de acceso:* Controlar el acceso a las copias de seguridad.
- *Copias de seguridad de la información crítica:* Hacer copias de la información crítica y la exigida por la ley.
- *Periodicidad de las copias de seguridad:* Realizar copias de seguridad cada cierto tiempo.
- *Tipo de copia apropiada:* Hacer copias de seguridad dependiendo de lo que sea necesario para la empresa.
- *Caducidad de las copias de seguridad:* Conservar las copias de seguridad durante un tiempo estipulado.
- *Ubicación de las copias de seguridad:* Guardar una copia completa fuera de la organización y guardar copias en una caja ignífuga y bajo llave.
- *Copias en la nube:* Tomar las medidas de seguridad necesarias con el proveedor.
- *Procedimientos de copia y restauración:* Aplicar los procedimientos elaborados y revisarlos anualmente y con cada cambio en los activos.

- *Comprobar que las copias están bien realizadas y que pueden restaurarse:* comprobar cada cierto tiempo la fiabilidad de las copias.
- *Soporte de las copias de seguridad:* Revisar que el soporte para hacer la copia es adecuado y esta en buen estado.
- *Control de los soportes de la copia:* etiquetar y llevar un registro sobre los soportes en los que se haya realizado alguna copia.
- *Destrucción de soportes de copia:* Destruir de forma segura los soportes desechados.
- *Cifrado de las copias de seguridad:* Cifrar las copias de seguridad con información confidencial y las subidas a la nube.

Gestión de logs

La empresa necesita un sistema que registre la actividad de los usuarios y los procesos internos constantemente.

El objetivo es determinar eventos dentro del sistema y detectar intrusiones o errores.

Los controles relativos en los logs son:

- *Que actividad debe ser registrada:* Analizar qué eventos quieras registrar.
- *Información relevante incluida en el registro:* Determinar la información más significativa a almacenar.
- *Formato de la información registrada:* Detallar el formato de los logs.
- *Elección del mecanismo de registro:* Seleccionar el sistema más apropiado para la empresa.
- *Protección y almacenamiento:* Proteger la información registrada en los logs.
- *Sincronización del reloj:* Revisar la sincronización temporal de todos los dispositivos.
- *Sistemas de monitorización y alerta:* Configurar los sistemas para generar en tiempo real alertas.

Protección de la página web

La empresa ha de tener en cuenta las medidas de seguridad apropiadas de su empresa para contratar a los proveedores que diseñen la página web.

El objetivo es proteger la página web de posibles ataques y cumplir con la legislación garantizando la seguridad de nuestros clientes.

Los controles relativos en la protección de la página web son:

- *Certificado web*: Proteger mediante cifrado los canales por los que se transmite la información.
- *Información del usuario*: Aplicar las normas del RGPD.
- *Desarrollo de terceros*: Tener los criterios de seguridad en el desarrollo de terceros.
- *Cumplimiento legal*: Cumplir los aspectos legales de LSSI y LPI.
- *Alojamiento en servidor propio*: Disponer de medidas de seguridad.
- *Alojamiento en servidor externo*: Asegurar que se sigan las medidas pactadas con el proveedor.
- *Administración por terceros*: Mantener un registro de la actividad. Configuración del CMS: Aplicar medidas de seguridad.
- *Acceso al panel de control*: Asegurar que las claves de acceso cumplan los criterios de seguridad.
- *Limitación de accesos*: Configurar los servidores con un máximo de accesos a la vez.
- *Usuarios por defecto*: Eliminar los usuarios por defecto.
- *Guardado de registros*: Guardar cualquier interacción durante un cierto tiempo.
- *Comercio electrónico*: Elaborar una normativa siguiendo la política de comercio electrónico.
- *Sellos de confianza*: Disponer del sello de confianza que acredite la seguridad de la web.
- *Copias de seguridad*: Realizar copias de seguridad periódicas. Auditorías: Realizar auditorías externas.
- *Software actualizado*: Actualizar cada cierto tiempo el CMS, sus complementos y el software del servidor.
- *Protección frente al malware*: Instalar antivirus en los equipos.

Respuesta a incidentes

La empresa deberá preparar un plan de acción para los incidentes de ciberseguridad.

El objetivo es asegurarnos de que todos los trabajadores actúen correctamente ante cualquier incidente.

Los controles relativos en la respuesta a incidentes son:

- *Equipo responsable*: Seleccionar el equipo encargado de gestionar los incidentes.
- *Mejora continua*: Adoptar mejoras gracias a la información recogida.
- *Caducidad del plan de gestión*: Revisar cada cierto tiempo el plan de gestión y la respuesta del mismo.
- *Detección del incidente*: Concretar las situaciones catalogadas como incidentes.
- *Evaluación del incidente*: Categorizar los incidentes por criticidad.
- *Notificación del incidente*: Establecer una buena manera de notificar el incidente.
- *Resolución del incidente*: Desarrollar procedimientos de actuación detallados.
- *Tratamiento del registro del incidente*: Registrar toda la información relativa del incidente.
- *Cumplimiento del RGPD*: Tener prevista una notificación del incidente si éste afecta a datos personales.

Uso de técnicas criptográficas

La empresa debe proteger la información sensible y confidencial cuando está en tránsito o almacenada, deberá garantizar la confidencialidad e integridad de la información y deberá utilizar protocolos seguros en las comunicaciones.

El objetivo es garantizar el uso adecuado de estas técnicas para asegurar la confidencialidad, integridad y autenticidad de la información de la empresa.

Los controles relativos en el uso de técnicas criptográficas son:

- *Información susceptible de ser cifrada:* Identificar la información a cifrar.
- *Uso de firma electrónica:* Implantar su uso en acuerdos comerciales.
- *Certificados web:* Adquirir un certificado web.
- *Cifrado de datos sensibles cuando se contratan servicios externos:* Comprobar que se utilizan los canales y las herramientas dadas para cifrar la información.
- *Cifrado de datos sensibles cuando se solicitan desarrollos de aplicaciones:* Comprueba que se cifren las credenciales acordadas.
- *Acceso desde el exterior con VPN:* Autorizar el acceso mediante canales de VPN cifrados.
- *Algoritmos de cifrado autorizado:* Aplicar los algoritmos más adecuados para tus sistemas.
- *Aplicaciones autorizadas para usos criptográficos:* Disponer de una lista de aplicaciones para el cifrado.
- *Uso de protocolos seguros de comunicación:* Implementar protocolos para acceder a los servidores.
- *Cifrado de la wifi de la empresa:* Configurar la wifi con el cifrado más seguro, WPA2.

Actualización de software

La empresa deberá mantener actualizados los equipos y las aplicaciones teniendo en cuenta la vida útil de los dispositivos.

El objetivo es elaborar procedimientos que permitan instalar las actualizaciones de forma segura y controlada.

Los controles relativos en la actualización de software son:

- *Determinar el software que debe ser actualizado:* Realizar un listado del software de la empresa.
- *Determinar cuándo y qué actualizaciones instalar:* Revisar las actualizaciones antes de instalarlas.
- *Probar las actualizaciones:* Contrastar las actualizaciones en un entorno de pruebas.
- *Deshacer los cambios:* Contar con procedimientos para deshacer los cambios después de una actualización.

- *Herramientas de diagnostico y actualizacion:* Utilizar herramientas de autodiagnóstico en los equipos.
- *Configuración de un sistema de alertas:* Configurar un sistema de alertas para recibir avisos de vulnerabilidades.
- *Registro de actualizaciones:* Registrar cada actualización instalada.

Almacenamiento en los dispositivos extraíbles

La empresa deberá aplicar medidas de seguridad para los dispositivos de almacenamiento extraíble, deberá decidir si permite su uso y deberá disponer de su correspondiente normativa.

El objetivo es establecer ciertas normas con respecto a los dispositivos extraíbles para mejorar la seguridad.

Los controles relativos en el almacenamiento en los dispositivos extraíbles son:

- *Normativa de almacenamiento en dispositivos extraíbles:* Elaborar una normativa para el uso de estos dispositivos.
- *Concienciación de los empleados:* Involucrar a los empleados en la protección de los dispositivos.
- *Alternativas a los medios de almacenamiento extraíble:* Implementar alternativas para no utilizar los dispositivos extraíbles.
- *Registro de usuarios y dispositivos:* Mantener un registro actualizado.
- *Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en el dispositivo extraíble:* Aplicar medidas para el almacenamiento seguro.
- *Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información en los dispositivos a los que se conecta:* Aplicar medidas seguras en los dispositivos a los que se conecta.
- *Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información sobre los documentos:* Aplicar medidas seguras en los documentos que se transfieren.

- *Cumplimiento de la normativa:* Conocer y aceptar la normativa corporativa del uso de dispositivos extraíbles.

Políticas para el empleado

Contraseñas

La empresa debe garantizar que las credenciales de autenticación se generen, actualicen y se revoquen de forma óptima y segura estableciendo un procedimiento claro para llevarlo a cabo.

El objetivo es establecer y difundir las buenas prácticas en las contraseñas.

Los controles relativos en las contraseñas son:

- *No utilizar las contraseñas por defecto:* Ir cambiando las contraseñas de la empresa.
- *Contraseñas robustas:* Generar contraseñas teniendo en cuenta su fortaleza.
- *No hacer uso del recordatorio de contraseñas:* No usar nunca el apartado de recordatorio.
- *Doble factor para servicios críticos:* Incorporar sistemas de autenticación multiplataforma.
- *No utilizar la misma contraseña para diferentes servicios:* Variar las contraseñas por cada servicio utilizado.
- *Utilizar gestores de contraseñas:* Usar gestores de contraseña seguros para poder recordarlas.
- *No compartir las contraseñas con nadie:* Mantener en secreto las claves y no decirlas a nadie.
- *Cambiar las contraseñas periódicamente:* Hacer que las contraseñas se cambien cada cierto tiempo.
- *Gestión de contraseñas:* Definir un sistema de gestión de contraseñas avanzado.
- *Técnicas de autenticación externas:* Consideración de la utilización de autenticadores externos.
- *Herramientas para garantizar la seguridad de las contraseñas:* Ayudarse de técnicas y herramientas informáticas.

Uso de dispositivos móviles no corporativos

La empresa debe garantizar que los dispositivos móviles se utilizan de forma segura y cautelosa en las instalaciones de la empresa y fuera de ella.

El objetivo es establecer y difundir las buenas prácticas de los dispositivos móviles.

Los controles relativos de los dispositivos móviles son:

- *Normas y procedimientos BYOD:* Elaborar normas y procedimientos si permitimos el BYOD en la empresa.
- *Prohibición de uso de dispositivos manipulados:* Prohibir el uso de dispositivos rooteados o a los que se le ha aplicado el jailbreak.
- *Concienciación de los empleados:* Involucrar a los empleados a su propia protección de sus dispositivos.
- *Formación de los empleados:* Proporcionar charlas y cursillos para los empleados.
- *Limitar el acceso a redes externas:* Prohibición del uso de redes externas e inalámbricas.
- *Listado de aplicaciones no permitidas:* Mantener un listado de aplicaciones no permitidas en la empresa.
- *Controlar el almacenamiento en la nube de datos corporativos:* Supervisar el almacenamiento en la nube.
- *Proceso de borrado de la información:* Aplicación de una normativa de eliminación de datos.
- *Control de usuario y dispositivos:* Mantener un riesgo actualizado con usuarios, dispositivos y privilegios de acceso.
- *Aplicar medidas técnicas para garantizar un almacenamiento seguro de la información:* Instalación de medidas de seguridad para mantener seguro el almacenamiento de datos.
- *Bloqueo programado:* Tras un periodo de inactividad programar un bloqueo del dispositivo.
- *Desconexión wifi y Bluetooth:* Desactivación de la búsqueda de señal wifi y bluetooth en tu dispositivo.

- *Cumplimiento de la normativa:* Conoces y sigues la normativa para una buena ejecución.
- *Control de acceso a la red:* Implantación de un control de red para mayor seguridad.
- *Extravío de dispositivos:* Configuración de medidas de seguridad para la protección de información corporativa.

Uso del correo electrónico

La empresa debe garantizar que el correo electrónico se utiliza de forma segura y cautelosa en las instalaciones de la empresa y fuera de ella.

El objetivo es establecer y difundir las buenas prácticas del correo electrónico.

Los controles relativos del correo son:

- *Normativa de uso de correo electrónico:* Creación de un seguido de normas a la hora de usar el correo electrónico.
- *Antimalware y antispam:* Instalación de aplicaciones para la protección contra el malware y el spam.
- *Ofuscar las direcciones de correo electrónico:* No publicar en ninguna red social ni página web la dirección de correo electrónico de la empresa.
- *Uso apropiado del correo corporativo:* Nunca usar el correo corporativo con fines personales.
- *Contraseña segura:* Uso de una contraseña segura para acceder al correo.
- *Correos sospechosos:* Si se sospecha de un correo electrónico nunca abrirlo sin antes pedir ayuda.
- *Identificación del remitente:* Siempre saber quien es el remitente de un correo si no, no abrirlo hasta que se sepa.
- *Análisis de adjunto:* Análisis práctico y seguro de los archivos adjuntos a los correos ya que podrían ser maliciosos.
- *Inspección de enlaces:* Saber que los enlaces sean seguros y fiables antes de acceder o utilizarlos.
- *No responder al spam:* Nunca contestar un spam ya que podrías dar información a alguien que no la merece.
- *Utilizar la copia oculta (BCC o CCO):* Utilización de la copia oculta cuando envíes correos a múltiples direcciones.

- *Evitar las redes públicas:* No consultar el correo corporativo si estás en una red pública.
- *Cifrado y firma digital:* Instalación de cifrado y firma digital para una mayor seguridad.
- *Desactivar el formato HTML, la función de macros y las descargas de imágenes:* Desactivación del formato HTML, la función de macros y la descarga de imágenes para una protección adicional.

Uso de wifi y redes externas

La empresa debe garantizar que el uso de wifi y redes externas está siendo bien realizado y es seguro.

El objetivo es establecer y difundir las buenas prácticas del wifi y las redes externas.

Los controles relativos del wifi y las redes externas son:

- *Política de conexión:* Normativa reguladora de las conexiones externas.
- *Uso de la VPN:* Otorgar el conocimiento de acceso vía VPN a las redes y en qué situaciones hacerlo.
- *Acceso a redes wifi ajenas:* Al conectarte a redes ajenas tienes que comprobar que usa el protocolo WPA2 además de comprobar que es un sitio seguro y se puede navegar por él.
- *Redes inalámbricas de los dispositivos móviles:* Utilización de redes inalámbricas y bluetooth en móvil solo cuando se vaya a utilizar.
- *Uso de dispositivos móviles:* Revisión de las políticas de móviles en ámbito corporativo.
- *Uso de ordenadores no corporativos:* Evitar el uso de ordenadores no corporativos y revisar la seguridad de tus dispositivos domésticos.
- *Configuración de la VPN:* Configuración de la VPN para acceder desde el exterior con cuentas con permiso de acceso.
- *Configuración de la Wifi doméstica:* Antes de su utilización debemos configurarlas y asegurarnos que tienen el protocolo WPA2, cambiamos el SSID y las credenciales.

Protección del puesto de trabajo

La empresa debe garantizar que el puesto de trabajo es seguro y se puede trabajar como corresponde.

El objetivo es establecer y difundir la protección del puesto de trabajo y su buen estado.

Los controles relativos del puesto de trabajo son:

- *Normativa de protección del puesto de trabajo:* Informar a todo el personal de la buena protección del puesto de trabajo y la mejor forma de mantenerlo seguro.
- *Sistemas operativos actualizados:* Mantienes el sistema operativo actualizado y listo para el trabajo.
- *Antivirus actualizado y activo:* El antivirus siempre tiene que estar activo y perfectamente actualizado para una buena protección.
- *Desactivar por defecto los puertos USB:* Desactivar todos los puertos y activarlos únicamente para los empleados que necesitan dicha función.
- *Seguridad de impresoras y equipos auxiliares:* Verificación de la protección de las impresoras y equipos auxiliares que puedan estar conectados a la red o guardando información.
- *Prohibición de alteración de la configuración del equipo e instalación de aplicaciones no autorizadas:* Siempre que se requiera algo así avisar al personal informático y demandar un cambio de configuración o una instalación de un programa que necesites.
- *Política de mesas limpias:* Siempre tener ordenada tu mesa sin papeles confidenciales a la vista.
- *Destrucción básica de documentación mediante mecanismos seguros:* Utilización del destructor de papeles para la eliminación de papeles así eliminando información confidencial.
- *No abandonar documentación sensible en impresoras o escáneres:* Recoger inmediatamente los documentos imprimidos para prevenir la malversación de estos.
- *No revelar información a usuarios no debidamente identificados:* No revelar la información ya que podrías estar hundiendo a la empresa.

- *Obligación de confidencialidad:* Aceptas y cumples la política de confidencialidad.
- *Uso de contraseñas:* No publiques ni compartas tus claves, tampoco las notas ni otro tipo de información clave para la empresa.
- *Obligación de bloqueo de sesión y apagado de equipos:* Cierre de todo tipo de equipos con su respectivo cierre de sesión.
- *Uso adecuado de internet:* Conoces y aplicas la normativa del uso de internet.
- *Uso de portátiles y dispositivos móviles de la empresa:* Conoces y aceptas la normativa de uso de la empresa para sus dispositivos portátiles y móviles.
- *Obligación de notificar incidentes:* Notificar cualquier tipo de incidente que veas sea el tipo que sea.
- *Destrucción avanzada de documentación mediante mecanismos seguros:* Destruyes la información de forma segura teniendo en cuenta el método apropiado.
- *Bloqueo programado de sesión:* Programar un bloqueo automático de sesión en todos los ordenadores al no detectarse actividad.
- *Uso de los medios de almacenamiento:* Conoces y aplicas las políticas relativas al almacenamiento seguro de la información.
- *Cifrado de la información confidencial:* Conoces y aplicas la normativa al cifrado de información.

Conclusiones

Dados los datos mencionados en este documento, estamos convencidos de que vamos a saber cómo guiar correctamente la seguridad de New Normal Life, así como controlarla, entenderla, distribuir los conocimientos y gestionarla correctamente entre el equipo directivo, los empleados y los clientes.

Presupuesto

Políticas de seguridad para el empleado

Estas políticas son necesarias para mantener el orden y la seguridad de los empleados, ya que es esencial para la empresa y su funcionalidad.

- Protección del puesto de trabajo 125€
- Uso de WIFI y redes externas 125€
- Uso del correo electrónico 125€
- Uso de dispositivos móviles no corporativos 125€
- Contraseñas 125€

Todo esto tiene un coste de 625€

Esto se debe a que el coste de la creación del plan que son 85€ por punto, además nuestro trabajador trabajara mas ya que tendrá que explicar el plan a los trabajadores indicados, nuestro trabajador cobra 15€ la hora y tendrá que trabajar 2h 30€ y por ultimo serian 10 para el cercioramiento de la seguridad.

Políticas para el empresario

Política empleada para la seguridad en el ámbito del empresario

- Gestión de recursos humanos 100€
- Almacenamiento en la red corporativa 100€
- Almacenamiento en los equipos de trabajo 100€
- Almacenamiento en la nube 100€
- Aplicaciones permitidas 100€
- Clasificación de la información 100€
- Concienciación y formación 100€
- Continuidad de negocio 100€
- Cumplimiento legal 100€
- Plan director de seguridad 100€
- Relación con proveedores 100€

Precio Final: 1100€

Estos puntos son los tratados en este plan de seguridad

Este es el plan del empresario, el cual está destinado a la organización y seguridad de este mismo. Todos estos puntos son necesarios e indispensables para tu empresa.

Precio e indicaciones

En total son 1100 euros, 100€ por cada implementación realizada.

Esto se debe a que cada punto necesita una estructuración y preparación previa la cual se tiene que llevar a cabo en la empresa.

Esta estructuración la tiene que hacer un profesional el cual cobra 15€ la hora y tendrá que trabajar para la explicación de dicha estructuración a los trabajadores. La estructuración puede variar pero su precio redondeado son 85€ por punto del plan.

Y para acabar quedan 15€ por el seguimiento y la aseguranza de que la seguridad sea correcta y esté todo correcto, para asegurarse que si en cualquier momento hay un incidente.

Cada subplan tiene un coste de 10€

Políticas de seguridad para el servicio técnico

Políticas de seguridad en el ámbito del servicio técnico las cuales se aseguran de tener una buena seguridad.

- Teletrabajo seguro 100€
- Borrado seguro y gestión de soportes 100€
- Uso de dispositivos móviles corporativos 100€
- Antimalware 100€
- Auditoria de sistemas 100€
- Comercio electrónico 100€
- Control de acceso 100€
- Copias de seguridad 100€
- Gestión de logs 100€



- Protección de la página web 100€
- Respuesta a incidentes 100€
- Uso de técnicas criptográficas 100€
- Actualizaciones de software 100€
- Almacenamiento en dispositivos extraíbles 100€
-

Precio final: 1400€

Estos puntos son los tratados en este plan de seguridad

Son 14 con un precio de 100 por cada uno, los cuales están indistintamente preparados para la protección de tu empresa desde el servicio técnico.

Estos puntos son esenciales para tu empresa además de claves para la mejora de vuestra empresa.

Precio e indicaciones

El precio es tal ya que necesitamos entre 50 y 85 euros para crear el plan de seguridad, ya que ninguna empresa es igual y tenemos que seguir un protocolo para la creación del mejor plan.

Y para acabar serían 15€ por el seguimiento del plan, ya que vendría un técnico que cobre 15€ la h una hora al mes para comprobar que todo sigue correcto y que no haya ningún error.

Y cada subplan tiene un coste de 10€

Referencias

Incibe

Para la realización de toda la teórica de la seguridad de New Normal Life ha sido imprescindible la información disponible en la página web de incibe, sobre todo estas tres páginas en específico.

[Itinerarios de ciberseguridad por sectores empresariales \(incibe.es\)](http://incibe.es)

[Kit de concienciación | INCIBE](http://incibe.es)



[Políticas de seguridad para la pyme | INCIBE](#)

Implementación de los servicios de red

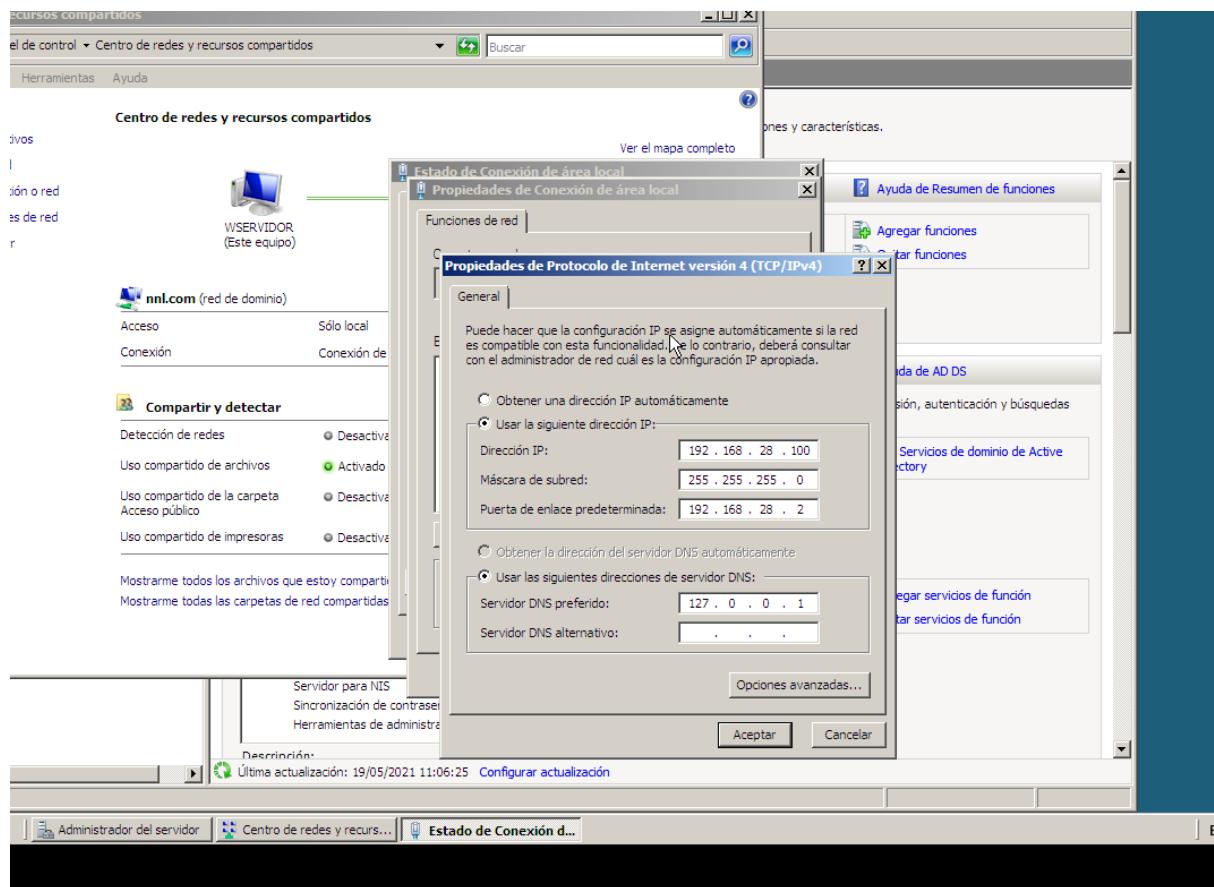
Servicios: Windows Server

Servicios de función: 1 instalado(s)	
Servicio de función	Estado
Controlador de dominio de Active Directory	Instaladas
Administración de identidades para UNIX	No instalado
Servidor para NIS	No instalado
Sincronización de contraseña	No instalado
Herramientas de administración	No instalado

Primero de todo agregamos la función de active directory, a la hora de instalarla debemos usar la opción avanzada para configurar e instalar dns de golpe también, así cuando acabemos la instalación lo tendremos todo listo.

Administrador de DNS				
Nombre	Tipo	Datos	Marca de tiempo	
_msdcs				
_sites				
_tcp				
_udp				
DomainDnsZones				
ForestDnsZones				
(igual que la carpeta principal)	Inicio de autoridad (SOA)	[29], wservidor.nnl.com., h...	15/04/2021 20:00:00	
(igual que la carpeta principal)	Servidor de nombres (NS)	wservidor.nnl.com.	18/05/2021 13:00:00	
(igual que la carpeta principal)	Host (A)	192.168.28.100	18/05/2021 13:00:00	
wcliente	Host (A)	192.168.28.110	static	
wservidor	Host (A)	192.168.28.100	18/05/2021 13:00:00	
www	Alias (CNAME)	www.nnl.com.	static	

una vez instalado tenemos que ir a herramientas, DNS y ahí crear una zona directa e inversa , una vez creadas hay que editarlas para poner la dirección ip del cliente y de nuestro propio servidor, que tiene que coincidir con la que tengamos puesta.



Como podemos ver aquí la ip del servidor es la misma que apuntamos para que no haya ningún error igual que en el cliente .

Preparación del entorno de trabajo

Instalación de webmin

Se abre una sesión gráfica de Ubuntu 16.04 desktop y se inicia sesión como administrador del servidor. Tras ello, se abre un terminal y se edita el archivo sources.list añadiendo el siguiente argumento:

```
deb http://download.webmin.com/download/repository sarge contrib
```

El siguiente paso es añadir la clave de webmin para que el sistema confíe en su nuevo repositorio y actualizamos los paquetes disponibles.

```
adminnnnl@adminnnnl:~$ sudo nano /etc/apt/sources.list  
[sudo] password for adminnnnl:  
adminnnnl@adminnnnl:~$ wget http://www.webmin.com/jcameron-key.asc
```

```
adminnnnl@adminnnnl:~$ sudo apt-key add jcameron-key.asc  
OK  
adminnnnl@adminnnnl:~$ sudo apt update
```

Una vez realizados los pasos descritos, instalamos webmin con el siguiente comando:

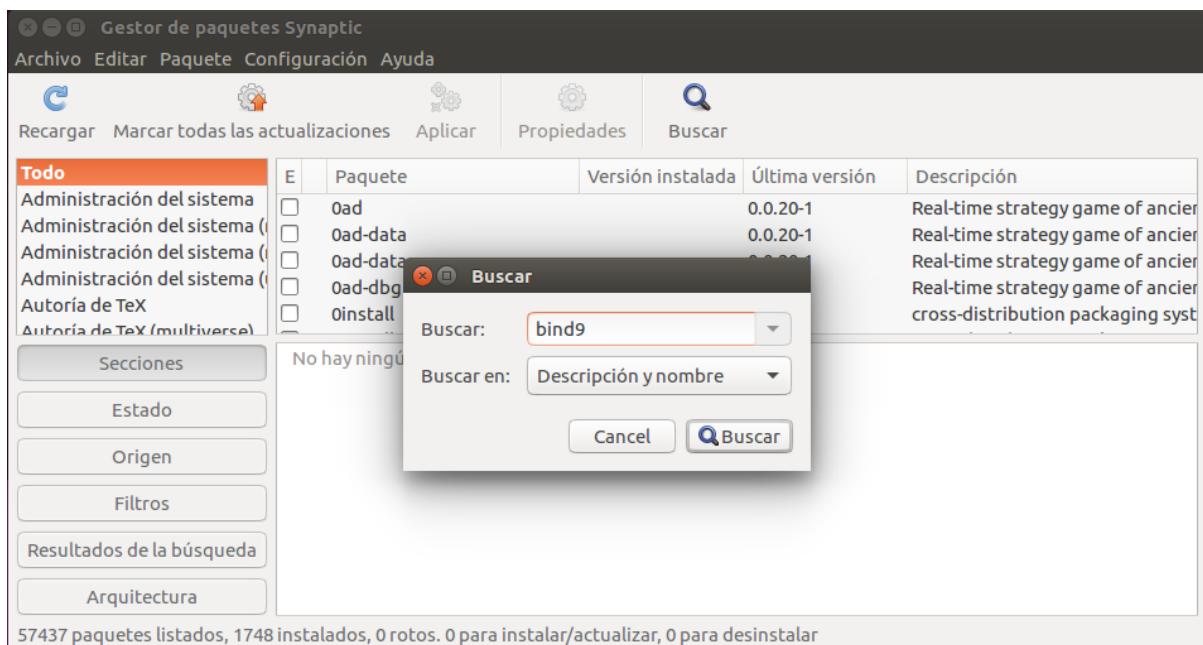
```
adminnnnl@adminnnnl:~$ sudo apt install webmin
```

Servidor dns

Ahora procedemos a la instalación del servidor DNS en Ubuntu 16.04 desktop, pero antes de eso es necesario tener instalado el gestor de paquetes Synaptic, para instalarlo, utilizaremos el siguiente comando:

```
adminservidor@userservidor:~$ sudo apt-get install synaptic
```

Lo siguiente es abrir Synaptic y acceder a la opción de buscar en el menú superior, se introduce bind9 en el campo buscar y se hace click en la opción buscar, una vez realizada la búsqueda, marcamos la casilla de selección, hacerlo abrirá una ventana donde nos pregunta si queremos marcar todos los paquetes necesarios para que el servicio DNS funcione, haremos click en Marcar. Después de eso haremos click en la opción Aplicar del menú superior y comenzará la instalación



Una vez realizada la instalación de bind9 nos dirigiremos a webmin, desde donde se administrarán todos los servicios. Para hacerlo abriremos el navegador y escribimos localhost:10000 en la barra de búsqueda

Una vez en webmin, nos dirigimos al menú lateral, donde encontramos varios submenús, debajo de ellos, se encuentra el botón *Recargar Módulos*.

Recargar Módulos

Una vez recargados, nos dirigimos otra vez al menú lateral, esta vez al apartado servidores, donde podremos ver lo siguiente:

Servidor de DNS BIND

Una vez accedemos a Servidor de DNS BIND seleccionamos la opción Crear nueva zona maestra del menú que nos aparece y lo rellenamos como aparece en la

captura

a

continuación:

Opciones de nueva zona maestra

Tipo de zona Reenvío (Nombres a Direcciones) Inversas (Direcciones a Nombres)

Nombre de Dominio/Red

Archivo de Registros Automático ...

Servidor Maestro ¿Añadir registro NS para servidor maestro?

Dirección de correo

¿Utilizar plantilla de zona? Si No

¿Aregar reversos para direcciones de plantilla? Si No

Dirección IP para registros de plantilla

Tiempo de refresco segundos

Tiempo de reintento de transferencia segundos

Tiempo de expiración segundos

Tiempo-que-está-viva por Defecto segundos

una vez creada la zona maestra, crearemos otra zona nueva siguiendo los mismos pasos y completando como en la siguiente captura:

Opciones de nueva zona maestra

Tipo de zona Reenvío (Nombres a Direcciones) Inversas (Direcciones a Nombres)

Nombre de Dominio/Red

Archivo de Registros Automático ...

Servidor Maestro ¿Añadir registro NS para servidor maestro?

Dirección de correo

¿Utilizar plantilla de zona? Si No

¿Aregar reversos para direcciones de plantilla? Si No

Dirección IP para registros de plantilla

Tiempo de refresco segundos

Tiempo de reintento de transferencia segundos

Tiempo de expiración segundos

Tiempo-que-está-viva por Defecto segundos

Tras ello nos dirigiremos a la primera zona maestra creada, y en el menú que aparece, accederemos al apartado Direcciones. Completamos los campos poniendo el nombre del servidor en el campo nombre, y su dirección IP en el campo dirección, las demás opciones se quedarán como por defecto.

The screenshot shows the 'Dirección Registros' (Address Registrations) page. At the top right are three buttons: 'Aplicar zona' (Apply zone), 'Aplicar configuración' (Apply configuration), and 'Stop BIND'. Below the buttons is a link 'En nnl'. The main area has a title 'Añadir Registro Dirección' (Add Address Registration). It contains fields for 'Nombre' (Name) with a text input, 'Tiempo de vida' (TTL) with a dropdown set to 'Por defecto' (Default) and 'segundos' (Seconds), 'Dirección' (Address) with a text input and a browse button, and checkboxes for '¿Actualizar?' (Update?) with options 'Si' (Yes) and 'Sí (y reemplazar las existentes)' (Yes (and replace existing)), and 'Inversas?' (Inverses?) with 'No' (No). A 'Crear' (Create) button is at the bottom left. Below this is a search bar 'Mostrar registros coincidentes:' (Show matching records:) and a 'Buscar' (Search) button. A link 'Seleccionar todo | Invertir selección.' (Select all | Invert selection.) is present. A table lists existing registrations:

Nombre	TTL	Dirección
<input type="checkbox"/> uservidor.nnl.	Por defecto	192.168.176.100
<input type="checkbox"/> clientennl.nnl.	Por defecto	192.168.176.111
<input type="checkbox"/> mail.nnl.	Por defecto	192.168.176.100

Below the table are links 'Seleccionar todo | Invertir selección.', 'Eliminar seleccionado' (Delete selected), and '¿Eliminar reversos también?' (Also delete reverses?). At the bottom are links 'Regresar a lista de zonas' (Return to zones list) and 'Regresar a tipos de registro' (Return to registration types).

Tras ese paso, repetiremos lo anterior cambiando el campo Nombre por el nombre del cliente y otro con mail, poniendo la dirección IP del cliente y del servidor respectivamente, tras acabar, nos dirigimos al botón Índice de Módulo.

Una vez hecho eso, nos dirigiremos al apartado Alias de nombre, ahí completamos el campo nombre con www y el campo Nombre Real con el nombre del servidor y luego haremos clic en crear. De la misma forma lo haremos con dns y ftp. Luego haremos click en Índice de Módulo.

[Indice de Módulo](#)[Aplicar zona](#)[Aplicar](#)[configuración](#)[Stop BIND](#)

Nombre de Alias Registros

En nnl

Añadir Registro Nombre de Alias

Nombre	<input type="text"/>	Tiempo de vida	<input checked="" type="radio"/> Por defecto	<input type="radio"/> <input type="text"/>
Nombre Real	<input type="text"/>	(Los nombres absolutos deben de terminar con un .)		

[Crear](#)Mostrar registros coincidentes: [Buscar](#)[Seleccionar todo.](#) | [Invertir selección.](#)

Nombre	TTL	Nombre Real
<input type="checkbox"/> www.nnl.	Por defecto	uservidor.nnl.com
<input type="checkbox"/> dns.nnl.	Por defecto	uservidor.nnl.com
<input type="checkbox"/> ftp.nnl.	Por defecto	uservidor.nnl.com

[Seleccionar todo.](#) | [Invertir selección.](#)[Eliminar seleccionado](#)[!\[\]\(84c1da4fabe1f32477a07218654167dc_img.jpg\) Regresar a lista de zonas](#) | [Regresar a tipos de registro](#)

Nos dirigimos a Servidor de Correo, ahí rellenamos el campo Nombre con mail en el campo Servidor de correo escribimos el nombre del servidor y, en Prioridad ponemos 10.

Añadir Registro Servidor de Correo

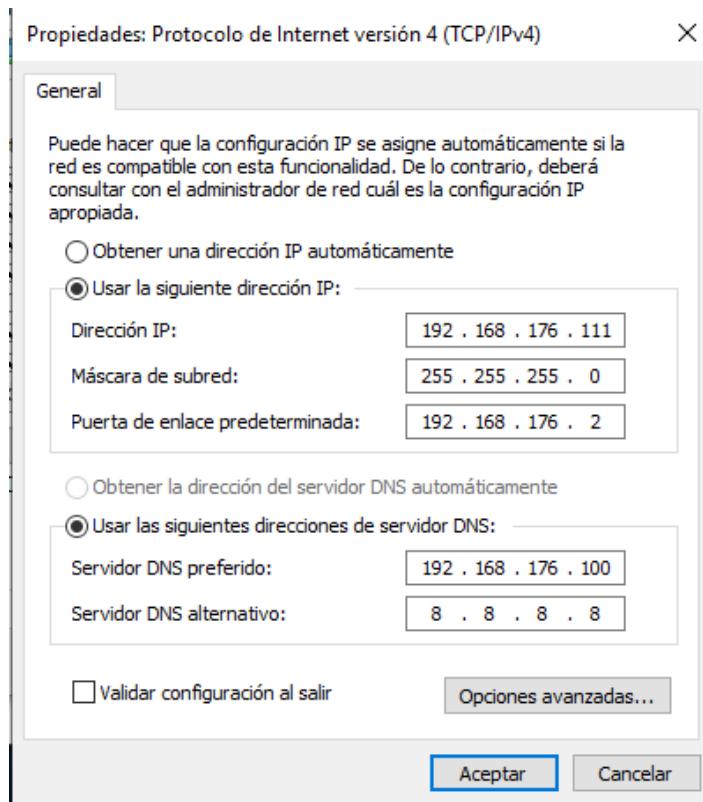
Nombre	<input type="text"/>	Tiempo de vida	<input checked="" type="radio"/> Por defecto	<input type="radio"/> <input type="text"/>
Servidor de Correo	<input type="text"/>	Prioridad	<input type="text"/>	

[Crear](#)Mostrar registros coincidentes: [Buscar](#)[Seleccionar todo.](#) | [Invertir selección.](#)

Nombre	TTL	Prioridad	Servidor de Correo
<input type="checkbox"/> mail.nnl.	Por defecto	10	uservidor.nnl.com

Cliente

Una vez en el cliente, nos dirigimos a *Centro de Redes y Recursos compartidos*, una vez ahí vamos a *Ver estado* y en la ventana que se abre damos click a *Propiedades*, marcamos la opción de *usar la siguiente dirección IP*(Ya que hemos decidido usar IP fija) y rellenamos los campos con las direcciones correspondientes, poniendo en el campo *Servidor DNS preferido* la dirección IP de nuestro servidor DNS



Cuando hayamos completado los campos necesarios, haremos click en Aceptar y abriremos el terminal. En él, haremos ping al servidor para comprobar que lo encuentra y que el servicio funciona correctamente.

```

C:\Users\nnl0s>ping uservidor.nnl.com

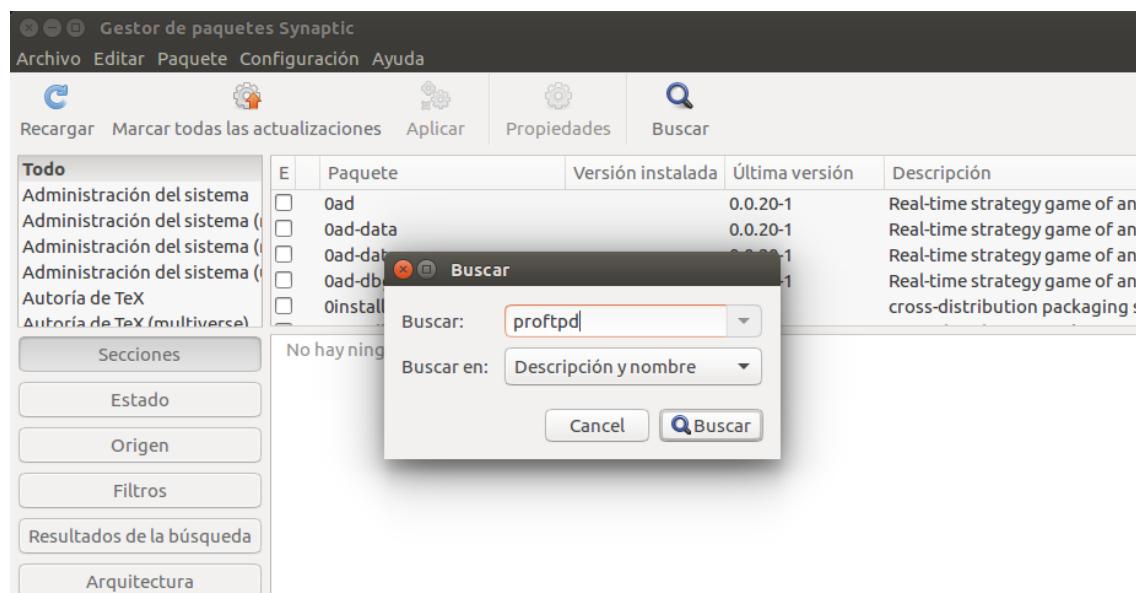
Haciendo ping a uservidor.nnl.com [173.255.194.134] con 32 bytes de datos:
Respuesta desde 173.255.194.134: bytes=32 tiempo=158ms TTL=128

Estadísticas de ping para 173.255.194.134:
  Paquetes: enviados = 1, recibidos = 1, perdidos = 0
              (0% perdidos),
  Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 158ms, Máximo = 158ms, Media = 158ms
Control-C
^C
C:\Users\nnl0s>

```

Servidor ftp

Accederemos a una sesión gráfica GNOME en el servidor, arrancaremos el gestor de paquetes Synaptic y haremos click en la opción buscar, en la barra de búsqueda de la ventana que se abre, escribiremos proftpd y haremos click en buscar.



Seleccionamos proftpd-basic y lo marcamos para instalar, eso abrirá una ventana de diálogo para preguntar si quieras instalar otros paquetes adicionales, haz click en el botón Marcar. Seguidamente haremos click en el botón Aplicar, se abrirá una ventana de resumen de los paquetes que vas a instalar, haz click en Aplicar. Acto seguido, una vez acabada la instalación, se abrirá otra ventana llamada Debconf en servidor. Selecciona independiente de la lista desplegable y haz click en Adelante. En la ventana de Cambios aplicados haz click en Cerrar.

Accederemos a Webmin, del mismo modo que antes, y volveremos a hacer click en el botón Recargar Módulos, desplegaremos el apartado Sistema del menú lateral y haremos click en Usuarios y grupos

Usuarios y Grupos

Ahí crearemos un nuevo usuario llamado adminweb, rellenando los campos como en la figura a continuación.

Detalles de Usuario

Nombre de Usuario	adminweb
ID de Usuario	<input checked="" type="radio"/> Automático <input type="radio"/> Calculado <input type="radio"/> 1001
Nombre Real	administrador www.nnl.com
Directorio inicial	<input type="radio"/> Automático <input checked="" type="radio"/> Directorio /var/www-anonimo
Shell	/bin/false
Contraseña	<input type="radio"/> No se pide contraseña <input type="radio"/> No está permitido el login <input checked="" type="radio"/> sx20SX20 Contraseña normal <input type="radio"/> Clave de acceso pre- encriptada <input checked="" type="checkbox"/> Login temporalmente deshabilitado

Opciones de Contraseña

En el apartado Al Crear... seleccionaremos las casillas de la siguiente forma:

Al Crear...

¿Crear directorio inicial? Si No

¿Copiar archivos a directorio inicial? Si No

¿Crear usuario en otros módulos? Si No

Ahora buscaremos el usuario ftp de la lista de usuarios, cambiaremos el directorio inicial por /var/www-anónimo, dejaremos el resto de valores por defecto y haremos click en el botón Salvar.

A continuación accedemos al enlace Servidor ProFTPD, y luego al Servidor por defecto.

▼ **Servidores**

- [Lectura de Correo de Usuarios](#)
- [Servidor de DNS BIND](#)
- [Servidor ProFTPD](#)

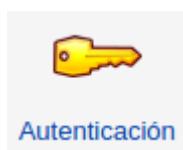
Dentro del módulo Servidor por defecto, accederemos a Archivos y Directorios.



Seleccionamos Directorios de inicio de la sección Directorios de Chroot y hacemos click en Salvar.

Directorios **Directorio de Chroot** Ninguna Directorio de inicio

Ahora accedemos a la sección Autenticación.



Accedemos al enlace Regresar a menú principal, y hacemos click en Aplicar cambios. Tras ello accedemos a FTP anónimo.



Rellenamos los campos como en la captura a continuación y hacemos click en Crear.

¿Sólo permitir login a usuarios con shell válidos?

Si No Valores por defecto

Volveremos a acceder a Autenticación.

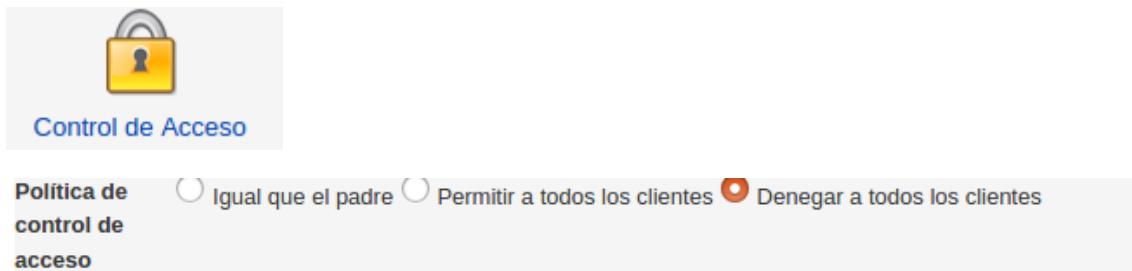


Escribimos un asterisco (*) en el cuadro de texto Trayectoria de directorio y hacemos click en el botón Crear.

Añadir opciones de por-comando para...

Comandos FTP WRITE

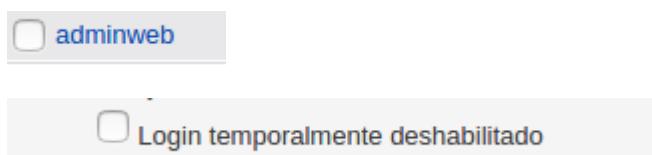
Escribimos la orden WRITE en Comandos FTP y hacemos click en Crear. Hacemos click en el enlace Control de Acceso. Seleccionamos la opción Denegar a todos los clientes del control Política de control de acceso, y hacemos click en Salvar.



Volvemos a la sección Usuarios y Grupos del menú lateral de Webmin

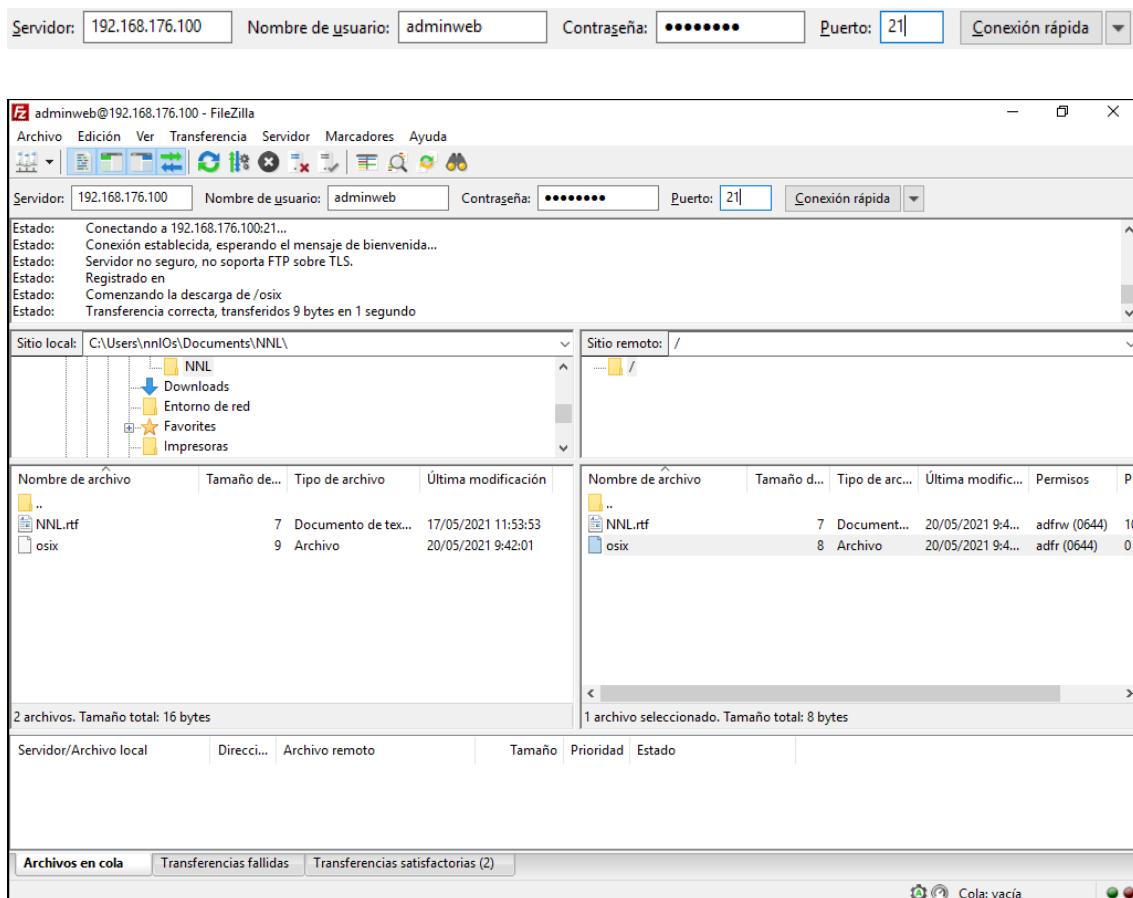


Ahí buscamos el usuario Adminweb y habilitamos nuevamente el login.



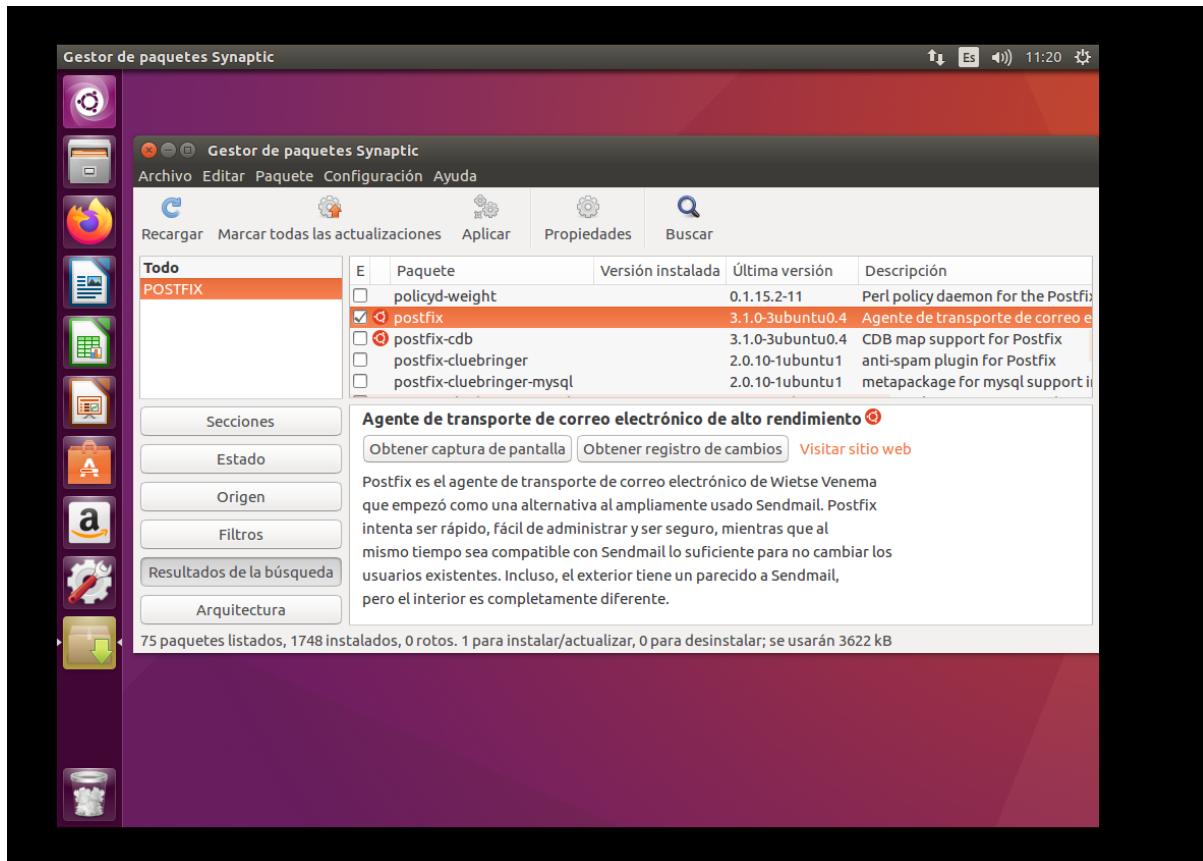
Cliente

En el cliente abrimos una sesión gráfica GNOME y accedemos a Filezilla. Rellenamos el campo Servidor con la dirección IP de nuestro servidor, el campo Nombre de usuario con adminweb y el campo contraseña con la contraseña de nuestro servidor y el campo puerto con 21 que es el puerto por defecto, acto seguido pinchamos en Conexión rápida.



Para subir y descargar archivos es tan sencillo como buscarlo, hacer click derecho y pinchar en subir/descargar respectivamente.

Servidor de correo Thunderbird



Para la configuración del servicio de correo tenemos que instalar desde synaptic tanto postfix como dovecot-pop3 y todas sus salientes.

Una vez lo instalamos lo tendremos que configurar en webmin desde el servidor.

Para empezar deberíamos crear un usuario de prueba para usarlo de receptor del primer mensaje y a su vez lo usaremos para iniciar sesión en thunderbird

1955 en servidor (Ubuntu Linux 16.04.2) - Mozilla Firefox

Webmin 1.955 en servidor | +

Historico de sesiones de

<input type="checkbox"/>	dnsmasq	112	nogroup	dnsmasq	/var/lib/misc	/bin/false
<input type="checkbox"/>	colord	113	colord	colord colour management daemon	/var/lib/colord	/bin/false
<input type="checkbox"/>	speech-dispatcher	114	audio	Speech Dispatcher	/var/run/speech-dispatcher	/bin/false
<input type="checkbox"/>	hplip	115	lp	HPLIP system user	/var/run/hplip	/bin/false
<input type="checkbox"/>	kernoops	116	nogroup	Kernel Oops Tracking Daemon	/	/bin/false
<input type="checkbox"/>	pulse	117	pulse	PulseAudio daemon	/var/run/pulse	/bin/false
<input type="checkbox"/>	rtkit	118	rtkit	RealtimeKit	/proc	/bin/false
<input type="checkbox"/>	saned	119	saned		/var/lib/saned	/bin/false
<input type="checkbox"/>	usbmux	120	plugdev	usbmux daemon	/var/lib/usbmux	/bin/false
<input type="checkbox"/>	adminservidor	1000	adminservidor	adminservidor	/home/adminservidor	/bin/bash
<input type="checkbox"/>	bind	121	bind		/var/cache/bind	/bin/false
<input type="checkbox"/>	proftpd	122	nogroup		/run/proftpd	/bin/false
<input type="checkbox"/>	ftp	123	nogroup		/var/www-anonimo	/bin/false
<input type="checkbox"/>	adminweb	1001	users	administrador www.nnl.com	/var/www-anonimo	/bin/false
<input type="checkbox"/>	dovecot	124	dovecot	Dovecot mail server	/usr/lib/dovecot	/bin/false
<input type="checkbox"/>	dovennull	125	dovennull	Dovecot login user	/nonexistent	/bin/false
<input type="checkbox"/>	postfix	126	postfix		/var/spool/postfix	/bin/false
<input type="checkbox"/>	prueba	1002	users	prueba@nnl	/var/mail	/bin/sh

Seleccionar todo. | Invertir selección. | Crear un nuevo usuario
 Borrar Usuarios Seleccionados Deshabilitar Seleccionados Habilitar Seleccionados

Mostrar logins por Todos los usuarios Solo usuario ... Muestra los inicios de sesión recientes de uno o todos los usuarios de Unix que se han

Mozilla Firefox parece lento... al... Conocer más sobre cómo acelerar No preguntar de nuevo X

Una vez creado usaremos el usuario admin para enviarle un correo si todo va bien deberían salir los bytes correspondientes al correo

Configuración de
Módulo

Leer correo de usuario

Servidor de correo: Postfix

Buzones de usuario			
_apt	adminservidor	adminweb	avahi
avahi-autoipd	backup	bin	bind
colord	daemon	dnsmasq	dovecot
dovenuull	ftp	games	gnats
hplip	irc	kernooops	lightdm
list	lp	mail	man
messagebus	news	nobody	postfix
proftpd	proxy	prueba (831 bytes en 1)	pulse
root	rtkit	saned	speech-dispatcher
sync	sys	syslog	systemd-bus-proxy
systemd-network	systemd-resolve	systemd-timesync	usbmux
uucp	uuidd	whoopsie	www-data

1.955 en servidor (Ubuntu Linux 16.04.2) - Mozilla Firefox

Webmin 1.955 en servidor X + https://localhost:10000

Sistema de Archivos
Históricos (Logs) del Sistema
Paquetes de Software
Procesos en curso
Programas tipo MIME
Páginas del Manual
Rotación de Históricos (Logs)
Sistemas de Archivo de Disco y Red
Tareas Planificadas (Cron)
Usuarios y Grupos

↓ Servidores
Configuración de Postfix
Dovecot: Servidor de IMAP/POP3
Lectura de Correo de Usuarios
Servidor de DNS BIND
Servidor ProFTPD
↓ Otros
↓ Red
↓ Hardware
↓ Cluster
↓ Módulos sin usar

Buscar:

Indice de Módulo

Correo de Usuario

Mensajes 1 a 1 de 1 en /var/mail/prueba Cambio

Borrar mensajes seleccionados Marcar los seleccionados como: Leídos Remitir seleccionado

Mover a: Copiar a: ... Componer nuevo correo

Seleccionar todo. | Invertir selección.

Desde	Fecha	Medida	Asunto
<input type="checkbox"/> adminservidor@servidor	2021/05/21 08:38	0.81 KIB	primer mail

Seleccionar todo. | Invertir selección.

Borrar mensajes seleccionados Marcar los seleccionados como: Leídos Remitir seleccionado

Mover a: Copiar a: ... Componer nuevo correo

Mensajes 1 a 1 de 1 en /var/mail/prueba Cambio

Buscar: Búsqueda Avanzada Eliminar todos

Regresar a Lista de usuarios

Para poder entrar en thunderbird y tener algo de seguridad configuraremos el SSL para el thunderbird

Configuración SSL

Opciones de modo SSL de IMAP y POP3

- Archivo de certificado SSL: Valores por defecto /etc/dovecot/nnl.pem
- Archivo de clave privada SSL: Valores por defecto /etc/dovecot/nnl.pem
- Contraseña para archivo clave: Ninguno necesario
- Archivo de certificado de CA del cliente SSL: Valores por defecto
- Intervalo entre la regeneración de parámetro de SSL: Valores por defecto horas

¿No permitir autenticación en texto plano en modo en modo no SSL?

- Si No Valores por defecto (Si)

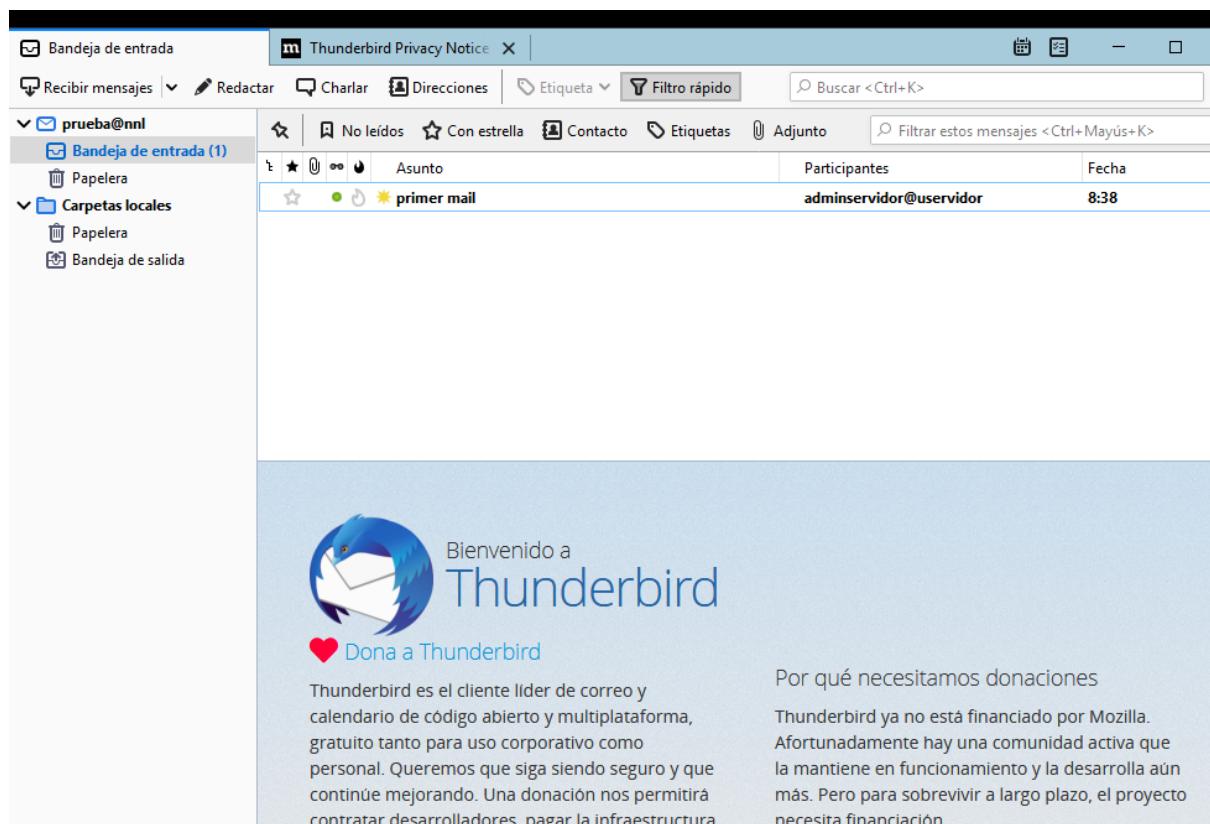
Guardar

Indice de Módulo

Indice de Servidores Webmin

- Sistema
 - Actualizaciones de paquetes de software
 - Arranque y apagado
 - Autenticación PAM
 - Cambio de Contraseñas
 - Copia de Seguridad de Sistema de Archivos
 - Históricos (Logs) del Sistema
 - Paquetes de Software
 - Procesos en curso
 - Programas tipo MIME
 - Páginas del Manual
 - Rotación de Históricos (Logs)
 - Sistemas de Archivo de Disco y Red
 - Tareas Planificadas (Cron)
 - Usuarios y Grupos
- Servidores
 - Configuración de Postfix
 - Dovecot: Servidor de IMAP/POP3
 - Lectura de Correo de Usuarios
 - Servidor de DNS BIND
 - Servidor ProFTP
 - Otros

Por último si todo es correcto, la configuración del ssl está bien y aplicada + los usuarios son correctos y el dns está bien ya que las dos máquinas se reconocen deberías poder entrar en thunderbird y ver el mensaje del administrador y le podríais contestar desde el propio thunderbird



Creación del gestor Joomla

A screenshot of the Osix website. The header features a small green circular logo on the left, followed by the word "Osix" in a large, bold, black sans-serif font. To the right of the logo are four smaller links: "Sobre Nosotros", "¿Qué Ofrecemos?", "Marketing", and another "Osix" link. The main content area has a light gray background and contains a large, stylized circular logo for "OSIX" in the center. The logo consists of concentric circles with horizontal wavy lines in shades of blue and green.



Primero de todo en nuestra página de Joomla podremos encontrar una cabecera en la home con el logo de nuestra empresa, también tenemos en la parte superior derecha los apartados que hay en el Joomla.

También tenemos una función que sirve para que el logo y el menú permanezcan cuando quieras cuando deslices por las páginas principales o por los artículos.

The screenshot shows a Joomla website with a header containing the logo, 'Osix', 'Sobre Nosotros', '¿Qué Ofrecemos?', and 'Marketing'. Below the header are three main menu items:

- Redes Sociales**: Includes links to Instagram (@osix.es), Facebook (@osix.es), Twitter (@osix.es), and a page link to osix.es.
- Facilidades de Pago**: Describes payment methods available via virtual payment on the website using credit cards like Visa and MasterCard.
- Packs**: Details service packages for entrepreneurs, listing various services with their prices:
 - Gestión de recursos humanos: 100€
 - Almacenamiento en la red corporativa: 100€
 - Almacenamiento en los equipos de trabajo: 100€
 - Almacenamiento en la nube: 100€
 - Aplicaciones permitidas: 100€
 - Clasificación de la información: 100€
 - Concienciación y formación: 100€
 - Continuidad de negocio: 100€
 - Cumplimiento legal: 100€
 - Plan director de seguridad: 100€
 - Relación con proveedores: 100€

Precio Final: 1100€

At the bottom of the page are navigation icons for page 1, 2, and more.

También tenemos en la parte inferior de nuestro Joomla tres apartados principales, en uno nos aparecen las redes sociales de nuestra empresa, también se puede hacer click encima de cada título donde te explica o hace 5 céntimos del apartado.

Para añadir, tenemos dos apartados más, uno de ellos es el de las facilidades de pago, donde te hace una breve explicación de cómo puedes pagar nuestros servicios, las tarjetas de crédito disponibles, y una pequeña explicación de la seguridad de pago que tenemos en nuestra empresa.

Y el otro apartado es el de packs, en el cual el usuario que entre en nuestro Joomla, podrá ver todos los servicios de nuestra empresa, juntamente con los precios de este, por ejemplo, las políticas para el empresario, para el trabajador o para el usuario, cada uno de ellos con un precio diferente dependiendo de los servicios que incluya, también falta aclarar, que cada servicio que se ofrece como

pack también está disponible de manera individual al precio que aparece al lado de él mismo.



[Osix](#) [Sobre Nosotros](#) [¿Qué Ofrecemos?](#) [Marketing](#)

Osix

Osix fue fundada en la ciudad de Lleida en España en el transcurso de los años 2020 y 2021.

La sede de la empresa se encuentra en su ciudad natal que es la propia ciudad de Lleida.

En la segunda página de nuestro Joomla podremos encontrar una pequeña explicación de quiénes somos y de cómo fue creada nuestra empresa, manteniendo siempre el menú en la parte superior derecha y también el logo de nuestra empresa permanente y remarcado arriba a la izquierda, que también sirve para volver a la página principal/home.



Donde nos ubicamos

Somos una empresa de la ciudad de Lleida en España, con la sede ubicada en la misma ciudad natal, exactamente en la calle Anselm Clavé nº12.

Productos

Placas base:



Fuentes de alimentación:



Gráficas:



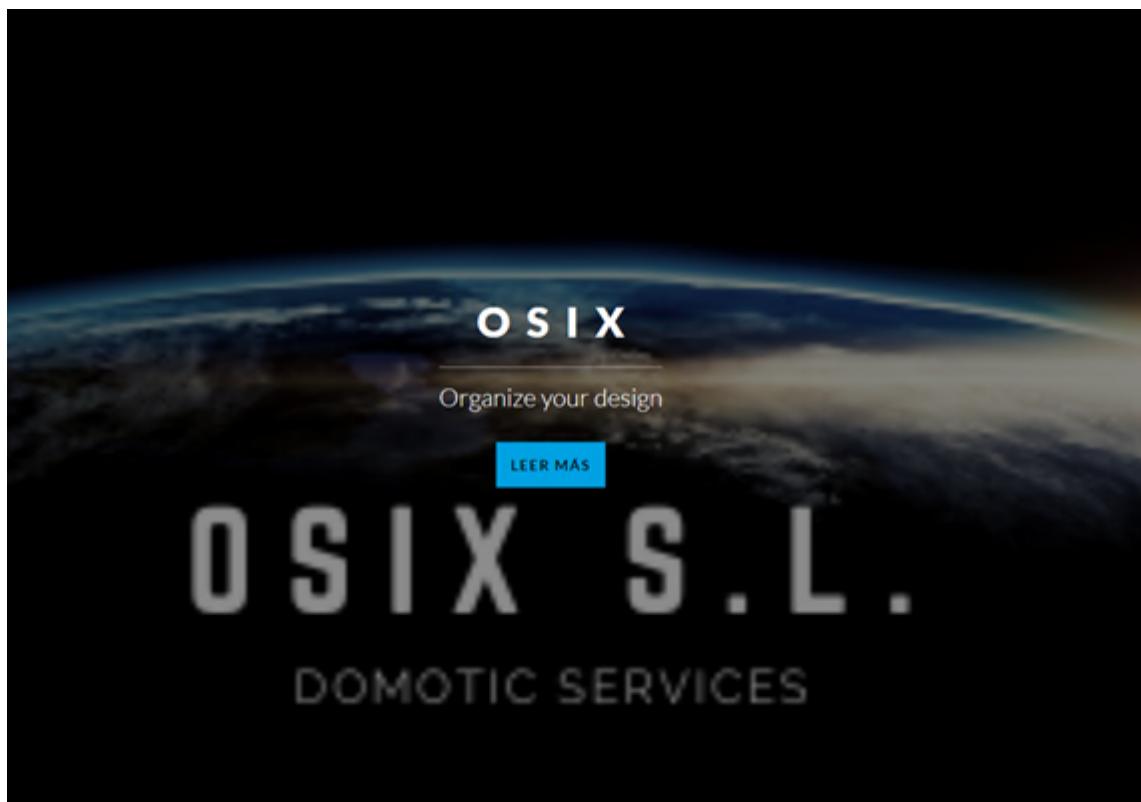
Cajas ordenadores:



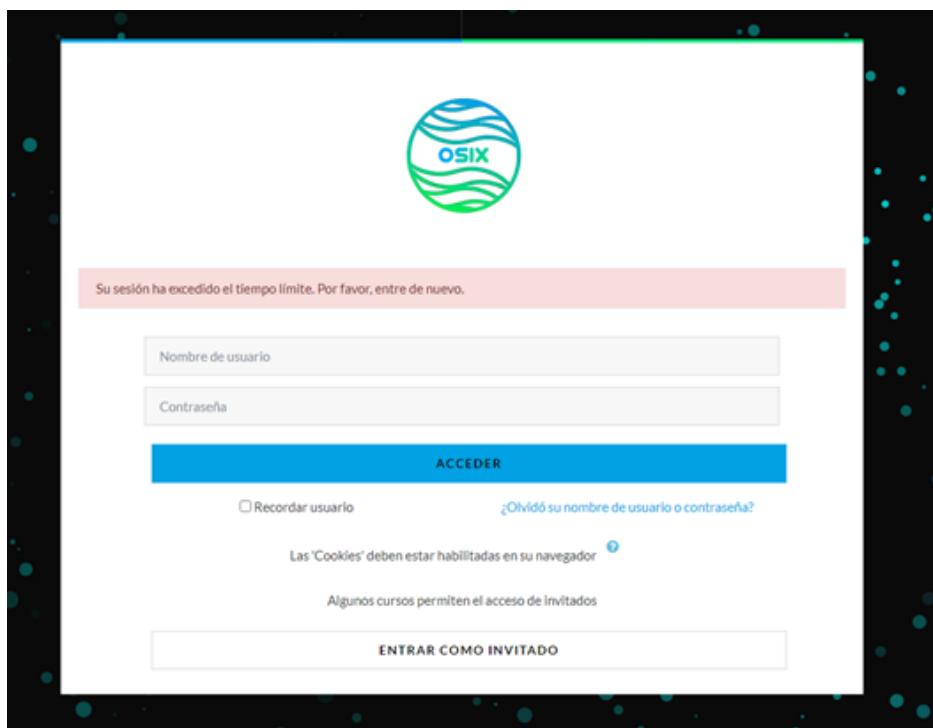
También podremos encontrar la ubicación de nuestra sede en la ciudad natal de nuestra empresa, que es Lleida, exactamente en la calle Anselm Clavé nº12.

Al lado de esta pequeña explicación con la ubicación de la empresa, se encuentra nuestro catálogo de próximos productos que se podrán encontrar, y que ahora mismo tenemos en desarrollo.

Creación de cursos en Moodle



Primero de todo en nuestra página principal de nuestro Moodle encontraremos de fondo las letras de osix con nuestro logo y un apartado de leer más para ir a la descripción y donde se podrá ver todos los apartados del Moodle.



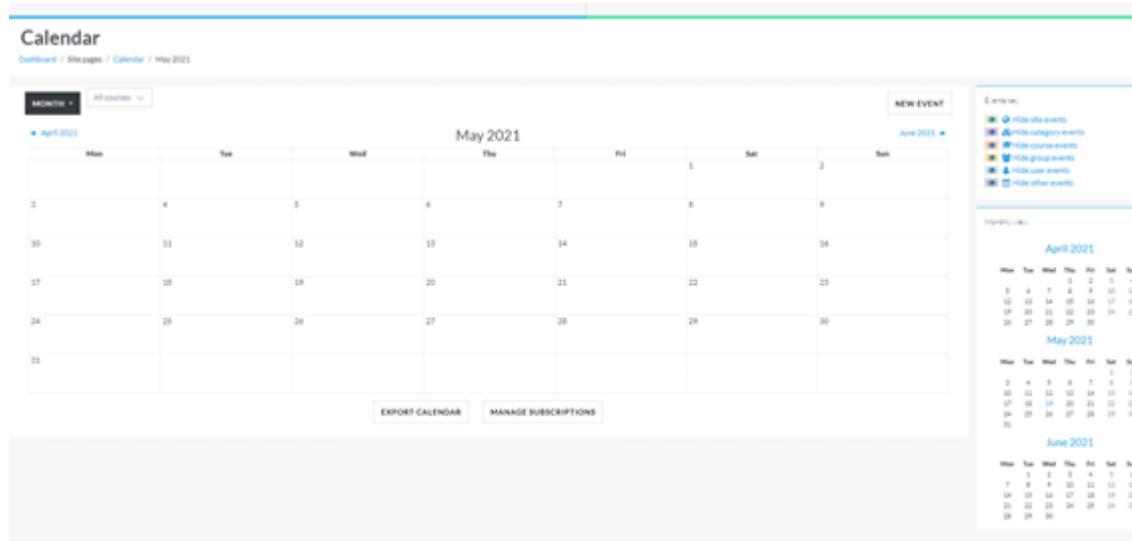
También podríamos ver el login de los usuarios en nuestro Moodle, donde si tuvieran las credenciales podrían acceder a nuestros cursos que tuvieran contratados y aparte ver los cursos que tienen disponibles.

Cursos formativos de Osix

Cursos disponibles

 Marketing Digital Profesor: Alejandro Berengena VER MÁS	 Programación de videojuegos Profesor: Alejandro Berengena VER MÁS	 Diseño de videojuegos Profesor: Alejandro Berengena VER MÁS
--	--	---

En este apartado podríamos encontrar los cursos disponibles que ofrece osix, donde si le diéramos en leer más podríamos ver una pequeña descripción de los cursos que se ofrecen en el momento.



También aparece un calendario donde aparecerán todas las tareas del curso a realizar con la fecha de entrega y la hora. Aparte dependiendo del color que aparezca la tarea es dependiendo del nivel.

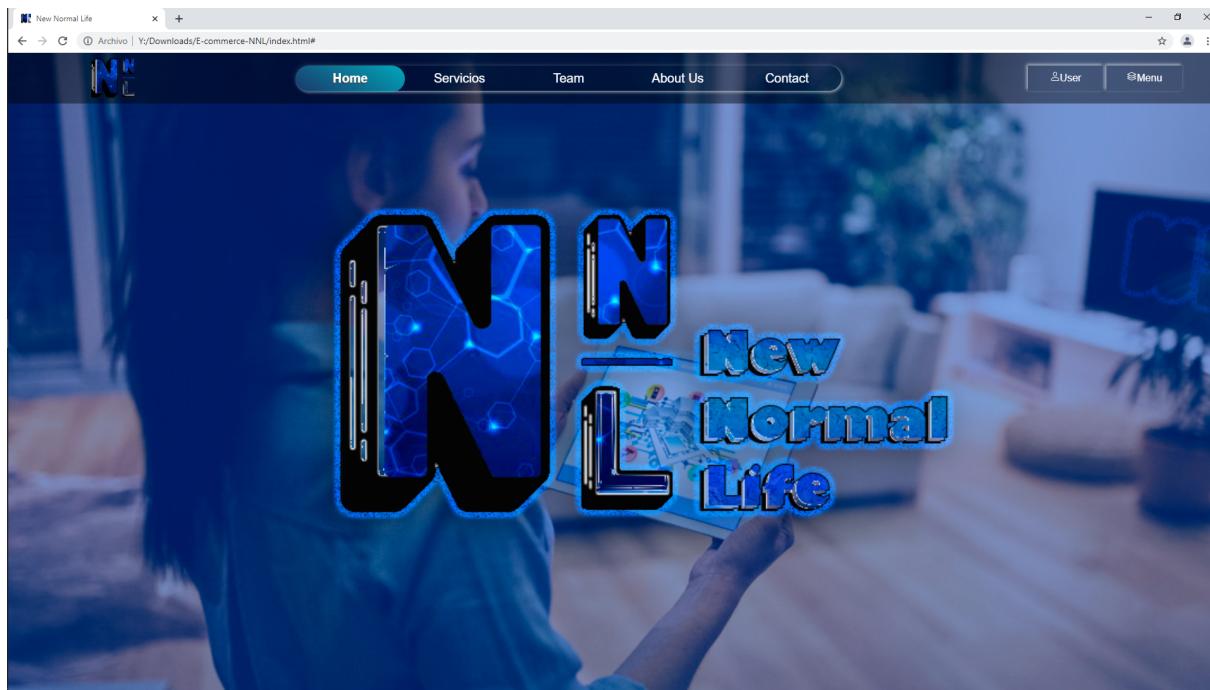
Creación de la página web

Como página web principal de New Normal Life, tenemos creada y establecida una beta de la misma, la cual solo consta del front-end de la propia web, este front end queríamos hacerlo solamente en lenguaje puro, tanto html puro, como css puro, no hemos querido integrar ningún tipo de programación de javascript ya que pensábamos que sería demasiado avanzado para el proyecto.

Dentro de toda la estructura de nuestro front-end, podemos encontrar un indice.html principal con sus propio estilo.css, como páginas secundarias, tenemos la página de login de la empresa y la página de registro, que comparten el mismo código de css, a parte tenemos una plantilla preparada para hacer un menú para los usuarios en una página aparte con su propio estilo.css, finalmente, tenemos un que nos lleva a cuatro diferentes páginas web con la información de cada uno de los fundadores de New Normal Life.

La web de New Normal Life está en un apartado Alpha, el cual no dispone aún de una web funcional y bien diseñada para móviles ni tabletas, tampoco tiene ninguna base de datos acoplada a ella.

Inicio



Al entrar a la página vemos un header que ocupa todo el amplio de la pantalla, está basado en que puedas moverte por toda la página web, que es One-Page. Con el menú central podemos bajar y subir por toda la web y podemos volver arriba de la misma con el propio botón de home o clicando en el logo de NNL, también podemos acceder al login de la web con el botón de "User" o acceder al menú con el botón de "Menú"

Tenemos un background con una foto tranquila intentando hacerte sentir tranquilo y el nombre de nuestra empresa en un blanco básico en medio de la pantalla.

Teoría del NavBar

```
<!--navegacion principal-->
<header>
    <a href="#" class="logo">
        
    </a>
    <div class="wrapper">
        <nav>
            <input type="radio" name="tab" id="Home" checked>
            <input type="radio" name="tab" id="About">
            <input type="radio" name="tab" id="Services">
            <input type="radio" name="tab" id="ContactUs">
            <input type="radio" name="tab" id="Team">
            <label for="Home" class="Home"><a href="#home">Home</a></label>
            <label for="About" class="About"><a href="#servicio">Servicios</a></label>
            <label for="Services" class="Services"><a href="#team">Team</a></label>
            <label for="ContactUs" class="ContactUs"><a href="#about">About Us</a></label>
            <label for="Team" class="Team"><a href="#footer">Contact</a></label>
            <div class="tab"></div>
        </nav>
    </div>
    <div class="user">
        <nav>
            <div class="nav left">
                <div class="btn left" id="left">
                    <a href="Login/login.html">
                        <ion-icon name="person-outline"></ion-icon>User
                    </a>
                    <div class="d1"></div>
                    <div class="d2"></div>
                    <div class="d3"></div>
                    <div class="d4"></div>
                </div>
            </div>
            <div class="nav left">
                <div class="btn left" id="right">
                    <a href="Menu/Menu.html">
                        <ion-icon name="layers-outline"></ion-icon>Menu
                    </a>
                    <div class="d1"></div>
                    <div class="d2"></div>
                    <div class="d3"></div>
                    <div class="d4"></div>
                </div>
            </div>
        </nav>
    </div>
</header>
```

En el html, para hacer la animación de la navegación principal sin usar javascript, hemos necesitado crear por cada label, un input que nos ayuda junto a el css a hacer la propia animación, estos labels los relacionamos entre los inputs para que detecten cuando clicas en ellos, al final de la navegación tenemos un div llamado tab que es la propia forma del fondo del menú.

En la derecha del header, los botones de user y menú, son varios divisores donde dentro esta el link para ir a los diferentes sitios, esto esta hecho asi porque

tenemos cuatro animaciones que rodean el botón principal, los cuales son los 4 divs que tiene cada botón, podríamos haber puesto un botón pero no pensamos en ello en el momento y no funcionaban varios intentos.

```
/*navegacion principal*/

header {
    position: fixed;
    top: 0;
    left: 0;
    width: 100%;
    height: 20px;
    display: flex;
    justify-content: space-between;
    align-items: center;
    place-items: center;
    text-align: center;
    transition: 0.6s;
    padding: 40px;
    z-index: 100000;
    background-color: #rgba(0, 0, 0, 0.432);
}

header .logo {
    position: relative;
    margin-left: 40px;
    transition: 0.6s;
    width: 170px;
}

.wrapper {
    height: 40px;
    width: 45vw;
    line-height: 40px;
    border-radius: 50px;
    box-shadow: 2px 2px 5px #rgba(255, 255, 255, 0.603), -3px -3px 7px #rgba(255, 255, 255, 0.05);
    margin-right: 40px;
}

header .wrapper nav {
    position: relative;
    display: flex;
}

header .wrapper nav label {
    flex: 1;
    width: 100%;
    z-index: 1;
    position: relative;
    cursor: pointer;
}
```

en el css simplemente ponemos que el header sea fijo para que pueda moverse por la pantalla y distribuimos el espacio con la opción de flex, también lo ponemos delante de cualquier cosa de la web con z-index y vemos que tamaños y algunas otras opciones del logo y la navegación principal.



Sección Servicios

Servicios de domotica para todos los usuarios					
Camaras Desde 50 €	Sensores Desde 45 €	Seguridad Desde 70 €			
Instalación	Instalación	Instalación			
Configuración	Configuración	Configuración			
Implementación	Implementación	Implementación			
Reparación	Reparación	Reparación			
Luces Desde 30 €	Ventanas Desde 80 €	Persianas Desde 60 €			
Instalación	Instalación	Instalación			
Configuración	Configuración	Configuración			
Implementación	Implementación	Implementación			
Reparación	Reparación	Reparación			
Información	Información	Información			

Tenemos unas tarjetas modificadas con el título del paquete del servicio, el precio del mismo, y los servicios que incluye, esta sección también tiene varias animaciones sin javascript.

```

<!--tarjetas productos-->
<section class="servicios">
    <h1>Servicios tanto a particulares como a empresas recien creadas
    </h1>
    <div class="contenedor">
        <div class="linea">
            <div class="columna">
                <div class="box">
                    <div class="titulo1"><i class="fa fa-paper-plane"></i>
                        <h2>Construcción</h2>
                    </div>
                    <div class="precio">
                        <h4>2500<sup>€</sup></h4>
                    </div>
                    <div class="opciones">
                        <ul>
                            <li><i class="fa fa-check"></i>Instalación</li>
                            <li><i class="fa fa-check"></i>Configuración</li>
                            <li><i class="fa fa-check"></i>Implementación</li>
                            <li><i class="fa fa-check"></i>Creación</li>
                        </ul>
                    </div>
                    <a href="#">Información</a>
                </div>
            </div>
            <div class="columna">
                <div class="box">
                    <div class="titulo1"><i class="fa fa-paper-plane"></i>
                        <h2>Diseño</h2>
                    </div>
                    <div class="precio">
                        <h4>2000<sup>€</sup></h4>
                    </div>
                    <div class="opciones">
                        <ul>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                        </ul>
                    </div>
                    <a href="#">Información</a>
                </div>
            </div>
            <div class="columna">
                <div class="box">
                    <div class="titulo1"><i class="fa fa-paper-plane"></i>
                        <h2>Seguridad </h2>
                    </div>
                    <div class="precio">
                        <h4>1500<sup>€</sup></h4>
                    </div>
                    <div class="opciones">
                        <ul>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                            <li><i class="fa fa-check"></i>10GB space</li>
                        </ul>
                    </div>
                    <a href="#">Información</a>
                </div>
            </div>
        </div>
    </div>

```

Para los servicios tenemos cada tarjeta en su propio div, y estas están en otro div en grupos de tres, las siguientes tres están en otro div diferente.

```
.container {
  width: 100%;
}

.container h1 {
  text-align: center;
  margin-bottom: 50px;
  font-size: 38px;
  text-shadow: 0px 5px 10px rgba(168, 168, 168, 0.685);
  background: -webkit-linear-gradient(#c57242, #eff0e0);
  -webkit-background-clip: text;
  -webkit-text-fill-color: transparent;
}

/*Servicios tarjetas*/

.servicios {
  padding: 100px 0px;
  box-sizing: border-box;
  background: linear-gradient(30deg, #2fb30e, #159ba0);
}

.contenedor {
  width: 1200px;
  height: 520px;
  margin: 0 auto;
}

.contenedor .columna {
  position: relative;
  width: 400px;
  float: left;
  transition: 0.5s;
}

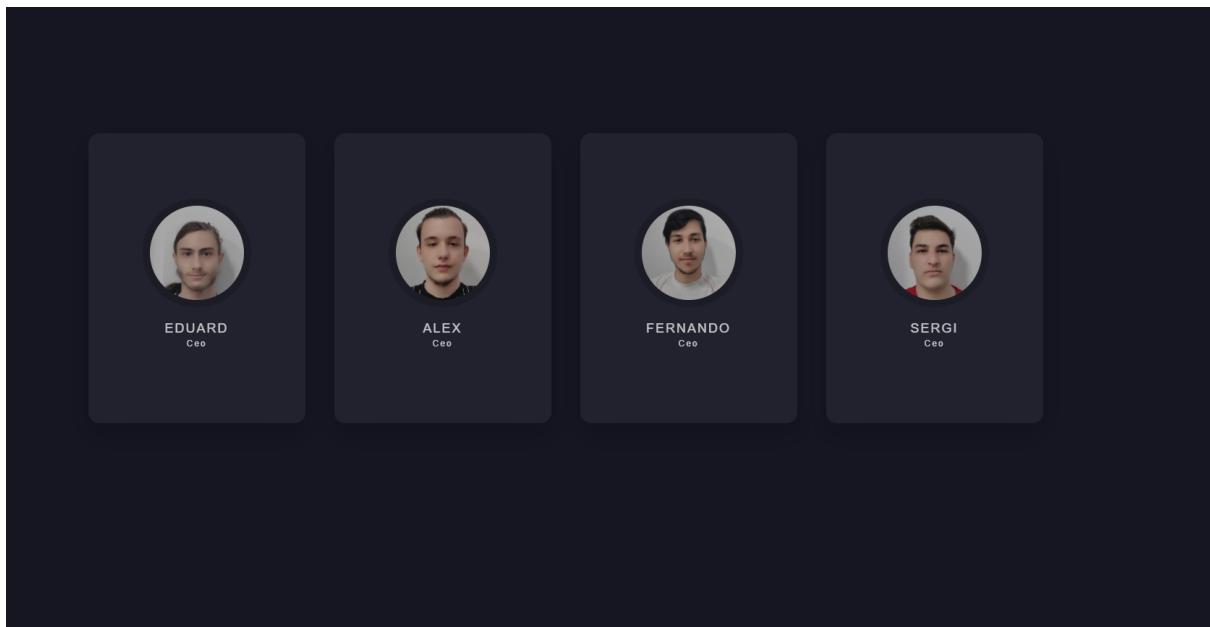
.contenedor .columna .box {
  position: relative;
  width: 320px;
  min-height: 550px;
  margin: 0 auto;
  padding: 20px;
  box-sizing: border-box;
  text-align: center;
  border-bottom-left-radius: 150px;
  border-bottom-right-radius: 150px;
  border: 1px solid rgba(255, 255, 255, 0.04);
  border-right: 1px solid rgba(255, 255, 255, 0.02);
  border-bottom: 1px solid rgba(255, 255, 255, 0.02);
  box-shadow: 0 5px 45px rgba(0, 0, 0, 0.1);
  overflow: hidden;
  transition: 0.5s;
}

.contenedor .columna .box:hover {
  transform: translateY(-20px);
}
```

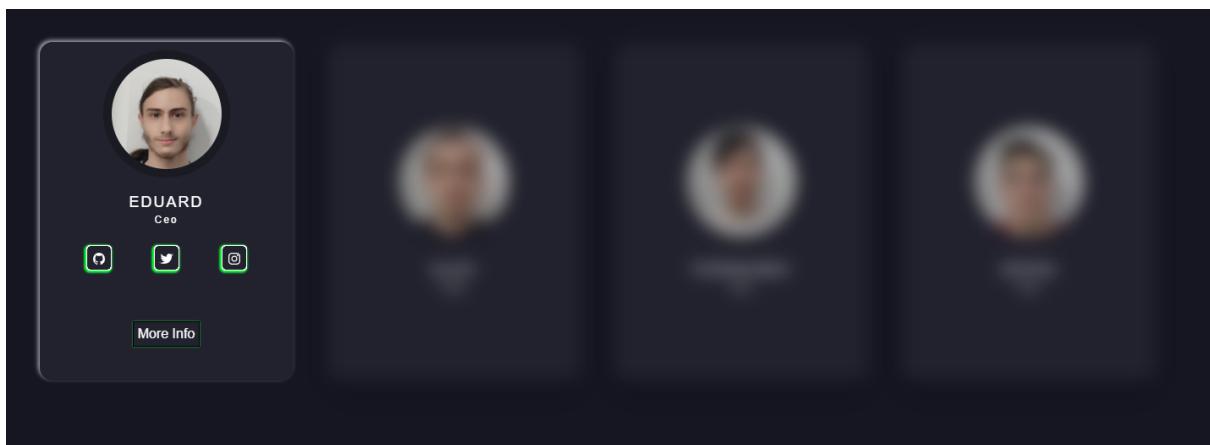
El css es un poco más complicado en este caso porque hemos de hacer la forma de la tarjeta modificando el radio de los lados, le añadimos el tiempo de la transición y el movimiento y el degradado de verde a azul del fondo.



Equipo



Queríamos diseñar algo minimalista para este trozo de la web, diseñando así una tarjeta con una portada base para cada miembro de Osix.



Al poner el ratón sobre uno de los miembros, los demás miembros se difuminan y aparece desde abajo varias redes sociales del miembro y un botón que lleva a otra pagina donde hay más información.

```

<!--cartas-->


<section class="workers">
        <div class="contenedorcarta">
            <div class="cartas">
                <div class="contenido">
                    <div class="imagen">
                        
                    </div>
                    <div class="contenidotext">
                        <h3>Eduard<br><span>Ceo</span></h3>
                    </div>
                </div>
                <ul class="cli">
                    <li style="--i:1">
                        <div class="iconos"><a href="https://github.com/kutedo2001">
                            <div class="layer">
                                <span></span>
                                <span></span>
                                <span></span>
                                <span></span>
                                <span class="fab">
                                    <ion-icon name="logo-github"></ion-icon>
                                </span>
                            </div>
                            <div class="textito" id="face">Github</div>
                        </a>
                    </div>
                    <li style="--i:1">
                        <div class="iconos"><a href="https://twitter.com/kutedo19">
                            <div class="layer">
                                <span></span>
                                <span></span>
                                <span></span>
                                <span></span>
                                <span class="fab">
                                    <ion-icon name="logo-twitter"></ion-icon>
                                </span>
                            </div>
                            <div class="textito" id="twitt">Twitter</div>
                        </a>
                    </div>
                    <li style="--i:1">
                        <div class="iconos"><a href="https://www.instagram.com/eduard_castello/">
                            <div class="layer">
                                <span></span>
                                <span></span>
                                <span></span>
                                <span></span>
                                <span class="fab">
                                    <ion-icon name="logo-instagram"></ion-icon>
                                </span>
                            </div>
                            <div class="textito">Instagram</div>
                        </a>
                    </div>
                </ul>
                <div class="more">


```

Para el html creamos un div donde están varios divs que son los diferentes contenidos de cada carta,

```

/*cartas*/
.cartitas {
  display: flex;
  justify-content: center;
  align-items: center;
  flex-wrap: wrap;
  min-height: 100vh;
  background: #161623;
}

.workers {
  position: relative;
}

.contenedorcarta {
  position: relative;
  z-index: 1;
  display: flex;
  justify-content: center;
  flex-wrap: wrap;
  margin: 40px 0;
}

.contenedorcarta .cartas {
  position: relative;
  width: 300px;
  height: 400px;
  background: rgba(255, 255, 255, 0.05);
  margin: 20px;
  box-shadow: 0 15px 35px rgba(0, 0, 0, 0.2);
  border-radius: 15px;
  display: flex;
  justify-content: center;
  filter: blur(0px);
}

.contenedorcarta .cartas .more {
  position: absolute;
  bottom: -60px;
  display: flex;
  transform: translateY(100px);
  transition: 0s;
  opacity: 0;
  text-decoration: none;
}

.contenedorcarta .cartas:hover .more {
  transform: translateY(-100px);
  transition: 0.5s;
  opacity: 1;
  box-shadow: 0px 0px 2px #14f339;
}

.contenedorcarta .cartas:hover .more a {
  text-decoration: none;
  color: #fff;
  background: transparent;
  border: 1px solid black;
  padding: 5px;
}

.contenedorcarta .cartas .more a:hover {
  background-color: #14f339;
  color: black;
}

```

El css define primero los márgenes entre las cartas de los miembros, añade el color del fondo de la sección y añade una animación al botón de más información de cada carta.

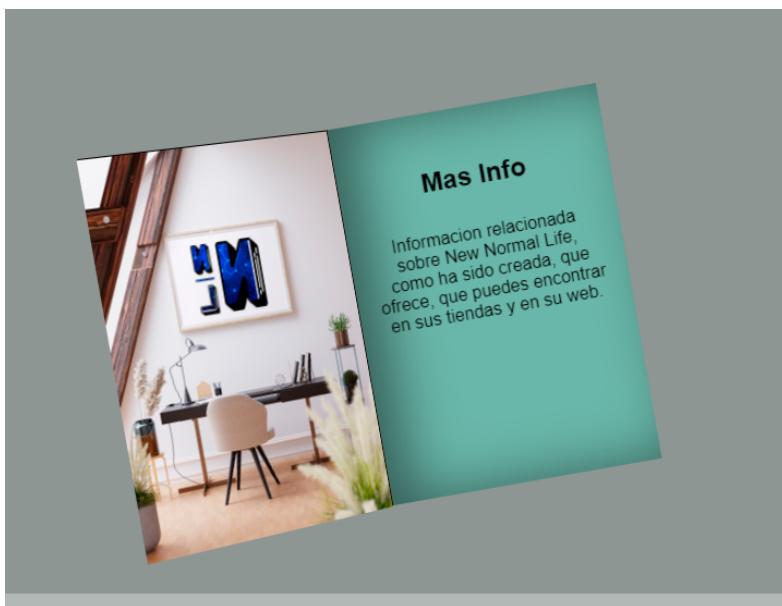


Después definimos la animación y por donde queremos que lleguen las redes sociales, y metemos blur en el div donde están las cuatro cartas para quitarlo después de la carta en la que está el ratón, añadimos que el div de la foto tenga esa circunferencia y que tenga una animación que le suba arriba de la carta.

Sobre Nosotros

The screenshot shows a website section titled "About Us". At the top, there is a large image of a workspace with a desk, chair, and a framed picture of the letters "NL". To the right of the image, the text "NEW NORMAL LIFE" is displayed. Below the image, there is a paragraph of text about the company. At the bottom, there are three social media links: Instagram (blue circle), Twitter (red circle), and GitHub (blue circle).

Esta sección tiene un pequeño texto a la izquierda donde nos presentamos, con las redes sociales de la empresa debajo de ese div y a la izquierda tenemos la portada de un libro que al ponernos en ella se abre mostrando otro texto.



La propia carta tiene una animación de 360 grados para abrirse y al abrirse tenemos un borde difuminado en negro para darle contorno al libro.

```

<!--Conocenos-->


<div class="containerAU">
        <div class="lin">
            <div class="section-title">
                <h1>About Us</h1>
            </div>
        </div>
        <div class="lin">
            <div class="inner-container">
                <div class="inner-box">
                    <div class="izqui">
                        <div class="cartAU">
                            <div class="imgca">
                                
                            </div>
                            <div class="detalles">
                                <h2>HOLI</h2>
                                <p>Lorem ipsum dolor sit amet, consectetur adipisicing elit. Officia, ratione!</p>
                            </div>
                        </div>
                    </div>
                    <div class="dere">
                        <h1>Osix Enterprise</h1>
                        <p class="tt">Osix Enterprise es una empresa dedicada a proporcionar diversos servicios a emprendedores con ganas de hacer sus ideas d negocio realidad, ayudamos en todo lo que podamos a estos emprendedores y les acompañamos en su primer año, Osix Enterprise tambien esta dedicada a la creacion y mejora de software privado para empresas que deseen adquirirlo.
                    </p>
                    <div class="rede">
                        <span>Instagram</span>
                        <span>Twitter</span>
                        <span>Github</span>
                    </div>
                    <div class="soci">
                        <a href="https://www.instagram.com/osix.es/">
                            <ion-icon class="ico insta" name="logo-instagram"></ion-icon>
                        </a>
                        <a href="https://twitter.com/kutedo19">
                            <ion-icon class="ico twi" name="logo-twitter"></ion-icon>
                        </a>
                        <a href="https://github.com/Osix-Enterprise">
                            <ion-icon class="ico fac" name="logo-github"></ion-icon>
                        </a>
                    </div>
                </div>
            </div>
        </div>
    </div>
<!--Fin de conocenos-->


```

Tenemos un div donde tenemos el h1 del título de la sección y después un div que es para la carta de la izquierda y otro div que contiene el resumen de la empresa y otro con las redes sociales.



```

/*Conocenos*/
.about-section {
  padding: 10px;
  background: #rgba(108, 119, 117, 0.527);
}

.section-title h1 {
  justify-content: center;
  align-items: center;
  text-align: center;
  padding: 25px;
  font-size: 48px;
  text-shadow: 0px 5px 10px #rgba(168, 168, 168, 0.685);
  background: -webkit-linear-gradient(120deg, ##045891e3, ##1a352fef);
  -webkit-background-clip: text;
  -webkit-text-fill-color: transparent;
}

.inner-container {
  display: flex;
  justify-content: center;
  align-items: flex-end;
  padding: 20px 50px;
  flex-wrap: 0 0 80%;
  z-index: 1;
  position: relative;
}

.izqui {
  display: flex;
  background-size: cover;
  height: 100%;
  border-radius: 2%;
  margin-left: 200px;
  margin-bottom: 20px;
  justify-content: center;
  align-items: center;
  text-align: center;
}

.cartAU {
  position: relative;
  margin-left: 50px;
  width: 250px;
  height: 350px;
  background: #rgba(89, 199, 179, 0.692);
  transform-style: preserve-3d;
  transform: perspective(2000px);
  transition: 1s;
  box-shadow: inset 30px 0 50px #rgba(0, 0, 0, 0.5);
  cursor: pointer;
}

.cartAU:hover {
  z-index: 1000px;
  transform: perspective(2000px) rotate(-370deg);
  box-shadow: inset 20px 0 50px #rgba(0, 0, 0, 0.5);
}

.cartAU .imgca {
  position: relative;
}

```

Alineamos el título de la sección y utilizamos flex para dividir las dos partes, agregamos la animación del libro dándole la rotación y el tiempo para ello en los ejes correspondientes y las animaciones de los hover de cada red social.

Footer



Debajo de la pagina principal añadimos un Footer con un fondo negro y los titulos en blanco, el texto esta en un gris claro y tenemos las redes sociales y algunos links con unas pequeñas animaciones al ponernos encima de ellas.

```
<!--Footer-->
<Footer>
  <div class="foot" id="footer">
    <div class="sect uno">
      <h2>Esta web</h2>
      <p>La web de Osix Enterprise, es un proyecto educativo y personal a partes iguales, esta, está diseñada y programada por Eduard Castelló, el CEO de la propia empresa, tambien ficticia, cada linea de codigo a sido escrita a mano, tanto de HTML como de CSS y sin utilizar ningun codigo de JavaScript, esto a sido posible gracias a el estudio y la repeticion de muchas lineas de programacion encontrada por internet. No obstante New Normal Life es una web totalmente legitima y no vulnera ningun derecho, ni la web, ni Osix Enterprise como empresa dueña de la misma.</p>
      <ul class="lis">
        <li><a href="https://www.instagram.com/eduard_castello/">
          <ion-icon class="dec" name="logo-instagram"></ion-icon>
        </a></li>
        <li><a href="https://twitter.com/kutedo19">
          <ion-icon class="dec" name="logo-twitter"></ion-icon>
        </a></li>
        <li><a href="https://github.com/kutedo2001">
          <ion-icon class="dec" name="logo-github"></ion-icon>
        </a></li>
        <li><a href="https://www.linkedin.com/in/eduard-castelló-55a62614b">
          <ion-icon class="dec" name="logo-linkedin"></ion-icon>
        </a></li>
      </ul>
    </div>
    <div class="sect dos">
      <h2>Enlaces</h2>
      <ul>
        <li><a href="#">Nosotros</a></li>
        <li><a href="#">Ayuda</a></li>
        <li><a href="#">Politica de privacidad</a></li>
        <li><a href="#">Terminos y condiciones</a></li>
        <li><a href="#">Contactar</a></li>
      </ul>
    </div>
    <div class="sect tres">
      <h2>Informacion de contacto</h2>
      <ul class="inf">
        <li><span>
          <ion-icon class="dec" name="locate-outline"></ion-icon>
          </span><span>Lleida<br>Cronista Muntaner<br>25001</span>
        </li>
        <li><span>
          <ion-icon class="dec" name="call-outline"></ion-icon>
          </span>
          <p><a href="#">+34 644166918</a><br><a href="#">973 21 21 04</a></p>
        </li>
        <li><span>
          <ion-icon class="dec" name="mail-outline"></ion-icon>
          </span>
          <p><a href="#">1secuncala@gmail.com</a></p>
        </li>
      </ul>
    </div>
  </div>
</Footer>
```

El html tiene un div principal que contiene las tres columnas del footer, con varios spans para editar esas partes en concreto de una manera específica.

```

/*Footer*/
footer {
    position: relative;
    width: 100%;
    height: auto;
    padding: 50px 100px;
    background: #111;
    display: flex;
    justify-content: space-between;
    flex-wrap: wrap;
    flex-direction: row;
}

footer .foot {
    display: flex;
    justify-content: space-between;
    flex-wrap: wrap;
    flex-direction: row;
}

footer .foot .sect {
    margin-right: 30px;
}

footer .foot .sect.uno {
    width: 40%;
}

footer .foot h2 {
    position: relative;
    color: #fff;
    font-weight: 500;
    margin-bottom: 15px;
    text-shadow: 2px -2px 4px rgba(223, 99, 99, 0.344);
}

footer .foot h2:before {
    content: '';
    position: absolute;
    bottom: -5px;
    left: 0;
    width: 50px;
    height: 2px;
    background: #f00;
}

footer p {
    color: #999;
}

.lis {
    margin-top: 20px;
    display: flex;
}

.lis li {
    list-style: none;
}

.lis li a {
    display: inline-block;
    width: 40px;
}

```

El css del footer también está dividido con flex, dividiendo cada columna con el mismo espacio entre ellas y dándole a los h2 un subrayado rojo al ponernos encima de ellos.

