Bionica Automations

Estructura lógica del Bionica Automation

Daniel Ubalde

Contenido

[1 Glosario 3](#_Toc119856247)

[2 Introducción 3](#_Toc119856248)

[3 Ubicación del proyecto 4](#_Toc119856249)

[4 Justificaciones técnicas 5](#_Toc119856250)

[4.1 Tipos de medios de transmisión 5](#_Toc119856251)

[4.2 Elementos de la estructura física 5](#_Toc119856252)

[4.3 Estructura lógica 5](#_Toc119856253)

[4.4 Electrónica de red 6](#_Toc119856254)

[4.5 Ubicación del CPD 9](#_Toc119856255)

[5 Desarrollo del proyecto 10](#_Toc119856256)

[5.1 Estructura física y cableado estructurado 10](#_Toc119856257)

[5.1.1 Tipos de medios de transmisión 10](#_Toc119856258)

[5.1.2 Tomas de red 10](#_Toc119856259)

[5.1.3 Armarios de distribución o racks y pasacables 10](#_Toc119856260)

[5.1.4 Pach-panels 10](#_Toc119856261)

[5.1.5 Cableado horizontal 10](#_Toc119856262)

[5.1.6 Cableado vertical 10](#_Toc119856263)

[5.2 Estructura lógica 11](#_Toc119856264)

[5.2.1 Topología de red 11](#_Toc119856265)

[5.2.2 Diseño de la red 11](#_Toc119856266)

[5.2.3 Tipo de protocolo IP 11](#_Toc119856267)

[5.2.4 Direccionamiento IP y subredes 11](#_Toc119856268)

[5.3 Administración de servidores 11](#_Toc119856269)

[5.3.1 Sistemas operativos y software 11](#_Toc119856270)

[5.3.2 Servicios en red 12](#_Toc119856271)

[5.3.3 Active Directory - Usuarios y Grupos 12](#_Toc119856272)

[5.3.4 Active Directory – Recursos compartidos y cuotas de disco 12](#_Toc119856273)

[5.3.5 Sistemas de seguridad 12](#_Toc119856274)

[5.3.6 Directivas de grupo 13](#_Toc119856275)

[5.4 Administración de clientes 14](#_Toc119856276)

[5.4.1 Acceso clientes 14](#_Toc119856277)

[5.4.2 Sistemas de seguridad 14](#_Toc119856278)

[5.5 Seguridad Informática 14](#_Toc119856279)

[5.5.1 Firewall 14](#_Toc119856280)

[5.5.2 Switches 15](#_Toc119856281)

[5.5.3 Antivirus 15](#_Toc119856282)

[5.5.4 Directivas de seguridad 15](#_Toc119856283)

[5.5.5 Copias de seguridad 16](#_Toc119856284)

[Anexo 1 – Diagrama Packet tracer 17](#_Toc119856285)

[Anexo 2 – Esquema de conexiones 17](#_Toc119856286)

[Anexo 3 - Presupuesto 17](#_Toc119856287)

# Glosario

|  |  |
| --- | --- |
| VLAN | Red virtual |
| Active Directory | Para gestionar usuarios en entornos empresariales |
| CPD | Armario centrar para los dispositivos de red (Rack) |
| DHCP | Servicio para proveer de configuración de red a los dispositivos |
| HSRP | [Hot Standby Routing Protocol](https://www.cisco.com/c/en/us/td/docs/routers/sdwan/configuration/system-interface/ios-xe-17/systems-interfaces-book-xe-sdwan/m-hot-standby-router-protocol.html) |
| DNS | Servidor de nombres de dominio |

# Introducción

Todas las grandes empresas dedicadas al sector informático tienen una serie de características en común que las hace diferentes unas de otras tales como, el esfuerzo por ofrecer un producto superior a la competencia, tener una buena plataforma fácil de usar donde vender sus productos, además de tener en cuenta la satisfacción del cliente y sus valoraciones para poder mejorar y, por último, el soporte que ofrecen a sus clientes cuando tienen problemas con sus productos.

Todo esto hace una imagen de la empresa solida de cara al público.

Las cualidades de nuestro sector informático van desde resolver problemas complejos a clientes, al desarrollo e implementación de nuevos productos.

Estas son algunas empresas del sector Informático en Zaragoza:

|  |  |
| --- | --- |
| EMPRESA | DEDICACIÓN |
| Informática Madi S L | Empresa de software |
| Ecomputer | Tienda de informática |
| Tecnovalia informática | Soporte y servicios |
| Tempus Informática, S.L. | Empresa de software |
| Implementación Informática Lyra | Consultoría |
| Informática Zaragoza | Soporte y servicios |
| Calat Sistemas y Comunicaciones S.L. | informática para empresas |
| DSI S.L. | Consultora |
| Izquierdo Informática S.L. | Soporte y servicios |
| SUIN | Soporte y servicios |
| Informática Torrero S.L. | Soporte y servicios |
| APP Informática | Soporte y servicios |
| Programas Y Sistemas Informaticos S.L. | Soporte y servicios |
| Formacion Y Desarrollo de Software Aplicado SL | Empresa de software |

El nombre de la empresa sobre la que vamos a trabajar es Bionica Automations.

Los productos que se van a vender y desarrollar van a ser productos de IoT, teles como enchufes inteligentes, luce, persiana, cerraduras, sistemas de climatización, monitorización de consumo eléctrico, etc….

He optado orientar la empresa en productos de IoT porque es un mercado emergente que tiene mucho que ofrecer, ya que de aquí a porco tiempo se van a empezar a implementar sistemas de domótica que se basan en IoT y en ese campo queremos ganar nuestro nicho de mercado.

# Ubicación del proyecto

La empresa estará ubicada en el polígono de Plaza Zaragoza, sitio elegido por ser un enclave logístico sin igual.

A continuación, vamos a realizar el diseño de una red informática de la empresa.

La empresa tiene un edificio de 2 plantas donde hay que realizar el diseño de la red para los siguientes departamentos:

* Recepción 1 persona
* Informática 5 personas
* Comercial 6 personas
* Call-Center 8 Personas
* Contabilidad 6 Personas
* Dirección 4 Personas
* Recursos Humanos 1 Persona
* Programadores 18 Personas
* Desarrolladores 18 Personas

# Justificaciones técnicas

## Tipos de medios de transmisión

Los medios de transmisión escogidos para el proyecto han sido: fibra óptica para las comunicaciones entre los dispositivos del CPD y el cableado vertical, cable de par trenzado para el cableado horizontal y el aire (WiFi).

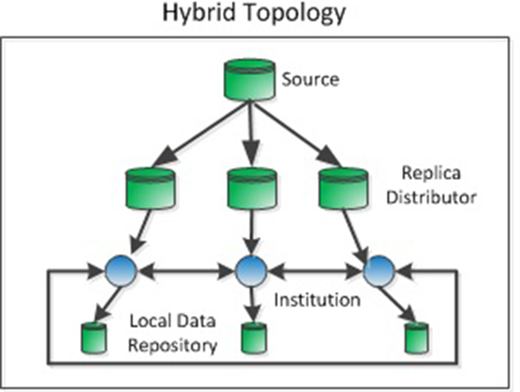
## Elementos de la estructura física



Está más detallado en el documento del Presupuesto en Excel.

## Estructura lógica

La topología de la red es una topología mixta o híbrida.

Existe una VLAN por departamento con su propio direccionamiento y servidor DHCP, el acceso a internet está garantizado gracias a dos Reuters configurados con el protocolo HSRP, también hay redundancia en el primer salto, todas las bocas que no están en uso están deshabilitadas y asignadas a una VLAN donde no hay nada, para maximizar la seguridad.

Los departamentos que lo necesiten tendrán disponibles en su subred los servicios necesarios para desempeñar su trabajo, como las impresoras en cado de los comerciales o contabilidad o también un NAS para los programadores y desarrolladores.

Para más información consultar el ANEXO 1 y 2

## Electrónica de red

Routers: Unifi Dream Machine Pro

Switches: Switch Pro 48 PoE y Switch Pro 48 PoE

Servidores: Dell PowerEdge R840 para rack. 64 GB Ram, x4 Intel Xeon.

NAS: Storinator Q30 Enhanced

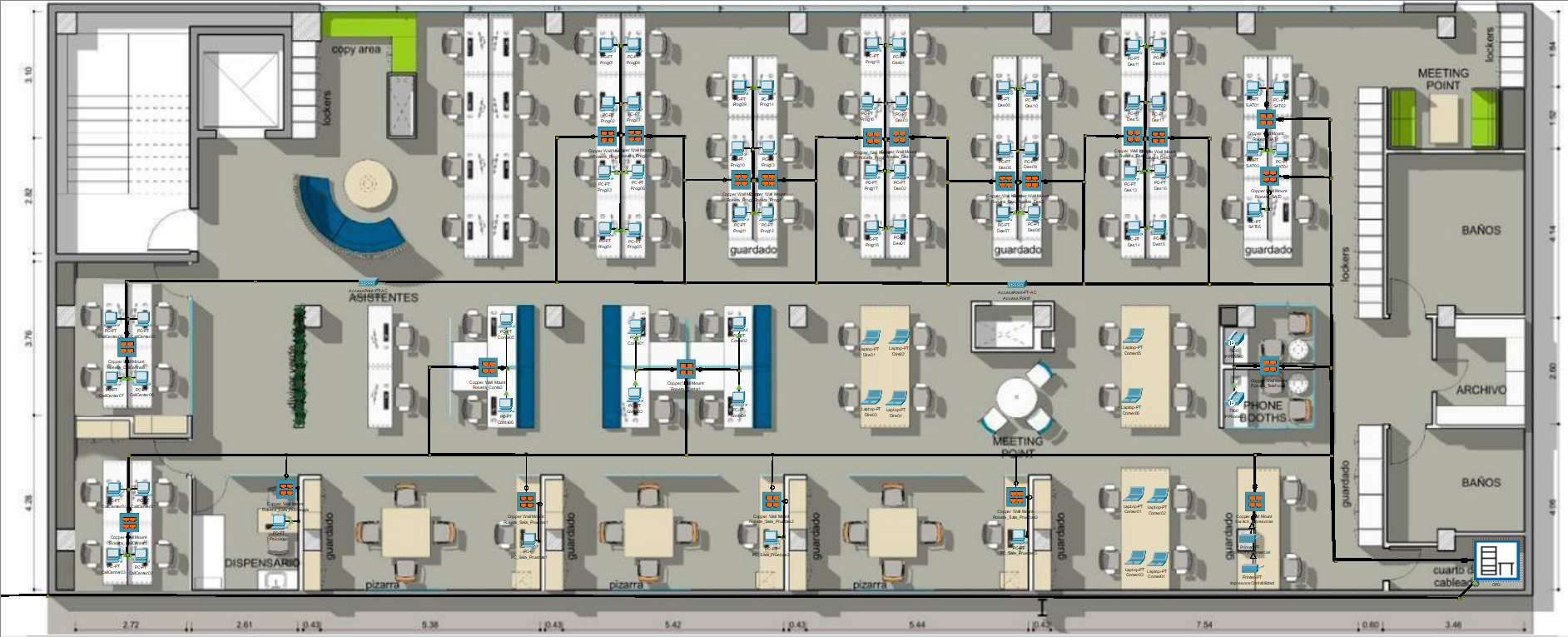
Todos los monitores salvo los de recepción van con soporte vesa.

|  |  |  |
| --- | --- | --- |
| Departamento | Ordenador | Periféricos |
| Recepción | Dell OptiPlex 3070 Micro Form Factor Config. Base | Monitor Dell 22 | P2219H  Teclado y ratón inalámbricos Dell | KM636 |
| Programadores | Dell Vostro Desktop 3670 MT  Intel® Core™ i5-8400  8 GB RAM  GTX 1050 Ti | Conjunto de teclado y ratón inalámbricos KM636  X2 Monitor Dell 24 P2419H |
| Desarrolladores | Dell Vostro Desktop 3670 MT  Intel® Core™ i5-8400  8 GB RAM | X2 Monitor Dell 24 P2419H  Conjunto de teclado y ratón inalámbricos KM636 |
| Dirección | Portátil XPS 13  Intel® Core™ i5  8 GB RAM | Opcional: Ratón inalámbrico Dell Premier WM527 |
| Comercial | Dell 2 en 1 XPS de 13  Intel® Core™ i5  8 GB RAM | Opcional: Ratón inalámbrico Dell Premier WM527 |
| Contabilidad | Dell OptiPlex 3070 Small Form Factor  Intel® Core™ i3-9100  4 GB RAM | Monitor Dell 22 | P2219H  Conjunto de teclado y ratón inalámbricos KM636 |

|  |  |  |
| --- | --- | --- |
| CallCenter | Dell OptiPlex 3070 Small Form Factor  Intel® Core™ i3-9100  4 GB RAM | Monitor Dell 22 | P2219H  Conjunto de teclado y ratón inalámbricos KM636  Auriculares estéreo Dell Pro UC350 |
| Salas de pruebas | Dell Embedded Box PC 5000 | Monitor Dell 22 | P2219H  Conjunto de teclado y ratón inalámbricos KM636 |
| Informática | Dell OptiPlex 3070 Small Form Factor  Intel® Core™ i3-9100  4 GB RAM | Monitor Dell 22 | P2219H  Conjunto de teclado y ratón inalámbricos KM636 |

## Ubicación del CPD

El CPD está situado en el cuarto del cableado eléctrico.



# Desarrollo del proyecto

## Estructura física y cableado estructurado

### Tipos de medios de transmisión

Los medios de transmisión escogidos para el proyecto han sido: fibra óptica de 10 Gb para las comunicaciones entre los dispositivos del CPD y el cableado vertical, cable de par trenzado CAT-7 para el cableado horizontal y el aire (WiFi): bandas de 2.4 estándar IEEE 802.11n y 5 GHz IEEE 802.11ac.

### Tomas de red

Las rosetas van acordes al número máximo de ordenadores que se pueden colocar en los puestos de trabajo cercanos.

Ejemplo: si se pueden colocar 8 ordenadores en un área de trabajo, se pondrán 4 rosetas de 2 bocas cada una para esos supuestos 8 ordenadores. Si solo se puede colocar 1 ordenador, en ese caso se pondrán rosetas individuales.

### Armarios de distribución o racks y pasacables

Para el CPD hay un rack donde están todos los equipos junto con 2 pasacables laterales que recorren el rack de arriba abajo con 3 paneles de parcheo.

Para la planta baja hay un armario de distribución que contiene un panel de parcheo y un switch para abastecer a la planta.

### Pach-panels

En el siguiente documento está el mapeado de las bocas del panel de parcheo a las respectivas bocas de las rosetas identificadas por “S1, S2, S3” en caso de que pertenezcan a la planta superior o “B1, B2, B3” si son de la planta baja.

### Cableado horizontal

Para el cableado horizontal vamos a utilizar cable de par trenzado CAT-7 con rosetas en cada zona de trabajo numeradas con la nomenclatura.

Todos los cables se pasarán por el suelo o techo técnicos, dependiendo de lo que haya disponible con sus respectivos aislantes para evitar las interferencias, eso supone canaletas especiales dependiendo si los cables pasan al lado de los cables eléctricos.

### Cableado vertical

Para el cableado vertical hemos optado por cables de fibra plástica de 10 Gb de ancho de banda para evitar cuellos de botella en la red y porque es fácil de manejar debido a que no necesitan de canalizaciones especiales como el cable de par trenzado, al no ser impulsos eléctricos le que va a viajar por esos cables, se pueden ubicar justo al lado de los cables eléctricos sin que haya ninguna interferencia, por lo que se pueden aprovechar las canalizaciones ya existentes.

## Estructura lógica

### Topología de red

La topología de la red es una topología mixta porque integramos la estructura en árbol y en estrella a la vez.

### Diseño de la red

La red está formada por 2 routers conectados a 2 switches que están conectados entre ellos para garantizar la redundancia del primer salto, ambos routers están configurados en fail over, para que así si se interrumpe el servicio de alguno de los 2, el otro asuma la carga.

Luego tenemos los switches de cada plata conectados con los switches principales por fibra plástica de 10 Gb, con sus respectivos paneles de parcheo de RJ45 de CAT-7 conectado a las rosetas de las plantas, y estas a los dispositivos finales.

Los servidores están conectados a un switch central a través de cables CAT-7 RJ45.

Todas las conexiones con los equipos de trabajo se realizan bajo cable de par trenzado CAT-7 de 1Gb, las rosetas por supuesto son CAT-7 también.

### Tipo de protocolo IP

Solo se implementa el protocolo IPv4 ya que como máximo vamos a escalar la red hasta los 255 equipos y no necesitamos más.

IPv6 estará deshabilitado por seguridad.

### Direccionamiento IP y subredes

Consultar el ANEXO 1 y 2

## Administración de servidores

### Sistemas operativos y software

Servidores: VMware vSphere Hypervisor (ESXi), VMware vCenter Server, Windows Server 2022 standard, donde habrá máquinas virtuales en función de los proyectos.

Trabajadores: Todos los ordenadores de los trabajadores llevan Windows 10 pro.

Software Servidores: Instalaremos Pulseway para la administración remota de Windows Server, un antivirus, software de copias de seguridad.

Software Trabajadores: Utilizaremos cuentas corporativas de Google para usar sus servicios, visual studio para los programadores y desarrolladores, antivirus, software de copias de seguridad.

### Servicios en red

Los servicios presentes son los siguientes: DNS, DHCP, SMB para los trabajadores que tengan que almacenar sus datos de trabajo, además de las copias de seguridad, una VPN y RDP por si los trabajadores tienen que trabajar desde casa, Active Directory para la gestión de los usuarios, para las actualizaciones de Windows WSUS y para la autentificación de los empleados en las redes corporativas RADIUS.

### Active Directory - Usuarios y Grupos

Cada departamento tendrá su grupo y su unidad organizativa con un nombre identificativo del departamento, además los usuarios se identificarán con nombre y apellidos y se meterán dentro de los grupos de trabajo correspondientes para la gestión de los permisos.

* Departamentos – Unidad organizativa
  + Contabilidad – Unidad organizativa
    - Contabilidad - Grupo
    - Jorge Pinto Panto - Usuario
  + SAT – Unidad organizativa
    - SAT – Grupo
    - Pepe Marco – Usuario

### Active Directory – Recursos compartidos y cuotas de disco

El servidor de Active Directory tendrá recursos compartidos del NAS con los departamentos de programadores y desarrolladores para guardar sus proyectos en carpetas compartidas con la siguiente nomenclatura: Nombre departamento->Proyecto->Nombre del trabajador.

Los permisos de cada usuario solo afectan a su carpeta, no pueden ver el trabajo del resto de sus compañeros a no ser que sea necesario, para garantizar la seguridad.

Además, los usuarios solo pueden escribir 50 GB en disco, sin posibilidad de superar dicha cantidad, a no ser que se le amplié por alguna circunstancia.

### Sistemas de seguridad

Para evitar los inicios de sesión no autorizado contaremos con una autentificación en 2 factores.

Los usuarios deberán cambiar la contraseña cada 2 meses

Se activarán las horas activas para que no se pueda iniciar sesión cuando estas fuera del horario establecido.

Los discos duros de los ordenadores de trabajo estarán cifrados.

Los trabajadores no pueden modificar ningún parámetro de los sistemas de seguridad tales como antivirus, firewall.

Se van a grabar las acciones de un usuario o un grupo en el registro de eventos.

### Directivas de grupo

Se configurar las actualizaciones gradualmente, es decir, primero habrá un ordenador de cada departamento que reciban las actualizaciones antes que los demás, para verificar que todo sigue funcionando y no hay ningún error. Si no hay ningún error, el resto de los ordenadores se actualizarán en el tiempo establecido por el administrador de red. Y si falla en los primeros ordenadores se pausará la actualización en el resto para que el fallo no se extienda.

Más información de esta política [Windows Update for Business](https://docs.microsoft.com/es-es/windows/deployment/update/waas-wufb-group-policy).

Implementar Windows hello para el inicio de sesión. [Directivas de Windows Hello](https://docs.microsoft.com/es-es/windows/security/identity-protection/hello-for-business/hello-key-trust-policy-settings).

Directiva para cifrar cualquier unidad extraíble. [Directivas de grupo de BitLocker](https://docs.microsoft.com/es-es/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings)

Directiva para activar la protección del DMA del kernel.

El fondo de pantalla se les cambiará en función del departamento.

## Administración de clientes

### Acceso clientes

Los clientes tendrán acceso a un portal cautivo, además de una aplicación para dispositivos móviles donde podrán gestionar los dispositivos que adquieran, con el añadido de que todos los productos son compatibles con el asistente de Google, Alexa, etc…, por lo que también se pueden controlar por voz.

Los clientes deberán crearse una cuenta de Bionica Automations para poder acceder a la app y el portal cautivo, está se asociará con la cuenta Google, Amazon, otros, para el control por voz.

### Sistemas de seguridad

Los clientes pueden activar si lo desean una verificación en 2 factores para añadir más seguridad a la cuenta.

Todas las comunicaciones están cifradas con protocolos seguros de comunicación.

## Ciberseguridad

### Firewall

#### Firewalls de red (Router)

Las conexiones de fuera hacia dentro están bloqueadas y las conexiones salientes permitidas.

Si permitimos que los trabajadores trabajen desde casa se dispondrá de una VPN para que los trabajadores puedan acceder a los recursos de la empresa.

#### Firewalls de los ordenadores

Por defecto con el perfil de red corporativa.

#### Firewalls de los servidores

Expuestos solo los servicios necesarios.

### Switches

Los switches tendrán un faltado por Mac que va por puerto, si conectas un ordenador con distinta Mac que el que había antes, el puerto de deshabilitará.

### Antivirus

#### Para todos los equipos

Vamos a usar el antivirus de Panda con los servicios de Panda Systems Management, Panda Fusion, Panda Fusion 360, Panda Email Protection, Panda Patch Management, Panda Full Encryption, Aether Platform.

### Directivas de seguridad

Más información de esta política [Windows Update for Business](https://docs.microsoft.com/es-es/windows/deployment/update/waas-wufb-group-policy).

Implementar Windows hello para el inicio de sesión. [Directivas de Windows Hello](https://docs.microsoft.com/es-es/windows/security/identity-protection/hello-for-business/hello-key-trust-policy-settings).

Directiva para cifrar cualquier unidad extraíble. [Directivas de grupo de BitLocker](https://docs.microsoft.com/es-es/windows/security/information-protection/bitlocker/bitlocker-group-policy-settings)

Directiva para activar la protección del DMA del kernel.

Poner el número mínimo de caracteres para las contraseñas.

Las contraseñas no se pueden repetir y tienen que cumplir una serie de criterios.

Las contraseñas se cambiarán cada 2 meses.

### Copias de seguridad

El software de copias de seguridad que vamos a utilizar es Easeus la edición Advanced Server.

#### Análisis

Los datos más importantes que podemos tener son los siguientes:

* Sistema operativo de Windows Server de Active Directory (aunque sea una VM, la copia se hará aparte).
* El resto de los servicios que están en otras máquinas virtuales asociadas a los proyectos.

La información de los proyectos puede cambiar seriamente cada hora, los datos de contabilidad cada día, los datos de los clientes cada media hora, el sistema operativo de Windows server de Active Directory cada 1 semanas, el resto de las máquinas virtuales cada 1 semanas también.

Los datos de los proyectos se almacenarán durante 6 meses, los de contabilidad durante 3 años, los datos de los clientes durante 1 año, el S.O. del Windows Server de Active Diectory se almacenará durante 4 meses, el resto de los servicios de otras máquinas virtuales de proyectos se almacenarán durante otros 6 meses.

#### Diseño

En el siguiente esquema relacionado con el horario en el que se van a ejecutar las copias de seguridad y su ubicación, no están incluidas las copias de los datos de los clientes (Base de datos de clientes), ya que esto hay que hablarlo con la empresa que contratemos para dichos servicios para acordar un plan de copias de seguridad.

### Puesto de trabajo

Consultar el Anexo 3 documento:

**UBALDE\_Plan\_de\_Ciberseguridad\_en\_puestos\_de\_trabajo**

Anexo 1 - Diagrama Packet tracer

[Anexos\Anexo 1 - Diagrama Packet Tracer](Anexos/Anexo%201%20-%20Diagrama%20Packet%20Tracer)

Anexo 2 - Esquema de conexiones

Se detallan todas las conexiones cableadas de los ordenadores y dispositivos de la empresa.

[Anexos\Anexo 2 - Esquema de conexiones](Anexos/Anexo%202%20-%20Esquema%20de%20conexiones)

Anexo 3 – Plan de ciberseguridad

[Anexos\Anexo 3 - Ciberseguridad](Anexos/Anexo%203%20-%20Ciberseguridad)