

# APUNTES.pdf



Celia\_483201



Administracion de Sistemas



3º Grado en Ingeniería Informática



Escuela Politécnica Superior  
Universidad Francisco de Vitoria

**WUOLAH + BBVA**

**Llévate**

**15€**

Al abrir tu Cuenta Online Sin Comisiones y hacer una compra superior a 15€.

**1/6**

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

¿Cómo? →



1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

1  
Abre tu Cuenta Online sin comisiones ni condiciones

2  
Haz una compra igual o superior a 15€ con tu nueva tarjeta

3  
BBVA te devuelve 15€

¿Cómo?



Cuéntame más



## ADMINISTRACIÓN DE SISTEMAS

### TEMA 1 8 SISTEMAS DE COMPUTACIÓN

**CPO** → espacio físico que alberga los servidores, equipos informáticos, sistemas de red y almacenamiento. Su objetivo es el procesamiento de la información de una empresa. Se debe contar al menos con un CPO de medida o con urnas que permiten la distribución de las cargas de procesamiento. El problema de tener un CPO físico es que hay que actualizarlo y preocuparse por urnas caras a la vez que de su coste.

- **SISTEMAS DE CLIMATIZACIÓN**: sistemas de aire acondicionado convencionales, enfriamiento por agua, por aire libre o refrigeración eólica. Los costes varían según el sistema, mantenimiento y capacidad.

#### - SISTEMAS ANTINCENDIOS

↳ TIPOS: detección de humo y calor, extinción automática, suspensión de oxígeno y protección perimetral.

↳ NORMAS: para instalación, desempeño, diseño y pruebas, requisitos de seguridad y requisitos técnicos.

- **POU**: dispositivo que distribuye energía eléctrica a urnas equipos. Se conecta a una fuente de alimentación para distribuir urnas señales de energía para alimentar distintos dispositivos.

- **SAI**: dispositivo que protege equipos electrónicos sensibles contra interrupciones en el suministro de energía eléctrica.

#### - SISTEMAS DE CONTROL DE ACCESO FÍSICO

↳ TIPOS: - **TARJETAS ACCESO**: fácil implementación, control de acceso granular y posibilidad de auditor de acceso. Se pueden perder o robar.

- **COMBINACIONES Y PIN'S**: bajo coste y fácil implementación. Vulnerable a ataques.

- **BIOMETRÍA**: huellas, reconocimiento facial,... Alta seguridad pero costoso e implementación difícil.

- **BARRERAS FÍSICAS**: alta seguridad y control de acceso granular pero costosa y restringe flujo personas.

VIRTUALIZACIÓN → equipos reales que ofrecen mayor funcionalidad que un equipo físico. Las máquinas virtuales no tienen dependencia del hardware sobre el cual se ejecutan.

El hypervisor se encarga de mapear los recursos hardware para cada máquina virtual. Por lo tanto, para la capa de virtualización, una máquina virtual es un proceso.

Las máquinas virtuales protegen a los sistemas operativos que corren en las mismas realidades hardware. Se consigue así ejecutar varias máquinas en un mismo hardware y ejecutar una en equipos de distintos fabricantes sin tener que modificar nada en la máquina. También se pueden definir redes virtuales.

#### ⇒ CARACTERÍSTICAS

- **Aislamiento**: cada máquina es independiente del resto
- **Encapsulación**: las máquinas se representan con un conjunto de ficheros
- **Compatibilidad**: es lo que se instala en una máquina
- **Independencia del hardware**: se protegen del hardware físico

#### ⇒ BENEFICIOS

Las cargas de trabajo virtuales pueden correr también como físicas, las cargas de trabajo virtuales pueden ejecutarse mejor.

#### ⇒ CONCEPTOS

- **Poole de recursos**: elemento organizativo que contiene MV y permite establecer prioridades a la hora de dividir recursos de computación, para determinar quien accede a un recurso físico en caso de conflicto.
- **Cluster**: agrupa hosts y administra sus recursos en conjunto, que da soporte a funcionalidades.

CLOUD → la nube permite a usuarios almacenar la información en servidores de terceros para que puedan ser accesibles desde cualquier terminal con acceso a Internet sin tener que instalar un software adicional. Es un servicio bajo demanda a través de la red caracterizado por su adaptabilidad, flexibilidad, escalabilidad, rapidez, ...



4  
Colours®

# UN BOLÍGRAFO



## PARA CADA



## UNO DE TUS



## ESTILOS.

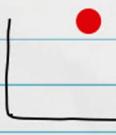


TUS NOTAS O TU PLAN PARA EL FINDE

#



■



MÁS COLORES. MÁS DISEÑOS.

ELIGE UN BOLÍGRAFO QUE DIGA MÁS DE TI QUE TU ESCRITURA.

El establecimiento de un SISI está basado en el principio de mejora continua. Sigue siendo aplicable en el caso de computación en la nube.

⇒ CARACTERÍSTICAS: autoservicio a la carta, amplio acceso a la red, recursos de recursos en común, rapidez y elasticidad, servicio supervisado

⇒ AMENAZAS: pérdida de información, robo de sesión, riesgos por descuidamiento, amenaza interna, mal uso o abuso del servicio

⇒ MODELOS DE NEGOCIO

- RGPD: el modelo de negocio a la hora de contratar servicios en la nube determina aspectos importantes respecto a la responsabilidad de la seguridad de los datos. El tipo de despliegue puede influir en la relación entre el responsable y el encargado de tratamiento que lleva a cabo la gestión del servicio.

- IaaS: el proveedor proporciona a los usuarios acceso a recursos de cálculo. Las empresas usan sus plataformas y aplicaciones en una infraestructura de proveedor de servicios. El responsable del fichero no gestiona ni controla la infraestructura de nube pero tiene control sobre los SO, almacenamiento, operaciones desplegadas y componentes de red.

- PaaS: oferta de cloud computing que proporciona a los usuarios un entorno de cloud en el que desarrollar, gestionar y distribuir aplicaciones. Se usan las herramientas del proveedor para la programación de operaciones y servicios, se tendrá que considerar que las plataformas permiten la tutela efectiva de los derechos ejercitados.

- SaaS: oferta de cloud computing que proporciona acceso a los usuarios al SW basado en cloud de un proveedor. Los usuarios no instalan aplicaciones en sus dispositivos locales, las aplicaciones residen en una red cloud remota a la que se accede a través de la red o una API.

TRANSFORMACIÓN DIGITAL → proceso por el que las organizaciones empresas reorganizan sus métodos de trabajo y estrategias para obtener más beneficios gracias a la digitalización de procesos e implementación dinámica de las nuevas tecnologías.

⇒ **BARRERAS:** innovación digital, profesionales que entienden y comparten principios

⇒ **VENTAJAS:** mejor comunicación con cliente, nuevas oportunidades de negocio, ahorra en vida de la empresa, reduce costes, fidelización de personal y empleados felices

⇒ **CLAVES**

- Formación digital de las personas
- Conocimiento de las herramientas digitales
- Reconocimiento de marca
- Ser innovador
- Uso del big data
- Compromiso del equipo directivo

⇒ **FINTECH:** La transformación digital, desde un modelo de negocio, es cómo repensar el modelo de negocio de la organización en función del impacto de:  
1) el nuevo escenario competitivo,  
2) nuevas demandas de consumidores  
3) nuevas tecnologías

eje de modelo de negocio  
de las FinTech

**1/6**

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

**1**  
Abre tu Cuenta Online sin comisiones ni condiciones

**2**  
Haz una compra igual o superior a 15€ con tu nueva tarjeta

**3**  
BBVA te devuelve 15€

¿Cómo?



Cuéntame más



## CREDENCIALES

- ⇒ **Cuentas de usuario:** existen 4 tipos de nombres asociados a las cuentas de usuario de dominio. Los usuarios usan este nombre sólo al iniciar sesión.
- ⇒ **Grupos:** conjunto de cuentas. Los miembros de un grupo están formados por cuentas de usuario, de equipo y otros grupos. Administrar la forma ejerce el acceso a los recursos, y simplificar la administración y mantenimiento de esa red.
  - **De seguridad:** para asignar derechos y permisos de usuario
  - **Anidamiento:** aumenta cuentas de miembros afectadas por una acción

## ⇒ PERMISOS

- **Administrador de equipos:** NTFS es un sistema de archivos disponible en Windows, es fiable, seguro, administra almacenamiento, permisos a varios usuarios.
- Puede conceder permisos para objetos o grupos y usuarios locales del equipo en el que reside el objeto y a grupos, usuarios e identidades del dominio.
- **Permisos estandarizados:** varía en función del tipo de objeto para el que se está modificando la seguridad.
- **Permisos Especiales:**

## ⇒ CARPETAS COMPARTIDAS: pueden acceder varios usuarios a través de la misma red. Una vez se haya compartido puede acceder cualquier usuario conectado a la misma red, siempre que tenga permisos. Los permisos de las carpetas compartidas solo se aplican a los usuarios que se conectan a la carpeta a través de la red. No restringen el acceso de los usuarios a la carpeta del equipo en el que está almacenada. Puede conceder permisos de carpeta compartida a cuentas de usuario, grupos y cuentas de equipo.

## ⇒ SERVIDOR FILES & PRINT: un servidor de archivos proporciona una ubicación central en la red donde se pueden almacenar archivos y compartirlos con otros usuarios de la red. Un servidor de impresión proporciona una ubicación central en la red donde los usuarios pueden imprimir.

## PERFILES

### ⇒ PROYECTOS

- ↳ GESTIÓN DE PROYECTOS: introducción de la dirección y de participantes
- ↳ ALCANCE DEL PROYECTO: productos entregables y trabajo necesario para crear
- ↳ IMPLANTACIÓN: poner en funcionamiento el sistema

### ⇒ DIRECCIÓN DE PROYECTOS

- ↳ DIRECTOR DE LA INFORMÁTICA

- ↳ DIRECTOR DE PROYECTO:

- ↳ JEFE DEL PROYECTO: dirige el equipo de trabajo formado por:

- Analistas jerárquicos: comprenden los procesos de negocio y cómo se pueden mejorar con soluciones tecnológicas
- Analistas de aplicaciones: se centran en el análisis, diseño, implementación y mantenimiento de sistemas de software.
- Programadores: escriben código informático para crear software, aplicaciones y sistemas informáticos

### ⇒ SISTEMAS Y REDES

- ↳ JEFE DE SISTEMAS: sistemas informáticos y el software

- ↳ JEFE DE REDES: infraestructura de red y conectividad

- ↳ ADMINISTRADOR DE RED Y/O SISTEMAS: garantiza que la infraestructura funcione, implementación medidas seguras de red. Diseño lógico y físico

- ↳ TÉCNICO DE REDES: instalar, configurar, mantener y reparar la infraestructura de red. Que los usuarios accedan a la red de manera eficiente y segura.

- ↳ OPERADOR DE REDES / MICROINFORMÁTICA Y DE SISTEMAS: mantiene redes, sistemas, resuelve incidencias

### ⇒ BASES DE DATOS

- ↳ ADMINISTRADOR DE BBDD: gestiona y mantiene la BBDD

**SGSI**: no se puede exigir nada a ningún usuario que no se haya establecido previamente. Basado en el principio de mejora continua.

⇒ **control interno**: proceso mediante el cual se garantiza la consecución de sus objetivos. Su finalidad es detectar si la organización mantiene preventivas, detección y corrección de errores, faltas y fraudes o sabotajes.

⇒ **administración de riesgo**: finaliza con la determinación de las acciones a seguir.

⇒ **control de riesgos**

↳ **amenaza**: acciones que pueden ocasionar consecuencias negativas en la plataforma informática.

↳ **vulnerabilidad**: debilidades o carencias.

↳ **rriesgo intrínseco**: probabilidad de que una amenaza se materialice de acuerdo al nivel de vulnerabilidad existente de un activo.

↳ **impacto**: consecuencias de las amenazas.

\* **TIPOS DE CONTROLES**

- Preventivos: evitar el hecho
- Deterrentes
- Detectivos: cuando fallan los preventivos, para conocer cuanto antes el evento.
- Correctivos: permiten la vuelta a la normalidad cuando hay incidentes.

⇒ **Gobierno IT**: para gobernar IT hay que determinar actividades y riesgos que deben ser administrados.

↳ **dominio 1: PLANEAR Y ORGANIZAR**

↳ **dominio 2: ADQUIRIR E IMPLEMENTAR**

↳ **dominio 3: EMPLEAR Y DAR SOSTIEN**

↳ **dominio 4: MONITOREAR Y EVALUAR**

1/6

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

1  
Abre tu Cuenta Online sin comisiones ni condiciones

2  
Haz una compra igual o superior a 15€ con tu nueva tarjeta

3  
BBVA te devuelve 15€

¿Cómo?

Cuéntame más



## TEMA 4 8 SERVICIO DE DIRECTORIOS

### ACTIVE DIRECTORY

Almacena información de usuarios, equipos y recursos de red y permite el acceso a los recursos por parte de usuarios y aplicaciones. Es un servicio de directorio que almacena información de usuarios y cuentas y de seguridad. Permite que la información se comparte con otros dispositivos de la red.

#### ⇒ funciones

- ↳ centralizar el control de los recursos de red: solo los usuarios autorizados pueden obtener acceso a los recursos de AD.
- ↳ centralizar y descentralizar la administración de recursos.
- ↳ almacenar objetos de forma sencilla en una estructura lógica.
- ↳ optimizar el tráfico de red: la estructura física de AD permite usar el ancho de banda de red de forma más efectiva.

⇒ ESTRUCTURA LÓGICA: AD proporciona almacenamiento seguro de información. Los objetos de AD representan a usuarios y recursos. Algunos objetos son contenedores de otros.

Los **objetos**: cada objeto tiene una única combinación de valores de atributos.

Los **unidades organizativas**:

Los **dominios**: unidades jerárquicas centrales, conjunto objetos definidos de forma administrativa que comparten RBSO, direcciones de seguridad y relaciones

con otros dominios. Proporcionan un límite administrativo para objetos, un medio de administración de la seguridad para recursos compartidos, y una unidad de replicación para objetos.

Los **árboles de dominios**: árboles agrupados en estructuras jerárquicas.

Los **bosques**: instancia completa de AD. Consiste de uno o varios árboles

⇒ ESTRUCTURA FÍSICA: optimiza el tráfico de red mediante la determinación de lugar y el momento en que se produce la replicación y el tráfico de conexión.

Los **controladores de dominio (CD)**: solo puede admitir un dominio. Cada CD contiene partición del dominio de configuración y de esquema. Pueden replicarse en los CD del bosque. La partición de dominio se replica en los CD del dominio.

**Los sitios de AD:** grupos de equipos conectados.

**Los vínculos WAN:** facilitan la replicación y la sincronización

⇒ **MAESTROS DE OPERACIONES:** cuando se hace un cambio en un dominio, el cambio puede replicarse a través de los controladores del dominio. Algunos cambios como los que se hacen en el esquema, pueden replicarse en todos los dominios del bosque. Esta replicación se llama **replicación de buenas maestras**. AD define 5 funciones de maestro de operaciones que abarcan el bosque o el dominio.

**Las funciones para todo el bosque (únicas para un bosque)**

- **maestro de esquema:** controla actualizaciones del esquema. El esquema contiene una lista de clases de objetos y atributos usados para crear los objetos de AD. Solo existe uno en todo el bosque.
- **maestro de nombres de dominio:** controla la adición o eliminación de dominios del bosque. Solo el CO que tiene esta función puede agregar un nuevo dominio al bosque. Solo existe uno en todo el bosque.

**Las funciones para todo el dominio (únicas para cada dominio de un bosque)**

- **emisor del comando de dominio principal (PDC):** primer CO que se crea en un dominio nuevo.
- **maestro de identificadores relativos:** asigna bloques de administradores relativos a cada CO. El CO asigna un RID a los objetos creados a partir de su bosque asignado de identificadores relativos.
- **maestro de infraestructura:** al desplazar objetos de un dominio a otro, este actualiza las referencias a objetos de su dominio que apuntan al objeto en el otro dominio. La referencia al objeto contiene el identificador único global del objeto (GUID).

Cada dominio de un bosque dispone de su propio emisor del PDC, maestro de RID y de infraestructura.

GPO (objeto de directiva de grupo): Es una entidad de AD para administrar los usuarios y equipos de la red mediante la directiva de grupo se puede definir el entorno de trabajo de un usuario una sola vez y dejar que Windows Server aplique la configuración de Directiva de grupo definida. Se puede aplicar la configuración en todo la organización o sólo a grupos específicos de usuarios y equipos.

⇒ DIRECTIVA DE GRUPO PARA USUARIOS: incluye el comportamiento del SO, de escritorio, de seguridad, ... La configuración de directiva de grupo relativa al usuario se aplica cuando éste inicia sesión en el equipo y durante el ciclo de actualización periódico. La configuración de directiva de grupo que personaliza el entorno de escritorio del usuario, o aplica directivas de bloqueo a usuarios.

⇒ DIRECTIVA DE GRUPO DEL EQUIPO: la configuración de Directiva de grupo relativa al equipo se aplica cuando el sistema operativo se inicia y durante el ciclo de actualización. En general, tiene prioridad sobre otra configuración Directiva de grupo relativa al usuario con el que pueda estar en conflicto.

Para modificar un objeto de Directiva de grupo existe hay que iniciar sesión como miembro del grupo Administradores del dominio, de organización o propietario del creador de Directiva de grupo.

⇒ HERENCIAS Y PRIORIDAD: el orden en que se aplican los GPO depende de contenedor de AD al que se unen los objetos, se aplican primero al sitio, luego a los dominios y después a unidades organizativas de los dominios. Los objetos de Directiva de grupo se pueden heredar, un contenedor secundario hereda los GPO del contenedor primario. Si hay varios GPO establecidos en el mismo lugar, el último que se aplica tiene prioridad.

## dns

- ⇒ **Integración de DNS y AD**: esencial para que un equipo dentro de una red pueda localizar un DC para que los usuarios puedan iniciar sesión en un dominio o bien los servicios proporcionados por AD. Localizan los DC y servicios usando registros de recurso A y registros SRV.
- Una jerarquía de servidores DNS contiene los registros de recursos que relacionan los nombres con las direcciones.

## DHCP

Sin DHCP, las IP de los equipos nuevos o que se mueven de una subred a otra deben configurarse manualmente. Con DHCP este proceso es automático.

## DTS

Esquema de almacenamiento y gestión de datos que permite a usuarios o a las operaciones acceder a archivos desde un almacenamiento compartido en cualquier de los servidores en red.

- ⇒ **Características**: transparencia de acceso, de su ubicación, búsqueda de archivos y cifrado de datos en tránsito.

## ⇒ **funcionamiento**:

Los datos pueden residir en varios dispositivos o sistemas de almacenamiento. Cuando un usuario hace clic en un nombre de archivo para acceder a esos datos, el DTS comprueba varios servidores. Esto evita que cualquiera de los servidores se atasque cuando muchos usuarios acceden a los archivos y mantenga los datos disponibles. A través de la función de replicación de archivos DTS, cualquier cambio realizado en un archivo se copia en todos los instancias de ese archivo en los nodos del servidor.

**1/6**

Este número es indicativo del riesgo del producto, siendo 1/6 indicativo de menor riesgo y 6/6 de mayor riesgo.

BBVA está adherido al Fondo de Garantía de Depósitos de Entidades de Crédito de España. La cantidad máxima garantizada es de 100.000 euros por la totalidad de los depósitos constituidos en BBVA por persona.

**1**  
Abre tu Cuenta Online sin comisiones ni condiciones

**2**  
Haz una compra igual o superior a 15€ con tu nueva tarjeta

**3**  
BBVA te devuelve 15€

¿Cómo?

Cuéntame más



Llévate

**15€**



### TEMA 5 8 PLAN DE RECUPERACIÓN DE DESASTRES

PCN → es el plan de continuidad de negocio. está pensado y organizado para que pueda producir la interrupción del servicio informático sobre el resto de la compañía al mínimo, restaurando sistemas y comunicaciones en el menor tiempo posible con nuestros empleados y colaboradores.

#### • FASES

- Determinación de alcance: se incluyen los archivos de más criticidad
- Análisis de la organización: reuniones, análisis de impacto y de riesgo
- Definición estratégica de continuidad: se establece con información sobre los procesos afectados (tiempos y requisitos de recuperación) y riesgos de la infraestructura IT.
- Funcionamiento en caso de contingencia
  - ↳ AActivación: condicionantes y órdenes de decisiones
  - Comunicación: canales, equipo de crisis y datos de contactos
  - Actuaciones: priorización, estrategia de la infraestructura y requisitos temporales
  - Ríenes operativos: negocio y DRP (TI)
- Prueba, mantenimiento y revisión: es primordial

#### ④ NIVELES DE CRITICIDAD

- críticos: sus funciones no pueden ser ejecutadas a menos que sean reemplazadas por recursos idénticos. Costo de interrupción muy alto
- urbanos: sus funciones pueden ser ejecutadas manualmente durante un periodo corto. Mayor tolerancia a interrupciones. Costo de interrupciones menores
- sensitivos: sus funciones pueden ser ejecutadas manualmente durante un periodo relativamente largo. Mientras se hace manualmente requiere pantalla táctil. Costos de interrupciones medios
- no críticos: sus funciones pueden ser interrumpidas durante un periodo relativamente largo, con poco o ningún costo

PRO → un plan de recuperación ante desastres es un proceso de recuperación que permite a las empresas recuperar los datos y operaciones de misión crítica en el menor tiempo posible. Se definen sobre hardware y software crítico. El objetivo es que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre. Los conceptos clave a la hora de definir un PRO son "Alta disponibilidad" que consiste en la capacidad de un sistema para asegurar la continuidad de los servicios y "Respaldo" que es la salvaguardia de la información crítica que permite su restauración en caso de pérdida o fallos de su integridad. Es importante definir tres parámetros que nos permitirán definir y evaluar la calidad de nuestro PRO:

- RTO: tiempo máximo durante el cual es aceptable que se interrumpan las actividades de la empresa, es decir, tiempo que podemos soportar que dure una interrupción.
- RPO: cantidad de datos que la empresa está dispuesta a perder entre la última copia de seguridad y una contingencia.
- ROL: nivel mínimo de recuperación que debe tener una actividad para que se considere recuperada.

⇒ Regla 3.2.1: La norma establece que deben tener al menos tres copias de tus datos. Dos de las copias de seguridad deben estar almacenadas en distintos medios, y al menos una copia de seguridad fuera del sitio o en la nube.

⇒ TIPOS básicos: back up completo, back up incremental (hace una copia de seguridad de los cambios desde el último back up), back up diferenciales (contiene todos los datos que han cambiado desde la última copia completa).

⇒ REPLICAS: permite tener otra copia la la que acceder en caso de desastre.

- síncrona: proporciona un RPO cercano a cero para los datos. Depende del ancho de banda. Requiere de mayores recursos y PCK en ambos sitios. Retraso de proceso.

- semi-síncrona:

- ↳ Asíncrona: se inicia la replica al sitio remoto después de que los datos están bien escritos en la fuente (PCK).

El RPO proporcionado depende de su configuración y recursos.