Verónica González Amor

Ejercicios de Evaluación Continua
UF1466: SISTEMAS DE ALMACENAMIENTO

Ejercicio 1:
Nomenclatura y Clasificación de Ficheros

Normativa de Nomenclatura:

Escribe una normativa detallada para la nomenclatura y clasificación de ficheros en una organización ficticia.

Normativa de Nomenclatura y Clasificación de Ficheros

1. **Estructura de Nombres**

Para garantizar la organización y la facilidad de recuperación de los archivos, se establece la siguiente estructura de nombres de ficheros:

Formato general: [Tipo]_[Departamento]_[Proyecto]_[Fecha]_[Versión].[Extensión]

-Tipo: Abreviatura del tipo de documento (Ejemplo: DOC, IMG, VID, DB, etc.).
-Departamento: Siglas del departamento responsable del archivo (Ejemplo: FIN para Finanzas, MKT para Marketing, IT para Tecnología, etc.).
-Proyecto: Nombre corto del proyecto o cliente.
-Fecha: Formato YYYYMMDD.
-Versión: v1, v2, v3, etc.
- Extensión: Tipo de archivo (.docx, .jpg, .mp4, .xlsx, etc.).

1.1 Separadores
- Se utilizará el guion bajo (_) para separar los elementos del nombre del archivo.
- No se permiten espacios ni caracteres especiales (excepto el guion bajo y el punto para la extensión).

1.2 Ejemplos
1. Documento de presupuesto de Marketing del Proyecto Alpha, creado el 5 de febrero de 2025:
   - DOC_MKT_Alpha_20250205_v1.docx
2. Imagen de logotipo de un cliente en diseño:
   - IMG_DES_ClientX_20250120_v3.png
3. Base de datos de clientes actualizada:
   - DB_SALES_Customers_20250115_v2.sql

2. **Clasificación por Tipo de Documento**

Los archivos se organizarán en las siguientes categorías:

- Documentos (DOC): Archivos de texto, hojas de cálculo, presentaciones.
- Imágenes (IMG): Fotografías, diseños, logotipos.

- Videos (VID): Archivos multimedia en formatos MP4, AVI, etc.
- Bases de datos (DB): Archivos SQL, CSV, backups de bases de datos.
- Código fuente (SRC): Archivos de programación y desarrollo.
- Contratos y legales (LEG): Documentos legales y administrativos.

3. Aplicación de la Normativa

A continuación, se presenta un ejemplo de organización de archivos:

3.1 Estructura de Directorios

```
/EmpresaX/
  /Marketing/
    DOC_MKT_Campana2025_20250210_v1.docx
    IMG_MKT_LogoEmpresaX_20250105_v2.png
  /Finanzas/
    DOC_FIN_Presupuesto2025_20250115_v1.xlsx
  /Tecnologia/
    SRC_IT_Website_20250120_v3.zip
    DB_IT_Usuarios_20250110_v1.sql
  /Legal/
    LEG_ADM_ContratoProveedor_20250112_v1.pdf
```

4. Justificación y Beneficios

4.1 Organización
- Facilita la categorización y búsqueda de archivos.
- Evita la duplicidad de documentos con nombres ambiguos.

4.2 Recuperación Rápida
- La estructura de nombres permite identificar archivos de forma eficiente sin abrirlos.
- La inclusión de la fecha y versión evita confusiones con documentos obsoletos.

4.3 Seguridad de la Información
- Permite establecer permisos de acceso según los directorios.
- Reduce riesgos de sobrescritura accidental.
- Facilita la implementación de copias de seguridad y auditorías.

Esta normativa garantiza una gestión eficiente y segura de los archivos en la organización ficticia, promoviendo el orden y la trazabilidad de la información.

Ejercicio 2: Nomenclatura Estandarizada de Máquinas y Servicios de Nomenclatura Estandarizada de Máquinas y Servicios

1. Normativa para Nombres de Servidores

Para garantizar una identificación clara y estandarizada de los servidores en la red empresarial, se establece el siguiente formato:

Formato general: SRV-[Función]-[Ubicación]-[Número]

- SRV: Prefijo que indica que se trata de un servidor.
- Función: Abreviatura de la función del servidor (Ejemplo: DB para bases de datos, WEB para servidor web, FS para servidor de archivos).
- Ubicación: Código de la ubicación del servidor (Ejemplo: HQ para sede central, BCN para Barcelona).
- Número: Identificador secuencial del servidor.

Ejemplos
1. Servidor de bases de datos en la sede central:
   - SRV-DB-HQ-01
2. Servidor web en Barcelona:
   - SRV-WEB-BCN-02

2. Normativa para Nombres de Servicios

Para identificar los servicios dentro de la red, se usará la siguiente nomenclatura:

Formato general: SVC-[Tipo]-[Aplicación]-[Número]

- SVC: Prefijo para identificar un servicio.
- Tipo: Categoría del servicio (Ejemplo: WEB para servicio web, API para servicios de API, AUTH para autenticación).
- Aplicación: Nombre de la aplicación o plataforma.
- Número: Identificador secuencial del servicio.

Ejemplos
1. Servicio de autenticación para un sistema CRM:
   - SVC-AUTH-CRM-01
2. Servicio API de facturación:
   - SVC-API-BILLING-02

3. Normativa para Nombres de Aplicaciones

Las aplicaciones desplegadas en la infraestructura seguirán la siguiente estructura:

Formato general: APP-[Nombre]-[Entorno]-[Número]

- APP: Prefijo para identificar una aplicación.
- Nombre: Nombre corto de la aplicación.
- Entorno: Dev, Test o Prod.
- Número: Identificador único.

Ejemplos
1. Aplicación de CRM en producción:
   - APP-CRM-PROD-01
2. Aplicación web en entorno de desarrollo:
   - APP-WEB-DEV-02

4. **Ejemplo de Mapa de Red**

A continuación, se muestra un ejemplo de un mapa de red con la nomenclatura aplicada:

/Red Empresarial/
  /Servidores/
    SRV-DB-HQ-01
    SRV-WEB-BCN-02
    SRV-FS-HQ-03
  /Servicios/
    SVC-AUTH-CRM-01
    SVC-API-BILLING-02
  /Aplicaciones/
    APP-CRM-PROD-01
    APP-WEB-DEV-02

5. **Explicación de la Eficiencia**

5.1 Identificación Rápida
- Permite identificar de manera rápida la función de cada equipo y servicio.
- Facilita la administración de la red en empresas de gran tamaño.

5.2 Reducción de Errores
- Evita confusiones en la gestión de recursos.
- Reduce el riesgo de asignaciones incorrectas.

5.3 Gestión Optimizada
- Mejora la implementación de políticas de seguridad y monitoreo.
- Facilita la escalabilidad y mantenimiento de la infraestructura tecnológica.

Con esta normativa, la red empresarial se gestiona de manera eficiente, minimizando errores y mejorando la administración de servicios y máquinas.

Ejercicio 3: Políticas de Migración y Archivado de Ficheros

1. **Descripción de Políticas**

A continuación, se presentan tres políticas diferentes de migración y archivado de ficheros.

1.1 Política de Migración Periódica
- Tipos de datos: Archivos activos utilizados en producción.
- Frecuencia: Mensual.
- Herramientas: Rsync, Robocopy, herramientas de copia en la nube (AWS S3, Google Drive).
- Objetivo: Mantener datos actualizados en sistemas nuevos y optimizar el rendimiento de los servidores.

1.2 Política de Archivado de Datos Históricos
- Tipos de datos: Documentos, registros contables, informes obsoletos.
- Frecuencia: Trimestral.
- Herramientas: Compresión (ZIP, TAR), almacenamiento en frío (Glacier, Azure Archive Storage).
- Objetivo: Liberar espacio en almacenamiento primario y conservar datos importantes.

1.3 Política de Migración por Actualización de Infraestructura
- Tipos de datos: Bases de datos, configuraciones críticas.
- Frecuencia: Según actualización de hardware/software.
- Herramientas: MySQL Dump, pg_dump, herramientas de snapshot (VMware, Hyper-V).
- Objetivo: Garantizar la continuidad operativa durante cambios de infraestructura.

2. Aplicación de una Política

Escenario: Migración de 100 GB de datos de un servidor antiguo a uno nuevo
Pasos:
1. Evaluación del entorno: Identificación de datos críticos y no críticos.
2. Planificación: Selección de herramientas (por ejemplo, Rsync para transferencia eficiente).
3. Pruebas previas: Migración de un subconjunto de datos para validar procesos.
4. Ejecución: Transferencia total de datos con validaciones de integridad.
5. Verificación: Comparación de hash entre archivos originales y migrados.
6. Optimización: Configuración de copias de seguridad en el nuevo servidor.

3. Análisis del Impacto

3.1 Disponibilidad de Espacio
- Liberación de almacenamiento: Reducción de carga en el servidor antiguo.
- Optimización del uso de disco: Implementación de almacenamiento en niveles (primario y archivado).

3.2 Tiempo de Ejecución
- Estimación: Transferencia de 100 GB con Rsync (~50 MB/s) → 34 min aprox.
- Factores de retraso: Latencia de red, I/O del disco, interrupciones operativas.

Esta estrategia asegura la continuidad operativa, minimizando riesgos y optimizando el almacenamiento de datos.

Ejercicio 4: Mapa de Direcciones IP

1. **Generación de Mapa de Direcciones IP**

A continuación, se presenta la asignación de direcciones IP para una red ficticia con 5 subredes y 20 dispositivos.

1.1 Direcciones de IP asignadas:

Subred	**Rango de IP**	**Máscara**
Administración	192.168.1.0/24	255.255.255.0
Ventas	192.168.2.0/24	255.255.255.0
Soporte Técnico	192.168.3.0/24	255.255.255.0
Servidores	192.168.4.0/24	255.255.255.0
Dispositivos IoT	192.168.5.0/24	255.255.255.0

1.2 Subredes configuradas

Dispositivo	IP Asignada	Subred
Router Principal	192.168.1.1	Administración
Servidor Web	192.168.4.2	Servidores
Servidor Base de Datos	192.168.4.3	Servidores
Estación de Trabajo 1	192.168.1.10	Administración
Estación de Trabajo 2	192.168.2.10	Ventas
Estación de Trabajo 3	192.168.3.10	Soporte Técnico
Impresora	192.168.1.20	Administración
Switch de Red	192.168.1.5	Administración
Cámara de Seguridad 1	192.168.5.10	IoT
Cámara de Seguridad 2	192.168.5.11	IoT
Laptop Ejecutivo	192.168.1.15	Administración
Punto de Acceso Wi-Fi	192.168.1.6	Administración
Telefono IP 1	192.168.3.15	Soporte Técnico
Telefono IP 2	192.168.2.15	Ventas
Servidor Backup	192.168.4.4	Servidores
PC de Soporte 1	192.168.3.20	Soporte Técnico
PC de Soporte 2	192.168.3.21	Soporte Técnico
Dispositivo IoT 1	192.168.5.15	IoT
Dispositivo IoT 2	192.168.5.16	IoT
Firewall	192.168.1.2	Administración

1.3 Puertas de Enlace y Servidores DNS

Puerta de enlace principal: 192.168.1.1

Servidor DNS primario: 192.168.4.2

Servidor DNS secundario: 192.168.4.3

2. Justificación y Coherencia

Este esquema de asignación de direcciones IP proporciona:

Segmentación eficiente de la red, reduciendo congestión y mejorando la seguridad.

Fácil administración, con direcciones organizadas según departamento o función.

Escalabilidad, permitiendo agregar nuevos dispositivos en subredes específicas sin afectar la infraestructura existente.

Ejercicio 6: Seguridad y Protección de Datos

1. **Conceptos Fundamentales de Seguridad**

1.1 Confidencialidad

Garantiza que la información solo sea accesible para personas o sistemas autorizados. Se implementa mediante técnicas como cifrado de datos, control de accesos y autenticación multifactor.

1.2 Integridad

Asegura que la información no sea alterada de manera no autorizada. Se aplican técnicas como firmas digitales, hashes criptográficos y controles de versiones.

1.3 Disponibilidad

Garantiza que los datos y sistemas estén accesibles cuando sean necesarios. Se logra mediante respaldos periódicos, redundancia de hardware y balanceo de carga.

2. **Recuperación y Continuidad del Servicio**

Las políticas de seguridad afectan la capacidad de recuperación y continuidad de las operaciones ante incidentes. Ejemplos incluyen:

Copias de seguridad periódicas en múltiples ubicaciones.

Planes de contingencia en caso de fallos de hardware o ataques cibernéticos.

Monitoreo y alertas en tiempo real para detectar y mitigar amenazas rápidamente.

3. Caso Práctico: Recuperación ante Ataque de Ransomware

3.1 Pasos para la Recuperación de Datos

Aislar los sistemas infectados para evitar la propagación.

Identificar y evaluar el alcance del ataque.

Restaurar los datos desde copias de seguridad seguras.

Reinstalar sistemas afectados y aplicar parches de seguridad.

Monitorear la red para evitar futuras infecciones.

3.2 Medidas Preventivas

Implementación de cifrado de datos para proteger información sensible.

Uso de firewalls y sistemas de detección de intrusos.

Capacitación del personal sobre ingeniería social y phishing.

3.3 Herramientas y Métodos de Protección

Software antivirus avanzado para la detección temprana de amenazas.

Segmentación de red para limitar la propagación de ataques.

Autenticación multifactor (MFA) para proteger accesos críticos.

Estas estrategias garantizan la continuidad del servicio y minimizan el impacto de ataques informáticos en la empresa.