TRABAJO PRACTICO

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| FACULTAD: | **TECNOLOGIA INFORMATICA** | | | | |
| CARRERA: | **INGENIERIA EN SISTEMAS INFORMATICOS** | | | | |
| ALUMNO/A: | Di Domenico, Nicolás | | | | |
| SEDE: | **ROSARIO** | | LOCALIZACIÓN: | **LAGOS** | |
| ASIGNATURA: | **TRABAJO DE DIPLOMA** | | | | |
| CURSO: | **3 A** | | TURNO: | Mañana | |
| PROFESOR: | **ING. PABLO AUDOGLIO** | | FECHA: | 22/10/ 2024 | |
| TIEMPO DE RESOLUCIÓN: | | - | TRABAJO PRACTICO  NRO: | | - |
| MODALIDAD DE RESOLUCIÓN: | | | Presencial / Virtual / Escrito / Oral /  Individual / Grupal | | |
|  | | |  | | |
| RESULTADOS DE APRENDIZAJE: | | | | | |

# PROPÓSITO:

Evaluar la capacidad del estudiante para establecer los puntos clave a considerar en un backup y que pueda apropiarse de los conocimientos necesarios para implementar una política de backup.

# CONSIGNAS:

1. Definir en no más de 3 renglones que es un backup.
2. Analizar las ventajas y desventajas de implementar una política de backup.
3. Determinar los tipos de backup existentes. Describir brevemente.
4. Seleccionar un tipo de backup e indicar en qué soporte lo realizaría y donde lo ubicaría. Justificar.
5. Especificar cual sería la frecuencia de realización de este respaldo.
6. Elaborar un plan de la copia. Determinar cómo se va a comprobar que se realiza, quien es el responsable, seguridad, etc.

# ENTREGA:

Deberán remitir sus trabajos en formato digital en el espacio destinado a tal fin en la plataforma, y tener en cuenta las formalidades como: portada, resumen ejecutivo, índice de contenidos, introducción, desarrollo, y cierre, conclusiones y bibliografía.

1. **¿Qué es un backup?**

Un backup es una copia de seguridad de datos importantes que permite restaurar información en caso de pérdida, corrupción, o fallo del sistema. Es una práctica esencial para proteger información ante incidentes imprevistos.

1. **Ventajas y desventajas de implementar una política de backup**

**Ventajas:**

* Garantiza la recuperación de datos ante fallos o ciberataques.
* Minimiza el tiempo de inactividad y las pérdidas económicas.
* Facilita la continuidad operativa de la organización.

**Desventajas:**

* Requiere inversión en infraestructura y almacenamiento.
* Puede generar tiempos de mantenimiento prolongados.
* La gestión inadecuada del backup puede llevar a copias desactualizadas o incompletas.

1. **Tipos de backup existentes**

**Backup completo:** Copia todos los archivos y datos seleccionados cada vez que se realiza.

**Backup incremental:** Solo copia los cambios realizados desde el último backup (completo o incremental).

**Backup diferencial:** Copia los datos modificados desde el último backup completo.

1. **Selección de un tipo de backup y justificación**

**Tipo seleccionado:** Backup incremental.

**Soporte:** Disco duro externo.

**Ubicación:** En un armario cerrado o caja fuerte en la oficina del administrador de TI.

**Justificación:** Se cuenta con un gimnasio **pequeño**, con un volumen moderado de datos, principalmente registros de socios, reservas de turnos y rutinas de entrenamiento. Dado que no se generan grandes cantidades de información a diario, un **disco duro externo** es suficiente para gestionar los backups sin necesidad de infraestructura compleja o costosa como la nube. Esta opción también ofrece una solución **más controlada**, ya que el personal encargado puede supervisar el respaldo manualmente. Además, el uso de un disco portátil permite que los datos se mantengan fuera de línea, minimizando el riesgo de **ciberataques** y accesos no autorizados.

1. **Frecuencia de realización del respaldo**

**Backup incremental:** Diario, al finalizar la jornada laboral (por ejemplo, a las 23:00 horas).

**Backup completo:** Semanalmente, los domingos, para consolidar los cambios de la semana.

1. **Plan de la copia**
   1. **Procedimiento para realizar el backup incremental diario**

**Paso 1: Preparar el entorno**

* Conectar el disco duro externo al equipo mediante un puerto USB.
* Verificar que el disco esté en buen estado y tenga espacio suficiente para los backups programados.
* Asegurarse de que el disco esté formateado en un sistema compatible (por ejemplo, NTFS para Windows o ext4 para Linux).

**Paso 2: Selección de datos para respaldo**

* Utilizar un software de backup sencillo como Cobian Backup o Backup and Restore en Windows.
* Seleccionar “Backup Incremental” en la interfaz del software.
* Marcar las carpetas y archivos importantes que se definieron en la política de respaldo (documentos, bases de datos, etc.).

**Paso 3: Configuración del destino del backup**

* Elegir el disco duro externo como destino del backup.
* Crear una carpeta específica con la fecha del día, por ejemplo: /Backups/Incremental\_2024-10-22.
* Asegurarse de que la ruta esté correctamente configurada para evitar errores.

**Paso 4: Cifrado y compresión**

* Activar la opción de compresión para ahorrar espacio en el disco duro.
* Si se requiere mayor seguridad, habilitar el cifrado (algunas herramientas permiten establecer contraseñas para los archivos comprimidos).

**Paso 5: Programación del backup**

* Programar la tarea para que se ejecute automáticamente todos los días a las 23:00 horas.
* Verificar que el backup completo esté configurado para realizarse los domingos al mismo horario.
* Guardar la configuración y probar la ejecución manualmente para asegurarse de que funcione.

**b) Restauración de datos (comprobación mensual)**

* Conectar el disco duro externo y abrir el software de backup.
* Seleccionar una copia específica y realizar una restauración parcial en una carpeta de prueba.
* Revisar que los archivos restaurados sean funcionales y coincidan con los originales.

**c) Responsable del proceso**

* Administrador de TI: Encargado de configurar y supervisar los backups.
* Personal de soporte: Capacitado para ejecutar el proceso en ausencia del administrador.
* Documentar cada ejecución en un registro de backups (fecha, tipo, resultado).

**d) Seguridad y control de acceso**

* Ubicación segura: Guardar el disco duro en una caja fuerte o un armario cerrado fuera del horario de respaldo.
* Acceso limitado: Solo personal autorizado tendrá acceso al disco.
* Cifrado de archivos sensibles: Proteger los archivos respaldados mediante contraseñas.

**e) Frecuencia y retención del backup**

* Incremental diario: Retener durante 30 días.
* Completo semanal: Retener durante 6 meses.
* Eliminación automática: Revisar manualmente los archivos del disco cada mes para eliminar backups obsoletos.