Fase 3.3 - Mecanismos de Protección de Datos, Uso de Respaldos Periódicos, Cifrado de Datos Sensibles e Implementación de Controles de Acceso Estrictos

1. Respaldos Periódicos

Estrategias de respaldo:

- Implementar un plan de respaldo automatizado utilizando herramientas como `rsync` o `Bacula`.
- Programar copias de seguridad diarias, semanales y mensuales según la criticidad de los datos.
- Almacenar los respaldos en ubicaciones externas o en servicios de almacenamiento en la nube con cifrado.

Verificación de respaldos:

- Realizar pruebas periódicas para confirmar la integridad y restaurabilidad de los respaldos.
- Documentar los procedimientos de recuperación para garantizar una restauración rápida y efectiva.

2. Cifrado de Datos Sensibles

Cifrado en reposo:

- Utilizar herramientas como `dm-crypt` o `LUKS` para cifrar discos y particiones donde se almacenen datos sensibles.
- Aplicar cifrado a bases de datos críticas utilizando soluciones integradas como las de MariaDB o PostgreSQL.

Cifrado en tránsito:

- Implementar protocolos seguros como TLS (Transport Layer Security) para comunicaciones entre servidores y dispositivos.
- Configurar servicios como SSH para usar algoritmos de cifrado modernos y robustos.

Gestión de claves:

- Almacenar claves de cifrado en hardware seguro (HSM) o sistemas de gestión de claves como HashiCorp Vault.
- Rotar claves de cifrado regularmente y revocar aquellas que ya no sean necesarias.

3. Controles de Acceso Estrictos

Políticas de acceso:

- Implementar el principio de “mínimos privilegios”, asegurando que los usuarios solo tengan acceso a los recursos necesarios para sus tareas.
- Utilizar listas de control de acceso (**ACL**) para gestionar permisos en archivos y directorios.

Autenticación robusta:

- Configurar autenticación multifactor (**MFA**) en todos los sistemas críticos.
- Requerir contraseñas seguras y configurarlas con expiración periódica.

Monitoreo y auditoría:

- Implementar herramientas para registrar y monitorear intentos de acceso.
- Realizar auditorías regulares para identificar accesos no autorizados o configuraciones inseguras.

4. Prevención de Pérdida de Datos (DLP)

Detección y control de datos:

- Utilizar sistemas de **DLP** para monitorear y controlar la transferencia de datos sensibles.
- Configurar políticas que bloqueen la copia o el envío de información crítica a dispositivos externos o plataformas no autorizadas.

Educación y concienciación:

- Capacitar a los empleados sobre la importancia de proteger la información sensible.
- Establecer políticas claras sobre el manejo de datos críticos y las consecuencias de violar estas normas.