Políticas y Procedimientos de Seguridad

1. Política General de Seguridad de la Información

El Hospital General se compromete a proteger la información de sus pacientes cumpliendo con el RGPD y las normativas sanitarias. La seguridad es responsabilidad de todos los empleados. El incumplimiento de estas políticas puede conllevar sanciones disciplinarias.

2. Política de Control de Acceso

- **Altas:** Solo RRHH puede solicitar la creación de usuarios.
- **Principio de Menor Privilegio:** El personal médico solo tendrá acceso a los historiales de sus pacientes asignados o de su planta.
- **Bajas:** El acceso se revoca inmediatamente (mismo día) tras la finalización del contrato.

3. Plan de Respuesta a Incidentes

- **Fase 1: Detección.** Cualquier empleado que sospeche un incidente debe reportarlo al correo seguridad@hospital.publico.
- **Fase 2: Clasificación.** El CISO determinará la severidad.
- **Fase 3: Contención.** Si es malware, desconectar el equipo de la red. No apagar para análisis forense.
- **Fase 4: Erradicación y Recuperación.** Restauración desde backups limpios.
- **Fase 5: Lecciones Aprendidas.** Informe post-mortem.

4. Plan de Concienciación

- Curso obligatorio anual de ciberseguridad para todo el personal.
- Simulacros de Phishing trimestrales.