**UNIVERSIDAD NACIONAL DE JUJUY - FACULTAD DE INGENIERÍA**

**INGENIERÍA INFORMÁTICA – LICENCIATURA EN SISTEMAS**

**SEGURIDAD Y AUDITORÍA INFORMÁTICA**

**TRABAJO PRÁCTICO Nº 2**

**Fecha de presentación: 16/09/25**

**Análisis de riesgo. Ejercicio práctico - clínica médica "salud digital"**

**Contexto**

La Clínica Médica "Salud Digital" es un centro médico de mediana escala que atiende aproximadamente 500 pacientes por día. Recientemente implementaron un sistema de gestión hospitalaria (HIS) y están evaluando migrar completamente sus historias clínicas a formato digital. La clínica maneja información médica sensible y debe cumplir con regulaciones de protección de datos personales.

**Inventario de Activos Identificados**

|  |  |  |
| --- | --- | --- |
| **Categoría** | **Activo** | **Descripción** |
| **Datos** | Historias clínicas digitales | Registros médicos completos de pacientes |
| **Datos** | Base de datos de pacientes | Información personal y de contacto |
| **Datos** | Registros financieros | Facturación, seguros médicos, pagos |
| **Software** | Sistema HIS | Sistema integral de gestión hospitalaria |
| **Software** | Base de datos médica | Motor de BD que almacena toda la información |
| **Hardware** | Servidor principal | Servidor donde reside el sistema HIS |
| **Hardware** | Estaciones de trabajo médicas | PCs utilizadas por médicos y enfermeros |
| **Hardware** | Red LAN | Infraestructura de red interna |
| **Personal** | Médicos y enfermeros | Staff médico con acceso a historias clínicas |
| **Personal** | Personal administrativo | Recepcionistas, administrativos |
| **Personal** | Personal de IT | Técnico encargado del mantenimiento |

**Amenazas Identificadas**

* **Acceso no autorizado**: Personas sin autorización acceden a información médica
* **Ransomware**: Cifrado malicioso de historias clínicas
* **Falla de hardware**: Fallo del servidor principal
* **Error humano**: Personal médico borra o modifica incorrectamente registros
* **Fuga de información**: Filtración de datos médicos sensibles
* **Corte de energía**: Interrupciones eléctricas prolongadas

**Escalas de Valoración**

**Tabla 1: Confidencialidad**

|  |  |
| --- | --- |
| **Valor** | **Criterio** |
| 1 | Información pública o de bajo impacto |
| 2 | Información interna, impacto moderado si se divulga |
| 3 | Información altamente sensible, impacto severo si se divulga |

**Tabla 2: Integridad**

|  |  |
| --- | --- |
| **Valor** | **Criterio** |
| 1 | Errores menores aceptables, fácil corrección |
| 2 | Precisión importante, errores causan inconvenientes |
| 3 | Precisión crítica, errores pueden ser peligrosos |

**Tabla 3: Disponibilidad**

|  |  |
| --- | --- |
| **Valor** | **Criterio** |
| 1 | Puede estar no disponible por horas sin mayor impacto |
| 2 | Indisponibilidad causa inconvenientes operativos |
| 3 | Debe estar disponible 24/7, indisponibilidad es crítica |

**Tabla 4: Probabilidad de Amenazas (anual)**

|  |  |
| --- | --- |
| **Amenaza** | **Probabilidad** |
| Acceso no autorizado | 30% |
| Ransomware | 25% |
| Falla de hardware | 15% |
| Error humano | 60% |
| Fuga de información | 20% |
| Corte de energía | 40% |

**Actividades a Realizar**

**1. Definición del Alcance (Fase 1)**

Defina claramente el alcance de este análisis de riesgo. Considere:

* ¿Qué sistemas incluye?
* ¿Qué áreas de la clínica abarca?
* ¿Qué regulaciones debe considerar?

**2. Valoración de Activos (Fase 2)**

Complete la siguiente tabla asignando valores de 1-3 para cada criterio:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Activo** | **Confidencialidad** | **Integridad** | **Disponibilidad** | **Valor Total** |
| Historias clínicas digitales |  |  |  |  |
| Base de datos de pacientes |  |  |  |  |
| Registros financieros |  |  |  |  |
| Sistema HIS |  |  |  |  |
| Base de datos médica |  |  |  |  |
| Servidor principal |  |  |  |  |
| Estaciones de trabajo médicas |  |  |  |  |
| Red LAN |  |  |  |  |

El valor total se calcula como la suma de los valores de los tres parámetros.

**3. Fase 3 realizada al principio al enumerar las amenazas. Fase 4 se supone ya realizada para no hacer mas largo el trabajo practico.**

**4. Evaluación de Riesgos (Fase 5)**

Para cada activo, calcule el riesgo usando la fórmula: **Riesgo = Valor del Activo \* Probabilidad de Amenaza**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Valor del activo** | Acceso no autorizado | Ransomware | Falla hardware | Error humano | Fuga información | Corte energía | **Riesgo** |
| **Probabilidad de amenaza** |  | 30% | 25% | 15% | 60% | 20% | 40% |  |
| Historias clínicas |  |  |  |  |  |  |  |  |
| BD pacientes |  |  |  |  |  |  |  |  |
| Registros financieros |  |  |  |  |  |  |  |  |
| Sistema HIS |  |  |  |  |  |  |  |  |
| BD médica |  |  |  |  |  |  |  |  |
| Servidor principal |  |  |  |  |  |  |  |  |
| Estaciones trabajo |  |  |  |  |  |  |  |  |
| Red LAN |  |  |  |  |  |  |  |  |

Se tomará como valor del riesgo para el activo el valor promedio que arrojen los valores individuales de cada amenaza.

**5. Tratamiento de Riesgos (Fase 6)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Posición** | **Activo** | **Riesgo Promedio** | **Nivel** |
| 1 |  |  |  |
| 2 |  |  |  |
| 3 |  |  |  |
| 4 |  |  |  |
| 5 |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

El nivel puede ser: critico, alto o medio.

Si hay empate en los riesgos se tratan de manera conjunta.

Para los 5 riesgos más altos identificados, proponga:

* Estrategia de tratamiento (transferir, eliminar, mitigar, asumir).
* Medidas de seguridad activa y pasiva a implementar.
* Cronograma estimado de implementación.