ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

Curso: Auditoría de Sistemas de Información

Áreas de Riesgo en Sistemas de Información según el organigrama de EsSalud

---

Integrantes:

Elmer Andres Collanqui Casapia (2020204043)
Carlos Alberto Machaca Choque (2020204058)
Almir Carlos Vargas Mamani (2020204067)

Fecha: April 11, 2025

Áreas de Riesgo en Sistemas de Información según el organigrama de EsSalud

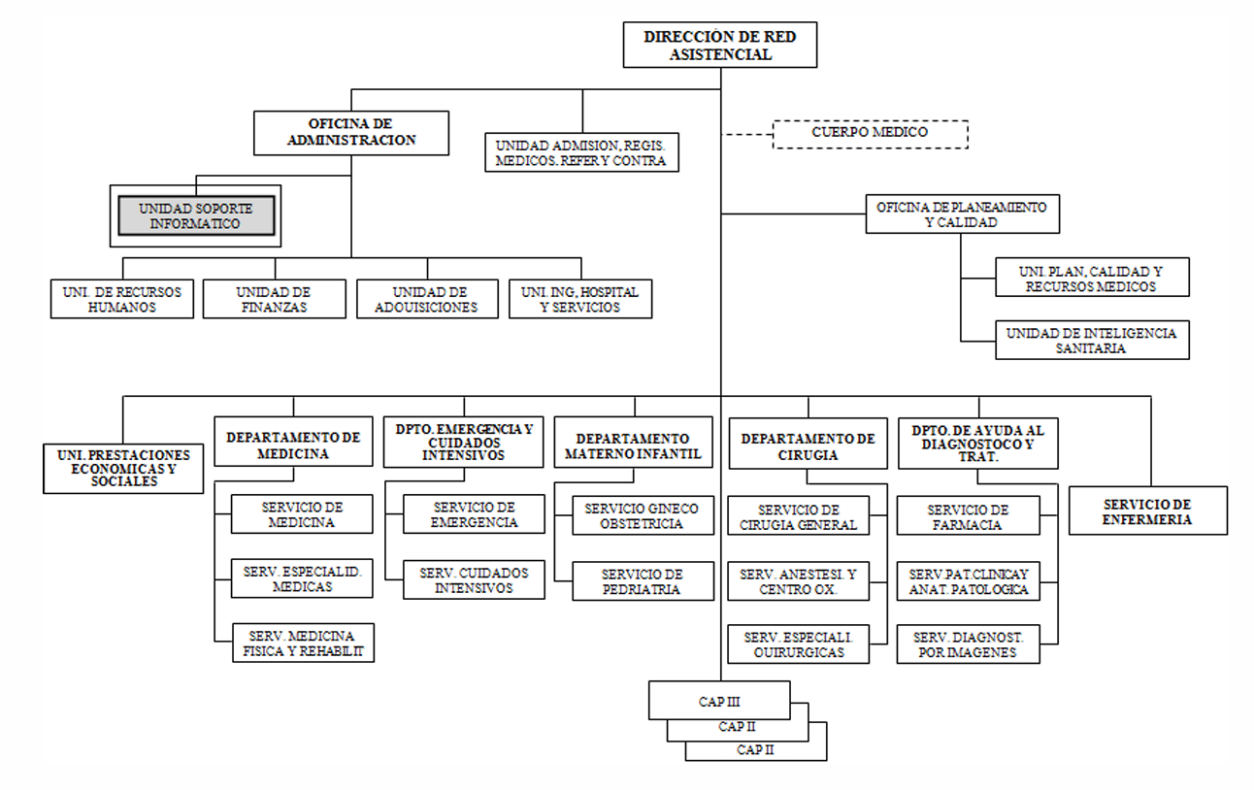

Figure 1: Organigrama de EsSalud

1. Unidad de Soporte Informático

Amenaza: Caídas de servidores, problemas en la red o ciberataques.
Riesgo: Si esta unidad falla, literalmente todo lo digital se cae. No se puede acceder a historiales médicos, sistemas administrativos ni bases de datos.

2. Unidad de Recursos Humanos

Amenaza: Robo o filtración de datos personales del personal médico y administrativo.
Riesgo: Suplantaciones, chantajes o incluso conflictos laborales. Además, si no se protege bien esta info, puede haber sanciones por no cumplir con la Ley de Protección de Datos.

3. Unidad de Finanzas

Amenaza: Accesos indebidos o errores en la gestión del sistema financiero.
Riesgo: Desde pagos mal hechos hasta fraudes internos. También podrían perderse registros clave para auditorías.

4. Unidad de Adquisiciones

Amenaza: Manipulación de datos en los procesos de compra o corrupción digital.
Riesgo: Se pueden alterar precios, proveedores o contratos. En el peor caso, se termina comprando mal o a empresas fantasmas.

5. Unidad de Ingeniería Hospitalaria y Servicios

Amenaza: Fallos en equipos médicos conectados (como monitores o sistemas de oxígeno).
Riesgo: Riesgo directo a la salud de los pacientes. También podría ser blanco de ciberataques que afecten los dispositivos.

6. Unidad de Admisión y Registros Médicos

Amenaza: Pérdida, robo o modificación de historias clínicas.
Riesgo: Cambiar un diagnóstico, borrar datos importantes o hacer mal una referencia puede tener consecuencias muy graves para los pacientes.

7. Oficina de Planeamiento y Calidad

Amenaza: Alteración de indicadores o informes falsos.
Riesgo: Si los datos están mal o manipulados, se toman decisiones equivocadas a nivel de gestión. Y eso afecta a todos.

8. Unidad de Inteligencia Sanitaria

Amenaza: Ataques a las bases de datos de vigilancia epidemiológica.
Riesgo: Filtración de datos sensibles, sabotaje de campañas de salud pública, o pérdida de trazabilidad en brotes.

9. Departamento de Ayuda al Diagnóstico y Tratamiento

Amenaza: Fallas en el software de diagnóstico por imágenes o sistemas de farmacia.
Riesgo: Un mal diagnóstico, o entregar un medicamento equivocado por culpa de un error informático, puede ser fatal.

10. Servicio de Enfermería y Departamentos Médicos

Amenaza: Uso indebido de sistemas por parte de personal no autorizado.
Riesgo: Cambios sin control en fichas clínicas, diagnósticos o medicación. También se expone la privacidad de los pacientes.

Referencias

- Reátegui Ríos, B. (2014). *Seguridad informática en los sistemas de información de las instituciones de salud pública.* Universidad Nacional de la Amazonía Peruana. Recuperado de: https://repositorio.unapiquitos.edu.pe/bitstream/handle/20.500.12737/4506/Boris_Tesis_Tit

- Instituto Nacional de Ciberseguridad (INCIBE). (s.f.). *Tipos de amenazas informáticas y su impacto en las organizaciones.* Recuperado de: https://www.incibe.es/