FECHA:	10/04/2025
ACTIVIDAD:	Identificar los riesgos de seguridad y privacidad de la información
PROCESO VINCULADO:	MIPG Evidencias conjunto de datos abiertos.
RESPONSABLE:	Equipo de sistemas
OBJETIVO	establecer un marco integral y sistemático para identificar, evaluar y gestionar los riesgos de seguridad y privacidad de la información
Dimensión:	Gestión con Valores para Resultados
Política:	Gobierno Digital

CONTENIDO DEL INFORME

El objetivo principal de este informe es establecer un marco integral y sistemático para identificar, evaluar y gestionar los riesgos de seguridad y privacidad de la información en el hospital mental, con el fin de proteger la confidencialidad, integridad y disponibilidad de los datos de los pacientes y de la institución.

1. **Introducción**

La protección de la información sensible de los pacientes es primordial en un hospital mental. Este documento describe el proceso para identificar, evaluar y gestionar los riesgos de seguridad y privacidad de la información, buscando la aprobación del Comité de Gestión y Desempeño Institucional para implementar las medidas necesarias que garanticen la confidencialidad, integridad y disponibilidad de estos datos críticos.

2. **Los objetivos específicos:**

- Identificar exhaustivamente los activos de información del hospital mental, incluyendo sistemas, bases de datos, archivos físicos y dispositivos, clasificándolos según su sensibilidad y criticidad.

- Determinar las amenazas y vulnerabilidades potenciales que podrían comprometer la seguridad y privacidad de la información identificada.

- Desarrollar planes de tratamiento específicos para los riesgos evaluados, definiendo controles de seguridad y privacidad proporcionales al nivel de riesgo.

- Documentar detalladamente todo el proceso de evaluación de riesgos y los planes de tratamiento propuestos para su presentación al Comité de Gestión y Desempeño Institucional.

- Presentar de manera clara y concisa al Comité de Gestión y Desempeño Institucional los resultados de la evaluación de riesgos y los planes de tratamiento recomendados para su revisión y aprobación.

- Obtener la aprobación formal del Comité de Gestión y Desempeño Institucional para la implementación de los planes de tratamiento de riesgos de seguridad y privacidad de la información.

- Establecer un mecanismo de seguimiento y revisión periódica de los riesgos y la efectividad de los controles implementados, garantizando una gestión continua de la seguridad y privacidad de la información.

3. **Metodología**

Identificar Qué Proteger:

- Hacer una lista de toda la información importante
- Decidir qué tan sensible es cada tipo de información, muy importante, importante, poco importante.

2. Identificar Riesgos:

- Pensar en las cosas que podrían dañar o exponer la información
- Identificar qué tan probable es que cada cosa mala suceda y qué tan grave sería si sucediera.

3. Evaluar los Riesgos:

- Usar una tabla sencilla para ver qué riesgos son los más importantes
- Decidir qué riesgos necesitan atención inmediata.

4. Decidir Qué Hacer con los Riesgos:

- Para cada riesgo importante, pensar en cómo reducir la posibilidad de que suceda o el daño que
- Crear un plan simple para implementar estas acciones.

5. Presentar al Comité:

- Explicar al Comité de Gestión y Desempeño Institucional cuáles son los riesgos más importantes y qué se propone hacer para manejarlos.
- Pedir su aprobación para seguir adelante con el plan.

6. Revisar y Mejorar:

- Revisar periódicamente si los riesgos han cambiado y si las acciones tomadas están funcionando.
- Hacer ajustes al plan según sea necesario.

4. Resultados.

La implementación del proceso de identificación, evaluación y gestión de riesgos de seguridad y privacidad de la información en el hospital mental debería generar los siguientes resultados:

- Identificación Clara de los Riesgos: Un catálogo completo y actualizado de los riesgos de seguridad y privacidad que amenazan la información sensible del hospital y sus pacientes.

- Priorización de Riesgos Significativos: Una comprensión clara de los riesgos más críticos, basada en su probabilidad e impacto potencial, permitiendo enfocar los esfuerzos y recursos donde más se necesitan.

- Planes de Tratamiento Aprobados: Planes de acción definidos y aprobados por el Comité de Gestión y Desempeño Institucional para mitigar, transferir, evitar o aceptar los riesgos identificados.

- Implementación de Controles: Implementación efectiva de controles de seguridad y privacidad (técnicos, procedimentales y físicos) para reducir la exposición a los riesgos prioritarios.

- Reducción de la Probabilidad e Impacto de Incidentes: Disminución de la ocurrencia y la severidad de incidentes de seguridad y privacidad de la información.

4.1. Resultados Medibles.

- Número de riesgos identificados y clasificados por nivel.
- Porcentaje de riesgos de alto y medio nivel con planes de tratamiento aprobados.
- Estado de implementación de los controles definidos en los planes de tratamiento.
- Número y tipo de incidentes de seguridad y privacidad de la información reportados.
- Tiempo de respuesta y resolución de incidentes.
- Resultados de auditorías internas y externas relacionadas con la seguridad y privacidad de la información.

5. Conclusión

La implementación de un proceso estructurado para la identificación, evaluación y gestión de riesgos de seguridad y privacidad de la información en el hospital mental representa una inversión fundamental para la protección de los derechos de los pacientes y la integridad operativa de la institución. A través de este proceso, se logra una comprensión profunda de las amenazas y vulnerabilidades que podrían comprometer la información sensible, permitiendo la priorización de acciones y la asignación eficiente de recursos para mitigar los riesgos más significativos.