**Riesgo:**Usuario del Sistema Sanatorial con acceso a las historias clínicas da a conocer públicamente el estado de un paciente lo que genera acciones legales del paciente hacia el Sanatorio.

**INVENTARIO DE ACTIVOS**

**Escalas de valores:**

1. Muy bajo, 2. Bajo, 3. Medio, 4. Alto, 5. Muy alto

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **ACTIVO** | **TIPO** | **CONTENEDOR** | **RELACIONADOS** | **DUEÑO** | **CUSTODIO** | **C** | **I** | **D** | **Crit.** |
| 1 | Proceso de Atención Ambulatoria | Proceso |  |  | Jefe de Atenciones Ambulatorias | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 5 | 15 |
| 2 | Historias clínicas | Información | Base de datos del Sistema Sanatorial | 1,3,4,5 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 3 | 13 |
| 3 | Informes de Prácticas | Información | Base de Datos del Sistema Sanatorial | 2,4 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 3 | 13 |
| 4 | Sistema sanatorial | Software | Servidor | 1,2,3,5 | Jefa de Sistemas | Empleados de Sistemas, Usuarios del Sistema Sanatorial | 5 | 5 | 5 | 15 |
| 5 | Base de datos del Sistema Sanatorial | Información | Servidor | 4,6 | Jefa de Sistemas | Personal de Sistemas | 4 | 5 | 5 | 13 |
| 6 | Servidor | Hardware | Instalaciones del Departamento de Sistemas |  | Jefa de Sistemas | Personal de Sistemas | 3 | 5 | 5 | 13 |

**IDENTIFICACIÓN DE RIESGOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Id.** 01 |  | | | |
| **Identificador** |  |  | | |
| **Especificación** | Usuario del Sistema Sanatorial con acceso a las historias clínicas da a conocer públicamente el estado de un paciente lo que genera acciones legales del paciente hacia el Sanatorio. | | | |
| **Clasificación** | **Eventos Externos** | | **Cuestiones Legales** | **Litigio.** |
| **Contexto** | | | | |
| **Descripción** | Se trata de un usuario con permisos de acceso al sistema sanatorial, donde, entre otra información sensible, se almacena la historia clínica de los pacientes.  La historia clínica de un paciente contiene información sensible referida a la salud y a las prácticas realizadas en el sanatorio. La divulgación de la información es un delito según lo establecido en la Ley de Protección de Datos Personales (Ley 25326).  Si bien este riesgo, de materializarse, no interrumpe el proceso crítico al que refiere el contexto, está relacionado con la confidencialidad de la información que debe salvaguardarse y a la que acceden todos los usuarios con permiso al sistema. Cuando un usuario divulga información sensible del paciente repercute en la confidencialidad de la información que se maneja en el proceso. | | | |
| **Valoración del Riesgo** | | | | |
| **Factores para evaluar la magnitud de pérdida**  **Activos**: En la planilla de activos se ha establecido el nivel de criticidad de los activos afectados. Además, se pueden considerar:   * **Productividad**: No aplica * **Costo de reemplazo**: Está en relación a la demanda que puede iniciar el paciente afectado. * **Sensibilidad**: En este riesgo se trata la divulgación o uso indebido de información confidencial.   + **Reputación:** Puede verse seriamente afectada   + **Ventaja competitiva**: Los competidores (otros sanatorios) pueden utilizar esto para bajar la imagen del sanatorio   + **Legal / Regulatoria:** Sanciones impuestas por la Ley   + **General**: La información sensible de las prácticas realizadas a los pacientes puede ser utilizada por otras organizaciones (empleadores, medios de comunicación, entidades crediticias) para generar un perjuicio mayor al paciente que puede ser trasladada al sanatorio en una acción legal. * **Volumen:** En este caso el volumen está dado por la cantidad de historias clínicas de pacientes de los que se puede redundar en mayor cantidad de litigios y una mayor repercusión en la credibilidad del sanatorio.   **Amenazas**: la amenaza es la divulgación de la información por un usuario interno   * **Competencia:** el usuario interno tiene las capacidades para acceder a la información por los permisos que se le hayan otorgado * **Internas/Externas:** . * **Acción:**   + **Acceso**: El usuario tiene acceso   + **Uso indebido**: Hace un uso indebido   + **Divulgación**: La divulga (no especifica en el contexto a quien)   + **Modificación**: No aplica   + **Denegación de acceso**: no aplica   **Organización:** El riesgo existe dentro del contexto del sanatorio y ocasiona una acción legal   * **Momento**: No aplica. * **Debido cuidado:** No se conocen medidas preventivas (indicadas en el contexto del riesgo) para mitigar esta amenaza por lo que se deberán considerar en las estrategias de tratamiento del mismo. * **Detección:** No se puede detectar salvo por acciones legales del paciente * **Respuesta:** No se especifica en el riesgo si la organización está preparada para operar ante la materialización del riesgo. En función de esto se puede analizar:   + **Contención**: Se podrían especificar en el momento del contrato laboral acuerdos de confidencialidad (no se conoce su existencia actual). (Ver Seguros)   + **Remediación**: Negociación en el litigio (Conciliación)   + **Recuperación**: Buscar alternativas para mejorar la imagen.   **Factores externos:** Es un riesgo que puede ser utilizado por entidades externas para aumentar el impacto de la pérdida   * **Detección:** Puede ser detectado a través de la información que da el mismo personal, puede que el paciente vaya a los medios de comunicación, etc * **Legal / Regulatorio**: Si. * **Competidores**: Si * **Medios de comunicación**: Si. * **Otros grupos de interés:** Si.   **Utilizando la escala de valores se puede decir que el impacto es: Muy Alto (5).**  **Factores utilizados para el cálculo de la probabilidad:**  **Frecuencia de amenazas**:   * **Contacto**: El contacto de los usuarios con la información de los pacientes es constante   **Aleatorio: -- Regular**: **X** **Intencional**: **X**   * **Acción**: Materializada la amenaza de este riesgo (el acceso y divulgación de información confidencial) el proceso no se ve afectado en su operatoria normal.   + **Beneficio**: No se especifica en el riesgo pero el usuario puede haber cobrado por divulgar la información.   + **Nivel de esfuerzo**: No existe nivel de esfuerzo (el usuario tiene acceso a la información)   + **Riesgo de detección**: Es muy bajo. Pueden ser utilizados los privilegios de acceso pero debería existir trazabilidad de los accesos ya sea para consulta o modificación de datos de cada usuario a cada una de las historias clínicas.   **Vulnerabilidades**:   * **Capacidad de las amenazas**: el usuario tiene la capacidad para identificar las historias clínicas de los pacientes. * **Capacidad de resistencia**(CR): está dada por los acuerdos de confidencialidad (de los cuales no se conoce la existencia) y de la trazabilidad del sistema (que tampoco se conoce).   **Utilizando la escala de valores se puede decir que la probabilidad es: Alta (4).** | | | | |
| **Consecuencias** | Pérdida de credibilidad de los pacientes hacia la organización  Pérdida de credibilidad de el directorio del sanatorio hacia sus empleados | | | |
|  |  |  |  |  |

**TRATAMIENTO DE RIESGOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Id.** 01 | |  | |
| **Identificador** | |  |  |
| **Especificación** | | Usuario del Sistema Sanatorial con acceso a las historias clínicas da a conocer públicamente el estado de un paciente lo que genera acciones legales del paciente hacia el Sanatorio. | |
| **E S T A T E G I A S** | **Evitar** | | |
| No se puede evitar. | | |
| **Transferir** | | |
| Se puede transferir tomando seguros (actúa sobre el impacto) | | |
| **Mitigar** | | |
| En cuanto a mitigar la probabilidad:   1. En el momento de la contratación realizar un análisis más acabado de los valores de las personas contratadas (selección y reclutamiento) 2. Firma de acuerdos de confidencialidad donde se especifiquen las sanciones. 3. Capacitación permanente en seguridad de la información 4. Implementar encriptación de datos de datos sensibles en las historias clínicas y solo accesible a usuarios finales a través de firma digital 5. Implementar ofuscación de datos para datos de prueba antes del pase a entorno de producción (pensando en la posibilidad de la existencia de entorno de prueba en la organización o de datos que maneje la empresa tercerizada) 6. Implementar trazabilidad: Trazabilidad en registros de la base de datos para accesos a cada historia clínica específica en el entorno de producción (ya sea para consulta o modificación). | | |
| **C O N**  **T**  **R**  **O**  **L**  **E**  **S** | Los controles que garantizan las estrategias de transferencia y mitigación mencionadas son:   * Conformidad Normativa y Legal   + Conformidad Legal     - Identificación de la legislación aplicable     - Protección de datos y privacidad de la información personal     - Prevención del uso indebido de recursos de tratamiento de la información   Evidencias objetivas: Informe de revisión periódica de la legislación aplicable (emitido por el estudio jurídico asesor). Constancia de pago de seguros por ataques informáticos que pongan en juego la confidencialidad (más allá de los seguros por responsabilidad civil que pueda haber contratado el sanatorio)  Los controles que garantizan las estrategias de mitigación mencionadas son:   * Seguridad ligada a los recursos humanos   + Previo a la contratación     - Investigación de antecedentes     - Términos y condiciones de la relación laboral   Evidencias objetivas: Documentación del proceso de reclutamiento y selección del personal (informe de antecedentes - investigación de puestos laborales anteriores). Acuerdos de confidencialidad   * + Durante la contratación     - Concientización, educación y capacitación en seguridad de la información   Evidencias objetivas: planes de capacitación, informe de asistencia a capacitaciones, evaluaciones de desempeño   * Control de Accesos   + Requerimientos de Control de Accesos     - Política de Control de Accesos   + Gestión de Accesos de Usuarios (todos los controles incluidos en el objetivo)   Evidencias Objetivas: Documentación de la política de control de accesos (firma digital, definición de perfiles y usuarios). Registros de logs y trazabilidad   * Seguridad en la operativa   + Responsabilidades y procedimientos de operación.     - Separación de los entornos de desarrollo, prueba y producción     - Documentación de procedimientos de operación (para la ofuscación de datos).   + Registro de actividad y supervisión (todos los controles)   Evidencias objetivas: Documentación del procedimiento y definición de responsabilidades, registros de trazabilidad | | |
| **Riesgo Residual** | | | |
| Se puede analizar que:  La probabilidad se puede ver disminuida en función de aplicar las estrategias de mitigación  El impacto se puede disminuir aplicando las estrategias de transferencia  Se puede decir que se baja la severidad del riesgo por bajar el impacto a medio (considerando el pago del seguro) y la probabilidad a medio. | | | |
|  |  |  |  |

**PLANES DE CONTINGENCIA, RECUPERACIÓN Y CONTINUIDAD DE NEGOCIO**

|  |  |  |
| --- | --- | --- |
| **Id.** 01 |  | |
| **Identificador** |  |  |
| **Especificación** | Usuario del Sistema Sanatorial con acceso a las historias clínicas da a conocer públicamente el estado de un paciente lo que genera acciones legales del paciente hacia el Sanatorio | |
| **Disparadores** | 1. El paciente que hace la demanda al Sanatorio | |
| **Contingencia** | 1. Se indagan los posibles responsables en función de las estrategias de mitigación identificadas en Trazabilidad 2. Aplicar lo definido en el acuerdo de confidencialidad (puede ser quitarle permisos de acceso) | |
| **Recuperación** | 1. Resolución del conflicto 2. Ver qué sanción aplica a él/los usuarios que divulgaron la información | |
| **Continuidad de Negocio** | 1. Dependiendo de los usuarios afectados se tendrá que recurrir a otros usuarios que realicen las tareas afectadas. | |
| **Controles de Garantía de los Planes** | Los controles que garantizan la ejecución de planes de contingencia, recuperación y continuidad de Negocios mencionadas son:   * Aspectos de la Seguridad de la información en la gestión de la continuidad de Negocio   + Continuidad de la seguridad de la información.     - Verificación, revisión y evaluación de la continuidad de la seguridad de la información.   Evidencias Objetivas: Informes de simulacros de materialización del riesgo revisando trazabilidad   * Gestión de Incidentes en la seguridad de la información.   + Gestión de incidentes de seguridad de la información y mejoras.   + Responsabilidades y procedimientos.   + Notificación de los eventos de seguridad de la información.   + Notificación de puntos débiles de la seguridad.   + Valoración de eventos de seguridad de la información y toma de   + decisiones.   + Respuesta a los incidentes de seguridad.   + Aprendizaje de los incidentes de seguridad de la información.   + Recopilación de evidencias.   Evidencias objetivas:Documentación de la materialización del riesgo, documentación de los procedimientos de Contingencia, Recuperación y Continuidad de Negocio  Cumplimiento de requisitos legales/contractuales (de los usuarios). | |