**Riesgo:**

Un cambio requerido a la empresa proveedora del Software Sanatorial relacionado con el sistema de atención ambulatoria y que refiere al registro de datos específicos de los pacientes para la realización de las atenciones ambulatorias a partir de una determinada fecha, no cumple con los plazos establecidos en el SLA

**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 | Sistema sanatorial | Software | Servidor | 1,3,4,5,6,7 | Jefa de Sistemas | Empleados de Sistemas, Usuarios del Sistema Sanatorial | 5 | 5 | 5 | 15 |
| 3 | Informes de Prácticas | Información | Base de Datos del Sistema Sanatorial | 1,5 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 5 | 15 |
| 4 | Turnos | Información | Base de Datos del Sistema Sanatorial | 1,2 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 3 | 3 | 5 | 11 |
| 5 | Historias clínicas | Información | Base de datos del Sistema Sanatorial | 1,2,3 | Paciente | Empleados de Atención Ambulatoria  Enfermeras  Médicos de Atención Ambulatoria | 5 | 5 | 3 | 13 |
| 6 | Base de datos del Sistema Sanatorial | Información | Servidor | 7,8 | Jefa de Sistemas | Personal de Sistemas | 4 | 5 | 5 | 13 |
| 7 | Gestor de Base de Datos | Software | Servidor | 8 | Jefa | Personal de Sistemas | 1 | 5 | 5 | 11 |
| 8 | Servidor | Hardware | Instalaciones del Departamento de Sistemas |  | Jefa de Sistemas | Personal de Sistemas | 3 | 5 | 5 | 13 |

**IDENTIFICACIÓN DE RIESGOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Id.** 01 |  | | | |
| **Identificador** |  |  | | |
| **Especificación** | Un cambio requerido a la empresa proveedora del Software Sanatorial relacionado con el sistema de atención ambulatoria y que refiere al registro de datos específicos de los pacientes para la realización de las atenciones ambulatorias a partir de una determinada fecha, no cumple con los plazos establecidos en el SLA. | | | |
| **Clasificación** | **Eventos Externos** | | **Cuestiones de Negocio** | **Fallas en el suministro.** |
| **Contexto** | | | | |
| **Descripción** | No se cumplen los tiempos preestablecidos en el SLA con la empresa tercerizada.  Esto ocasiona que en el proceso de atención ambulatoria no se puedan registrar en el sistema datos específicos de los pacientes para la realización de las atenciones ambulatorias que se requieren a partir de una determinada fecha.  Los administrativos del sector ambulatorio están capacitados para registrar todos los datos inherentes al proceso y conocen los requerimientos del proceso para operar correctamente.  En este específico caso al no contar con la posibilidad de registrar datos de los pacientes que se requieren registrar a partir de una determinada fecha, el problema recaerá en la imposibilidad de continuar con el proceso en forma correcta. | | | |
| **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**: La imposibilidad de registrar los datos de los pacientes para las atenciones ambulatorias pueden repercutir en el flujo del proceso y generará un impacto en la productividad ya que de alguna forma dichos datos deberán ser evaluados en forma manual para ejecutar las actividades del proceso (ya no por el registro en el sistema) * **Costo de reemplazo**: No existe costo de reemplazo ya que el activo en sí no ha sido dañado, sin embargo, puede considerarse el costo de reproceso para registrar los datos en el sistema una vez que el software haya sido efectivamente actualizado. * **Sensibilidad**: En este riesgo no se trata la divulgación o uso indebido de información confidencial.   + **Reputación:** No aplica   + **Ventaja competitiva**: No aplica   + **Legal / Regulatoria:** No aplica   + **General**: No aplica * **Volumen:** En este caso el volumen está dado por la cantidad de pacientes que se han presentado a partir de la fecha determinada en la que se debían registrar sus datos. Más tiempo pase en que la empresa tercerizada incumpla con el requerimiento se deberá considerar una mayor magnitud de pérdida.   **Amenazas** el incumplimiento del SLA por parte de la empresa tercerizada constituye la amenaza.   * **Competencia:** la empresa tercerizada conoce las pautas consideradas en el SLA y tiene las competencias necesarias para conocer el perjuicio que causa sobre el proceso. * **Internas/Externas:** el desarrollo de la funcionalidad requerida está en manos de la empresa tercerizada (externa), por lo que no se tiene control total sobre la misma. * **Acción:**   + **Acceso**: No aplica   + **Uso indebido**: No aplica   + **Divulgación**: No aplica   + **Modificación**: No aplica   + **Denegación de acceso**: en principio podría considerarse una denegación de acceso a la nueva versión de software a utilizar   **Organización:** El riesgo existe dentro del contexto del sanatorio y el riesgo ocasiona la pérdida de la capacidad de operar normalmente   * **Momento**: La atención sanatorial es continua por lo que la no entrega en tiempo y forma de la funcionalidad requerida tendrá un impacto de pérdida alto. * **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:** La detección (si no se han tomado medidas anteriores para conocer el grado de avance en el desarrollo de la funcionalidad) se dará el día que se requieran procesar los datos y la funcionalidad no esté instalada * **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**: El personal está capacitado para conocer los requerimientos de información del proceso (podría actuar ante la materialización.   + **Remediación**: No aplica   + **Recuperación**: Una vez instalada la nueva versión y actualizados los datos que no se han podido registrar hasta el momento en el sistema, recién podrá volver a la normalidad el funcionamiento   **Factores externos:** No es un riesgo que pueda ser utilizado por ninguna entidad externa para aumentar el impacto de la pérdida   * **Detección:** No aplica. * **Legal / Regulatorio**: No aplica. * **Competidores**: No aplica. * **Medios de comunicación**: No aplica. * **Otros grupos de interés:** No aplica   **Utilizando la escala de valores se puede decir que el impacto es: Alto (4).**  **Factores utilizados para el cálculo de la probabilidad:**  **Frecuencia de amenazas**:   * **Contacto**: La solicitud de requerimientos a la empresa tercerizada es frecuente ya que la misma se encarga del mantenimiento del software y de ella se depende para la correcta operatoria del mismo   **Aleatorio: -- Regular**: **X** **Intencional**: **--**   * **Acción**: Materializada la amenaza de este riesgo (la no entrega en tiempo y forma de la solución a los requerimientos solicitados) el proceso se ve afectado en su operatoria normal.   + **Beneficio**: No existe beneficio de la empresa tercerizada   + **Nivel de esfuerzo**: No existe nivel de esfuerzo (ya que es un requerimiento que todavía no ha sido instalado y lo que se debe hacer es cumplir con el mismo)   + **Riesgo de detección**: es fácilmente detectable en no cumplimiento de la entrega de la nueva versión del software   **Vulnerabilidades**: La única posibilidad de resistir las acciones del agente de amenaza es no utilizando el sistema para el registro de los datos que se deben requerir desde una determinada fecha.   * **Capacidad de las amenazas**: El nivel probable de fuerza de la empresa tercerizada(agente de amenaza) sobre el proceso (activo) es muy alto ya que se depende de la mismo para poder operar. Tiene las habilidades y los recursos para materializar la amenaza. * **Capacidad de resistencia**(CR): Los empleados administrativos que operan en la atención al público están altamente capacitados para requerir al paciente toda la información que se necesita para cada tipo de atención ambulatoria (capacidad de resistencia) por lo que solicitarán al paciente dicha información, pero la misma no quedará registrada en el sistema para continuar con el proceso.   **Utilizando la escala de valores se puede decir que la probabilidad es: Muy Alta (5).** | | | | |
| **Consecuencias** | Toda información que se requiera del sistema, en la que los datos que no han podido registrarse deban ser analizados, no podrá obtenerse hasta tanto se recupere el proceso una vez materializado el riesgo. | | | |
|  |  |  |  |  |

**TRATAMIENTO DE RIESGOS**

|  |  |  |  |
| --- | --- | --- | --- |
| **Id.** 01 | |  | |
| **Identificador** | |  |  |
| **Especificación** | | Un cambio requerido a la empresa proveedora del Software Sanatorial relacionado con el sistema de atención ambulatoria y que refiere al registro de datos específicos de los pacientes para la realización de las atenciones ambulatorias a partir de una determinada fecha, no cumple con los plazos establecidos en el SLA | |
| **E S T A T E G I A S** | **Evitar** | | |
| La única forma de evitar la materialización de este riesgo sería implementar el desarrollo del software en la organización y no depender de una empresa externa. No obstante, el mismo riesgo podría ser tratado ya que el incumplimiento de plazos en la puesta en producción de una nueva versión de software puede darse con un equipo de desarrollo interno. | | |
| **Transferir** | | |
| No se puede transferir. | | |
| **Mitigar** | | |
| En cuanto a mitigar la probabilidad e impacto de la materialización del riesgo:   1. Aumentar la detección temprana de la posible materialización del riesgo: Realizar controles y seguimientos periódicos a la empresa tercerizada sobre el avance del desarrollo de los requerimientos solicitados en función del plan de trabajo establecido (que debe constar en el SLA acordado) 2. Incluir en los SLA cláusulas de sanción por incumplimiento de plazos que especifiquen el monto a ser retenido por el sanatorio a la empresa tercerizada por cada día de incumplimiento en el plazo estipulado. Este monto podrá ser calculado en función de la cantidad de horas que lleve el reproceso de cada día de incumplimiento.   En cuanto a mitigar el impacto de la materialización del riesgo:   1. Especificar procedimiento manual para la actividad afectada:    1. Especificar el procedimiento para dejar asentados manualmente los datos requeridos ante cada ingreso donde los datos no puedan ser procesado por el sistema. Identificar estos ingresos en una planilla para que en el momento en que se cuente con la posibilidad de registro, los datos sean procesados en el sistema.    2. Capacitar a los empleados que intervienen en el proceso en la operatoria manual y en el reproceso de los datos (sobre el uso y salvaguarda de los datos)    3. Especificar el procedimiento para el vuelco de la información manual al sistema una vez instalada la versión del software | | |
| **C O N**  **T**  **R**  **O**  **L**  **E**  **S** | Los controles que garantizan las estrategias de mitigación mencionadas son:  Estrategias 1 y 2.   * Relaciones con suministradores   + Seguridad de la información en la relación con suministradores     - Tratamiento del riesgo en relación con suministradores   + Gestión de la prestación del servicio por suministradores.     - Supervisión y revisión de los servicios prestados por terceros.   Evidencias objetivas: Informe de seguimiento del plan de trabajo, SLA con planes de trabajo acordados.  Estrategia 3:   * Aspectos de la Seguridad de la información en la gestión de la continuidad de Negocio   + Continuidad de la seguridad de la información.     - Planificación de la continuidad de la seguridad de la información.   Evidencias objetivas: Análisis de tratamiento de la información y especificación de procedimientos en caso de fallas en los sistemas específicos   * Adquisición, desarrollo y mantenimiento de los sistemas de información   + Seguridad en los procesos de desarrollo y soporte     - Procedimientos de control de cambios en los sistemas   Evidencias objetivas: Casos de uso del requerimiento, procedimientos normales de operación y de operación manual en caso de fallas en los sistemas específicos   * Seguridad en la operativa   + Responsabilidades y procedimientos de operación.     - Documentación de procedimientos de operación.   Evidencias objetivas: Documentación del procedimiento y definición de responsabilidades   * Seguridad ligada a los recursos humanos   + 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 | | |
| **Riesgo Residual** | | | |
| Se puede analizar que:  La probabilidad se puede ver disminuida en función de aplicar las estrategias 1 y 2  El impacto se puede disminuir aplicando las estrategias 1, 2 y 3  Se puede decir que se baja la severidad del riesgo, el impacto a medio y la probabilidad a bajo. | | | |
|  |  |  |  |

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

|  |  |  |
| --- | --- | --- |
| **Id.** 01 |  | |
| **Identificador** |  |  |
| **Especificación** | Un cambio requerido a la empresa proveedora del Software Sanatorial relacionado con el sistema de atención ambulatoria y que refiere al registro de datos específicos de los pacientes para la realización de las atenciones ambulatorias a partir de una determinada fecha, no cumple con los plazos establecidos en el SLA | |
| **Disparadores** | 1. El seguimiento del plan de trabajo puede advertir que la nueva versión del software no podrá ser instalada en tiempo. Esto puede detectarse gracias a la estrategia de mitigación 1 evaluada. A partir de esto el personal ya estará informado que se seguirá con el procedimiento manual para el que fueron capacitados | |
| **Contingencia** | 1. Utilizar el procedimiento manual desde el ingreso. | |
| **Recuperación** | Una vez instalada la nueva versión y para nuevos ingresos de pacientes se seguirá el procedimiento manual.  Para la recuperación de los ingresos de los cuales no se hayan registrado los datos se seguirá el procedimiento especificado en la estrategia de mitigación 3, item 3.  Se deberá calcular la mora incurrida por la empresa tercerizada para establecer la sanción por incumplimiento y se debitará de la cuenta de la misma.  Documentar el tratamiento del incidente | |
| **Continuidad de Negocio** | 1. Se sigue con el procedimiento manual hasta que la nueva versión del software haya sido instalada. | |
| **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   * 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: SLA, Documentación de la materialización del riesgo, documentación de los procedimientos de Contingencia, Recuperación y Continuidad de Negocio   * Relaciones con suministradores   + Gestión de la prestación del servicio por suministradores.     - Supervisión y revisión de los servicios prestados por terceros.   Evidencias Objetivas: Informe de incumplimiento del SLA acordado. Crédito a favor del Sanatorio en la cuenta corriente de la Empresa tercerizada | |