**Riesgo:**

Una falla en los discos del servidor deja inutilizable la base de datos en el momento de mayor afluencia de pacientes al área de admisión imposibilitando el uso del sistema y generando pérdida de la información

**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 | Disco Rígido | Hardware | Instalaciones del Departamento de Sistemas | 3,4,5,6 | Jefa de Sistemas | Personal de Sistemas | 4 | 5 | 5 | 14 |
| 3 | Base de datos del Sistema Sanatorial | Información | Servidor, PC de los usuarios | 4 | Jefa de Sistemas | Personal de Sistemas | 4 | 5 | 5 | 13 |
| 4 | Gestor de Base de Datos | Software | Servidor | 3 | Jefa | Personal de Sistemas | 1 | 5 | 5 | 11 |
| 5 | Servidor | Hardware | Instalaciones del Departamento de Sistemas |  | Jefa de Sistemas | Personal de Sistemas | 3 | 5 | 5 | 13 |
| 6 | Sistema Operativo | Software | Servidor | 4 | Jefa de Sistemas | Personal de Sistemas | 3 | 5 | 5 | 13 |
| 7 | Sistema sanatorial | Software | Servidor | 1,3,4,5,6,7 | Jefa de Sistemas | Personal de Sistemas, Usuarios del Sistema Sanatorial | 5 | 5 | 5 | 15 |
|  |  |  |  |  |  |  |  |  |  |  |

**IDENTIFICACIÓN DE RIESGOS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Id.** 01 |  | | | |
| **Identificador** | **Legajo:** | **Apellido y Nombres:** | | |
| **Especificación** | Una falla en los discos del servidor deja inutilizable la base de datos en el momento de mayor afluencia de pacientes al área de admisión imposibilitando el uso del sistema y generando pérdida de la información. | | | |
| **Clasificación** | **Fallas de Sistemas y Tecnología** | | **Hardware** | **Mantenimiento/Obsolescencia.** |
| **Contexto** | | | | |
| **Descripción** | El desarrollo del proceso requiere la interacción constante con el sistema sanatorial. Los datos registrados en la base de datos del sistema son requeridos en cada interacción, ya sea en la admisión (el caso particular de este riesgo) donde no se podrá corroborar el turno del paciente ni registrar su asistencia, como tampoco los datos requeridos para su atención.  Por otra parte, hay que analizar si en función de la magnitud de la falla del disco:   1. Puede repararse 2. Requiere reemplazo del disco   En cualquier situación, se deberá restaurar la información de una copia de la base de datos para poder seguir el proceso con normalidad (suponiendo que el disco era único o que no se pudo realizar el proceso de recuperación de un RAID). | | | |
| **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 utilizar el sistema (por rotura del disco donde reside la base de datos) para las atenciones ambulatorias pueden repercutir en el flujo del proceso y generará un impacto en la productividad ya que la información requerida para la atención deberá ser evaluada en forma manual para ejecutar las actividades del proceso (ya no por el registro en el sistema) * **Costo de reemplazo**: Este costo estará dado por: el arreglo o reemplazo del disco que ha fallado, el tiempo del personal de sistemas encargado de restaurar la copia, el tiempo que se requiere para reprocesar la información que no haya quedado en el sistema (la perdida por rotura y la nueva información que se procesará en forma manual hasta tanto se haya iniciado nuevamente el sistema). * **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 estará dado por:   + cantidad de pacientes que se han presentado a partir de la materialización del riesgo y todos los datos de la atención han debido registrarse en forma manual   + información perdida entre la última copia realizada de la base de datos y el momento de materialización del riesgo.   **Amenazas** El estado de los discos en el servidor constituye la amenaza.   * **Competencia:** El conocimiento del estado del servidor es responsabilidad de la Jefa de Sistemas y del Personal del área de sistemas * **Internas/Externas:** es una amenaza interna por lo que debería tenerse control total sobre la misma. * **Acción:**   + **Acceso**: No aplica   + **Uso indebido**: No aplica   + **Divulgación**: No aplica   + **Modificación**: No aplica   + **Denegación de acceso**: lo que sucede es la denegación de acceso a la base de datos del sistema sanatorial (relacionada con los activos de información)   **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 una falla del disco tendrá un impacto de pérdida alto sobre todo en los momentos de mayor afluencia de público. * **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 de este. * **Detección:** La detección se dará en el momento en que falle el disco, ya sea por un monitoreo por parte del Personal del área de Sistemas o por un aviso de los usuarios del sistema a los que se les ha denegado el acceso * **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**: Se podrá revisar la posibilidad de reparar/reemplazar el disco dañado   + **Recuperación**: Una vez reparado/instalado el nuevo disco se deberán realizar la instalaciones de software de base requeridas y la base de datos al estado más actual posible (desde una copia reciente). El sistema sanatorial podrá estar activo a partir de ese momento para nuevas admisiones. La información perdida (entre la última copia y el momento de materialización del riesgo) deberá ser reprocesada, como así también la que haya sido trabajada en forma manual a partir de la materialización del riesgo   **Factores externos:** Este puede ser un riesgo que pueda ser utilizado por entidades externas para aumentar el impacto de la pérdida   * **Detección:** No aplica. * **Legal / Regulatorio**: No aplica. * **Competidores**: Los competidores pueden utilizar esta información para bajar la imagen de la organización (bajo). * **Medios de comunicación**: Idem competidores. * **Otros grupos de interés:** No aplica   **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 uso de los discos es intensivo   **Aleatorio: -- Regular**: **X** **Intencional**: **--**   * **Acción**: Materializado el riesgo el proceso se ve afectado en su operatoria normal.   + **Beneficio**: No existe beneficio   + **Nivel de esfuerzo**: No existe nivel de esfuerzo si los discos no tienen mantenimiento o son obsoletos   + **Riesgo de detección**: es fácilmente detectable la caída del sistema por falla en un disco   **Vulnerabilidades**: Deben evaluarse estrategias para resistir las acciones del agente de amenaza, trabajando sobre el activo en sí y sobre los activos que afecta la materialización del riesgo.   * **Capacidad de las amenazas**: El nivel probable de fuerza de la falla del disco (agente de amenaza) sobre el proceso (activo) es muy alto ya que se depende del mismo para poder operar. La falta de mantenimiento y la obsolescencia son las capacidades que están en juego para la materialización del riesgo. * **Capacidad de resistencia** (CR): Los empleados administrativos que operan en la atención 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, como tampoco la información de las restantes actividades del proceso.   **Utilizando la escala de valores se puede decir que la probabilidad es: Alta (4).** | | | | |
| **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** | | **Legajo:** | **Apellido y Nombres:** |
| **Especificación** | | Una falla en los discos del servidor deja inutilizable la base de datos en el momento de mayor afluencia de pacientes al área de admisión imposibilitando el uso del sistema y generando pérdida de la información | |
| **E S T A T E G I A S** | **Evitar** | | |
| Se puede evitar la materialización del riesgo utilizando otro tipo de infraestructura para la operación de los sistemas del Sanatorio | | |
| **Transferir** | | |
| 1. Utilizar servicios en la Nube como infraestructura de los sistemas del Sanatorio | | |
| **Mitigar** | | |
| En cuanto a mitigar la probabilidad de materialización del riesgo:   1. Implementar infraestructura de RAID de discos en el Servidor. Baja la probabilidad de que más de un disco falle. Se utiliza la paridad en la recuperación y no se pierde información.   En este caso se analizará para la continuidad del negocio el tiempo de reposición del disco   1. Aumentar la detección temprana de la posible materialización del riesgo: Realizar controles y seguimientos periódicos del estado de los discos. Realizar recambios considerando el período de obsolescencia programado. Esta actividad es interna a la organización ya que el personal del área de sistemas es el que se encarga del soporte técnico de la infraestructura.   En cuanto a mitigar el impacto de la materialización del riesgo:   1. Contar con discos de recambio para poder reemplazarlos en caso de falla o con un acuerdo de suministro de los mismos en tiempo y forma contratando un servicio de este tipo que actúe 24 x 7 (SLA). Esto actúa sobre el tiempo de recuperación del incidente por lo que actúa sobre la magnitud de la pérdida (como se especificó en el análisis FAIR anterior) 2. Especificar procedimiento manual para las actividades afectadas (continuidad del negocio):    1. Especificar y definir la nueva versión del software para dejar asentados en otro formato digital todos los datos de las admisiones y su vuelco posterior al sistema una vez recuperado el mismo (solicitar a la empresa tercerizada)    2. Especificar el procedimiento de armado de un legajo físico que será luego transferido a cada sector correspondiente y deberá ser devuelto al área de admisión para el registro posterior una vez recuperado el sistema    3. Especificar el procedimiento para el vuelco de la información manual al sistema una vez recuperado el sistema    4. Capacitar a los empleados que intervienen en el proceso en la operatoria manual y en el reproceso de los datos (y sobre el uso y salvaguarda de los datos) 3. Analizar y mejorar el tiempo entre copias de seguridad y el resguardo físico o digital en otro medio de almacenamiento de la información procesada en el tiempo entre copias de seguridad con indicación temporal para que pueda ser registrada en el sistema nuevamente en caso de falla (según 4.c). Esto actúa sobre la magnitud de la pérdida de información registrada en el sistema anterior a la materialización del riesgo y posterior a la última copia de seguridad con posibilidad de ser resguardada. | | |
| **C O N**  **T**  **R**  **O**  **L**  **E**  **S** | Los controles que garantizan las estrategias de mitigación mencionadas son:  Estrategias 1 y 2:   * Seguridad Física y ambiental   + Seguridad de los equipos.     - Mantenimiento de los equipos   Evidencias objetivas: Especificación de la infraestructura. Informes de revisión de la infraestructura.  Estrategia 3:   * Relaciones con suministradores   + Gestión de la prestación del servicio por suministradores.     - Supervisión y revisión de los servicios prestados por terceros.   Evidencias objetivas: SLA en relación a la provisión de discos en caso de fallas. Pago del servicio en tiempo y forma.  Estrategia 4 y 5:   * 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   * 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  Estrategia 5:   * Seguridad en la operación   + Copias de seguridad.     - Copias de seguridad de la información.   Evidencias objetivas: Log de realización de copias de seguridad. Informe sobre análisis del tiempo entre copias de seguridad | | |
| **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 3 a 5  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** | **Legajo:** | **Apellido y Nombres:** |
| **Especificación** | Una falla en los discos del servidor deja inutilizable la base de datos en el momento de mayor afluencia de pacientes al área de admisión imposibilitando el uso del sistema y generando pérdida de la información | |
| **Disparadores** | 1. Personal del área de Sistema que monitorea los estados de la infraestructura detecta la caída del disco 2. Operación anormal (baja de performance) en caso de haberse implementado un sistema RAID (detección por parte del usuario) 3. Falla la conexión a la base de datos del sistema (detección por parte del usuario) | |
| **Contingencia** | En caso de RAID:  (Estrategias de mitigación 1 y 3)   1. Se solicitará a los usuarios minimizar los accesos al sistema si los discos son Hot Swap ya que se podrá seguir utilizando el mismo, pero bajará la performance. 2. Se indicará a los usuarios el tiempo (que deberá estar especificado ya que no deberá ser menor a XXX minutos para no demorar la ejecución de las actividades del proceso) en los que el sistema volverá a la normalidad en su operación 3. Se utiliza el disco adicional con el que se cuenta o se solicita al proveedor con el que se tiene el SLA acordado que suministre el disco que se necesita 4. Se hace el cambio del disco con la falla y el sistema copia la paridad de los otros discos hasta que se recupera.   En caso de una falla en más de un disco RAID o único disco:  (No se utilizó la estrategia 1)   1. Se avisa a los usuarios de la imposibilidad de utilizar el sistema hasta tanto se recupere indicando el tiempo estimado | |
| **Recuperación** | En caso de RAID y falla de un solo disco:  (Estrategias de mitigación 1 y 3)   1. Se utiliza el disco adicional con el que se cuenta o se solicita al proveedor con el que se tiene el SLA acordado que suministre el disco que se necesita 2. Se hace el cambio del disco con la falla y el sistema copia la paridad de los otros discos hasta que se recupera. 3. Se avisa a los usuarios que ya pueden utilizar el sistema 4. Documentar el tratamiento del incidente   En caso de una falla en más de un disco RAID o único disco:  (No se utilizó la estrategia 1)   1. Se utiliza el disco adicional con el que se cuenta o se solicita al proveedor con el que se tiene el SLA acordado que suministre el disco que se necesita 2. Se reinstalan sistema operativo, SGBD y se lo configura 3. Se recupera la última copia de seguridad de la Base de Datos 4. Se avisa a los usuarios que pueden comenzar a utilizar el sistema para nuevos ingresos de pacientes 5. 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 4, item c. 6. Para la recuperación de la información perdida entre la última copia y la materialización del riesgo se pone en práctica el procedimiento de registro indicado en la estrategia de mitigación 5. 7. Documentar el tratamiento del incidente | |
| **Continuidad de Negocio** | En caso de RAID y falla de un solo disco:   1. Se atienden solo las urgencias para no sobrecargar el sistema. En caso de ser muy bajo el rendimiento del equipo se solicita seguir con el procedimiento manual.   En caso de una falla en más de un disco RAID o único disco:  (No se utilizó la estrategia 1)   1. Se utiliza el procedimiento de registro manual identificado en la estrategia de mitigación 4. Item a. | |
| **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. | |