Modelo de plan de continuidad para un sistema de almacenamiento y comunicación de imágenes diagnósticas.

Continuity plan model for a picture archiving and communication systems for diagnostic images.

Jorge Armando Aquite Bedoya
jorge.aquite00@usc.edu.co

Isaac Nañez Encalada
isaac.nanez00@usc.edu.co

Diego Fernando Loaiza Buitrago
diego.loaiza02@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de Sistemas (1)
Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de Sistemas (2)

Resumen
Actualmente la manera más eficiente y segura de tener control y registro de grandes volúmenes de imágenes diagnósticas que se realizan en una institución de salud, es mediante un sistema de almacenamiento de comunicación de imágenes conocido como PACS (Picture Archiving and Communication System). Siendo este un sistema que se soporta en las infraestructuras tecnológicas, se necesita contar con procedimientos que permitan continuar el flujo normal de la operación del servicio, previniendo o mitigando los eventos adversos que puedan ocurrir y también permitir una recuperación del estado normal de la operación. Estos procedimientos quedarán consignados en un plan de continuidad que será diseñado con base en algunos de los subprocesos de Gestión de Riesgos y Gestión de la Continuidad, ambos procesos de Diseño del Servicio de ITIL V3. Bajo esta metodología se evaluaron los riesgos de acuerdo con su nivel de impacto y probabilidad de ocurrencia, logrando desarrollar un plan más conciso y enfocado a la contención, gestión y recuperación de estos riesgos.

Palabras Clave: PACS, plan de continuidad, imágenes diagnósticas, gestión de riesgos, gestión de continuidad.

Abstract
Currently the most efficient and safe way to have control and record large volumes of diagnostic images that are performed in a health institution is through a picture archiving and communication system known as PACS (Picture Archiving and Communication System). Being this a system that is supported in the technological infrastructures, it is necessary to have procedures that allow to continue the normal flow of the operation of the service, preventing or mitigating the adverse events that may occur and also allowing a recovery of the normal state of the operation. These procedures will be consigned in a continuity plan that will be designed based on some of the subprocesses of Risk Management and Continuity Management, both processes from Service Design from ITIL V3. Under this methodology, the risks were evaluated according to their level of impact and probability of occurrence, achieving to develop a more concise plan focused on the containment, management and recovery of an adverse event.

Keywords: PACS, continuity plan, diagnostic imaging, risk management, continuity management.

1. INTRODUCCIÓN

El sistema de almacenamiento y comunicación de imágenes (PACS), como cualquier otro sistema de información que sustenta la operación de un negocio, necesita de estrategias que maximicen la calidad de la información y se minimicen los riesgos. Pero el mundo real no se encuentra exento de eventos que atenten la continuidad de la operación del servicio. Por lo tanto, se han establecido marcos de gestión para la seguridad de la información, como el conjunto de estándares que reúne la ISO/IEC 27000 o ITIL V3 (Adams, Simon; OGC - Office of Government Commerce, 2008).

Basado en los estándares y buenas prácticas se establecen los planes de continuidad del servicio, estos planes son un conjunto de actividades dirigidas a contrarrestar las interrupciones, proteger los procesos críticos, limitar las fallas o desastres y buscar la reanudación oportuna de los servicios de TI (Verdú Fernández, 2015).

Los antecedentes que se tienen y en los que se enfocó el trabajo hacen referencia a hospitales y sus servicios de TICS, uno de ellos es el Hospital Italiano (Argentina) de Buenos aires (Hospital Italiano de Buenos Aires, 2009). Éste estableció

un plan de continuidad que alcanzaba 4 fases: desde el aviso de incidente e inicio de contingencia, la operatoria durante la misma, la comunicación del fin de la contingencia y el registro de datos una vez restablecido el sistema. Nos interesa y tomaremos como guía, el trabajo que hace el plan de continuidad, en la fase de inicio, donde abarca la activación y la notificación a los afectados.

En el Hospital Vitarte de Perú (Agui Reynoso & Huacho Aliaga, 2012) se presenta un plan de contingencia para asegurar la infraestructura de la red y sistemas de información del hospital. Se desarrolla desde el área de la Informática en coordinación con las sedes internas y externas de la entidad. Con la finalidad de tener las normas y procedimientos necesarios para afrontar cualquier eventualidad que se produzca en los servicios TI y comunicación del hospital, para proteger o estar preparados frente a un evento crítico y poder minimizar el impacto o las consecuencias de este evento. Es un plan de contingencia muy completo, y sería una guía para la presente investigación, porque es un plan que fue elaborado tomando base de la metodología de ITIL, su estructura está dividida en análisis de riesgos, plan de respaldo, plan de recuperación, plan de mantenimiento y plan de entrenamiento.

Para el caso del presente trabajo, se plantea poder continuar con la alta calidad de atención de la institución prestadora de servicios de salud (The Joint Commission, 2018), considerando que no hay un plan de acción en caso de una caída del servicio de almacenamiento y transferencia de imágenes diagnósticas. El servicio de imágenes diagnósticas cuenta con sub-servicios, éstos se encuentran físicamente dentro del mismo lugar, pero los métodos de captura de imagen e interpretación de estas difieren entre sí. Se realiza de manera diaria aproximadamente 500 estudios, solo contando imágenes diagnósticas, de los cuales en promedio 180 son de pacientes remitidos. El despliegue de las imágenes y la entrega del reporte al servicio que remite el paciente no debe superar las 2 horas, tiempo que se cuenta a partir de la solicitud de la adquisición del estudio. La caída prolongada del sistema de almacenamiento PACS, atentaría contra los acuerdos realizados por el servicio de imágenes diagnósticas con los servicios de hospitalización y tratamiento.

El plan de continuidad para el servicio de imágenes diagnósticas es necesario en vista de que el almacenamiento y transferencia de imágenes pueda fallar, no restablecer el funcionamiento normal u ofrecer una contingencia que, en el peor de los escenarios, podría afectar la atención de un paciente crítico en urgencias. Por lo tanto, la no adquisición e interpretación de una imagen clínica impide que el médico especialista lo remita con prioridad a cirugía, para efectuar un procedimiento que es urgente, permitiendo conservar su integridad o incluso su vida.

La finalidad del presente trabajo es poder diseñar y documentar un plan de continuidad de servicio para el sistema PACS de una institución prestadora de servicios de salud. Este documento estaría estructurado con ayuda de todo el contenido de una matriz de riesgos y las buenas prácticas de ITIL V3.

Este proceso se plantea con un método que va determinado por la gestión de la continuidad del servicio de ITIL V3, en la infraestructura que soporta la solución PACS de la institución prestadora de servicios de salud y su aplicación en este caso. Se construirá una matriz de riesgos (probabilidad e impacto), los riesgos inherentes que puedan atentar en la continuidad de la prestación del servicio, teniendo como soporte los procesos de diseño del servicio y empleando los datos obtenidos de la matriz de riesgos construida, se diseñará el plan de continuidad para mitigar los riesgos hallados y definir las estrategias para asegurar la continuidad del servicio.

2. MATERIALES Y MÉTODOS/METODOLOGÍA

Para la ejecución del trabajo de investigación era necesario realizar tareas específicas para obtener el resultado deseado. Se realizó con el apoyo de la institución prestadora de servicios de salud, lo que nos permitió tener acceso a la información que era fundamental para nuestro proyecto, con algunas restricciones acordadas.

Se planteó el diseño de un plan de continuidad del servicio para el sistema PACS de la institución prestadora de servicios de salud. El contenido del trabajo de investigación se llevó a cabo en cuatro etapas: la identificación del servicio, medidas actuales de contingencia y la evaluación de riesgos. Ésta se representó con una matriz de riesgo (probabilidad e impacto), la cual contiene los riesgos inherentes, con los que se afectan la continuidad del servicio y su respectivo control.

Después de elaborar lo anterior y con base a ITIL V3, pasamos al diseño del plan de continuidad, diseñando el plan con unas actividades que tenían la misión de mitigar los riesgos hallados y definir las estrategias para asegurar la operación con el menor tiempo de interrupción del servicio.

Los pasos son:

Identificación del servicio

La primera tarea que se realizó fue el levantamiento del diagrama de flujo de operación del servicio de imagenología, desde la solicitud de los procedimientos en los servicios hasta la entrega del informe. De esta manera se logró una mayor comprensión del proceso durante la ejecución del mismo, la operación diaria, los incidentes, eventos y problemas que se generan y los recursos (personas, infraestructura, información y aplicaciones) que componen al servicio.

Medidas actuales de contingencia

La segunda tarea fue la identificación y revisión de sistemas de contingencias existentes tanto en los procesos de imagenología, como la infraestructura tecnológica que soporta la operación del servicio.

Evaluación de riesgos

Conociendo el proceso y los actores que en él influyen, el tercer paso fue la estructuración de la matriz de riesgo. De este modo se identificó, valoró y categorizaron los riesgos que podían afectar la prestación del servicio. Esta matriz se analizó para establecer los controles o las contingencias necesarias para evitar las interrupciones del servicio.

Se procedió a realizar las siguientes actividades para evaluar los riesgos que pudieran afectar el flujo normal de las actividades diarias del servicio de imagenología, pero antes se evaluó el sistema de almacenamiento y comunicación de imágenes (PACS):

- Identificación de los activos o recursos que componen la operación del servicio: se llevó a cabo el análisis de cada recurso con su respectiva descripción y categorización que se encuentra en el servicio de PACS.

- Definir los riesgos de cada categoría de activo: se tomó cada categoría de los activos que existe en el servicio y se definieron los riesgos posibles.

- Calificar la probabilidad e impacto de afectación a la operación del servicio por cada riesgo. Para encontrar la calificación de cada riesgo inherente teniendo en cuenta el valor de la probabilidad y el impacto se utilizó la siguiente fórmula:

- Generar la matriz de riesgo: se tuvo en cuenta la valoración de los riesgos y se estableció su nivel de afectación, se procedieron a diseñar los controles destinados a evitar, mitigar o contener los riesgos. Se desarrolló teniendo la categoría del activo, la caracterización del riesgo y posteriormente los controles, con su respectivo responsable.

Diseño del plan

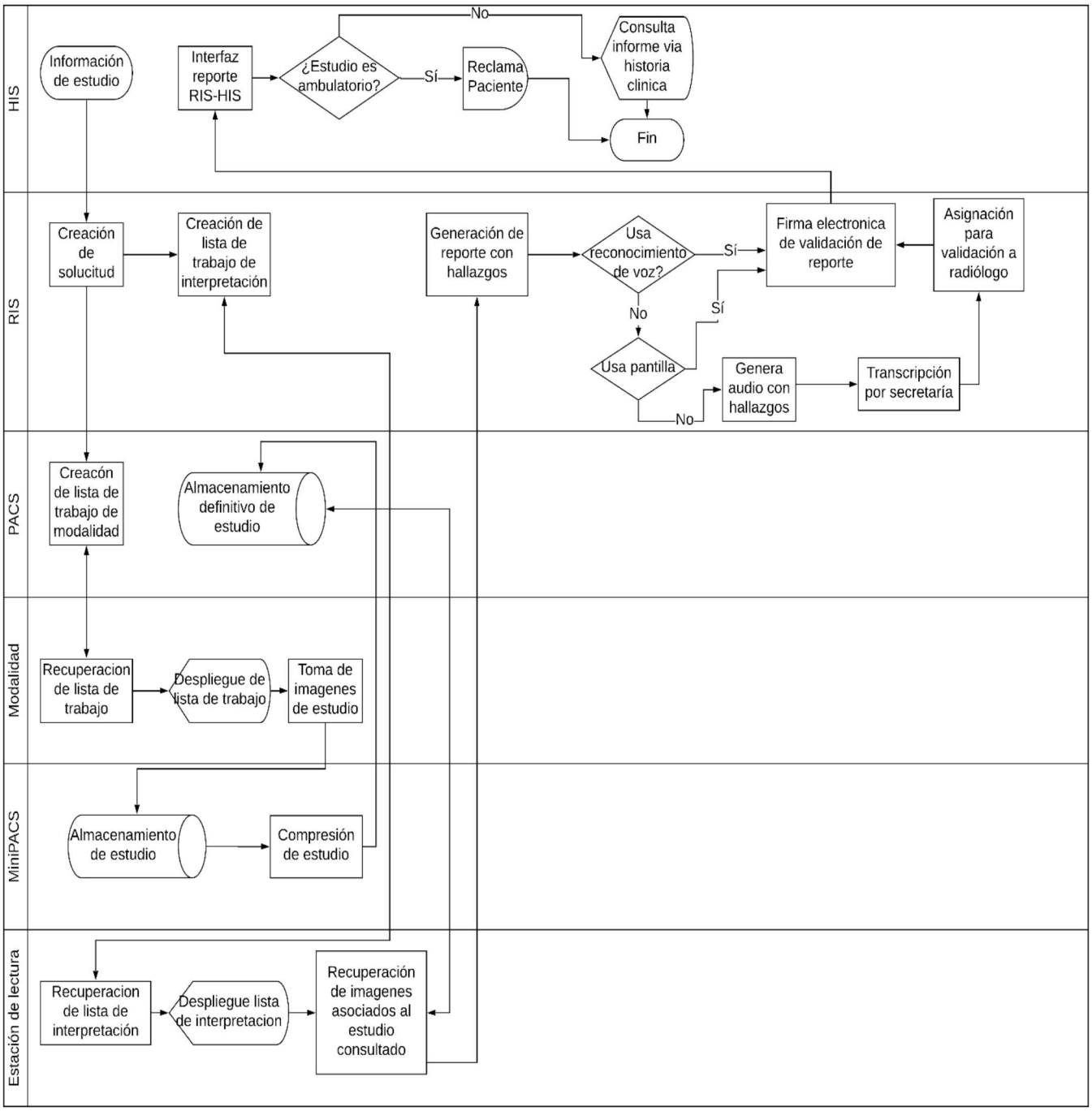
Para la cuarta tarea se hizo un acercamiento a la documentación generada durante la investigación, con la documentación con ITIL v3. De esta forma se realizó el diseño del plan de continuidad del servicio para mitigar los riesgos hallados, tomando diferentes actividades para asegurar la operación ininterrumpida del servicio (Rios Huercano, s.f.).

3. RESULTADOS Y DISCUSIÓN

La identificación del servicio:

En acompañamiento con las personas que trabajan en la operación diaria y en entrevista al coordinador del área de imágenes diagnosticas, se tomó la información necesaria para realizar el diagrama de operación del servicio desde el ingreso de una solicitud de estudio hasta su entrega al paciente, al médico solicitante o al HIS (Hospital information system).

Figura 1-Operación del Servicio de Imagenología



Fuente: Elaboración propia.

Medidas actuales de contingencia:

Se realiza la pertinente recolección de información del servicio de la operación del PACS, hallando las contingencias actuales, las que el Institución Prestadora de Servicios de Salud tiene para contrarrestar los riesgos posibles que pueda presentar el servicio en su operación diaria.

A continuación, los controles agrupados en las dimensiones en las que influye.

Procesos de imagenología:

- Creación manual de solicitudes en RIS (Cuando el HIS no envía solicitud)
- Creación de paciente de manera manual en las modalidades
- Configuración de nodos adicionales en las modalidades
- Alternativas de creación de informe de estudio (plugin, grabadora o RIS)

Infraestructura:

- MiniPACS como contingencia del principal.
- Respaldos de imágenes en medios offline (Cintas y HDD externos).
- Diferentes servidores de aplicaciones de HIS.

Estructurales:

- Sistema sismo indiferente en sede principal
- Sistema de detección de incendio y sistemas de aspersión en sede principal
- Bypass de proveedores de energía y plana de generación interna.

Antes de pasar al análisis y evaluación de riesgos, se realiza una valoración de criticidad de afectación parcial o total de los activos, dependiendo de los criterios de evaluación y teniendo en cuenta sólo los activos referentes a sistemas de información e infraestructura tecnológica.

A continuación, los criterios que serán utilizado en los análisis de riesgos:

Tabla 1-Criterios de evaluación de la operación del servicio de imagenología.

Criterio a Evaluar	Descripción del criterio
Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos
Confidencialidad	Propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada

Fuente: Recuperado de (González & Vanegas, 2012).

Identificación de los activos o recursos que componen la operación del servicio:

Como resultado de la identificación del servicio y de su flujo de trabajo se encontró que en la operación diaria se relacionan 34 activos o recursos diferentes los cuales se pueden agrupar en 9 categorías; para la categoría de equipos de información se encuentran 9 tipos de equipos diferentes, desde estaciones de admisión y facturación hasta modalidades y clientes e impresoras DICOM (digital imaging and communication on medicine), para la categoría de redes de comunicación se identificaron 3 componentes o activos diferentes, en la categoría de sistema eléctrico se identificaron 2 dispositivos asociados, para la categoría de servidores se encontraron 7 servidores entre físicos y virtuales que realizan labores diferentes dentro de la operación, para la categoría HIS (hospital information system) un solo componente, en la categoría RIS (radiology information system) existes 3 módulos que interfieren en la operación diaria, el propio sistema PACS se encuentra clasificado como una categoría con 3 módulos importantes a tener en consideración, la categoría de sistemas de audio con 3 activos diferentes relacionados y por último la categoría de datos de información con 3 tipos de datos sensibles a tener en cuenta durante el proceso.

Luego de identificar los activos tecnológicos que componen la operación del servicio y de su debida categorización, se proponen las siguientes actividades necesarias para evaluar los riesgos que pudieran afectar el flujo normal de las actividades diarias del servicio de imagenología.

Definir los riesgos de cada categoría de activo:

Los 33 riesgos que se identificaron en el análisis del diagrama de flujo construido, se conciliaron y se codificaron con las respectivas categorías de activos De esta forma se obtiene para la categoría equipos de información 9 riesgos que se encuentran codificados desde EI1 hasta el EI9, para la categoría redes de comunicación se obtuvo el riesgo RC1, para la categoría sistema eléctrico se obtuvieron los riesgos SE1 y SE2, para la categoría servidores se obtuvo el riesgo Se1, para la categoría HIS el riesgo HIS1 y HIS2, para la categoría RIS se obtuvieron los riesgos RIS1 hasta el riesgo RIS8, para la categoría PACS se obtuvieron os riesgos desde el PAC1 hasta PAC4, en la categoría sistema de audio se codificaron los riesgos desde SA1 hasta SA4 y para la categoría de datos e información se evidenciaron los riesgos DI1 y DI2.

Calificar la probabilidad e impacto de afectación a la operación del servicio por cada riesgo:

La metodología Margerit (metodología de análisis y gestión de riesgos de los sistemas de información) propone dar 2 calificaciones a cada riesgo para su valoración (Amutio Gómez & Candau, 2012), una calificación de viene dado a la probabilidad de la ocurrencia del riesgo y la otra calificación viene dado por el impacto que puede generar el riesgo a la operación del servicio.

A la característica "Muy bajo" con frecuencia de al menos una vez al año se calificó con 1 punto, a "Bajo" con frecuencia de al menos una vez en el semestre con 2 puntos, "Medio" con frecuencia de al menos una vez en el trimestre con 3 puntos, "Alto" con frecuencia de al menos una vez por mes con 4 puntos y "Muy Alto" con frecuencia de al menos una vez cada quince días con 5 puntos (Fajardo Diaz, 2017). De la misma forma, se identificó el nivel del impacto de cada riesgo al compararlo con cada uno de los niveles propuestos en la tabla 2.

Tabla 2-Impacto del riesgo

Impacto	Detalle del impacto
Muy bajo	• No afecta la seguridad de la información de la entidad. • No hay afectación de la imagen de la entidad ante los clientes y terceros. • Se puede recuperar la información con la misma calidad. • Se presenta reprocesos que no tiene mayor importancia.
Bajo	• No afecta la seguridad de la información de la entidad. • Se presenta una leve afectación de la imagen de la entidad ante los clientes y terceros. • Se puede recuperar la información con la misma calidad en un tiempo moderado. • Se presenta reprocesos menores en las actividades de la entidad.
Medio	• Hay una afectación en menor grado de la seguridad de la información de la entidad. • Afecta medianamente la imagen corporativa de la entidad ante los clientes y terceros. • La información se puede recuperar, pero no con la misma calidad. • Se presenta reprocesos moderados en las actividades de la entidad.
Alto	• Se genera una afectación importante en la seguridad de la información de la entidad. • Afecta altamente la imagen corporativa de la entidad. • La información es difícil de recuperar. • Se presenta reprocesos mayores en las actividades de la entidad.
Muy alto	• Se presenta una afectación crítica en la seguridad de la información de la entidad. • Afecta negativamente y en gran proporción la imagen corporativa de la entidad. • La información es difícil de recuperar. • Puede afectar las decisiones estratégicas de la organización y la continuidad del negocio.

Fuente: Recuperado de (Fajardo Diaz, 2017)

Al obtener las calificaciones de probabilidad y de imparto, se calcula el valor de cada riesgo. El valor del riesgo se obtuvo del producto de la calificación de la probabilidad por la calificación del impacto del riesgo. El nivel del riesgo viene dado de la siguiente forma; nivel "Muy bajo" para riesgos de valor entre 1 y 2, nivel "Bajo" para riesgos de valor entre 3 y 4, nivel "Medio" para riesgos de valor entre 5 y 9, nivel "Alto" para riesgos de valor entre 10 y 15 y nivel "Muy alto" para riesgos de valor entre 16 y 25.

Realizado el calculo de cada riesgo se encontró que en la probabilidad tiene más peso en la ocurrencia de 1 a 3 puntos, pero se hayo 6 riesgo con probabilidad de ocurrencia muy alta, ahora tomando el mismo análisis con el impacto, el más ocurrente es aproximado en 1 a 3 puntos, pero encontrando 3 riesgo de muy alto impacto. Después de hallar los cálculos de probabilidad e impacto, se realiza la ecuación que nos permite determinar el nivel de riesgo, encontrando que, entre los 33 riesgos del servicio, hay 3 "Muy Bajo", 10 "Bajo", 17 "Medio" y 3 "alto" es al final la valoración de riesgo.

Con el cálculo de los valores y niveles de los riesgos se evaluaron en un mapa de calor, de esta forma se evidenció aquellos riesgos más críticos y que necesitaban un mayor control para su mitigación o prevención. Gracias al mapa de calor (tabla 3), se evidencio que los riesgos más altos en el proceso de imágenes diagnosticar referente a la comunicación de imágenes son los riesgos asociados a los sistemas HIS y RIS, siendo estos las fuentes de información del PACS y los destinos de los resultados de los estudios enviados, consultados e interpretados en él.

Tabla 3-Mapa de calor de riesgos

Probabilidad	**Impacto**				
	Muy bajo (1)	**Bajo (2)**	**Medio (3)**	**Alto (4)**	**Muy alto (5)**
Muy bajo (1)		EI1, EI2, EI4		SE2, Se1	RC1, DI1, DI2
Bajo (2)		EI9, RIS2 SA3, SA4	RIS4, RIS5	PAC2, PAC3 PAC4	
Medio (3)	EI3, PAC1	RIS1, RIS3 RIS8,	SE1		
Alto (4)	EI5, SA1	EI8, SA2			
Muy alto (5)	EI6, EI7 RIS6	HIS1, RIS7	HIS2		

Fuente: Adaptada de (Fajardo Diaz, 2017)

Se generó entonces la matriz de riesgo (tabla 4) con base a los resultados obtenidos en análisis de la valoración de riesgos y el hallazgo del análisis del mapa de calor de los riesgos. En este mapa de relacionó el riesgo de seguridad previamente analizado con su respectivo nivel, las características de seguridad a las que impacta, pudiendo ser la confidencialidad, la integridad o la disponibilidad de la información. Adicional e propone 1 o más controles a cada riesgo y un rol responsable encargado de que el control exista y se cumpla. Concluido el análisis de los riesgos y establecido los controles se procede con la fase final, el plan de continuidad.

Tabla 4-Matriz de riesgo

Riesgo de seguridad	**Identificación del control**	**Responsable**
EI1	C1-EI1	Soporte sistemas
	C2-EI1	Soporte sistemas
	C3-EI1	Soporte sistemas
EI2	C1-EI2	Soporte sistemas
	C2-EI2	Soporte sistemas
EI3	C1-EI3	Soporte sistemas
EI4	C1-EI4	Soporte sistemas
	C2-EI4	Mantenimiento/ Ingeniería clínica
	C3-EI4	Soporte sistemas
EI5	C1-EI5	Soporte sistemas
	C2-EI5	Radiólogo
	C3-EI5	Soporte sistemas
EI6	C1-EI6	Soporte sistemas
	C2-EI6	Radiólogo
EI7	C1-EI7	Soporte sistemas
EI8	C1-EI8	Soporte sistemas
	C2-EI8	Soporte sistemas
	C3-EI8	Soporte sistemas
EI9	C1-EI9	Soporte sistemas

	C2-EI9	Soporte sistemas
RC1	C1-RC1	Administrador de la Red
SE1	C1-SE1	Mantenimiento
	C2-SE1	Mantenimiento
SE2	C1-SE2	Mantenimiento
Se1	C1-Se1	Infraestructura
	C2-Se1	Infraestructura
	C3-Se1	Infraestructura
HIS1	C1-HIS1	Auxiliar caja
	C2-HIS1	Auxiliar caja
HIS2	C1-HIS2	Soporte sistemas
	C2-HIS2	Transcriptora
RIS1	C1-RIS1	Infraestructura
RIS2	C1-RIS2	Auxiliar caja/ Tecnólogo/Auxiliar de enfermería
	C2-RIS2	Tecnólogo/Auxiliar de enfermería
RIS3	C1-RIS3	Tecnólogo/Auxiliar de enfermería
RIS4	C1-RIS4	Tecnólogo/Auxiliar de enfermería
	C2-RIS4	Radiólogo
RIS5	C1-RIS5	Radiólogo
	C2-RIS5	Radiólogo
RIS6	C1-RIS6	Soporte sistemas
	C2-RIS6	Radiólogo
RIS7	C1-RIS7	Radiólogo
	C2-RIS7	Radiólogo
RIS8	C1-RIS8	Soporte sistemas
	C2-RIS8	Radiólogo
PAC1	C1-PAC1	Tecnólogo/Auxiliar de enfermería
	C2-PAC1	Administrador PACS.
	C3-PAC1	Administrador PACS.
PAC2	C1-PAC2	Administrador PACS.
	C2-PAC2	Administrador PACS
	C3-PAC2	Administrador PACS
PAC3	C1-PAC3	Administrador PACS.
	C2-PAC3	Administrador PACS
PAC4	C1-PAC4	Administrador PACS.
SA1	C1-SA1	Soporte sistemas
	C2-SA1	Radiólogo
SA2	C1-SA2	Soporte sistemas
SA3	C1-SA3	Administrador PACS.
	C2-SA3	Administrador PACS
SA4	C1-SA4	Administrador PACS
DI1	C1-DI1	Desarrollo
DI2	C1-DI2	Desarrollo

Fuente: Adaptada de (Fajardo Diaz, 2017)

Diseño del plan de continuidad de acuerdo con los hallazgos de los puntos anteriores:

Plan de Continuidad

El plan de continuidad de servicio para el sistema PACS de la Institución Prestadora de Servicios de Salud, el cual diseñamos está comprendido por las siguientes etapas:

- Plan de Prevención de riesgos.
- Plan de Gestión de Emergencia.
- Plan de Recuperación.

Plan de prevención de riesgos

El alcance en la prevención de riesgos es mitigar el impacto de un desastre en el sistema de PACS, se realiza un plan de actividades a seguir, para las prevenciones necesarias y minimizar riesgos.

Tabla 5-Plan de Prevención

Actividades de Prevención	Responsable
Tener periódicamente mantenimiento del Software.	Soporte de sistemas
Verificar durante las tareas de mantenimiento del software, la activación de creación de puntos de restauración. En caso de no estar habilitado, se configura para crearlo.	Soporte de Sistemas
Contar con equipos (Switch, router, etc.) de contingencia de los cuales se pueda realizar un respaldo.	Soporte de Sistemas
Contar con dispositivos (Discos duros), para tener respaldo en caso de daños.	Soporte de Sistemas
Capacitar al usuario sobre primeros auxilios que puedan ejecutar ante errores en el Software/ Hardware (tales como reconectar cables de red, reconectar cables USB, reiniciar programas en ejecución, reiniciar el PC para liberar memoria, etc.).	Soporte de Sistemas
Tener comunicación y asistencia eficaz con los proveedores de equipos externos.	Mantenimiento/ Ingeniería clínica
Contar con equipos de grabadora de audio.	Radiólogo
Capacitar el personal de control de calidad sobre el flujo de trabajo.	Administrador PACS
Configurar en las estaciones de trabajo varios dispositivos de impresión.	Soporte sistemas
Contar con línea eléctrica de contingencia con otra empresa de servicios eléctricos.	Servicio Generales
Tener periódicamente el mantenimiento a la planta generadora de energía.	Servicio Generales
Revisar el estado de las UPS (Sistemas de alimentación ininterrumpida) de forma periódica.	Servicio Generales
Tener respaldo de las bases de datos.	DBA

Tener un servidor de internet que contenga exactamente la misma información que contiene el servidor en funcionamiento.	Infraestructura
Tener flujo de papel como contingencia, como la impresión de las solicitudes de estudio para entregar al técnico o tecnólogo para el inicio de la toma del estudio y la impresión y entrega de la orden médica al radiólogo para el inicio de la interpretación. Todo esto sin dependencia de los sistemas de información y así servir de apoyo en el momento que el RIS/PACS estén Offline.	Tecnólogo/Auxiliar de enfermería
Realizar Rutina de revisión de almacenamiento disponible en los PACS y MiniPACS.	Soporte de Sistemas
Realizar imágenes del sistema operativo de las estaciones sensibles para el flujo normal del servicio, cuando no se pueda tener equipos de contingencias.	Soporte de Sistemas

Fuente: Elaboración propia.

Plan de gestión de emergencias

Al momento del desastre o emergencia el personal encargado se debe encontrar capacitado, de tal forma que pueda atender la emergencia de modo rápido y sin esperar el responsable de realizar soporte, que pueda actuar con los protocolos aprendidos. Si se tuvo éxito en aplicar la solución, se debe igual informar al personal encargado de soporte. En el caso de que la solución no fuera efectiva, se tiene que realizar un llamado al encargado del soporte.

El equipo de soporte de sistemas está adecuado con herramientas de comunicación directa, igual que el personal que se encuentra realizando soporte a los activos más críticos y de los servicios más esenciales para la organización. Al personal que interviene con el servicio del sistema PACS, se le informa y comparte el directorio de todos los contactos de soporte y así, ante cualquier situación problemática, se le informa al soporte encargado para que éste comience con la identificación de las causas del problema e inicie el proceso de recuperación de los sistemas. Los roles que se involucran con el plan de continuidad, que deben tener el contacto y comunicación eficaz; son:

- Soporte de Sistemas.
- Mantenimiento/ ingeniería clínica.
- Radiólogo.
- Soporte de servicios generales.
- Auxiliar de caja.
- Transcriptora.
- Auxiliar de enfermería o Tecnólogo.
- Agente de control y verificación.
- DBA

Se presentan a continuación las actividades que serán ejecutadas en caso de presentar una emergencia, podrá efectuar y poder controlar el riesgo que se esté presentando.

Tabla 6-Plan de emergencias.

Actividades en caso de emergencia	Responsable
Implementar los primeros auxilios que se puedan ejecutar tras fallo de Software/ Hardware. En caso de no sobreponerse al fallo llamar a soporte sistemas	Personal que se encuentre en el momento del fallo y este con la capacidad de efectuar la actividad
Usar grabadora de captura de audio en lugar de la diadema, en el caso de fallo de la diadema. Contactar a Administrador. PACS para reportar fallo.	Radiólogo.
Grabar los estudios en CD/DVD para la entrega de informe e imágenes.	Agente de control y verificación.

Contactar a Administrador. PACS para reportar fallo.	
Poner en funcionamiento el sistema de UPS, en caso de una falla eléctrica.	Mantenimiento.
Ejecutar los procedimientos estructurados de reinicio de base de datos, al momento de no poder acceder a la base de datos.	DBA.
Poner en función de reenvió solicitud desde el HIS, en caso de fallo de envió de notificación HL7 del HIS al RIS.	Auxiliar caja
Utilizar el flujo de papel como contingencia, en caso de fallo de envió de notificación HL7 del HIS al RIS.	Tecnólogo/Auxiliar de enfermería
Usar el módulo de transcripción del HIS, en caso de no ser visible el informe de procedimiento de las historias clínicas.	Transcriptora.
Realizar una creación de datos manuales, en caso de no poder interpretar solicitud HL7 procedente del HIS o no se redirecciona solicitud al PACS.	Tecnólogo/Auxiliar de enfermería

Fuente: Elaboración propia.

Plan de Recuperación.

Se propone las siguientes actividades para la normalización del servicio posterior al evento adverso.

Tabla 7-Plan de recuperación.

Actividades de recuperación.	Responsable
Restablecer el normal funcionamiento de los equipos retirados durante la emergencia y que fueron remplazados por sus contingencias. Se debe programar con el coordinador del departamento donde se retiró o que podría verse afectado para detener las operaciones, retirar el equipo de contingencia e instalar nuevamente el equipo retirado.	Dependiendo del equipo a restablecer: • Estación de trabajo (PC): Soporte sistemas • Impresoras de Papel: Soporte sistemas • Impresoras DICOM: Ingeniería clínica. • Estación de lectura: Administrador PACS • Servidor del PACS: Administrador PACS. • Servidor RIS: Administrador PACS. • Base de datos HIS: DBA. • Modalidad (ecógrafo, rayos x, etc.): Ingeniería clínica. • Dispositivos de red (Telecomunicaciones) • Diademas de grabación: Administrador PACS
Simulación en entornos de pruebas de las interfaces HL7 después de la rehabilitación de los servidores de HIS y RIS, de esta forma abandonar al flujo de papel de contingencia y regresar al flujo sistematizado.	Administrador PACS.
Pruebas en el RIS con simulación del evento que impidió la comunicación del mensaje HL7.	Administrador PACS.

Conciliación de los datos ingresados de manera manual en las modalidades en el PACS.	Administrador PACS.
Reinstalación o reconfiguración de aplicación de envío de audios.	Administrador PACS.
Regresar al flujo eléctrico principal.	Mantenimiento.

Fuente: Elaboración propia.

4. CONCLUSIONES

El trabajo se desarrolló de tal manera que se encamina hacia la identificación de los activos que componen al servicio y a la forma en la cual se relacionan para ejecutar el flujo natural de trabajo. En el análisis del sistema de almacenamiento y comunicación de imágenes, se encontró el impacto que éste tiene para al apoyo diagnóstico que se requiere en la atención de pacientes en la Institución Prestadora de Servicios de Salud. Los pacientes necesitan que sus médicos tratantes cuenten con información disponible para la toma de decisiones; que sea confiable para que no se incurra en errores durante el tratamiento, y segura para que sólo el personal que esté autorizado y requiera la información tenga acceso a ella. Conociendo que aunque existían medidas de contingencia, que actualmente permitían sobrellevar algunos riesgos, en la organización no se manejaba documentación que permitiera llevar a cabo un plan para evitar o mitigar aquellos incidentes que atentaran a la continuidad de la entrega del servicio, esto nos motivó a llevar a cabo este diseño del plan de continuidad.

Al final de la investigación se llevó a cabo la evaluación de riesgos, donde se realizó un análisis riguroso y con mucha atención, lo que permitió detectar 33 riesgos, en 7 activos del servicio, los cuales no tenían identificación del impacto sobre la operación del servicio, ni tampoco un tratamiento adecuado para el suceso de alguno de ellos, se analizó que el nivel de riesgo más alto está entre medio y alto, con un 60%, lo cual nos llevó a diseñar medidas para controlar y no afectar la disponibilidad del servicio. Teniendo elaborada la matriz de riesgo, se realizó un plan de acción con base en el proceso de Gestión de la Continuidad del Servicio de ITIL V3, aprovechando las orientaciones más afines al plan que se deseaba elaborar, tampoco sin olvidar toda la información de la matriz, la cual fue de gran ayuda para especificar las actividades que se propusieron para mitigar, o solucionar los incidentes. De esa forma se diseña el plan de continuidad que mejor se ajuste a la operación del servicio, el diseño se pensó para poder ayudar a evitar, controlar y reponerse ante los incidentes que puedan ocurrir y tener lo más disponible que sea posible el servicio del PACS.

I. REFERENCIAS

Adams, Simon; OGC - Office of Government Commerce. (2008). *ITIL V3 foundation handbook*. iTSMF.

Advisera. (s.f.). Obtenido de Advisera: https://advisera.com/27001academy/es/que-es-iso-22301/

Agui Reynoso, E., & Huacho Aliaga, G. (2012). *Archivos: Hospital Vitarte,Area Informatica*. Obtenido de Archivos: Hospital Vitarte,Area Informatica: http://www.hospitalvitarte.gob.pe/portal/mod/transparencia/download.php?transparencia=415

Amutio Gómez, M. A., & Candau, J. (2012). *MAGERIT – versión 3.0* . Madrid: Ministerio de Hacienda y Administraciones Públicas.

De Cespedes Vargas, C. (23 de Agosto de 2018). *Scielo*. Obtenido de Evolución de la radiología como especialidad médica en Costa Rica: http://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S0001-60022000000100010

Duarte, É. (25 de Abril de 2016). *Colombia estrena el centro de datos más grande del país en Medellín*. Obtenido de xataka colombia: https://www.xataka.com.co/otros/colombia-estrena-el-centro-de-datos-mas-grande-del-pais-en-medellin

El portal de ISO 27001 en Español. (18 de Noviembre de 2018). Obtenido de Serie 27000:

http://www.iso27000.es/iso27000.html

Español, E. p. (18 de Noviembre de 2018). Obtenido de https://www.iso27000.es/iso27000.html

Fajardo Diaz, C. E. (2017). *Análisis de los riesgos de seguridad de la información de un aplicativo de gestion documental lider en el mercado colombiano.* Intitución universitaria politécnico Grancolombiano. Obtenido de http://alejandria.poligran.edu.co/handle/10823/995

González, J. A., & Vanegas, C. A. (12 de 2012). *Articulos universidad distrital Francisco José de Caldas.* Obtenido de Universidad distrital Francisco José de Caldas: https://comunidad.udistrital.edu.co/revistavinculos/files/2012/12/LA-SEGURIDAD-EN-LAS-REDES-DE-COMUNICACIONES-ED5.pdf

Guilarte, M. (14 de Marzo de 2013). *Mcpro.* Obtenido de Mcpro: https://www.muycomputerpro.com/2013/03/14/que-es-un-tier

Hospital Italiano de Buenos Aires. (20 de Octubre de 2009). *Archivos: Hospital Italiano de Buenos Aires.* Obtenido de Hospital Italiano de Buenos Aires: https://www.hospitalitaliano.org.ar/multimedia/archivos/clases_attachs/2008-96.pdf

Luna, R. (Marzo de 2018). Plan de recuperacion de desastres para TI. Cali, Valle, Colombia.

Origen serie 27K. (18 de Noviembre de 2018). Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/iso27000.html

Ortega Hrescak, M. C., & Socolsky, G. A. (23 de Agosto de 2018). *Scielo.* Obtenido de Godfrey Newbold Hounsfield: historia e impacto de la tomografía computada: http://www.scielo.org.ar/scielo.php?script=sci_arttext&pid=S1852-99922012000400008

Pagani, M. (2009). *Encyclopedia of Multimedia Technology and Networking, Second Edition.* Hershey: Information science reference.

Rios Huercano, S. (s.f.). *Manual de ITIL V3.* Obtenido de https://docs.supersalud.gov.co/PortalWeb/planeacion/AdministracionSIG/GSDE01.pdf

SGS(Société Générale de Surveillance) . (s.f.). Obtenido de SGS(Société Générale de Surveillance) : https://www.sgs.co/es-es/health-safety/quality-health-safety-and-environment/sustainability/economic-sustainability/iso-22301-business-continuity-management-auditor-lead-auditor-training-course

The Joint Commission. (31 de Agosto de 2018). Obtenido de About The Joint Commission: https://www.jointcommission.org/about_us/about_the_joint_commission_main.aspx

Tong, C. K., & Wong, E. T. (2009). Information Security Management in Picture Archiving and Communication Systems for the Healthcare Industry. En M. Pagani, *Encyclopedia of Multimedia Technology and Networking, 2nd ed* (págs. 682-690). Hershey: Margherita Pagani.

Valdés Solís, P. (23 de Octubre de 2016). *Documentos Calidad: Radiodiagnóstico Agencia Sanitaria Costa del Sol.* Obtenido de Servicio de Radiodiagnóstico de la Agencia Sanitaria Costa del Sol: http://radiologiamarbella.com/calidad/index.php/2016/10/23/plan-contingencia-ante-averias/

Verdú Fernández, J. I. (2015). *Plan de contingencia de tecnologías de la información en entornos distribuidos.* Madrid: Universidad Carlos III de Madrid. Departamento de Informática.