UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO

ESCUELA DE POSGRADO

MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

TESIS PARA OPTAR EL GRADO ACADÉMICO DE MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

AUTOR

CESAR AUGUSTO VILLEGAS RIVERA

ASESOR

RICARDO DAVID IMAN ESPINOZA

https://orcid.org/0000-0003-0409-8773

Chiclayo, 2022

MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

PRESENTADA POR:

CESAR AUGUSTO VILLEGAS RIVERA

A la Escuela de Posgrado de la
Universidad Católica Santo Toribio de Mogrovejo
para optar el grado académico de

MAESTRO EN INGENIERÍA DE SISTEMAS Y COMPUTACIÓN CON MENCIÓN EN DIRECCIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN

APROBADA POR:

Huilder Juanito Mera Montenegro
PRESIDENTE

Héctor Miguel Zelada Valdivieso
SECRETARIO

Ricardo David Iman Espinoza
VOCAL

Dedicatoria

El presente trabajo de investigación va dedicado para mi Padre celestial Jehová, quien siempre me dio la motivación necesaria para no desfallecer y seguir avanzando a pesar de las adversidades que obstaculizaron el camino.

A mis padres César y Liliana, que me brindaron su amor, consejos, valores y enseñanzas de vida, forjándome como la persona que soy.

A mis hermanos Cecilia y Joaquín, quienes me apoyan constantemente y moralmente en las circunstancias más complicadas.

A Leyla, que me acompañó a lo largo de la trayectoria para culminar este reto; muchas gracias por toda la ayuda que me proporcionaste sin esperar algo a cambio. Parte del mérito es para ti.

Agradecimientos

A mi asesor Mtro. Ricardo David Imán Espinoza, quien me orientó mediante su experiencia profesional y me brindó la confianza necesaria para desarrollar el presente trabajo de investigación.

A los Dres: Gilberto Carrión Barco, Jessie Leila Bravo Jaico y Ernesto Karlo Celi Arévalo, quienes mediante sus conocimientos me ayudaron a fortalecer y concretar los procesos del modelo propuesto.

Índice

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Los hospitales de nivel II - I de la región Amazonas experimentan continuamente percances que involucran la protección de los activos de información. En base a un estudio realizado a una muestra de los hospitales, entre los acontecimientos más frecuentes se encuentra el uso inadecuado de los activos de información; el desconocimiento por parte de los usuarios y la alta gerencia de los riesgos que pueden comprometer a los activos críticos de los nosocomios.

El presente trabajo de investigación ofrece una propuesta de solución para los riesgos que acechan constantemente a los activos críticos. Por tal motivo se elaboró una comparativa de nociones y marcos de trabajo orientados a la gestión de riesgos de TI; las cuales al ser acondicionadas a las organizaciones del sector salud, brindan una serie de pasos y métodos indispensables para minimizar los niveles del riesgo.

Como objetivo general se propuso: desarrollar un Modelo de Gestión de Riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas.

El modelo propuesto fue validado mediante el juicio de 5 expertos; con el alfa de Cronbach se determinó la confiabilidad y en base a Kendall se midió la concordancia.

El modelo validado fue aplicado a un hospital de nivel II - I de la muestra; donde se identificaron 258 riesgos, seleccionando 137 riesgos críticos para el respectivo tratamiento. Además se formularon 11 proyectos con la finalidad de monitorear y revisar la gestión de riesgos.

Palabras clave: Activos de información, Gestión de riesgos de TI, hospitales de nivel II - I, región Amazonas.

ABSTRACT

Level II - I hospitals in the Amazon region continually experience mishaps involving the protection of information assets. Based on a study of a sample of the hospitals, among the most frequent events are the inadequate use of information assets; lack of knowledge on the part of users and senior management of the risks that can compromise critical assets of the hospitals.

This research paper offers a proposed solution for the risks that constantly beset critical assets. For this reason, a comparison of notions and frameworks oriented to IT risk management was developed. When adapted to health sector organizations, these provide a series of indispensable steps and methods to minimize risk levels.

The general objective was to develop an IT Risk Management Model that contributes to the protection of information assets in level II - I hospitals in the Amazon region.

The proposed model was validated by the judgment of 5 experts; with Cronbach's alpha the reliability was determined and based on Kendall the concordance was measured.

The validated model was applied to a level II - I hospital in the sample; where 258 risks were identified, selecting 137 critical risks for the respective treatment. In addition, 11 projects were formulated with the purpose of monitoring and reviewing risk management.

Keywords: IT risk management, information assets, level II - I hospitals, Amazon region.

INTRODUCCIÓN

Cuando hablamos de riesgos tenemos que mencionar activos, amenazas, frecuencias de ocurrencias, impactos, opciones de tratamiento y hasta salvaguardas; por lo tanto, en la presente tesis, se propuso un Modelo de Gestión de Riesgos de Tecnologías de la Información (TI) aplicado a los hospitales de nivel II – I de la región Amazonas - Perú, dado que el sector es uno de los más importantes pero menos atendidos, se aplica la gestión de riesgos de TI, la cual permitirá la protección de los activos.

Los riesgos de TI corresponden a aquellos riesgos implicados en las operaciones relacionados con la utilidad, la pertenencia, los negocios, la intervención, la influencia y el acogimiento de las TI dentro de una institución o empresa. Por ese motivo, desde hace mucho tiempo la información es considerada un activo tanto fundamental como valioso; a tal grado que "el 90% de los líderes de negocios citan a los datos como uno de los recursos esenciales y un factor distintivo elemental para las organizaciones" [1, p. 6]; por ende:

> … La dependencia de las organizaciones modernas hacia el área de TI ha crecido drásticamente y pretende seguir incrementándose; por lo que el crecimiento promedio de este sector ha sido del 10% anual en los últimos 10 años (en el 2017 el Perú facturó más de $ 4,700 000 en TI). [2]

Cabe señalar que cada compañía tiene debilidades, cuyos riesgos individuales deben ser identificados, evaluados y tratados caso por caso, con la finalidad de evitar que estos acontecimientos involucren de alguna forma, repercusiones en los procesos indispensables de negocio de la organización o en sus objetivos estratégicos.

El Foro Económico Mundial en su reporte de Riesgos Globales, detalla que los ciberataques así como el robo de datos o fraude, son algunos de los causantes que más daños económicos han provocado, situándose entre los riesgos con mayor probabilidad de impacto:

> … Las trasgresiones de ciberseguridad han causado repercusiones que a nivel financiero se están acrecentando; los ataques de Ransomware ocasionaron una de las más grandes pérdidas económicas en el 2017, lo que representó el 64% global de los e-mail malintencionados. Entre los casos más importantes de destaca: el ataque WannaCry, que abarcó 150 países vulnerando a

> 300 mil ordenadores, y NotPetya, que perjudicó a miles de organizaciones ocasionando déficit de $ 300,000,000 en un trimestre [3, p. 6].

En consecuencia, los ciberataques se posicionan en el tercer lugar de los 10 principales riesgos en términos de probabilidad y en el sexto puesto en términos de impacto; entre tanto el robo de datos o fraude se encuentra en el cuarto lugar en términos de probabilidad [3]. Llegando a la conclusión que los riesgos materializados pueden generar una auténtica crisis empresarial causando graves daños a la imagen de la entidad o provocando pérdidas financieras irreparables. De ahí la importancia de una adecuada gestión de riesgos de TI.

En el contexto internacional:

> … En febrero del 2016, en la ciudad de California, el hospital Hollywood Presbyterian Medical Center sufrió de hackeo en sus sistemas, a través del virus informático Ransomware (El Ransomware es una forma de malware que infecta la computadora de una víctima, la bloquea y exige que se pague un rescate, a menudo en bitcoins, para restaurar el acceso) los delincuentes se apoderaron e impidieron el acceso de todos los datos de los pacientes del hospital, dejando el sistema completamente inoperativo por más de una semana. Los sistemas del centro médico habían sido afectados por más de una semana, a tal punto que el personal se había visto obligado a realizar algunas tareas en papel. Los hackers, pedían al hospital un rescate por un valor de 40 bitcoins, equivalente a un aproximado de $ 17,000 para devolver la información secuestrada. El director ejecutivo del hospital, Allen Stefanek se pronunció: «La solución inmediata y eficaz de recuperar los sistemas y procesos administrativos, es mediante la clave que descifre el programa malicioso de secuestro por medio del pago exigido» [4].

En 2016, durante los meses de Junio y Julio las plataformas tecnológicas de Bancolombia (grupo financiero multinacional colombiano) perjudicaron considerablemente los servicios de tecnología, interfiriendo con la prestación de los servicios a los usuarios y clientes, por lo cual fueron sancionados por la Superintendencia Financiera con un monto que asciende a 840 000 000 de pesos [5].

En 2018, en El Salvador, la empresa Smartmatic (brindó servicios los cuales estuvieron financiados en al menos $3 millones) eran los responsables de elaborar y comunicar todos los resultados concernientes a de las elecciones municipales de diputas del mes de marzo de ese

año. No obstante, un «error humano» (calificación brindada por Smartmatic), forzó a la organización a detener el proceso de marcas preferenciales y reestructurar las preferencias muy diferente al que habían planteado originalmente; perjudicando a la fiabilidad de los procesos electorales. Por otro lado, la empresa Next Genesis Technologies mediante su director general Raúl Funes expresó: «para una organización internacional de ese prestigio, están cometiendo un error imperdonable»; pudiendo provocar una penalidad para la organización responsable, además de generar una mala reputación institucional respecto a la prestación de sus servicios [6].

En 2019, Ecuador sufrió la peor filtración en línea de datos personales en su historia y una de las más grandes a nivel de todo Latinoamérica por la cantidad de personas expuestas. El país sudamericano cuenta con casi 17 millones de habitantes, y la mayoría de datos personales de casi todas las personas fueron expuestos según notificó la compañía de seguridad informática vpnMentor. La firma de seguridad dio a conocer a través de un informe que un servidor usado por Novaestrat (empresa ecuatoriana de marketing y análisis de datos), almacenaba información privada de millones de ecuatorianos; dicho servidor no disponía de las políticas fundamentales para proteger la información alojada, dando acceso a cualquier intruso que pretenda adueñarse de ella. El reporte indica que se trató de 18 GB de información. La información vulnerable contenía: datos básicos de identidad, historias educativas, números de teléfono, registros de trabajo, fechas de matrimonio, registros familiares y números oficiales de identificación del gobierno. Adicionalmente, el caché de información guardaba archivos financieros que contaba con los montos de las cuentas bancarias de los clientes de una entidad financiera ecuatoriana y el registros de impuestos; situando a los clientes en riesgo de fraude financiero y robo de identidad. La filtración masiva de información puede ocasionar un gran impacto en las organizaciones ecuatorianas, debido a los datos vulnerados que contenían información sobre empleados y detalles de algunas empresas [7].

A nivel nacional:

> … Las organizaciones y usuarios más perjudicados en el Perú son por medio de Ransomware, Phishing (suplantación de identidad) y Cryptojacking (minería de criptomonedas maliciosa). Según la empresa de seguridad Eset, en el 2017 el 25.1% (la cifra más alta en América Latina) de ataques en nuestro país fueron identificados como Ransomware; estos ciberataques se elevaron un 25% durante el 2018. Por otro lado, el EternalBlue es uno de los distintos tipos de

> amenazas que utiliza el cibercrimen para difundir el Wannacry sacando ventaja de las vulnerabilidades, ocasionando que más de 200,000 sistemas se vean agraviados y muchas organizaciones en Perú queden afectadas [8].

Optical Networks (compañía peruana de Telecomunicaciones especializada en el sector corporativo), reveló en un estudio que:

> … En el año 2019 sólo el 30% de las empresas peruanas ha hecho un diagnóstico de vulnerabilidad informática. Ante esta situación, el director comercial de Optical Networks, Víctor Jauregui, explicó: «Lo primero que debe hacer una empresa es priorizar sus activos más valiosos y direccionar su presupuesto dependiendo de cuánto quiere mitigar el riesgo». Asimismo, el 30% de empresas encuestadas dedican entre 10% y 20% del presupuesto de TI en soluciones de ciberseguridad, para aminorar los riesgos de TI en los activos de información [9].

En la región Amazonas - Perú, los hospitales se dedican a brindar servicios médicos basado en las personas, familia - comunidad, con el fin de optimizar la salud de los habitantes y la calidad de vida de estos; en parte dicho propósito es logrado a través del uso de las tecnologías, manejando información muy sensible, siendo de los niveles críticos más altos, la información de sus pacientes (como historias clínicas, resultados de laboratorio, datos personales de los pacientes, resultados de exámenes médicos con diagnóstico reservado, etc.); dicha información debe ser protegida y resguardada por los nosocomios según el artículo 16 de la Ley 29733 "Ley de Protección de Datos Personales (LPDP)". De no cumplirse, en los artículos 38 y 39 indican lo siguiente: "La infracción de cualquier intento de evasión que infrinja o quebrante cualquier tipo de norma incluida en la presente Ley o dentro de su estatuto, serán sancionadas desde 0,5 hasta 100 Unidades Impositivas Tributarias (UIT), dependiendo el tipo de infracción" [10].

Por otra parte, en los hospitales del nivel II-I de la región Amazonas - Perú, el departamento de TI depende del directorio general; esta área está encargada de gestionar la seguridad de la información en la entidad. Centrándose en la producción y ejecución de los planes de contingencia para asegurar la continuidad de la gestión de riesgos de TI, protegiendo los activos de información más relevantes de los nosocomios.

En el levantamiento de información (**ANEXO N° 02**) realizado a los encargados de las oficinas de TI de los hospitales de nivel II - I de la región Amazonas; concluyeron con las siguientes observaciones:

El área de TI cuenta con un plan de desarrollo, pero actualmente no está alineada a los objetivos estratégicos de la organización; pudiendo impedir el cumplimiento de la misión, objetivos, metas, reglas, entre otros.

La filosofía de riesgos de la organización se encuentra en la etapa de definición; generando incertidumbre entre los trabajadores, ocasionando que la toma de decisiones no sea la más apropiada o no esté ajustada a las necesidades de la organización.

La cultura de riesgos existente en la organización requiere de un cambio o mejora para poder afrontar de forma eficiente la gestión de los riesgos; de esta manera no solo los responsables o encargados de la toma de decisiones trabajarán en la mitigación de los riesgos, si no que todos los empleados estarán encaminados al mismo propósito, alineando así los objetivos estratégicos de la organización.

Algunas organizaciones tienen implementadas políticas de seguridad informática, pero sólo de forma empírica, ya que estas políticas se encuentran en la fase de documentación; pudiendo crear confusión, desorientación o una mala toma de decisiones, originando posibles interrupciones de servicios.

Deberían establecerse reglamentos internos sobre la mención de la correcta utilización de los activos de TI, ya que la ausencia de dichos estatutos impiden proteger los activos, ubicándolos en situación de peligro. De esta manera también se lograrían identificar cuáles son los activos de TI más relevantes para la organización.

El procedimiento para identificar y analizar los riesgos está situado en la fase de planeación; colocando en inminente peligro no solo a los activos más relevantes, sino también a los procesos críticos; exponiéndolos continuamente ante los diferentes riesgos externos e internos de la institución; además de generar posibles interrupciones de servicios o pérdidas financieras, dañando la imagen institucional.

Debido a los problemas mencionados anteriormente, los hospitales de la región Amazonas cada vez son más conscientes que los activos de información deben estar bien protegidos y que así mismo deben tener la inmediata disponibilidad para la correcta toma de decisiones; por tal motivo, se deberá desarrollar un Modelo de Gestión de Riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas - Perú.

Después de revisar los antecedentes de la situación problemática expuesta previamente, se formuló la siguiente interrogante: ¿De qué manera el Modelo de Gestión de Riesgos de TI contribuirá en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas?; por tal motivo esta investigación propuso que con la implementación parcial del Modelo de Gestión de Riesgos de TI se contribuirá en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas.

Con este fin se planteó:

- Identificar y analizar comparativamente los marcos de trabajo adecuados que permitan determinar un Modelo de Gestión de Riesgos de TI.
- Proponer el Modelo de Gestión de Riesgos de TI basado en los diferentes marcos de trabajo, con el propósito de contribuir en la protección de los activos de información.
- Validar el modelo propuesto con la finalidad de garantizar su aplicación y contribución a los hospitales de nivel II - I de la región Amazonas.
- Implementar parcialmente el Modelo de Gestión de Riesgos de TI, acondicionado para proteger los activos de información en hospitales de nivel II - I de la región Amazonas.

La justificación de esta investigación en el ámbito social será porque se implantará en los empleados una mejor cultura con respecto a la importancia y los beneficios que conlleva la gestión de riesgos de TI, impactando eficientemente en el ámbito hospitalario, logrando así la mitigación de los riesgos en el contexto interno y externo de la organización, modelando una adecuada imagen organizacional, generando satisfacción y confianza en los pacientes de los nosocomios.

El enfoque de la justificación económica está basado en el hecho de que una gestión de riesgos eficiente logrará mitigar los riesgos que puedan causar un alto impacto financiero que involucre a los activos de TI, procesos críticos de negocio, servicios indispensables, objetivos estratégicos y demás; logrando evitar las pérdidas económicas que se generarían si los riesgos llegaran a materializarse.

Desde el punto de vista tecnológico, el modelo de gestión de riesgos de TI basado en los distintos frameworks adaptados para proteger los activos de información, logrará generar las métricas adecuadas, políticas y la proposición de salvaguardas para aplacar los riesgos significativos y de alto impacto para el negocio, el mal uso, así como cualquier otro daño que afecte directamente a los activos críticos y la reputación de los hospitales de nivel II - I de la región Amazonas.

Por último, esta propuesta se sustenta en modelos de gestión de riesgos desarrollados para una interacción formal entre los diversos profesionales que laboran en los diferentes hospitales de nivel II - I, de manera que pueda obtenerse una organización viable con procesos definidos.

CAPÍTULO I MARCO TEÓRICO CONCEPTUAL

1.1. Antecedentes

En el 2017, Alfaro [11] explicó como la organización carecía de un marco de trabajo actualizado sobre la gestión de riesgos de TI, ocasionando que los procesos principales de la organización queden desfasados respecto a la realidad actual; por consiguiente una de las funciones principales vinculada con la gestión de riesgos generaba más gastos en relación a los recursos humanos y el tiempo. En consecuencia, la falta de un marco de trabajo estandarizado dejaba expuesto a los activos más relevantes para la organización ante los distintos escenarios de riesgos. Por lo que Alfaro propuso un modelo de gestión de riesgos de TI apoyándose en la normativa de COBIT 5 (EDM03 y APO12), ISO 31000 e ITIL, considerando también otros marcos de referencia como OCTAVE, ISO 27005, COSO, Normativas SUGEF, MAGERIT y las Normas Técnicas de la Contraloría General de la República de Costa Rica, además de emplear planes estratégicos de TI y planes de continuidad de TI, los cuales contienen actividades y prácticas de riesgos que complementaron la propuesta, con la finalidad de armonizar las distintas funciones ejecutadas en la organización logrando así mejorar la calidad de sus servicios. El aporte de este trabajo a la presente investigación se basa en que el autor definió el alcance del proyecto a través de un modelo que propone una guía que puede ser utilizada en distintas organizaciones; dicha guía contiene los siguientes apartados: objetivos, alcances, políticas y gobierno de riesgos (definición del apetito de riesgo y la tolerancia de riesgos; periodicidad de seguimiento de riesgos), procesos de gestión de riesgos de TI y registro de documentación de riesgos; logrando así que la metodología propuesta pueda mitigar de manera efectiva o eficaz los posibles riesgos que puedan presentarse dentro o fuera del entorno de la organización.

En el 2017, Dugarte [12] en el análisis de la situación organizacional encontró ciertas falencias como la falta de conocimiento sobre los riesgos de TI, sus procesos, controles, el seguimiento de la gestión de riesgos, matriz de riesgos de TI, inexistencia de documentación, herramientas, estándares y otros; dejando en evidencia que las distintas áreas que componen la organización trabajaban por separado. Para dar solución a los problemas mencionados, Dugarte se basó en las buenas prácticas de gestión de riesgos, donde elaboró la definición y evaluación del proceso para el análisis, e implementó los planes de tratamiento con el respectivo seguimiento y monitoreo de los riesgos identificados, complementándolo con la evaluación de los riesgos residuales; usando como base COBIT, PMI e ISO 31000, ISO

38500, BOTTOM-UP e ITIL, logrando unificarlos en un proceso adaptable no solo para el área de TI de la organización, sino también para otras empresas del mismo o diferente rubro. Este antecedente proporcionó a la presente investigación la perspectiva de un estándar global para la gestión de riesgos en el cual se define el contexto, que es un proceso indispensable para la gestión de riesgos porque se analizan los objetivos, los stakeholders, el entorno externo e interno y una gama de criterios que posibilitan el conocimiento de la complejidad así como el origen de los riesgos, además de elaborar los procesos de comunicación y consulta, la valoración del riesgo y el monitoreo y revisión; el proceso de gestión de riesgos de TI fue determinado con el propósito de analizar futuros escenarios de riesgos potenciales que puedan perjudicar el área de TI, asimismo aportó posibles soluciones para asegurar de manera efectiva la mitigación de los riesgos sin que los objetivos de la organización se vean afectados de manera alguna.

En el 2017, Rudas [13] en el análisis de la evaluación, se percató que la organización a pesar de tener implementado un sistema de gestión de proyectos, presenta ciertas debilidades por el poco tiempo que lleva en funcionamiento; dichas carencias se ven reflejadas en la falta de herramientas y procesos para la prevención de sucesos que impacten sobre los objetivos de los proyectos. Además en los distintos indicadores analizados (de calidad, costo y tiempo), se observó el incumplimiento de los resultados esperados. Por lo que Rudas tuvo como finalidad integrar metodologías adaptadas (ISO 21500, PMBOK, PRINCE2 y APM) para contribuir en el control y prevención de los riesgos que obstaculizan que los objetivos estratégicos de la organización se cumplan; por tal motivo, el modelo propuesto está compuesto principalmente de un grupo de buenas prácticas alineadas a la misión de la institución, estructurándose en procesos que contienen elementos de entrada, actividades y resultados, patentados a través de plantillas; por lo cual esta tesis, entregó un gran aporte a la presente investigación demostrando que con la ejecución del modelo de gestión de riesgos se logró disminuir el presupuesto del proyecto, se respetó el tiempo programado para el desarrollo del proyecto, se fomentó una cultura proactiva con respuesta ante los posibles eventos que puedan perjudicar a la organización a través de sus procesos críticos y se verificó la calidad del proyecto; además, la colaboración de los stakeholders posibilitó la generación de un alto grado de conciencia, permitiendo que los demás trabajadores se logren armonizar con las políticas, las responsabilidades y los roles definidos en el modelo de gestión de riesgos. De modo global, la implementación del modelo de gestión de riesgos generó beneficios a corto y largo plazo en el

contexto de la organización, logrando garantizar la mitigación de los riesgos y la prevención en la toma de decisiones improvisadas que puedan generar efectos adversos a los objetivos de la organización.

En el 2018, Chambi [14] detalló como la organización carece de una herramienta que posibilite la gestión de riesgos de TI, generando pérdidas financieras, fuga de datos relevantes, interrupción de procesos core, entre otros, que en corto plazo acarrean con el desprestigio institucional. Así mismo, no estaba implementada la identificación de los activos informáticos, vulnerabilidades, amenazas y riesgos a los que se encuentran expuestos por la falta de análisis. Con el fin de dar solución a los problemas expuestos, Chambi propone un modelo con la capacidad de gestionar los riesgos, tomando las respectivas acciones provisorias con el objetivo de mitigar los distintos riesgos que puedan presentarse; basándose en las metodologías: NTC–ISO 27005, ISO 31000, COSO y COBIT 5; el modelo permite fomentar las actividades de TI a tal grado que logra generar seguridad ante terceros posicionando en mejor calidad la imagen de la organización. La importancia de esta investigación radicó en los procedimientos planteados en el marco de trabajo: Recopilar información, Analizar, Mantener el perfil, Definir acciones y Responder; los cuales avalan que los riesgos relacionados con TI no sobrepasen la tolerancia de riesgo definida por la alta gerencia y que los riesgos residuales no impacten de forma critica los procesos del negocio; brindando un gran aporte a la presente investigación porque demostró que su modelo brindó apoyo en la ubicación de las áreas críticas que existen en la organización, planteando mecanismos de control que lograron establecer límites para facilitar la mitigación de los diversos riesgos.

En el 2018, Llontop [15] a través del análisis situacional, observó que la organización cuenta con falencias relacionadas a los riesgos a tal grado que en varias ocasiones los servicios primordiales del negocio fueron suspendidos en el periodo de hasta un día por no contar con un modelo de gestión de riesgos implementado, retrasando así los objetivos propuestos. Para dar solución a este inconveniente, Llontop demostró que a través de su modelo basado en los diferentes estándares internacionales (ISO 17799, ISO 27001 y MAGERIT) compensó la ausencia de políticas ante desastres ocasionados por riesgos de TI, implementando políticas para antivirus, nuevas restricciones a los ambientes de los servidores, etc; el autor elaboró su investigación bajo un enfoque cuantitativo, teniendo como objetivo la

comparación de resultados a través de cuadros estadísticos; por lo que aplicó una encuesta a expertos seguidamente de haber ejecutado el modelo con el fin de medir la validez, y a través del coeficiente del alfa de Cronbach, demostró su confiablidad; después de usar los métodos estadísticos adecuados, se demostró con los resultados la eficacia con la que se gestionaron los riesgos de TI. Este antecedente contribuyó un gran aporte a través de la aplicación del modelo; ya que logró identificar, tratar y mitigar los riesgos tanto dentro como fuera de la organización; además logró aumentar la cultura consiente sobre riesgos en los empleados; teniendo como soporte, personal altamente capacitado en gestión de servicios y certificaciones en ITIL, siendo de gran ayuda a la presente investigación porque demostró cómo se logró de forma eficaz que el área de TI pueda confrontar riesgos estando preparados y documentados eficientemente definiendo políticas adaptadas a los objetivos estratégicos de la organización.

En el 2018, Moscoso *et al*. [16] detectaron que las empresas no tenían implementada una adecuada gestión de riesgos; así mismo la gerencia de la organización ignoraba acerca de una cultura de riesgos TI, arriesgándose a que la toma de decisiones no sea la más adecuada en caso de que un escenario de riesgos se materialice, pudiendo ocasionar el desprestigio de la institución y pérdidas financieras. El propósito de este trabajo sirvió como soporte para el establecimiento de un modelo de gestión de riesgos de TI mediante la ejecución de sus procesos de gestión, por lo que utilizaron el alfa de Cronbach para medir su confiabilidad y analizaron distintas metodologías (COBIT 5, GRAMM, MAGERIT, OCTAVE y NIST 800-30) usándolas como base para elaborar su modelo. Tras la aplicación del modelo, lograron identificar 165 riesgos, de los cuales 52 estaban con clasificación “de alta prioridad” según la definición de la tolerancia y del apetito al riesgo brindado por la organización; por esa razón se implementaron estrategias de tratamiento, logrando un total de 16 proyectos destinados a revisar y monitorear los posibles escenarios de riesgos que puedan manifestarse. La relevancia de este antecedente en el presente trabajo de investigación sirve de soporte a la ejecución del modelo propuesto; evidenciando que el encargado del departamento de TI puede utilizar el modelo como guía para mitigar los riesgos de la forma más eficiente.

En el 2019, Banda [17] mediante el análisis de evaluación situacional rescató algunos puntos críticos; entre los más significativos estuvo la falta de personal especializado en la gestión de riesgos de TI. Esta carencia permitió que la organización se haya visto afectada por

el ataque de Ransonware, inmovilizando procesos core, perjudicando áreas críticas para el negocio, extraviando información esencial que involucra temas económicos y datos confidenciales para la empresa. En consecuencia, la organización vio afectada no sólo información indispensable, también puso en juego la reputación institucional ante los clientes y proveedores. Por consiguiente, Banda realizó el estudio de los estándares, conceptos y distintos frameworks vinculados con la gestión de riesgos (MAGERIT, ISO 27005, OCTAVE Allegro, ISO 31000 y NIST SP 800-30), los cuales al ser ajustados al entorno de las organizaciones agroindustriales, brindan la orientación fundamental para minimizar los riesgos que sobrepasan el nivel aceptable de la organización; por lo que nos otorga una solución a través de su modelo propuesto, que a su vez está validado con el alfa de Cronbach y el juicio de expertos con base en Kendall. Este trabajo proporcionó una guía a la presente investigación de cómo implementar una correcta gestión de riesgos de TI, a través del desarrollo del modelo propuesto, empezando con el reconocimiento de los activos de información y los procesos críticos en los cuales están involucrados; de igual manera se elaboraron los escenarios de exposición del riesgo en los que se encuentran implicados los activos y procesos; seguidamente se plantearon las opciones de tratamiento para la mitigación de aquellos riesgos que superan la capacidad de tolerancia de la organización; por último, se establecen las métricas para supervisar los escenarios de riesgos; en resumen el modelo fue dividido en 4 fases: I. Definición del alcance, contextos y criterios, II. Evaluación del riesgo, III. Tratamiento del riesgo y IV. Seguimiento y revisión. Cabe mencionar que el modelo validado obtuvo un valor de 0.810 en el coeficiente del Alfa de Cronbach, puntaje que da la confiabilidad de "muy alta" al modelo propuesto.

En el 2019, Rodríguez [18] mediante el análisis de la situación organizacional, descubrió que la organización asumía diversos riesgos relacionados con el método de negocio; entre los riesgos más prevalentes que se dieron a cabo en los últimos 10 años fueron ataques asociados directamente a los activos de TI, otro ataque fue hacia la base de datos a través de la inyección SQL; así mismo la ausencia de políticas de seguridad permitió el acceso no autorizado de varios trabajadores a los servidores de producción; por último, se registró un ataque al servidor que aloja los sitios web mediante la denegación de servicios (DDos). Las consecuencias asumidas además del extravío de información fueron las paralizaciones de los servicios y en promedio $2500 dólares en pérdidas financieras, dañando no solo el prestigio de la organización, sino también la confianza ganada con los clientes; otro factor preocupante

es el hecho de que los eventos mencionados anteriormente han ocurrido hasta 8 veces en los dos últimos años ocasionando disputas entre los empleados. Con el fin de dar solución a los problemas ya mencionados, Rodríguez elaboró un modelo basado en distintas metodologías (ISO 31000, ISO/IEC 27005, COBIT 5, MAGERIT e ISO 22301) las cuales permitieron que se elabore un procedimiento para determinar los procesos críticos y sus funciones. Sin dejar de lado un punto clave, el modelo propuesto fue aprobado por expertos en la materia, evidenciando que es aplicable y válido para una adecuada gestión de riesgos de TI. El presente trabajo de investigación acoge este antecedente como soporte al modelo planteado por la capacidad que demostró al lograr la formulación para concientizar mediante la capacitación de los empleados de la organización, que los benefició en el conocimiento y la aplicación de medidas y controles para poder gestionar y mitigar los riesgos de TI. De igual manera permitió examinar el entorno tanto interno como externo de la institución, el estudio del sector en el que se desarrolla, la identificación y determinación de los activos significativos, las amenazas con sus respectivas vulnerabilidades, la valoración de los riesgos, la elaboración de los planes de tratamiento y los procesos de seguimiento, consulta y control.

En el 2019, García y Huamani [19] al analizar la situación actual de las organizaciones de estudio, comprobaron que los empleados no contaban el conocimiento de los activos de información más importantes para la institución, los riesgos a los que estaban expuestos los activos y sobre todo carecían de una cultura sobre la gestión de riesgos de TI, llevándolos a tomar decisiones de último momento cuando una amenaza o un escenario de riesgo se materializa. Para solucionar este inconveniente, los autores implementaron un modelo de gestión de riesgos usando como metodologías base a OCTAVE-S y la ISO/IEC 27005; con el fin de respaldar los activos más significativos que estén propensos a los diferentes riesgos, llegando a causar daños relevantes en la organización; asimismo, establecieron indicadores como apoyo en la fase de monitorización además de la proposición de controles para mitigar las amenazas y disminuir el impacto. Esta investigación aportó a la presente tesis una perspectiva con el fin de adoptar las metodologías de gestión de riesgos y demostró como a través de la implementación se concientizó a los trabajadores de adquirir nuevas nociones sobre la mitigación de los riesgos en base a los activos más críticos, planteando además políticas y controles para una adecuada gestión de los riegos de TI. Después de la implementación del modelo, se pudo observar como la organización logró progresar y establecer un adecuado plan de gestión de riesgos con el fin de mejorar la toma de decisiones;

por lo que el modelo a través de sus fases detalladas, sirve como guía a las organizaciones porque demuestra con gran sencillez como una adecuada gestión de riesgos de TI puede minimizar las amenazas y escenarios de riesgos que puedan materializarse.

En el 2018, Vásquez y Alva [20] a través del estudio del diagnóstico del sector encontraron los siguientes inconvenientes: En el año 2011 una de las organizaciones analizadas registró S/. 100,000.00 soles en pérdidas a causa de un fallo provocado al momento de incorporar una campaña nueva; otra de las entidades en evaluación tuvo problemas serios cuando el servidor principal se paralizó por la ausencia de un plan de continuidad; un contratiempo adicional hallado fue a través de los empleados al no contar con información oportuna para poder identificar los riesgos de TI; las empresas tampoco presentaron planes de comunicación de los riesgos, llegando a complicar el procedimiento de toma de decisiones por parte de la alta gerencia; así mismo, las instituciones no poseen un cultura sobre la gestión de riesgos, de modo que el cumplimiento de las políticas solo son atendidas exclusivamente ante la ejecución de alguna auditoría. De forma global, las compañías tratadas en esta investigación carecen de los medios indispensables para analizar eficientemente los riesgos, además de la falta de implementación de algún procedimiento para el tratamiento de los riesgos por lo que tampoco se detectó el monitoreo continuo de la gestión de riesgos. En busca de una solución eficiente, Vásquez y Alva dieron a conocer una propuesta de solución ante la carencia de gestión de riesgos de TI halladas en las entidades de estudio; por lo que aplicaron un análisis de estudio sobre la situación actual del sector microfinanciero y la gestión de riesgos de TI, a través del cual el riesgo forma parte de los negocios a causa de los cambios continuos que son parte del trabajo empresarial; añadiendo frameworks vinculados a la gestión de riesgos de TI (ISO/IEC 22301, ISO/IEC 27005, ISO/IEC 31000, COBIT 5, MAGERIT y OCTAVE), establecieron un modelo adaptado para este rubro. La propuesta de gestión de riesgos de TI se validó mediante el juicio de expertos, demostrando que el modelo es apto para aplicarlo en dicho sector. Esta tesis proporcionó un gran aporte al presente trabajo de investigación porque nos otorgó una guía a través de la implementación del modelo de gestión de riesgos de TI que fue de gran ayuda para la mitigación de los riesgos; además en el proceso de análisis de riesgos se lograron identificar cuáles son los procesos más críticos y en relación a estos procesos se determinaron los riesgos más propensos a impedir el logro de los objetivos estratégicos de la organización. Con la finalidad de poner en marcha los planes de acción indispensables para evitar que los riesgos se propaguen originando pérdidas económicas y

desprestigio de la organización, se otorgaron plantillas guías basados en los planes de acción incluyendo las políticas primordiales para una adecuada gestión de riesgos de TI.

1.2. Bases teóricas

1.2.1. Modelo de Gestión de Riesgos de TI

1.2.1.1. Definición de Modelo

Para COBIT 5 (Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa) [21, p. 92] puntualiza el "modelo" como: "Una forma de especificar un grupo de elementos y el modo en que estos interactúan entre sí con el fin de explicar el trabajo fundamental de un componente, sistema o su concepción".

Para mayor comprensión se define el término «modelo» como un conjunto procesos extraídos del análisis de las diferentes metodologías adaptadas a la necesidad de las organizaciones, con el fin de crear valor en los procesos core de las instituciones.

1.2.1.2. Gestión de Riesgos de TI

1.2.1.2.1. Definición de Gestión de Riesgos

En el marco de trabajo COBIT 5 (Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa) [21, p. 91], se establece la "gestión" como:

> … La decisión razonable de los procedimientos, usuarios, actividades, métodos, entre otros; con el propósito de obtener un medio identificado o una herramienta a través del cual la alta gerencia logra el cumplimiento de sus metas trazadas. La gestión es la encargada de la implementación en los procesos predefinidos por la gerencia. La gestión establece los procesos funcionales de planeamiento, elaboración y supervisión del alineamiento con la gerencia que determina quienes estarán al mando de los datos relacionados con dichos procesos.

Por otro lado, MAGERIT [22, p. 9] determina el riesgo como: "La evaluación del nivel de exhibición en el que las amenazas se manifiesten

impactando en los activos provocando la pérdidas y contratiempos en las instituciones".

Así mismo, NIST 800-39 [23, pp. B-7], menciona que el riesgo es: "Una medida donde la entidad se ve amenazada por circunstancias o eventos potenciales, y típicamente una función de: los impactos adversos que surgirían si ocurriera la circunstancia o evento; y la probabilidad de ocurrencia".

En manera de conclusión precisamos que el riesgo es la oportunidad de que un contratiempo o catástrofe se materialice provocando un daño o perjuicio a un objetivo o una organización.

Por otra parte, COBIT 5 (Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa) [21, p. 91], puntualiza que la gestión de riesgos:

> … Necesita identificar los riesgos, valorar el impacto y frecuencia de ocurrencia así como la elaboración de estrategias entre las cuales se encuentran: eludir el riesgo disminuyendo el impacto perjudicial o trasladando el riesgo con el propósito de tratarlo dentro de los rangos de apetito de la organización.

Así mismo, MAGERIT [24] concreta la gestión de riesgos como:

> … Las opciones de establecimiento para las políticas se seguridad más convenientes con el fin de identificar, obstaculizar, minimizar los riesgos reconocidos para disminuir su capacidad de perjudicial. La gestión de los riesgos se fundamenta en las respuestas extraídas del análisis de riesgos.

Por último, NIST 800-39 [23, p. 6] menciona que:

> … La gestión del riesgo es un proceso complicado y contiene muchas etapas por lo que es necesaria la intervención toda la organización: de

> altos ejecutivos que brindan la perspectiva organizacional, las metas gerenciales y objetivos para la empresa; a los gerentes que planean, ejecutan y administran proyectos; a individuos que manejan los sistemas informáticos que respaldan objetivos de la institución / funciones comerciales.

Por lo tanto, se infiere que la gestión de riesgos es un planteamiento organizado que tiene como objetivo minimizar la inseguridad relacionada a las amenazas por medio de un conjunto de metodologías o procedimientos que incorporan procesos que colaboran con la identificación, análisis, evaluación y el tratamiento de los riesgos, logrando establecer políticas o métricas adecuadas empleando recursos de la alta gerencia.

1.2.1.2.2. Definición de Riesgos de TI

Según COBIT 5 (para Riesgos) [25, p. 111], el riesgo de TI es: "El riesgo es el proceso vinculado con la utilidad, la pertenencia, la ejecución, la intervención, la repercusión y la implementación de TI en los procesos de la organización".

Por lo tanto, se concluye que el Riesgo de TI, es el grado de incertidumbre relacionado con las tecnologías de la información, que se presentan o manifiestan entre las organizaciones y sus procesos o actividades; por ejemplo: la probabilidad de paralización de los servidores o servicios a causa de un factor externo (corte de energía eléctrica, movimientos sísmicos, etc.) o interno (manipulación deliberada o por desconocimiento) de la organización.

1.2.2. Activos de Información

1.2.2.1. Definición de Activo

Para la UNE 71504 [26], establece que "un activo es un elemento fundamental en un sistema de información, que puede ser vulnerado de forma deliberada o intencional así como accidentalmente, lo que puede acarrear consecuencias negativas para la institución. Así mismo, menciona que un activo pude ser desde

algo tangible como son los equipos - hardware hasta productos intangibles como las aplicaciones o software".

CRAMM [27] lo define como: "Un componente o parte del sistema total. Los activos pueden ser de cuatro tipos: físicos, software de aplicación, datos o servicios para el usuario final".

OCTAVE [28, p. 34] establece que: "un activo es parte importante de una entidad ya que proporciona un valor monetario a la misma. Son utilizados por las instituciones para cumplir sus metas trazadas y generar superávit o ganancias".

Para INCIBE [29, p. 4], el activo es:

> … El medio indispensable que una organización utiliza para el desarrollo de las tareas, por ende el perjuicio de la disposición puede provocar un daño indirecto o financiero. El origen de los activos está sujeto a la organización, por lo que su seguridad estará definida por la gestión del riesgo. El proceso de valorar un activo es fundamental para analizar la dimensión del riesgo.

De acuerdo con COBIT 5 (para Riesgos) [25, p. 111], un activo es: "un objeto valioso y fundamental sin importar la estructura física o lógica, por lo que es indispensable su protección, los activos están constituidos por el personal mismo, los sistemas, la infraestructura, las finanzas y la reputación".

Con respecto a las definiciones anteriores se infiere que, los activos son recursos o componentes indispensables dentro de una organización, estos forman parte del desarrollo de sus actividades y del logro de los objetivos estratégicos de la organización; los activos pueden ser vulnerables ante algunas circunstancias o perjuicios por lo que es fundamental su protección a través de la gestión de riesgos.

1.2.2.2. Definición de Información

Según COBIT 5 (Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa) [21, p. 91], la información es:

> … Un tipo de activo que al igual que los demás, debe ser protegido por formar parte de los procesos fundamentales de una organización. La información está presente en distintos aspectos, ya se escrito, virtualmente, vía e-mail, impreso, grabado de una videoconferencia, entre otros.

Se puede concluir que la información puede estar conformada por bienes tangibles e intangibles, los cuales contienen datos relevantes ya sea en fragmentos o en su totalidad, por lo tanto representan la esencia de la organización.

1.2.2.3. Activo de Información vs Activos Tecnológicos

Por otro lado, OCTAVE [28, p. 34] puntualiza que:

> … El activo de información puede ser descrito como los datos o la información de suma importancia para la institución, incluyendo información tal como datos de pacientes, los datos de los clientes o los derechos de autor. Los activos se clasifica en: físicos (hojas, discos compacto y otros) y electrónicos (copias de respaldo, archivos, en los ordenadores portátiles).

Entonces, se dice que un activo de información es todo elemento de las instituciones que albergan los datos relevantes por diferentes tipos de medios, ya sean físicos o lógicos.

Además OCTAVE [28, p. 35] plantea que los activos tecnológicos: "Son depósitos electrónicos que tienen como función principal albergar a los activos de información, transportados o procesados. Este tipo de activos frecuentemente contienen servidores, aplicaciones, software, redes y hardware".

Se deduce que los activos tecnológicos a diferencia de los activos de información, son aquellos medios donde se pueden almacenar datos importantes solo mediante el uso de la tecnología.

1.2.3. Hospitales de Nivel II - I

1.2.3.1. Definición de Hospitales

Según la Organización Mundial de la Salud (OMS) [30, p. 122], "el Hospital conforma a la entidad social y médica, la cual tiene la misión brindar a la comunidad la atención de salud terapéutica y preventiva los cuales a través de su servicios alcanzan a cubrir el entorno familiar".

En consecuencia, los hospitales también llamados Nosocomios, son entidades que ofrecen atención de primera necesidad a todas las personas que padecen de alguna enfermedad y son atendidas por el personal de salud (técnicos, enfermeros y médicos) a tiempo completo durante los 365 días del año, usando como apoyo la «tecnología» para el tratamiento adecuado y especializado de los pacientes.

1.2.3.2. Tipos de Hospitales (Clasificación)

El Ministerio de Salud (MINSA) [31, p. 2] establece "las jerarquías de los nosocomios por niveles de atención":

2do Nivel de Atención: Conformado por todos aquellos nosocomios que prestan servicio de Atención General (Categoría II - 1 y Categoría II - 2) y aquellos que cuentan con Atención Especializada (Categoría II - E) [31, p. 2].

3er Nivel de Atención: Conformado por nosocomios con Atención General (Categoría III - 1) y nosocomios con Atención Especializada (Categoría III - E y Categoría III - 2) [31, p. 2].

Para esta clasificación se excluyen los establecimientos de Primer Nivel por estar conformados de Postas de Salud o Puestos de Salud con profesionales no médicos (técnicos, enfermeras, obstetras).

1.2.3.3. Características de Hospitales de Nivel II - I

Los hospitales de Categoría II - 1, son aquellos establecimientos que ofrecen servicios de salud con tratamientos recuperativos y especializados además de las atenciones de complejidad media en el centro quirúrgico.

Por ello, el MINSA establece las características básicas que conforman y definen a los nosocomios según la Categoría II - 1:

Son considerados en esta categoría todos los nosocomios que presten servicio de atención en general. Así como aquellos que cumplan las siguientes funciones principales: Promoción, prevención, recuperación, Rehabilitación, y gestión. Y por último, que contengan todas las Unidades Productoras del servicio de salud (UPSS).

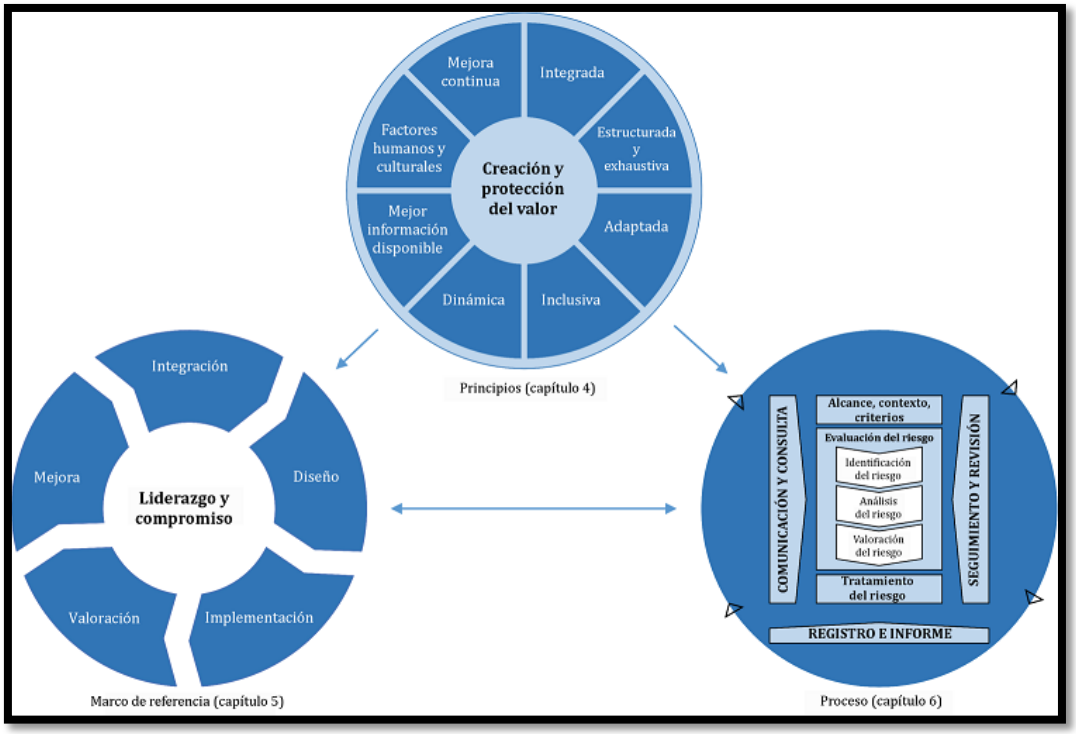
1.2.4. Metodologías de Gestión de Riesgos

ISO 31000:2018

La International Organization for Standardization [32] elaboró esta norma la cual está dirigida aquellas personas que se encargan o buscan el modo de resguardar los activos de valor dentro de las instituciones mediante la gestión de riesgos, la elección de las mejores propuestas cumpliendo con las metas planteadas y optimizando el desempeño.

La estructura de la ISO 31000 está enfocada en los principios, el marco de referencia y el proceso. Estos elementos existen anticipadamente en gran parte de las empresas, pero se sugiere una previa adaptación con la finalidad de que la gestión del riesgo sea eficaz y congruente de acuerdo a las necesidades de cada institución.

Figura 1: Principios, marco de referencia y proceso



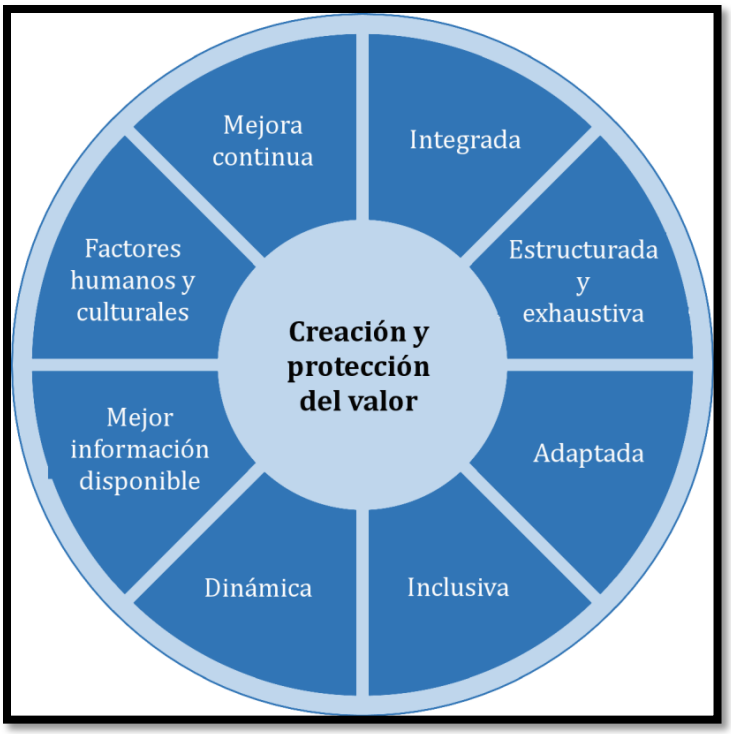
Fuente: UNE - ISO 31000:2018 [32, p. 6]

1. Principios:

El objetivo de la gestión del riesgo es proteger y crear valor en las empresas. Mejorando así el desempeño de las mismas promoviendo los aportes que impulsen el desarrollo de los objetivos trazados.

En la Figura 2 se muestran los principios desglosados que suministran una guía acerca de las características de la gestión del riesgo eficiente, generando valor a través de la aclaración de sus objetivos. Siendo el pilar de la gestión del riesgo teniendo que ser tomados en cuenta al momento de establecer el marco de referencia. Cuya función principal es ayudar en la gestión de incertidumbres con la finalidad de cumplir con las metas establecidas.

Figura 2: Principios de la ISO 31000



Fuente: UNE – ISO 31000:2018 [32, p. 9]

Una gestión del riesgo eficaz requiere los componentes de los principios mostrados en la figura anterior, los cuales se puntualizan de la siguiente manera:

a) Integrada.- Por ser fundamental para integrar todos los procesos que realiza la institución.
b) Estructurada y exhaustiva.- Porque ayuda a obtener respuestas optimas mejorando el proceso de gestión del riesgo.
c) Adaptada.- la metodología y la gestión de riesgo se adecuan llegando a ser equitativos en el cumplimiento de las metas de la organización.
d) Inclusiva.- porque permite que se tome en cuenta las opiniones brindadas en las intervenciones acertadas de los stakeholders.
e) Dinámica.- porque el comportamiento del riesgo varía de acuerdo a la situación en relación con los factores interno y externos de la institución.
f) Mejor información disponible.- la información utilizada está conformada por datos actuales y antiguos, al igual que los planes en desarrollo.
g) Factores humanos y culturales.- las decisiones tomadas y los factores impactan notablemente en los procesos de la gestión del riesgo.

h) Mejora continua.- A través de la experiencia y el aprendizaje diario, la gestión del riesgo demuestra una mejora continua.

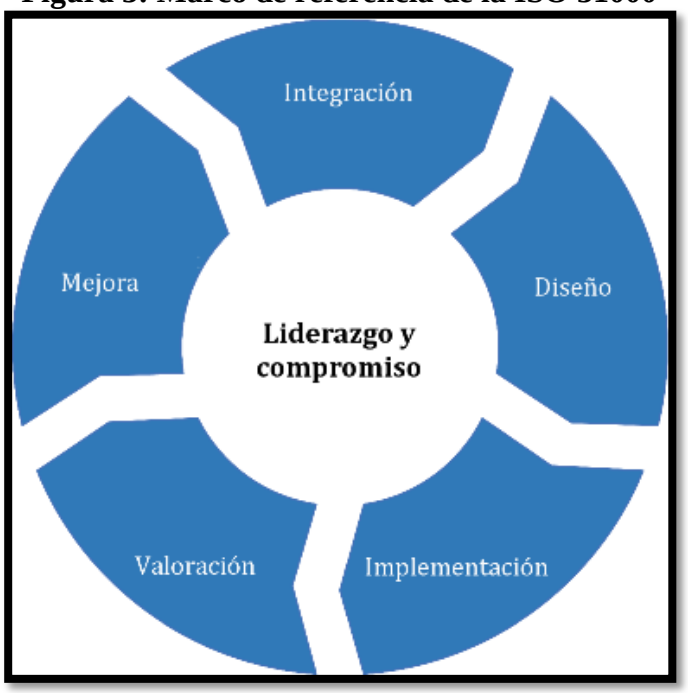
2. Marco de referencia:

La metodología de la gestión de riesgo tiene como objetivo fundamental unir todos los procesos importantes o relevantes. La eficiencia de la gestión del riesgo se deberá

El objetivo de la metodología de gestión de los riesgos, es brindar un soporte a la empresa integrando la gestión de los riesgos en sus fases y procesos importantes. La competencia de la gestión del riesgo está relacionada con la relación de gobierno en la institución, incorporando las decisiones tomadas. Naturalmente en necesario el aporte de los stakeholders y la gerencia.

El desenvolvimiento del framework incluye la integración, el diseño, la implementación, el valor y la mejoría de la gestión del riesgo a través de la institución. La siguiente figura muestra los elementos que lo conforman:

Figura 3: Marco de referencia de la ISO 31000



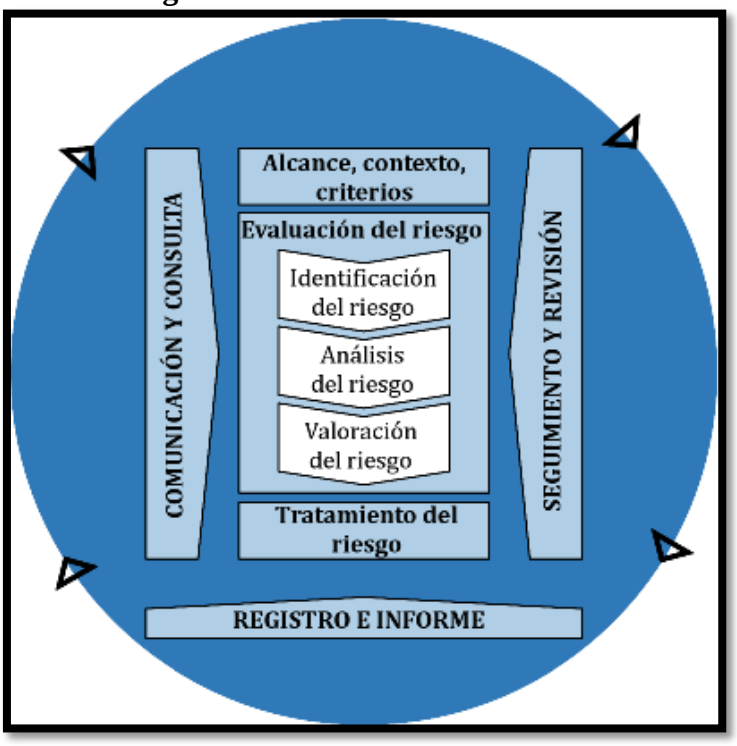
Fuente: UNE – ISO 31000:2018 [32]

El marco de referencia y sus elementos necesitan ser adaptados a los requerimientos de la organización.

3. Proceso:

La gestión del riesgo incluye la ejecución de procesos, políticas de las tareas de consulta y comunicación, identificación de los parámetros externos e internos, las opciones de tratamiento, el monitoreo y evaluación y por último el documento informativo del riesgo; esta actividad se muestra en la figura a continuación.

Figura 4: Proceso de la ISO 31000



Fuente: UNE – ISO 31000:2018 [32]

La gestión del riesgo tiene que ser incluida dentro de la constitución, las actividades y protocolos de la institución. Por lo que debe implementarse estratégicamente y operativamente.

Mediante el desarrollo de la gestión del riesgo de han tomado en cuenta las actitudes de las personas y su cultura.

ISO 27005:2018

La International Organization for Standardization [33] ISO/IEC 27005 se encuentra dentro del grupo de la ISO 27000, además conforma la agrupación incremental de metodologías sobre Sistemas de Gestión de la Seguridad de la Información (SGSI).

Esta metodología sirve como guía a los directores y las personas interesadas en la gestión de riesgos de la información en el contexto interno de la institución y, cuando corresponda, a las partes externas que apoyan tales actividades.

Alcance:

Este marco de trabajo establece pautas para gestionar los riesgos; avalando las definiciones establecidas en la ISO/IEC 27001, por lo cual su diseño apoya en la implementación beneficiosa basada en una perspectiva de gestión de riesgos. La información de los modelos, fases y las condiciones establecidas en la ISO/IEC 27001 es fundamental para el entendimiento general de este marco de trabajo. Así mismo, esta metodología poder ser utilizada en cualquier rubro de las instituciones que tienen como objetivo la gestión de los riesgos, tendiendo a perjudicar la protección de la información en las empresas.

Estructura:

Este marco de trabajo incluye las características del proceso de gestión de riesgos y sus procesos.

La información de fondo se detalla en la Cláusula 5.

En la Cláusula 6 se ofrece una descripción completa del proceso de gestión de riesgos:

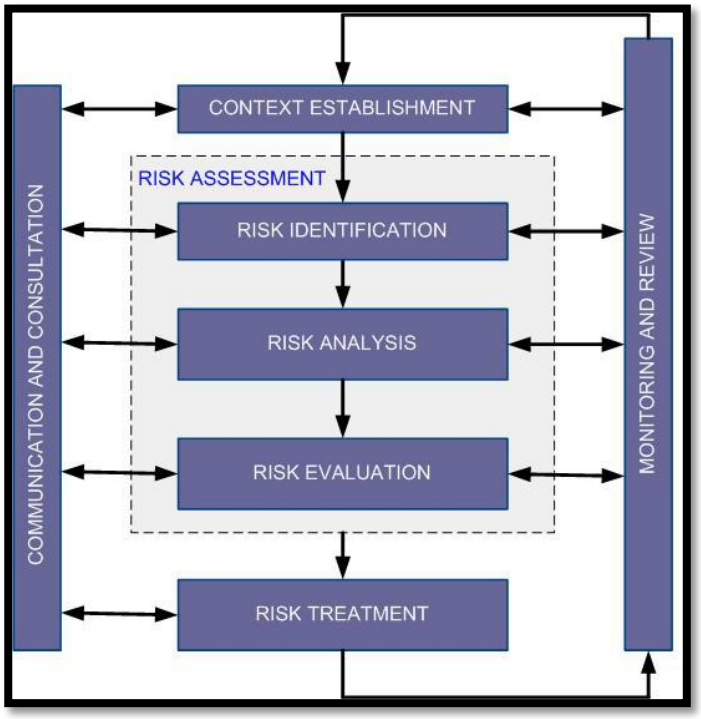
- Establecimiento de contexto en la Cláusula 7,
- Evaluación de riesgos en la Cláusula 8,
- Tratamiento de riesgos en la Cláusula 9,

- Aceptación de riesgos en la Cláusula 10,
- Comunicación de riesgos en la Cláusula 11,
- Monitoreo y revisión de riesgos en la Cláusula 12.

En los anexos se presentan detalles complementarios para los procesos del riesgo. La implementaciones de los parámetros externos internos, están respaldado por el Anexo A (establece los procesos y los límites del proceso de gestión de riesgos). La identificación y valoración de los activos y la valoración del impacto se revisan en el Anexo B. El Anexo C proporciona prototipos de amenazas habituales y el Anexo D analiza las vulnerabilidades y los procedimientos para el análisis de vulnerabilidades. En el Anexo E se presentan ejemplos de enfoques de evaluación de riesgos de seguridad de la información.

Una vista de la capacidad de la etapa de gestión de riesgos se especifica en ISO 27000 y se muestra en el siguiente diagrama.

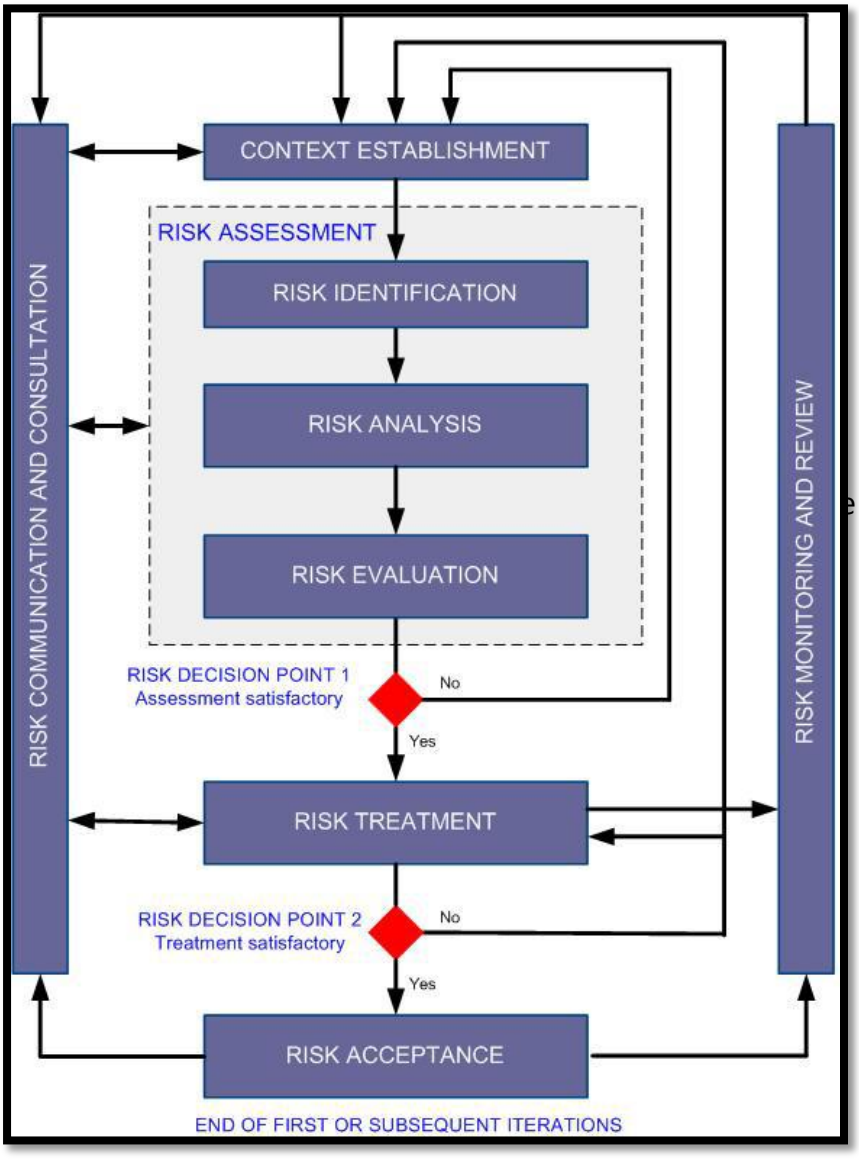
Figura 5: El proceso de gestión de riesgos



Fuente: ISO/IEC 27005:2018 [33]

La Figura 6 muestra cómo esta Norma Internacional aplica este procedimiento de gestión de riesgos, el cual consiste en el establecimiento del contexto (Cláusula 7), la evaluación del riesgo (Cláusula 8), el tratamiento del riesgo (Cláusula 9), la aceptación del riesgo (Cláusula 10), la comunicación y consulta del riesgo (Cláusula 11), y la supervisión y revisión del riesgo (Cláusula 12).

Figura 6: Ilustración de un proceso de gestión de riesgos de seguridad de la información



Fuente: ISO/IEC 27005:2018 [33]

Como ilustra la Figura 6, El contexto se establece primero. Después de ejecuta una valoración de riesgos. Si esto proporciona información necesaria para decidir de manera efectiva las tareas indispensables para mitigar los

riesgos a una categoría tolerable, se concluye la etapa y el tratamiento de riesgo sigue. Si los datos son insuficientes, se realizará otra tarea de la valoración de riesgos con un contexto analizado (por ejemplo, criterios de impacto del riesgo, criterios de aceptación de riesgos, o criterios de evaluación de riesgos), probablemente en zonas establecidas de todo el alcance.

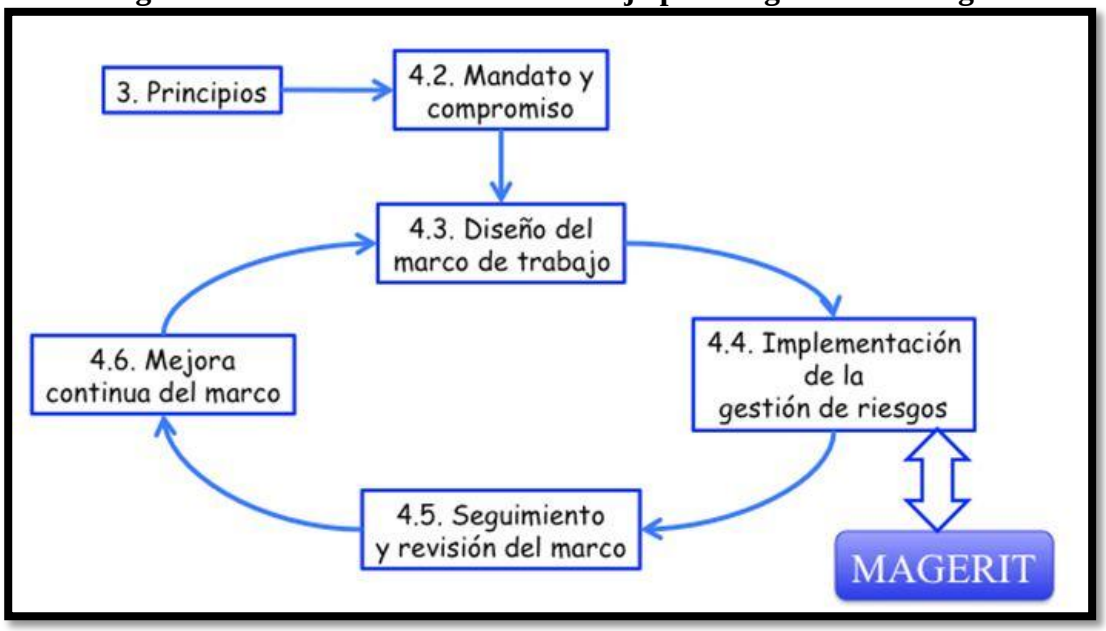
MAGERIT

El Consejo Superior de Administración Electrónica del Gobierno de España (CSAE) ha desarrollado y fomenta la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) [22] en modo de alternativa a la apreciación de que la Administración Pública (incluyendo toda comunidad) necesitan de los sistemas de información para cumplir sus metas trazadas.

Esta metodología brinda soporte a las empresas o personas que utilizan información digital, por ser el medio indispensable para la prestación de sus procesos o servicios. Al usar MAGERIT se tendrá conocimiento de la importancia que posee cada activo y brindará pautas para ponerlo a salvo. Comprender el riesgo que acecha a los componentes de trabajo es fundamental para procesarlo. MAGERIT establece un método con el fin de dar evitar improvisaciones.

Usando la ISO 31000 como pilar base, MAGERIT establece el proceso de gestión de riesgos mediante la “Implementación de la gestión de los riesgos”; es decir, establece la gestión de riesgos mediante un framework para que las empresas escojan las mejores opciones considerando los riesgos derivados de las tecnologías de información a través de su uso.

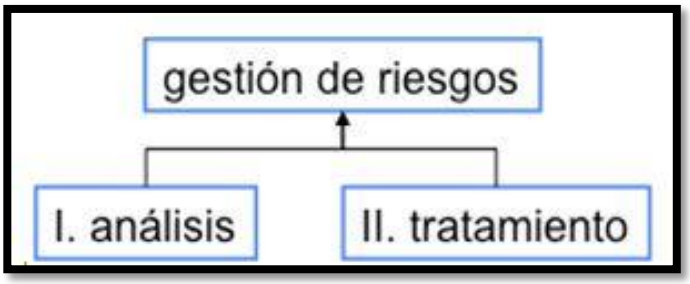
Figura 7: ISO 31000 - Marco de trabajo para la gestión de riesgos



Fuente: MAGERIT v3.0 [22]

El tratamiento y el estudio de los riesgos, son aspectos claves del contexto que la Administración Electrónica tiene como propósito para cumplir con principios fundamentales y los requerimientos básicos para proteger apropiadamente la información. MAGERIT es un mecanismo que pretende simplificar el establecimiento y la ejecución del Esquema Nacional de Seguridad.

Figura 8: Gestión de riesgos



Fuente: MAGERIT v3.0 [22]

Objetivos:

Los objetivos específicos de MAGERIT son los siguientes:

1. Establecer una cultura a las empresas y a los encargados de la información, de la realidad de los riesgos y de la importancia de mitigarlos.

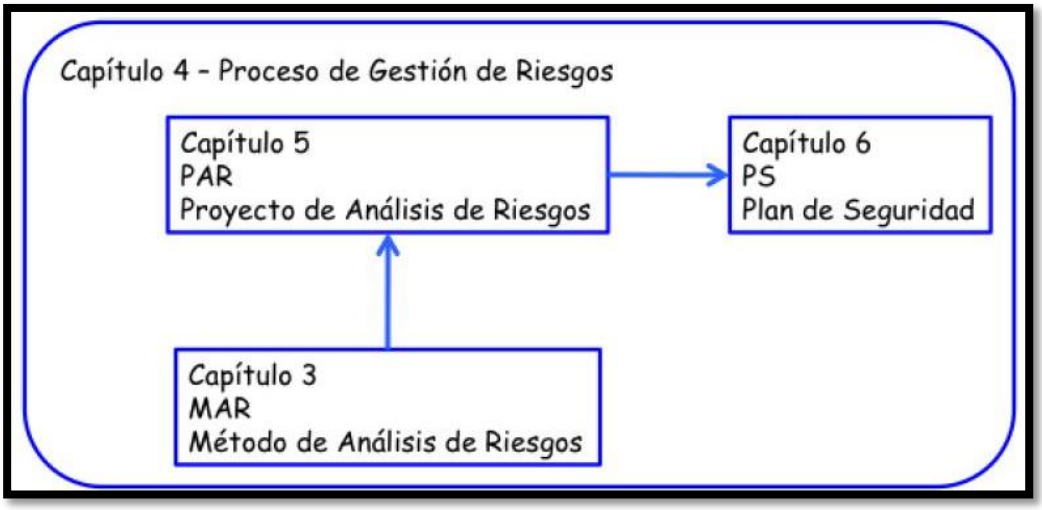
2. Proporcionar un procedimiento organizado para estudiar los riesgos provenientes de las TI.
3. Cooperan en la identificación y proyección del tratamiento adecuado con el fin de preservar los riesgos controlados.
4. Alistar la institución para la etapa de análisis, acreditación y auditoria para el caso más conveniente según sea la situación.

Método:

Se organiza a través de los siguientes capítulos:

- El capítulo 2 muestra nociones básicas haciendo referencias a los procesos del análisis y el tratamiento como parte de un procedimiento global de la gestión de riesgos.
- El capítulo 3 confirma los procedimientos y oficializa las tareas del estudio de los riesgos.
- El capítulo 4 detalla alternativas y perspectivas del tratamiento de riesgos confirmando las tareas de la gestión de riesgos.
- En el capítulo 5 se basan en el estudio del riesgo por medio de planes que serán implementados en el primer estudio de riesgos en un sistema y gradualmente cuando surjan modificaciones elementales teniendo que reestructurar el modelo de forma extendida.
- En el capítulo 6 se oficializan las tareas de los planes de seguridad.
- En el capítulo 7 se enfocan en la elaboración de los sistemas de información y cómo el estudio de los riesgos aporta en la gestión de seguridad del resultado final desde que empieza hasta que es puesto en marcha.
- En el capítulo 8 se adelantan algunos inconvenientes que van surgiendo al momento de ejecutar el análisis de riesgos.

Figura 9: Actividades formalizadas



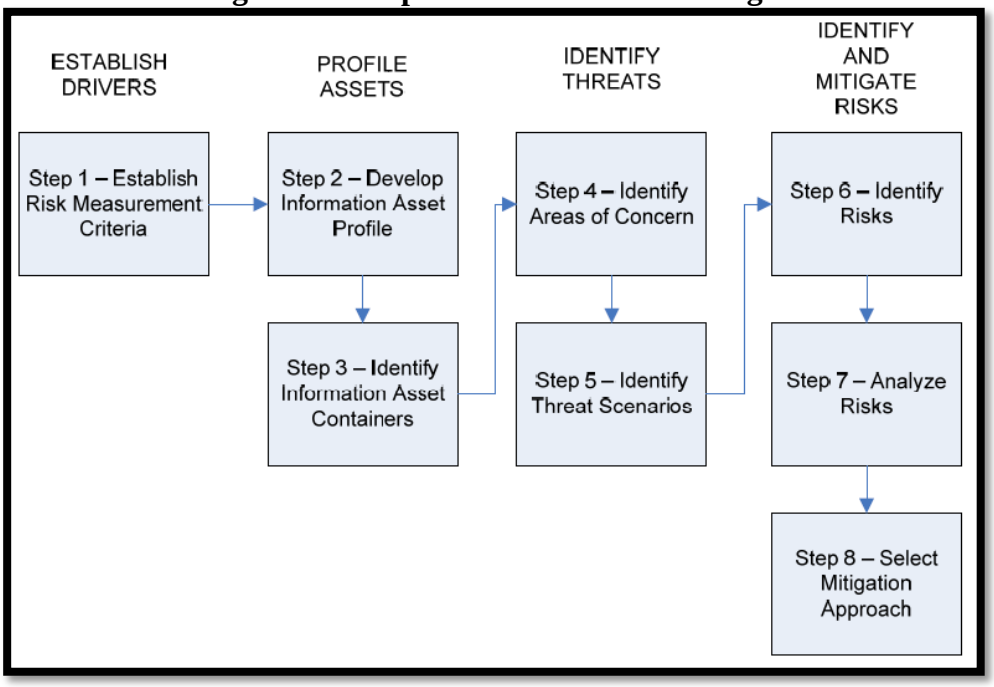
Fuente: MAGERIT v3.0 [22]

OCTAVE ALLEGRO

Elaborado por R. A. Caralli *et al.* [28], Operationally Critical Threat, Asset and Vulnerability Evaluation (OCTAVE) es un marco de trabajo para identificar y evaluar los riesgos de seguridad de la información. Su objetivo es contribuir a las organizaciones en:

- Establecer perspectivas de valoración de los riesgos cualitativos que describen la flexibilidad del riesgo operacional en la empresa.
- Reconocer todos los activos fundamentales que permitan cumplir con la misión planteada por la entidad.
- Identificar o determinar, en un listado de acuerdo a su importancia, las debilidades y posibles amenazas que posean cada uno de los activos en evaluación.
- Puntualizar y estimar los diferentes marcos del entorno interno o externo de la empresa en caso se materialicen las debilidades o amenazas.

Figura 10: Mapa Vial de OCTAVE Allegro



Fuente: OCTAVE Allegro [28]

OCTAVE Allego, es un marco de trabajo que está compuesto de ocho procesos, los cuales se reorganizan en cuatro fases, tal como se muestra en la Figura anterior.

Fase 1, Toda organización deberá de desarrollar diversos criterios con el propósito de calcular el riesgo, de acuerdo a los objetivos que ayuden en cumplir la misión de la entidad.

Fase 2, se busca determinar o establecer los activos de información críticos, los cuales deberán estar pulidos. Al pulir estos activos es necesario que se establezcan límites concisos, identificando así los requisitos que se necesitan para su seguridad y a su vez determinando los sitios estratégicos para almacenar dichos activos.

Fase 3, se busca establecer por medio de un listado, elaborado por grado de significancia, las amenazas o debilidades que puede tener un activo de información. Cabe señalar que esta relación se determinara evaluando el entorno, ya sea interno o externo, de los sitios estratégicos donde se almacenan dichos activos.

Fase 4, es la última fase donde se identifican y examinan los riesgos, mediante una previa valoración de los activos de información, desarrollando una perspectiva de mitigación eficaz.

Metodología:

OCTAVE Allegro, nos muestra en su metodología ocho pasos a seguir. Los cuales se desarrollan en cuatro áreas de actividad. Así tenemos:

Áreas de Actividad:

- Plantear procesos, donde la entidad desarrolla o establece sus criterios de medición referente a los riesgos encontrados, los cuales deberán ser acorde a los objetivos de la institución.
- Los activos de la empresa, que se enlistaron frente a la evaluación de riesgos.
- Determinar las amenazas y debilidades que poseen los activos previamente evaluados en su entorno a través de un proceso organizado.
- Identificar y minimizar los riesgos detectados en la evaluación. Así como establecer estrategias para afrontar a los riesgos encontrados, a fin de tener una respuesta optima en beneficio de la organización.

La información recolectada a través de las actividades anteriormente descritas, se va a considerar como salidas. Las cuáles serán consideradas parte de las hojas de trabajo, y formaran parte de las entradas de los procesos siguientes.

Como se mencionó este marco de trabajo está compuesto de ocho pasos los cuales se dan a conocer a continuación:

1 – Determinar o establecer los métodos de medición en relación al riesgo.

2 – Establecer un perfil o un conjunto de características que nos sea útil en la recolección de información referente a un activo.

3 – Identificar toda la información escondida dentro de los activos contenedores.

4 - identificar aquellos procesos que merecen ser atendidos por tener alto grado de amenaza en la valuación de riesgo.

5 - Identificar o determinar los diferentes marcos que pueden generar una amenaza.

6 – Identificar cada uno de los riesgos que posee la institución.

7 – Elaborar un análisis de riesgo de forma eficaz.

8 – Aplicar el enfoque de Mitigación de riesgos.

NIST SP 800-30

El propósito de National Institute of Standards and Technology (NIST) [34], es proporcionar orientación para determinar los diversos riesgos presentados en los sistemas y organizaciones donde se conservan información federal. Ampliando con esto la guía de la Publicación Especial 800-39.

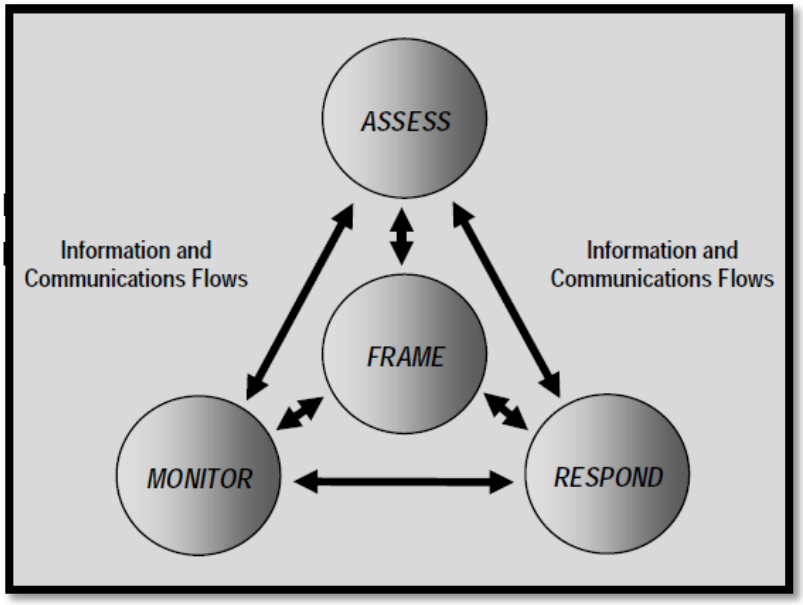
La evaluación de los riesgos se realiza en base tres niveles; las cuales forman parte del proceso para desarrollar una adecuada gestión de riesgos. Cuyos resultados serán otorgados a los líderes o ejecutivos, con la finalidad de que puedan determinar las acciones que deberán tomar en solución a los riesgos reconocidos.

Proceso de Gestión de Riesgos:

La publicación especial NIST 800-39 describe a la evaluación de riesgos como un factor importante dentro de una organización holística que abarca toda la organización.

Los procesos de gestión de riesgos incluyen: (i) enmarcar el riesgo; (ii) evaluar el riesgo; (iii) responder al riesgo; y (iv) seguimiento del riesgo. La Figura 11 ilustra los cuatro pasos en el proceso de gestión de riesgos, incluido el paso de evaluación de riesgos y los flujos de información y comunicación necesarios para que el proceso funcione de manera efectiva.

Figura 11: Evaluación de riesgos dentro del proceso de gestión de riesgos



Fuente: NIST SP 800-30 [34]

El primer componente de la gestión de riesgos determina que se debe enmarcar el riesgo, esto se logra estableciendo un contexto de riesgo, es decir, describir e identificar el ambiente externo e interno en el que se tomaran las decisiones en base a los riesgos encontrados.

El segundo componente de la gestión de riesgos aborda cómo las entidades evalúan el riesgo dentro del ambiente de riesgo organizacional.

El tercer componente de la gestión de riesgos determina la respuesta que tiene las instituciones en base a los resultados obtenidos de la evaluación de riesgos.

El cuarto componente de la gestión de riesgos busca hacer un seguimiento del riesgo. Como es que este se va desarrollando en el tiempo; si se mitiga, se mantiene o aumenta el riesgo dentro de la entidad.

Evaluación de riesgos:

La evaluación de riesgos pretende determinar el grado de afectación que tiene el riesgo dentro de una entidad, por ello se enmarcan un conjunto de pasos, tales como: (i) Preparación para evaluar los riesgos; (ii) evaluaciones

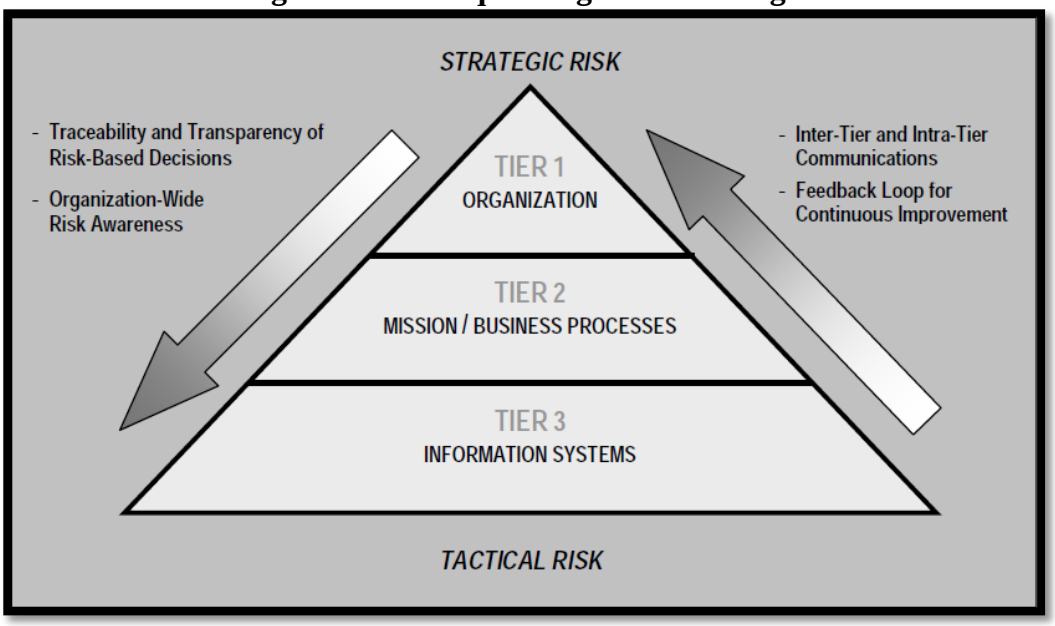
de riesgos; (iii) comunicación de resultados de la evaluación de riesgos; y (iv) evaluaciones de riesgos constantes.

Aplicación de evaluaciones de riesgo:

Las evaluaciones de riesgos se pueden realizar en los tres niveles de la jerarquía de gestión de riesgos: nivel de organización, nivel de misión / proceso de negocio, y nivel del sistema de información.

La Figura 12 ilustra la jerarquía de gestión de riesgos establecida en la Publicación Especial NIST 800-39, que proporciona múltiples perspectivas de riesgo desde el nivel estratégico hasta el nivel táctico. Las evaluaciones de riesgo tradicionales generalmente se centran en el nivel 3 (es decir, el nivel del sistema de información) y, como resultado, tienden a pasar por alto otros factores de riesgo significativos que pueden evaluarse de manera más apropiada en los niveles de Nivel 1 o Nivel 2.

Figura 12: Jerarquía de gestión de riesgos



Fuente: NIST SP 800-30 [34]

El proceso:

Este capítulo detalla los procesos que se llevan a cabo para la evaluación el riesgo dentro de una institución, centrándose en la incertidumbre que acarrea la seguridad de la información. Lo cual incluye:

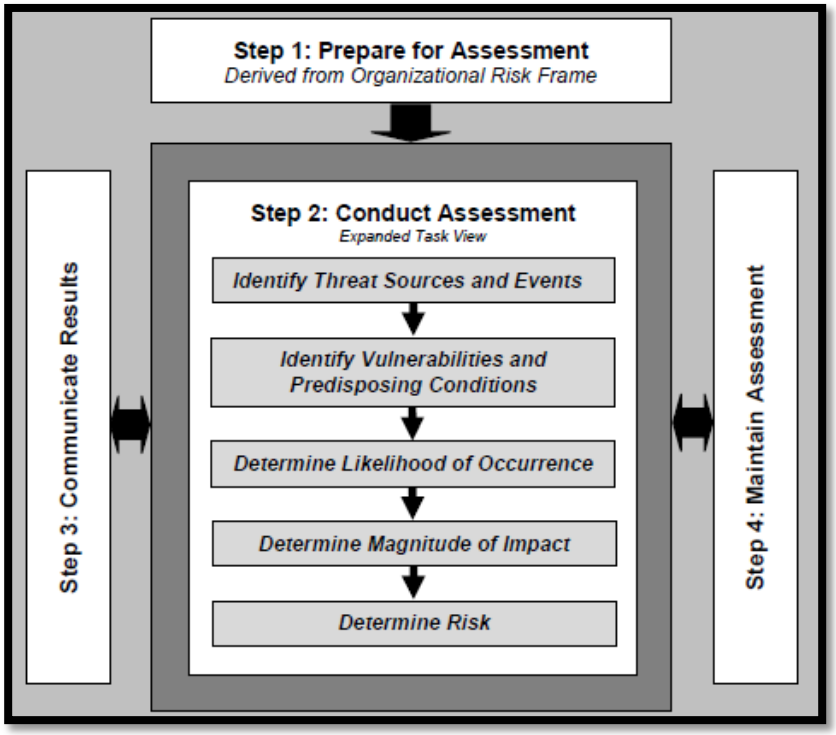
- Obtener una visión general de la totalidad de procesos para aplicar la evaluación de riesgos;
- Planificar actividades necesarias e importantes con la finalidad de estar preparados en las evaluaciones de riesgos;
- Establecer las actividades significativas que permitan desarrollar evaluaciones de riesgo con resultados óptimos;
- Determinar las actividades a realizar con la finalidad de proporcionar información acerca de los resultados obtenidos de la evaluación y a su vez compartir información relevante relacionada con el riesgo; y
- Mantener en acción las actividades importantes determinadas del proceso de la evaluación de riesgos, con la finalidad de mantener un control continuo.

La evaluación de riesgos está compuesta por cuatro pasos:

- preparar para la evaluación;
- conducta la evaluación;
- comunicar resultados de la evaluación; y
- mantener la evaluación.

La Figura 13 ilustra una guía básica para desarrollar un proceso óptimo en la evaluación de riesgos y destaca las tareas específicas para llevar a cabo la evaluación.

Figura 13: Procesos de evaluación de riesgo



Fuente: NIST SP 800-30 [34]

Paso 1:

Preparación Para La Evaluación De Riesgos.- Este paso busca preparar u obtener un conocimiento general del entorno o contexto en que se desarrollara la evaluación de riesgos

Paso 2:

Realización y evaluación de riesgos.- Este paso busca identificar los riesgos de seguridad de la información a través de un listado, los cuales puedan clasificarse por niveles y a su vez utilizados para dar a conocer las decisiones de respuesta a los riesgos encontrados.

Paso 3:

Comunicar Y Compartir Resultados De Evaluación De Riesgos.- Este paso tiene como objetivo principal asegurar que los encargados de tomar decisiones referente a los riesgos, cuenten con toda la información necesaria relacionada al mismo; para que así puedan tomar decisiones acertadas en respuesta al grado de incertidumbre.

Paso 4:

Mantener la Evaluación.- Este paso tiene como objetivo mantener una constante evaluación de riesgo con la finalidad de proporcionar a las organizaciones un conocimiento actualizado del comportamiento del riesgo dentro de entidad.

CAPÍTULO II MATERIALES Y MÉTODOS

2.1. Diseño de Investigación

El presente trabajo de investigación se basa en los Preexperimentos. Según Hernández *et al.* [35, p. 144], "Los preexperimentos son denominados bajo ese nombre porque su grado de control es mínimo".

Considerando la esencia de los Preexperimentos, se opta como diseño de investigación el tipo pre-prueba y post-prueba con un solo grupo.

El diseño de esta investigación tiene la siguiente estructura:

$$\mathbf{ME = V_1 \ X \ V_2}$$

Dónde:

- **ME:** Muestra seleccionada para el estudio.
- **V_1:** Contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas, antes de implantar el modelo de gestión de riesgos de TI.
- **X:** Modelo de Gestión de Riesgos de TI.
- **V_2:** Contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas, después de implantar el modelo de gestión de riesgos de TI.

2.2. Población, Muestra y Muestreo

Población

La población tomada en cuenta en esta tesis está constituida por 7 hospitales de nivel II - I de la región Amazonas según SUSALUD [36].

Muestra

Al tener en cuenta el tamaño de nuestra población, se considera usar la Población Censal, la cual consiste en implantar el Modelo de Gestión de Riesgos de TI a todas las organizaciones de nuestra población sin necesidad de aplicar una fórmula estadística.

Muestreo

El muestreo para nuestra investigación será de tipo probabilístico por racimos o conglomerados. Para Hernández *et al.* [35, p. 182]:

> … Existen ocasiones en las cuales el investigador se encuentra restringido a causa de factores económicos, de tiempo, de alejamiento territorial, y demás impedimentos, por lo que debe acogerse al muestreo por clousters o racimos. En esta clase de muestreo se disminuyen los precios, la energía y el tiempo, al tener en cuenta que en algunas ocasiones las organizaciones para el muestro y estudio están en encerrados o encapsuladas en ciertos territorios geográficos a los que se les llama racimos.

En consecuencia, por distintos motivos de accesibilidad geográfica o de información, se seleccionaron 3 hospitales de nivel II – I de la región Amazonas los cuales se detallan continuación:

- **Hospital 01:**

Creado el 23/11/1989, se encuentra ubicado en Av. Héroes Del Cenepa N° 980 – Bagua - Bagua; tiene como Misión: "Somos un Hospital II – I, que brinda unidades que producen servicios de salud médico quirúrgico de mediana complicación basada en las personas, familia – comunidad, desarrollando un nuevo modelo de gestión hospitalaria y atenciones integrales especializadas, preventivo, promocionales, recuperativas, rehabilitación, prescripción farmacológica con énfasis en materno infantil, con una mezcla de gran humildad, mucha voluntad, alto sentido humanístico y valores éticos"; y a su vez la Visión es: "cubrir las expectativas de los pacientes por medio de la atención sanitaria cálida y personalizada, apoyados por los buenos ambientes de los servicios, la tecnología actualizada y el mejor trato por parte del personal de salud, reforzando el nivel del nosocomio de complejidad mediana y del sistema de referencias y contra referencias en todas la regiones".

- **Hospital 02:**

Fue creado el 18/07/2005, se encuentra ubicado en Jr. San Felipe Santiago N° 111 – Bagua Grande - Utcubamba; tiene como Misión: "Es una Institución del Ministerio de Salud cuyos trabajadores identificados con ella, laboramos en equipo brindando una atención preventiva, promocional, recuperativa y de rehabilitación del usuario, con profesionalismo, calidad, calidez y equidad, comprometidos con la Construcción de un nuevo Hospital y continuar

siendo la Institución de mayor capacidad Resolutiva de la Región"; y a su vez la Visión es: "En el año 2023 el hospital estará constituido como un Hospital seguro y Acreditado en el nivel III-1 del MINSA, considerado el de mayor capacidad Resolutiva de la Región. Contando con un personal capacitado y certificado. Que realiza funciones de promoción, prevención, recuperación y rehabilitación de enfermedades transmisibles y no transmisibles. Para lo que cuenta con servicios especializados con equipamiento de alta tecnología, cumpliendo con las normas de bioseguridad y protección del medio ambiente. Orientado a mejorar la calidad de vida del usuario; a través de la investigación científica y tecnológica, una administración eficiente, cobertura al 100% del SIS y aplicando la Medicina basada en evidencias. Habiendo logrado una adecuada coordinación con sus aliados estratégicos"

- **Hospital 03:**

Creada el 09/12/2006, se encuentra ubicada en el Jr. Alonso de Alvarado Nº 915 – Mendoza – Rodríguez de Mendoza, tiene como Misión: "El hospital busca mejorar la calidad y calidez de atención a la persona, con compromiso social mística y respeto intercultural"; y a su vez la Visión es: "El hospital busca convertirse en una institución especializada con autonomía financiera, innovadora en la región que brinde atención oportuna y eficiente para disminuir el gasto social".

2.3. Métodos, Técnicas e Instrumentos de Recolección de Datos

Observación: Con el respaldo de esta técnica se empezó con el análisis de los principales activos de TI para determinar los posibles riesgos de exposición y conocer la realidad de los hospitales.

Revisión Bibliográfica: A través de este método se revisó y comparó los distintos frameworks sobre la gestión de riesgos de TI que se amoldaron más al sector de estudio.

Encuesta: El instrumento aplicado a los hospitales de la muestra, fue elaborado bajo los dominios relacionados con riesgos de COBIT® 2019 Framework Governance and Management Objectives; teniendo como objetivo identificar y valorar los activos de información así como los riesgos al que están expuestos.

Modelo: Con ayuda de este método, y en base a los diferentes frameworks revisados anteriormente, se logró establecer un modelo de gestión de riesgos de TI, para contribuir en la protección de los activos de información.

2.4. Técnicas de Procesamiento de Datos

Los resultados de la encuesta aplicada a los responsables del área de TI de los hospitales de nivel II – I de la región Amazonas, han sido ingresados y procesados en una hoja de cálculo de Microsoft Office, obteniendo resultados los cuales fueron analizados e interpretados mediante gráficos estadísticos para poder diagnosticar la situación actual de los nosocomios respecto a la gestión de sus activos y de los riesgos a los cuales se encuentran expuestos.

Los resultados de las matrices validadas por los expertos fueron ingresados y procesados en el programa estadístico informático SPSS con el propósito de analizar la confiabilidad del modelo propuesto mediante el Alfa de Cronbach y la concordancia a través del Coeficiente de Kendall.

2.5. Normas Éticas

Los principios éticos establecen las fuentes del conocimiento y el progreso de trabajos científicos y propiedad intelectual [37]; por ende, durante el desarrollo de la presente investigación designada como “Modelo de Gestión de Riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas”, se ha considerado de forma rigurosa acatar los fundamentos de ética que respalden particularidad de esta investigación. Igualmente, se ha mantenido la consideración del caso respecto a los derechos de autor con los libros consultados y las páginas electrónicas revisadas, indispensables organizar y plantear la estructura del marco teórico; asimismo la información adquirida por parte de los encuestados fue obtenida mediante el consentimiento informado, por tal motivo los datos e información plasmada en el presente trabajo de investigación no son ficticios.

CAPÍTULO III RESULTADOS Y DISCUSIÓN

3.1. Diagnóstico del sector

Para el desarrollo de esta sección se hizo uso de un cuestionario de evaluación situacional que fue entregado a los responsables del área de TI de los hospitales seleccionados de nivel II – I de la región Amazonas.

El cuestionario fue elaborado bajo los dominios relacionados con riesgos de COBIT® 2019 Framework Governance and Management Objectives; por tal motivo la herramienta usada está validada. Para más detalles, consulte el **ANEXO N° 01**.

El cuestionario de evaluación situacional aplicado a los responsables del área de TI de los hospitales de nivel II – I de la región Amazonas nos muestra los siguientes resultados:

En cuanto a la **Definición del Alcance y Contexto de la Organización** se pudo analizar que el 100% de las organizaciones no dispone de un plan estratégico establecido para el área de TI. El 33% de las empresas cuenta con políticas de seguridad informática, pero sólo de manera empírica, ya que dichas políticas no se encuentran documentadas. El 100% ha dejado desatendido el reforzamiento a los usuarios sobre las nociones de "Seguridad de la Información".

Respecto a la **Identificación de los Activos**, se observó que el 100% no posee reglamentos internos donde se haga mención de la correcta utilización de los activos de información. El 67% de los hospitales argumentan que los usuarios tienen conocimiento de cuáles son los activos de información más relevantes para la organización. El 67% tiene inventarios de activos de información. El 100% no dispone de una categorización para los activos de información según su valor, requisitos legales, sensibilidad y criticidad. El 33% manifiesta que cuenta con una asignación de activos de información respecto a las responsabilidades y roles de los usuarios. El 67% ha establecido un cronograma de backup de los datos más relevantes para los nosocomios. El 33% declara haber implementado políticas y procedimientos de seguridad para salvaguardar los activos de información.

De acuerdo a la **Evaluación del Riesgo**, el 100% no posee alguna metodología para la identificación y análisis de los riesgos internos y externos relacionados con los activos de

información. El 100% no dispone de una bitácora donde registren los riesgos que han causado impacto comprometiendo los activos de información. El 100% de las organizaciones no tiene definida una filosofía de riesgos. Sólo el 33% de los nosocomios es consiente que la cultura existente en la organización requiere de un cambio o una mejora para poder enfrentar de manera efectiva la gestión de riesgos. El 100% no ha elaborado una tasación de las posibles pérdidas económicas que pueden asumir si un escenario de riesgo de TI se llega a manifestar. El 100% no elaboró un estudio o investigación de los daños experimentados a raíz de la materialización de los riesgos. El 100% de los hospitales no dispone de una clasificación de los escenarios de riesgos.

En cuanto al **Tratamiento del Riesgo**, se pudo analizar que el 100% implementó actividades de control que se deban ejecutar para mitigar los riesgos. El 100% no cuenta con una guía de procedimientos si es que la materialización de un riesgo provoca un impacto significativo en la organización.

Relacionado al **Seguimiento y Evaluación**, el 100% de las empresas no realiza una supervisión del perfil de riesgo. El 100% expresó que la alta dirección no es notificada sobre los riesgos a los que se encuentran comprometidos los activos de información.

Para más detalles sobre las respuestas obtenidas de los cuestionarios de evaluación situacional, consulte el **ANEXO N° 02**.

Los gráficos obtenidos en base a las respuestas de los cuestionarios de evaluación situacional se encuentran en el **ANEXO N° 03**.

3.2. Análisis de marcos del trabajo, metodologías y estándares de gestión de riesgos de TI, relacionados

En este apartado se elaboró la comparación entre los diferentes estándares, marcos de trabajo y metodologías relacionadas con la gestión de riesgos de tecnologías de la información, para lo cual se consideraron los siguientes framework:

- COBIT 5 para Riesgos
- ISO 27005:2018

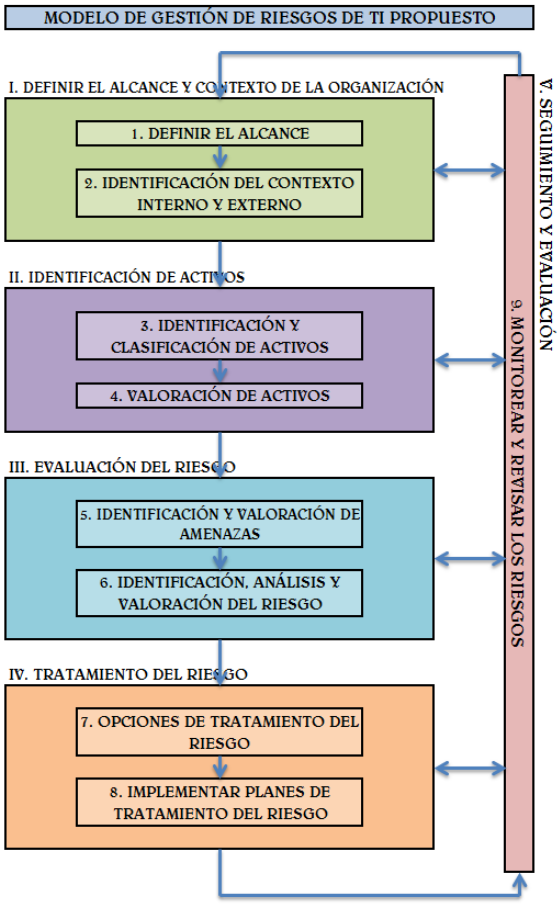
- ISO 31000:2018
- MAGERIT v3.0
- NIST SP 800-30
- OCTAVE Allegro

Para más detalles ver el **ANEXO N° 04**.

3.3. Propuesta del modelo

Como resultado de la comparación de entre los diferentes estándares, marcos de trabajo y metodologías relacionadas con la gestión de riesgos de tecnologías de la información, las cuales fueron amoldadas a los requerimientos de los hospitales de nivel II – I de la región Amazonas, se identificaron las siguientes fases y procesos:

Figura 14: Modelo de Gestión de Riesgos de TI propuesto



Fuente: Elaboración propia

Para más detalles consultar el **ANEXO N° 05**.

Fase I: Definir el Alcance y Contexto de la Organización

Para la ISO 31000 [32, pp. 17, 18], el objetivo de esta fase es el establecimiento del Alcance y los contextos externos e internos de la organización para amoldar el proceso de gestión de riesgos de TI, con el fin de calcular el riesgo eficaz y el tratamiento adecuado para los riesgos.

NIST SP 800-30 [34, p. 24], afirma que el objetivo de esta fase es: "Asegurar que el proceso para definir el alcance, proporcione la información apropiada y que garantice las decisiones tomadas".

Proceso 1: Definir el Alcance

ISO 27005 [33, p. 12], nos dice que: "Las empresas debe definir el alcance y las restricciones de la gestión de riesgos con el fin de respaldar a todos los activos importantes para se tomen en consideración en la evaluación de riesgos".

COBIT 5 para Riesgos [25, p. 114] determina que el Alcance "Tiene que estar integrado en las tareas diarias para constituir las prácticas de gestión cotidiana logrando brindar la seguridad requerida a los stakeholders".

Para NIST SP 800-30 [34, p. 25] es necesario establecer la Aplicabilidad Organizacional, la cual consiste en "Describir las áreas de las instituciones que serán impactadas en el proceso de evaluar el riesgo y las decisiones del riesgo resultante en la evaluación".

Después de analizar las diferentes propuestas por parte de las metodologías que determinan y definen el Alcance para el proceso de gestión de riesgos de TI; se asumirán una serie de pasos con el propósito de identificar el Alcance de la organización:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

1.1. Definir el Alcance por medio de la identificación de los procesos críticos y áreas involucradas de la organización con el fin de ser considerados en el transcurso del proceso de gestión de riesgos de TI.
1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que conforman el Alcance:

   2.1. Director de la organización.
   2.2. Administrador de la organización.
   2.3. Jefe de Recursos Humanos.
   2.4. Responsables de los procesos críticos.
   2.5. Jefes de las áreas involucradas.
   2.6. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

   3.1. Reglamento de Organización y Funciones (ROF).
   3.2. Manual de Organización y Funciones (MOF).
   3.3. Organigrama institucional.
   3.4. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

   4.1. Analizar el ROF, el MOF y el organigrama a detalle.
   4.2. Definir cuáles son los procesos con sus respectivas dependencias en los que la organización tiene como bases para el funcionamiento correcto del negocio; por lo que la paralización o retraso de dichos procesos, podría provocar que algunos escenarios de riesgos lleguen a materializarse.
   4.3. Definir por quién será elaborado el formato y colocar su firma respectiva.
   4.4. Definir por quién será revisado el formato y colocar su firma respectiva.

4.5. Definir por quién será aprobado el formato y colocar su firma respectiva.

4.6. Completar la información obtenida en el formato de definición del Alcance (**Tabla 01**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de los procesos críticos con las respectivas áreas de dependencia, definidas por la alta gerencia.

En consecuencia, se determinó el siguiente formato:

Tabla 01: Formato de Definición del Alcance

<table>
<tr><td rowspan="2">INSERTAR LOGO DE LA INSTITUCIÓN</td><td colspan="3">FORMATO DE DEFINICIÓN DEL ALCANCE</td></tr>
<tr><td colspan="2">Código del Formato: CF N° _____</td><td>Fecha: ____/____/20___</td></tr>
<tr><td colspan="3">Fase: I - Definir el Alcance y Contexto de la Organización</td><td>Proceso: 1 - Definir el Alcance</td></tr>
<tr><td>Objetivos:</td><td colspan="3">- Definir el Alcance por medio de la identificación de los procesos críticos y áreas involucradas de la organización con el fin de ser considerados en el transcurso del proceso de gestión de riesgos de TI.
- Otros.</td></tr>
<tr><td>Personal Involucrado:</td><td colspan="3">- Alta gerencia.
- Otros.</td></tr>
<tr><td>Entradas:</td><td colspan="3">- Reglamento de Organización y Funciones (ROF).
- Manual de Organización y Funciones (MOF).
- Otros.</td></tr>
<tr><td colspan="4">Salidas:</td></tr>
<tr><td colspan="2">PROCESOS CRÍTICOS</td><td colspan="2">ÁREAS INVOLUCRADAS</td></tr>
<tr><td colspan="2">Recepción y entrega de medicamentos</td><td colspan="2">Almacén Especial de Medicamentos (AEM)</td></tr>
<tr><td colspan="2">Recepción y entrega de exámenes de laboratorio</td><td colspan="2">Laboratorio clínico</td></tr>
<tr><td colspan="2">Otros …</td><td colspan="2">Otros …</td></tr>
<tr><td colspan="3">Responsables</td><td>Firmas</td></tr>
<tr><td>Elaborado por:</td><td colspan="2">Alta gerencia</td><td></td></tr>
<tr><td>Revisado por:</td><td colspan="2">Equipo analista</td><td></td></tr>
<tr><td>Aprobado por:</td><td colspan="2">Equipo analista</td><td></td></tr>
</table>

Fuente: Elaboración propia

Proceso 2: Identificación del Contexto Interno y Externo

Según ISO 31000 [32, p. 18] es:

> … La gestión de los riesgos necesita proponer el entendimiento de los entornos internos y externos a través de los cuales la institución se desarrolla laboralmente, teniendo la necesidad de evidenciar el contexto en el que se llevará a cabo el proceso de gestión de los riesgos.

MAGERIT v3.0 – Libro I [22, p. 57] sugiere "Establecer el contexto interno donde se desarrollan las tareas de la institución relacionados con: políticas propias, acuerdos con los stakeholders y con sus managers"; y respecto al contexto externo expresa: "Se debe describir las características del entorno externo que impacta en la institución: social, político y cultural. Incorporando elementos locales e internacionales que interactúan con el contorno de trabajo de la empresa".

COBIT 5 para Riesgos [25, p. 64] define esta sección como "Las circunstancias que intervienen en el impacto o probabilidad de ocurrencia de los riesgos y sus escenarios, debiendo ser tomados en cuenta durante cada análisis de riesgos".

Identificación el Contexto Interno:

Después de analizar las diferentes propuestas por parte de las metodologías que determinan y definen el establecimiento del contexto interno para el proceso de gestión de riesgos de TI; se propone establecer los siguientes parámetros:

a) **Objetivos Estratégicos.-** Ayudan a proporcionar la dirección de cómo la organización pretende alcanzar o trasladarse hacia las metas desarrolladas a nivel estratégico en un determinado periodo de tiempo basándose en la misión, visión y valores de la organización.

Fuente: Plan Estratégico de la Organización.

b) **Política Interna.-** Responde a una serie de fundamentos establecidos y que es necesario que sean difundidos, comprendidos y aceptados por los trabajadores de la organización.

Fuente: Reglamento de Organización y Funciones (ROF) y Manual de Organización y Funciones (MOF).

c) **Cultura Organizacional.-** Es un grupo de percepciones, actitudes, tradiciones, hábitos, valores y formas de interacción entre los grupos existentes de la organización.

Fuente: Plan estratégico, misión, visión, valores, objetivos estratégicos, organigrama de la institución, ROF, MOF, etc.

d) **Infraestructura de Tecnología.-** Está conformada por el hardware y software sobre el que se asientan los diferentes servicios que la organización necesita tener en funcionamiento para poder llevar a cabo todas sus actividades por parte de la administración o gestión interna.

Fuente: Reporte de activos de información.

e) **Estructura Organizacional.-** Es la metodología a través de la cual la organización planifica su trabajo y reparte formalmente sus responsabilidades, por ende, todos los usuarios tienen una responsabilidad que deben asumir aportando todas sus habilidades, para trabajar en conjunto de la mejor manera posible, logrando así el cumplimiento de los objetivos establecidos en la planificación.

Fuente: Organigrama institucional.

Una vez definidos los parámetros del contexto interno que serán considerados como parte de la institución, se asumirán una serie de pasos con el propósito de identificar el Contexto interno de la organización:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. Identificar los parámetros del contexto interno que influyen en el impacto de la organización para cumplir con los objetivos estratégicos.
    1.2. Tomar en consideración los parámetros identificados para la revisión periódica del proceso de gestión de riesgos de TI.
    1.3. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que conforman el Contexto Interno de la organización:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de Recursos Humanos.
    2.4. Jefe de Asesoría Legal.
    2.5. Jefe de Patrimonio.
    2.6. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

    3.1. Plan Estratégico de la organización.
    3.2. Reglamento de Organización y Funciones (ROF).
    3.3. Manual de Organización y Funciones (MOF).
    3.4. Misión, Visión, Valores y Objetivos Estratégicos.
    3.5. Organigrama de la institución.
    3.6. Reporte de activos de información.
    3.7. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

    4.1. Analizar a detalle el Plan Estratégico de la Organización para aclarar cuáles son los Objetivos Estratégicos de la organización.
    4.2. Analizar a detalle el ROF y el MOF para difundir entre los trabajadores cuales son los estatutos que se rigen por norma dentro de la organización y que estos sean comprendidos y aceptados por el personal como parte de la política interna.
    4.3. Analizar a detalle el Plan Estratégico, ROF, MOF y el Organigrama institucional para establecer un conjunto de hábitos y actitudes que formaran parte de la Cultura Organizacional.
    4.4. Analizar a detalle el reporte de activos de información para determinar en qué activos se llevan a cabo los procesos indispensables para que la organización ejecute con normalidad todas sus funciones.
    4.5. Analizar a detalle el Organigrama institucional para distribuir formalmente las distintas responsabilidades y funciones que el personal deberá asumir.
    4.6. Definir por quién será elaborado el formato y colocar su firma respectiva.
    4.7. Definir por quién será revisado el formato y colocar su firma respectiva.
    4.8. Definir por quién será aprobado el formato y colocar su firma respectiva.
    4.9. Llenar la información obtenida en el formato de Identificación del Contexto Interno (**Tabla 02**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

    5.1. Lista de parámetros que definirán el contexto interno.

En consecuencia, se determinó el siguiente formato:

Tabla 02: Formato de Identificación del Contexto Interno

INSERTAR LOGO DE LA INSTITUCIÓN	**FORMATO DE IDENTIFICACIÓN DEL CONTEXTO INTERNO**	
	Código del Formato: CF N° _____	**Fecha: ____/____/20___**
Fase: I - Definir el Alcance y Contexto de la Organización		**Proceso: 2 - Identificación del Contexto Interno y Externo**
Objetivos:	- Identificar los parámetros del contexto interno que influyen en el impacto de la organización para cumplir con los objetivos estratégicos. - Otros.	
Personal Involucrado:	- Alta gerencia - Otros.	
Entradas:	- Plan Estratégico de la organización, - Reglamento de Organización y Funciones (ROF). - Otros.	
Salidas:		
PARÁMETROS	**DESCRIPCIÓN**	
Objetivos Estratégicos	Ayudan a proporcionar la dirección de cómo la organización pretende alcanzar o trasladarse hacia las metas desarrolladas a nivel estratégico en un determinado periodo de tiempo basándose en la misión, visión y valores de la organización.	
Cultura Organizacional	Es el conjunto de percepciones, actitudes, tradiciones, hábitos, valores y formas de interacción entre los grupos existentes de la organización.	
Otros …	**Otros …**	
Responsables		**Firmas**
Elaborado por:	Alta gerencia	
Revisado por:	Equipo analista	
Aprobado por:	Equipo analista	

Fuente: Elaboración propia

Identificación el Contexto Externo:

Después de analizar las diferentes propuestas por parte de las metodologías que determinan y definen el establecimiento del contexto externo para el proceso de gestión de riesgos de TI; se propone establecer los siguientes parámetros:

a) **Económico.-** Es el conjunto de elementos financieros vinculados con los porcentajes financieros, la devaluación, la inflación, las diversas políticas monetarias a nivel nacional etc. que perjudican al país económicamente y como resultado impactan en las decisiones comerciales, de producción, logística, etc. en las organizaciones del sector salud.

   Entidades integran el entorno económico: Banco Central de Reserva del Perú (BCRP), Banco de la Nación (BN), Rimac Seguros, Caja Trujillo, Caja Piura, Cooperativa El Tumi, etc.

b) **Socio-Culturales.-** Es la agrupación de variables que involucran cambios en el entorno demográfico, cultural y social de la población, vinculado a los grupos de interés como densidad de la población asignada al hospital, tasa de natalidad, mortalidad y morbilidad, etc.

   Fuente: Información estadística INEI, censos, evolución de la pirámide poblacional, reportes de Gobiernos Regionales y Redes de Salud, valores sociales, morales y éticos, etc.

c) **Tecnológicos.-** Es la agrupación de los adelantos o novedades en la tecnología que la organización adquiere con el fin de distinguirse entre los adversarios. Su trascendencia es observada mediante los servicios, productos, equipos y artículos que cooperan en el crecimiento de la productividad en la empresa, y demás recursos.

   Fuente: Reporte de activos de información, políticas establecidas por TI.

d) **Políticos.-** Es el escenario de la organización que se relaciona con un entorno económico y social. Establecido por un conjunto de instrumentos, normas y entidades del gobierno que repercuten en la productividad, operatividad y factibilidad de las organizaciones del sector salud.

El contexto político está conformado por las siguientes organizaciones: Constitución Política del Perú, Gobiernos Regionales y Redes de Salud, etc.

e) **Legales.-** Constituido por organismos y reglamentos que limitan y regularizan el método de trabajo en las instituciones sanitarias, perjudicando de forma negativa o positivamente en los procedimientos clave, comprometiendo a la organización.

El contexto legal está conformado por las siguientes organizaciones: Ministerio de Salud (MINSA), Superintendencia Nacional de Salud (SUSALUD), Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI), Instituto Nacional de Defensa Civil (INDECI), Superintendencia Nacional de Registros Públicos (SUNARP), Ministerio de Economía y Finanzas (MEF), etc.

f) **Medioambientales.-** Son las descripciones propias de la región Amazonas donde las organizaciones del sector salud ejercen sus funciones, pudiendo perjudicar de forma positiva o negativa en sus procesos. Entre los elementos que debemos tener en cuenta, se encuentra la temperatura, la humedad, el clima, etc.

Fenómenos climatológicos que se deben considerar: Tormentas eléctricas, lluvias torrenciales, inundaciones, sequías, etc.

g) **Competitivo.-** Constituido por un conjunto de organizaciones que ejercen en el mismo sector laboral, utilizando otros métodos para cubrir requerimientos similares a través de servicios, productos y procedimientos diversos. Los datos sobre las instituciones de la competencia posibilitará que la organización pueda analizar y optimizar los servicios que se brindan en el día a día.

Los datos relevantes de las instituciones del ámbito competitivo, está compuesto por: Sus servicios brindados, su tecnología, calidad de sus productos, etc.

h) Proveedores.- Es el conjunto de empresas o personas que nos abastecen o suministran profesionalmente con bienes o servicios necesarios para el correcto funcionamiento del negocio.

Las entidades que forman parte de este entorno son: proveedor del servicio de internet, agua, luz, droguerías, proveedores de mantenimiento de equipos médicos e informáticos, etc.

Una vez definidos los parámetros que serán considerados como parte del contexto externo de la organización, se asumirán una serie de pasos con el propósito de identificar el Contexto externo de la organización:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. Identificar los parámetros del contexto externo que influyen en el impacto de la organización para cumplir con los objetivos estratégicos.
    1.2. Tomar en consideración los parámetros identificados para la revisión periódica del proceso de gestión de riesgos de TI.
    1.3. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que conforman el Contexto Externo de la organización:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de Recursos Humanos.
    2.4. Jefe de Asesoría Legal.

2.5. Jefe de Contabilidad.
2.6. Jefe de TI.
2.7. Jefe de Estadística.
2.8. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

3.1. Lista de entidades que forman parte del entorno económico.
3.2. Reportes estadísticos de los diferentes factores socio-culturales.
3.3. Reporte de activos de información que forma parte del entorno tecnológico y las Políticas internas impuestas por TI, respecto a las diferentes tecnologías que se manejan en la organización.
3.4. Lista de instituciones que conforman el contexto político.
3.5. Lista de entidades que forman parte del entorno legal.
3.6. Reporte de Senamhi de los diferentes fenómenos climatológicos en la región Amazonas.
3.7. Lista de instituciones que brindan servicios similares a los de la organización.
3.8. Lista de proveedores que ofrecen servicios a la organización.
3.9. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

4.1. Analizar a detalle la lista de entidades que forman parte del entorno económico para determinar el impacto en las decisiones comerciales y de logística de la organización.
4.2. Analizar a detalle los reportes de los factores socio-culturales para determinar cuáles son los grupos de interés en la población asignada al hospital.

4.3. Analizar a detalle el reporte de activos de información y las políticas internas impuestas por TI para rescatar las ventajas tecnológicas de la organización frente a la competencia.

4.4. Analizar a detalle la lista de instituciones que conforman el contexto político e influyen en la operatividad de la organización.

4.5. Analizar a detalle la lista de organizaciones que conforman el contexto legal para que la organización pueda cumplir con todos los requisitos y normativas impuestas por los diferentes entes reguladores del estado.

4.6. Analizar a detalle los distintos reportes brindados por Senamhi para estudiar los diversos fenómenos climatológicos que se producen en la región Amazonas y que de algún modo pueden perjudicar la operatividad de la organización.

4.7. Analizar a detalle la lista de instituciones que brindan servicios similares a los de la organización para estudiar el método de trabajo que tiene la competencia.

4.8. Analizar a detalle la lista de proveedores que ofrecen servicios a la organización para asegurar el abastecimiento adecuado de las necesidades que tiene la organización.

4.9. Definir por quién será elaborado el formato y colocar su firma respectiva.

4.10. Definir por quién será revisado el formato y colocar su firma respectiva.

4.11. Definir por quién será aprobado el formato y colocar su firma respectiva.

4.12. Llenar la información obtenida en el formato de Identificación del Contexto Externo (**Tabla 03**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de parámetros que definirán el contexto externo.

En consecuencia, se determinó el siguiente formato:

Tabla 03: Formato de Identificación del Contexto Externo

INSERTAR LOGO DE LA INSTITUCIÓN	**FORMATO DE IDENTIFICACIÓN DEL CONTEXTO EXTERNO**	
	Código del Formato: CF N° _____	**Fecha: ____/____/20___**
Fase: I - Definir el Alcance y Contexto de la Organización		**Proceso: 2 - Identificación del Contexto Interno y Externo**
Objetivos:	- Identificar los parámetros del contexto externo que influyen en el impacto de la organización para cumplir con los objetivos estratégicos. - Otros.	
Personal Involucrado:	- Alta gerencia. - Otros.	
Entradas:	- Lista de entidades que forman parte del entorno económico. - Otros.	
Salidas:		
PARÁMETROS	**ENTIDADES/ACTIVIDADES QUE FORMAN PARTE DEL PARÁMETRO**	
Económico	Banco de la Nación (BN), Banco Central de Reserva del Perú (BCRP), Rimac Seguros, Caja Trujillo, Caja Piura, Cooperativa El Tumi, etc.	
Socio-Culturales	Información estadística INEI, censos, evolución de la pirámide poblacional, reportes de Gobiernos Regionales y Redes de Salud, valores sociales, morales y éticos, etc.	
Otros …	**Otros …**	
Responsables		**Firmas**
Elaborado por:	Alta gerencia	
Revisado por:	Equipo analista	
Aprobado por:	Equipo analista	

Fuente: Elaboración propia

Fase II: Identificación de Activos

Para la ISO 27005 [33, p. 14]:

> … El activo es cualquier cosa que proporcione valor en las instituciones por lo que es de vital importancia que sean resguardados; por ende la identificación de activos debe realizarse especificando todos los detalles posibles, generando información indispensable para la evaluación de riesgos.

MAGERIT v3.0 - Libro I [22, p. 87] enfatiza que:

> … Lo primordial es la información que se trabaja y se vincula con los procesos; por lo que se tomará importancia solo aquellos procedimientos en los sistemas que sean considerados elementales y que son de valor para la empresa; ya sea por su misma estructura o porque a través de ellos de ejecutan operaciones críticas.

OCTAVE [28, p. 18] sugiere el desarrollo de un perfil de activos a través de una hoja de trabajo describiendo las características, calidades y el valor de cada activo de información.

COBIT 5 para Riesgos [25, p. 67], define un activo como: "un objeto valioso y fundamental de las organizaciones que al ser impactados por ciertos imprevistos dan cabida a que los procesos del negocio se vean afectados".

Después de analizar las diferentes propuestas por parte de las metodologías que determinan la identificación de activos; se concluye que esta fase tiene la finalidad de identificar, clasificar y valorar los activos que interactúan en los procesos de las operaciones fundamentales de la organización y es indispensable incorporarlos en el proceso de gestión del riesgo de TI con la finalidad de salvaguardados apropiadamente.

Proceso 3: Identificación y Clasificación de Activos

Los activos vienen siendo los componentes de valor o recursos del sistema de información indispensable para el desarrollo de las actividades diarias, por lo cual deben ser protegidos ante cualquier ataque o daño que ponga en peligro la integridad tanto del activo como de la organización. Los activos suelen estar conformados por elementos de hardware, software, recurso humano y hasta áreas físicas.

En el **ANEXO Nº 06** se expone el catálogo de los diferentes tipos activos que establece MAGERIT v3.0 - Libro II [38, pp. 7 - 13], dicho catálogo sirve de orientación para clasificar los activos que son críticos dentro la organización.

Finalmente, se asumirán una serie de pasos con la finalidad de identificar y clasificar los activos de la organización:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. La alta gerencia debe identificar los activos críticos para la institución; aquellos que al ser afectados generan un impacto negativo en la prestación de sus servicios o el desarrollo de sus actividades.
    1.2. Clasificar los activos identificados respecto al catálogo de tipos de activos ofrecido por MAGERIT.
    1.3. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que identificarán los activos críticos para la institución:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de TI.
    2.4. Responsables de los procesos críticos.
    2.5. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

    3.1. Reporte de activos de información.
    3.2. Manual de Organización y Funciones (MOF).
    3.3. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

4.1. Analizar a detalle el reporte de activos de información y la inclusión de estos activos en el MOF con el propósito de establecer cuáles son críticos para la institución.
4.2. Asignar un código identificador a cada activo.
4.3. Clasificar el activo respecto al catálogo de tipos de activos sugeridos por MAGERIT (**ANEXO N° 06**).
4.4. Detallar el nombre completo del activo.
4.5. Describir las especificaciones del activo.
4.6. Definir por quién será elaborado el formato y colocar su firma respectiva.
4.7. Definir por quién será revisado el formato y colocar su firma respectiva.
4.8. Definir por quién será aprobado el formato y colocar su firma respectiva.
4.9. Completar los datos obtenidos en el formato de Identificación y Clasificación de Activos (**Tabla 04**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de los activos críticos identificados y clasificados según el catálogo sugerido.

En consecuencia, se determinó el siguiente formato:

Tabla 04: Formato de Identificación y Clasificación de Activos

<table>
<tr><td rowspan="2">INSERTAR LOGO DE LA INSTITUCIÓN</td><td colspan="3">FORMATO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS</td></tr>
<tr><td colspan="2">Código del Formato: CF N° _____</td><td>Fecha: ____/____/20___</td></tr>
<tr><td colspan="3">Fase: II – Identificación de Activos</td><td>Proceso: 3 - Identificación y Clasificación de Activos</td></tr>
<tr><td colspan="2">Objetivos:</td><td colspan="2">- Clasificar los activos identificados respecto al catálogo de tipos de activos ofrecido por MAGERIT.
- Otros.</td></tr>
<tr><td colspan="2">Personal Involucrado:</td><td colspan="2">- Alta gerencia.
- Otros.</td></tr>
<tr><td colspan="2">Entradas:</td><td colspan="2">- Reporte de activos de información.
- Otros.</td></tr>
<tr><td colspan="4">Salidas:</td></tr>
<tr><td>CÓDIGO</td><td>CLASIFICACIÓN</td><td>ACTIVO</td><td>DESCRIPCIÓN</td></tr>
<tr><td>D - RPD</td><td>[backup]</td><td>Copias de respaldo</td><td>Ficheros de copias de respaldo de los distintos sistemas y aplicaciones.</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td></tr>
<tr><td colspan="3">Responsables</td><td>Firmas</td></tr>
<tr><td colspan="2">Elaborado por:</td><td>Alta gerencia</td><td></td></tr>
<tr><td colspan="2">Revisado por:</td><td>Equipo analista</td><td></td></tr>
<tr><td colspan="2">Aprobado por:</td><td>Equipo analista</td><td></td></tr>
</table>

Fuente: Elaboración propia

Proceso 4: Valoración de Activos

Para la ISO 27005 [33, p. 38] "El siguiente paso después de la identificación del activo es acordar la escala que se utilizará y los criterios para asignar una ubicación particular en esa escala a cada activo, en función de la valoración".

MAGERIT v3.0 – Libro I [22, p. 24] propone que "el proceso de valoración se puede tomar desde el punto o la necesidad de salvaguardar los activos más importantes, mientras el grado de protección sea más elevado, se necesitara evaluar mejor las dimensiones de valoración con el propósito de estas dimensiones sean las más pertinentes".

Después de analizar las propuestas por parte de las metodologías que determinan la valoración de activos, se establecerán 2 procesos; respecto a las dimensiones y respecto al impacto:

a) **Respecto a las Dimensiones de Valoración y Escalas Estándar.-** Se determinará la valoración de los activos de la organización respecto a las dimensiones de valoración y escalas estándar que establece MAGERIT:

Tabla 05: Dimensiones de Valoración

DIMENSIÓN DE VALORACIÓN	NOMENCLATURA	DEFINICIÓN
Disponibilidad	[D]	Esta dimensión hace referencia a la accesibilidad que tienen las organizaciones o personas sobre los activos en el momento o circunstancia que se requiera o necesite.
Integridad	[I]	Esta dimensión hace referencia a la condición de aquellos activos que no han sido manipulados deliberadamente.
Confidencialidad	[C]	Esta dimensión hace referencia a la privacidad y accesibilidad que tienen los activos hacia las organizaciones o personas no acreditadas.
Autenticidad	[A]	Esta dimensión hace referencia a la condición de los activos donde demuestran que son legítimos, corroborando que su procedencia está verificada.
Trazabilidad	[T]	Esta dimensión hace referencia a una secuencia de métodos o pasos que posibilitan el seguimiento del desarrollo de los activos en cada fase o proceso.

Fuente: MAGERIT v3.0 – Libro II [38, pp. 15, 16]

Escalas Estándar: En el **ANEXO N° 07** se exponen las escalas estándar propuestas por MAGERIT v3.0 – Libro II [38, pp. 19 - 22], dichas escalas tienen el propósito de valorizar los activos en base a las dimensiones de valoración.

En consecuencia, se asumirán una serie de pasos con el propósito de valorar los activos críticos de la organización respecto a las dimensiones de valoración:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. La alta gerencia debe valorar (respecto a las Dimensiones de Valoración (**Tabla 05**) y Escalas Estándar (**ANEXO N° 07**)) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos (**Tabla 04**) con el propósito de medir los efectos de una amenaza cuando se materializa.
    1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que realizarán la valoración de los activos críticos respecto a las dimensiones de valoración:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de TI.
    2.4. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

    3.1. Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
    3.2. Dimensiones de Valoración (**Tabla 05**).
    3.3. Escalas Estándar (**ANEXO N° 07**).
    3.4. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

4.1. Revisar el Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
4.2. Completar el código identificador de cada activo, asignado en el Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
4.3. Completar el nombre del activo relacionado con el código identificador (**Tabla 04**).
4.4. Asignar el valor correspondiente en las diferentes Dimensiones de Valoración usando como guía las Escalas Estándar (**ANEXO N° 07**).
4.5. Definir por quién será elaborado el formato y colocar su firma respectiva.
4.6. Definir por quién será revisado el formato y colocar su firma respectiva.
4.7. Definir por quién será aprobado el formato y colocar su firma respectiva.
4.8. Completar los datos obtenidos en el formato de Valoración de Activos respecto a las Dimensiones de Valoración (**Tabla 06**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de los activos críticos valorados respecto a las Dimensiones de Valoración.

En consecuencia, se determinó el siguiente formato:

Tabla 06: Formato de Valoración de Activos respecto a las Dimensiones de Valoración

<table>
<tr><td colspan="2" rowspan="2">INSERTAR LOGO DE LA INSTITUCIÓN</td><td colspan="5">FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO A LAS DIMENSIONES DE VALORACIÓN</td></tr>
<tr><td colspan="4">Código del Formato: CF N° _____</td><td>Fecha: ____/____/20___</td></tr>
<tr><td colspan="5">Fase: II – Identificación de Activos</td><td>Proceso: 4 - Valoración de Activos</td></tr>
<tr><td colspan="2">Objetivos:</td><td colspan="4">- La alta gerencia debe valorar (respecto a las Dimensiones de Valoración y Escalas Estándar) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos con el propósito de medir los efectos de una amenaza cuando se materializa.
- Otros.</td></tr>
<tr><td colspan="2">Personal Involucrado:</td><td colspan="4">- Alta gerencia.
- Otros.</td></tr>
<tr><td colspan="2">Entradas:</td><td colspan="4">- Dimensiones de Valoración.
- Otros.</td></tr>
<tr><td colspan="6">Salidas:</td></tr>
<tr><td rowspan="2">CÓDIGO</td><td rowspan="2">ACTIVO</td><td colspan="4">DIMENSIONES DE VALORACIÓN</td></tr>
<tr><td>DISPONIBILIDAD [D]</td><td>INTEGRIDAD [I]</td><td>CONFIDENCIALIDAD [C]</td><td>AUTENTICIDAD [A]</td><td>TRAZABILIDAD [T]</td></tr>
<tr><td>D - RPD</td><td>Copias de Respaldo</td><td>5</td><td></td><td>5</td><td></td><td></td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td></tr>
<tr><td colspan="3">Responsables</td><td colspan="3">Firmas</td></tr>
<tr><td colspan="2">Elaborado por:</td><td colspan="2">Alta gerencia</td><td colspan="2"></td></tr>
<tr><td colspan="2">Revisado por:</td><td colspan="2">Equipo analista</td><td colspan="2"></td></tr>
<tr><td colspan="2">Aprobado por:</td><td colspan="2">Equipo analista</td><td colspan="2"></td></tr>
</table>

Fuente: Elaboración propia

Continuando con la Valoración de los Activos, se asumirá una secuencia de pasos con el propósito de valorar los activos críticos de la organización respecto a las escalas estándar:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. La alta gerencia debe valorar (respecto a las Dimensiones de Valoración (**Tabla 05**) y Escalas Estándar (**ANEXO N° 07**)) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos (**Tabla 04**) con el propósito de medir los efectos de una amenaza cuando se materializa.
    1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que realizarán la valoración de los activos críticos respecto a las escalas estándar:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de TI.
    2.4. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

    3.1. Dimensiones de Valoración (**Tabla 05**).
    3.2. Escalas Estándar (**ANEXO N° 07**).
    3.3. Formato de Valoración de Activos respecto a las Dimensiones de Valoración (**Tabla 06**).
    3.4. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

    4.1. Revisar el Formato de Valoración de Activos respecto a las Dimensiones de Valoración (**Tabla 06**).
    4.2. Completar el código identificador de cada activo, asignado en el Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
    4.3. Asignar la nomenclatura de las dimensiones de valoración asignadas en el Formato de Valoración de Activos respecto a las Dimensiones de Valoración (**Tabla 06**).
    4.4. Describir el ítem asignado (de cada dimensión de valoración) según las escalas estándar (**ANEXO N° 07**).
    4.5. Definir por quién será elaborado el formato y colocar su firma respectiva.
    4.6. Definir por quién será revisado el formato y colocar su firma respectiva.
    4.7. Definir por quién será aprobado el formato y colocar su firma respectiva.
    4.8. Completar los datos obtenidos en el formato de Valoración de Activos respecto a Escalas Estándar (**Tabla 07**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

    5.1. Lista de los activos críticos valorados respecto a las Escalas Estándar.

    En consecuencia, se determinó el siguiente formato:

Tabla 07: Formato de Valoración de Activos respecto a las Escalas Estándar

<table>
<tr><td rowspan="2">INSERTAR LOGO DE LA INSTITUCIÓN</td><td colspan="3">FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO A LAS ESCALAS ESTÁNDAR</td></tr>
<tr><td colspan="2">Código del Formato: CF N° _____</td><td>Fecha: ____/____/20___</td></tr>
<tr><td colspan="3">Fase: II – Identificación de Activos</td><td>Proceso: 4 - Valoración de Activos</td></tr>
<tr><td>Objetivos:</td><td colspan="3">- La alta gerencia debe valorar (respecto a las Dimensiones de Valoración y Escalas Estándar) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos con el propósito de medir los efectos de una amenaza cuando se materializa.</td></tr>
<tr><td>Personal Involucrado:</td><td colspan="3">- Alta gerencia.
- Otros.</td></tr>
<tr><td>Entradas:</td><td colspan="3">- Dimensiones de Valoración.
- Otros.</td></tr>
<tr><td colspan="4">Salidas:</td></tr>
<tr><td>CÓDIGO</td><td>DIMENSIÓN DE SEGURIDAD</td><td colspan="2">DESCRIPCIÓN</td></tr>
<tr><td rowspan="2">D - RPD</td><td>[D]</td><td colspan="2">5.adm: Probablemente impediría la operación efectiva de más de una parte de la Organización.</td></tr>
<tr><td>[C]</td><td colspan="2">5.lg: Probablemente cause una pérdida en la confianza dentro de la Organización.</td></tr>
<tr><td>Otros …</td><td>Otros …</td><td colspan="2">Otros …</td></tr>
<tr><td colspan="2">Responsables</td><td colspan="2">Firmas</td></tr>
<tr><td>Elaborado por:</td><td colspan="2">Alta gerencia</td><td></td></tr>
<tr><td>Revisado por:</td><td colspan="2">Equipo analista</td><td></td></tr>
<tr><td>Aprobado por:</td><td colspan="2">Equipo analista</td><td></td></tr>
</table>

Fuente: Elaboración propia

b) Respecto al Impacto.- Para valorar los activos respecto al impacto en la organización, se usará como base al valor más alto asignado en los formatos de Valoración de Activos respecto a las Dimensiones de Valoración y Escalas Estándar (Consultar **Tabla 06** y **Tabla 07** respectivamente).

Tabla 08: Valoración de Activos respecto al Impacto

NOMENCLATURA	IMPACTO	VALOR	CRITERIO
MA	**MUY ALTO**	**10**	El impacto genera repercusiones muy altas en la institución que pueden ser irreparables.
A	**ALTO**	**7 - 9**	El impacto genera repercusiones perjudiciales en la institución.
M	**MEDIO**	**4 - 6**	El impacto genera repercusiones significativas en los procesos de la institución.
B	**BAJO**	**2 - 3**	El impacto genera repercusiones menores, sin embargo no perjudica a los procesos críticos de la institución.
MB	**MUY BAJO**	**1**	El impacto no genera repercusiones importantes en la institución.

Fuente: Elaboración propia

En consecuencia, se asumirán una serie de pasos con el propósito de valorar los activos críticos de la organización respecto al impacto:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

   1.1. La alta gerencia debe valorar (respecto al impacto) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos (**Tabla 04**) con el propósito de medir los efectos de una amenaza cuando se materializa.
   1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que realizarán la valoración de los activos respecto al impacto:

   2.1. Director de la organización.
   2.2. Administrador de la organización.
   2.3. Jefe de TI.
   2.4. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

    3.1. Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
    3.2. Formato de Valoración de Activos respecto a las Dimensiones de Valoración llenado (**Tabla 06**).
    3.3. Formato de Valoración de Activos respecto a las Escalas Estándar llenado (**Tabla 07**).
    3.4. Valoración de Activos respecto al Impacto (**Tabla 08**).
    3.5. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

    4.1. Revisar el Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
    4.2. Completar el código identificador de cada activo, asignado en el Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
    4.3. Completar el nombre del activo relacionado con el código identificador (**Tabla 04**).
    4.4. Seleccionar el valor más alto asignado en los formatos de Valoración de Activos respecto a las Dimensiones de Valoración y Escalas Estándar (Consultar **Tabla 06** y **Tabla 07** respectivamente)
    4.5. Asignar la nomenclatura correspondiente del impacto (**Tabla 08**) respecto al valor obtenido.
    4.6. Justificar la importancia del activo.
    4.7. Definir por quién será elaborado el formato y colocar su firma respectiva.
    4.8. Definir por quién será revisado el formato y colocar su firma respectiva.

4.9. Definir por quién será aprobado el formato y colocar su firma respectiva.

4.10. Completar los datos obtenidos en el formato de Valoración de Activos respecto al Impacto (**Tabla 09**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de los activos críticos valorados respecto al Impacto.

En consecuencia, se determinó el siguiente formato:

Tabla 09: Formato de Valoración de Activos respecto al Impacto

INSERTAR LOGO DE LA INSTITUCIÓN	**FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO AL IMPACTO**			
	Código del Formato: CF N° _____			**Fecha: ____/____/20___**
Fase: II – Identificación de Activos				**Proceso: 4 - Valoración de Activos**
Objetivos:	- La alta gerencia debe valorar (respecto al impacto) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos con el propósito de medir los efectos de una amenaza cuando se materializa.			
Personal Involucrado:	- Alta gerencia. - Otros.			
Entradas:	- Formato de Identificación y Clasificación de Activos llenado (Tabla 05). - Otros.			
Salidas:				
CÓDIGO	**ACTIVO**	**VALOR**	**IMPACTO**	**JUSTIFICACIÓN**
D - RPD	Copias de Respaldo	5	M	Las copias de respaldo son determinantes para la recuperación de archivos ante un desastre.
…	**…**	**…**	**…**	**…**
Otros …	**Otros …**	**Otros …**	**Otros …**	**Otros …**
Responsables				**Firmas**
Elaborado por:	Alta gerencia			
Revisado por:	Equipo analista			
Aprobado por:	Equipo analista			

Fuente: Elaboración propia

Fase III: Evaluación del Riesgo

La ISO 31000 [32, p. 19] define esta fase como: "el desarrollo general para identificar los riesgos, analizarlos y valorarlos".

Para la ISO 27005 [33, p. 13] "La evaluación de riesgos reconoce las vulnerabilidades y amenazas existentes (o probables), además de los controles establecidos y su efecto sobre el riesgo ya encontrado precisando los posibles impactos; por último, da prioridad a los riesgos identificados y los cataloga".

Para NIST 800-30 [34, p. 29],

> … El propósito de esta fase es elaborar una relación de riesgos que pueden priorizarse por nivel de riesgo y utilizarse para comunicar / las opciones de respuesta al riesgo. Con el fin de cumplir con este objetivo, las instituciones estudian las vulnerabilidades y amenazas, las probabilidades e impactos, y la incertidumbre relacionado con el proceso de evaluación de riesgos.

En esta fase, OCTAVE Allegro [28, pp. 17, 19 - 20] "establece los conductores de organización que se usaran con la finalidad de medir los efectos de un riesgo; identificando escenarios de amenazas además de identificar y analizar riesgos".

COBIT 5 para Riesgos divide esta fase en 3 etapas:

- Identificar el riesgo.- "Integra el conjunto de procesos o practicas aplicadas en la gestión, cuyo fin permite identificar aquellos riesgos y amenazas que se encuentren relacionados con los servicios y/o productos significativos de la institución, los cuales dependan de TI" [25, p. 93].
- Analizar del riesgo.- "Conjunto de pasos o procesos donde se valora el impacto y la frecuencia de los escenarios de riesgo de TI" [25, p. 93].
- Valorar el riesgo.- "Evalúa los riesgos respecto a la tolerancia de riesgo y al apetito de riesgo; además utiliza un mapa de riesgos para priorizar y mostrar gráficamente los riesgos por rangos de frecuencia e impacto" [25, p. 96].

En conclusión, la evaluación del riesgo, es el procedimiento para entender la esencia del riesgo diagnosticando su magnitud, preparándolo como base para las opciones de tratamiento de riesgo; no sin antes calcular previamente la identificación y valoración de las amenazas y oportunidades.

Proceso 5: Identificación y Valoración de Amenazas

a) Identificación de Amenazas: Las causas potenciales que afectan directamente a los activos, son originados por las amenazas; estas llegan a provocar perjuicios en una institución o en un sistema de información. Para poder identificar las amenazas, usaremos como referencia el catálogo establecido por MAGERIT v3.0, donde propone tipos de amenazas posibles, en los que se ven involucrados los activos.

Tabla 10: Catálogo de Amenazas posibles sobre los Activos

NOMENCLATURA	TIPO DE AMENAZA	CRITERIO
[N]	**De Origen Natural**	Son aquellos acontecimientos originados por la naturaleza y suelen manifestarse sin que la intervención humana sea participe o causante de dicha manifestación.
[I]	**De Origen Industrial**	Son los acontecimientos originados industrialmente con intervención de la mano del hombre; dichos sucesos pueden ser provocados intencionalmente o de manera imprevista.
[E]	**Errores y Fallos No Intencionados**	Son aquellos acontecimientos provocados involuntariamente, donde el causal suele provenir mediante la intervención humana.
[A]	**Ataques Intencionados**	Son los acontecimientos provocados deliberadamente o mal intencionados, donde el causal suele originarse mediante la intervención humana.

Fuente: MAGERIT v3.0 – Libro II [38, pp. 25 - 47]

b) Valoración de Amenazas: El primer paso para poder valorar las amenazas es determinar la frecuencia de ocurrencia (o probabilidad) de que una amenaza puede materializarse.

Se asumirán una serie de pasos con el propósito de establecer las frecuencias (o probabilidades), los rangos y el valor de las ocurrencias de los distintos tipos de amenazas:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. La alta gerencia debe definir las frecuencias (o probabilidades), los rangos y el valor de ocurrencias de las amenazas que acontecen en la organización.
    1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que serán los encargados de establecer las frecuencias (o probabilidades), los rangos y los valores según las manifestaciones de amenazas que se hayan presentado en la organización:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de TI.
    2.4. Responsables de los procesos críticos.
    2.5. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

    3.1. Registro de amenazas que se hayan manifestado en la organización.
    3.2. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

4.1. Establecer una lista de frecuencias (o probabilidades) de ocurrencia de las posibles materializaciones de amenazas con un mínimo y un máximo.
4.2. Establecer el periodo de tiempo por cada tipo de frecuencias (o probabilidad) establecidas en el paso anterior.
4.3. Establecer los valores por cada tipo de frecuencia (o probabilidad) establecida en el primer paso.
4.4. Definir por quién será elaborado el formato y colocar su firma respectiva.
4.5. Definir por quién será revisado el formato y colocar su firma respectiva.
4.6. Definir por quién será aprobado el formato y colocar su firma respectiva.
4.7. Completar los datos obtenidos en el formato de Frecuencias (o Probabilidad) de ocurrencias de las Amenazas (**Tabla 11**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de frecuencia (o probabilidad) de ocurrencias de las amenazas.

En consecuencia, se determinó el siguiente formato:

Tabla 11: Formato de Frecuencia o Probabilidad de ocurrencia de las Amenazas

INSERTAR LOGO DE LA INSTITUCIÓN	**FORMATO DE FRECUENCIA O PROBABILIDAD DE OCURRENCIA DE LAS AMENAZAS**	
	Código del Formato: CF N° _____	**Fecha: ____/____/20___**
Fase: III – Evaluación del Riesgo		**Proceso: 5 – Identificación y Valoración de Amenazas**
Objetivos:	- La alta gerencia debe definir las frecuencias, los rangos y el valor de ocurrencias de las amenazas que acontecen en la organización. - Otros.	
Personal Involucrado:	- Alta gerencia. - Otros.	
Entradas:	- Registro de amenazas que se hayan manifestado en la organización. - Otros.	
Salidas:		

FRECUENCIA O PROBABILIDAD	**PERIODO**	**VALOR**
Probabilidad muy elevada	Interdiario	1000
Probabilidad media	Quincenal	500
Otros …	**Otros …**	**Otros …**

Responsables		**Firmas**
Elaborado por:	Alta gerencia	
Revisado por:	Equipo analista	
Aprobado por:	Equipo analista	

Fuente: Elaboración propia

Por otro lado, se puede tomar como sugerencia la siguiente tabla de frecuencias (o probabilidades) y adaptarla en base a los incidentes suscitados en la organización:

Tabla 12: Frecuencia o Probabilidad de ocurrencia de las Amenazas (sugerido)

FRECUENCIA O PROBABILIDAD	**PERIODO**	**VALOR**
MA - Probabilidad muy alta	Diaria (todos los días)	5
A - Probabilidad alta	Semanal (todas las semanas)	4
M - Probabilidad media	Mensual (cada 2 meses)	3
B - Probabilidad baja	Semestral (cada 6 meses)	2
MB - Probabilidad muy baja	Anual (todos los años)	1

Fuente: MAGERIT v3.0 – Libro I [22, p. 28]

Una vez establecidas las probabilidades con sus respectivos periodos y valores; se asumirán una serie de pasos con el propósito de identificar y valorar aquellas amenazas que repercuten sobre los activos críticos de la institución:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. La alta gerencia debe identificar cuáles son los distintos tipos de amenazas que se efectúan sobre los activos críticos y determinar la probabilidad con la que se reiteran estas amenazas.
    1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que serán los encargados de realizar la identificación y valoración de amenazas sobre los activos:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de TI.
    2.4. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

    3.1. Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
    3.2. Catálogo de Amenazas posibles sobre los activos (**Tabla 10**).
    3.3. Formato de Frecuencia o Probabilidad de ocurrencia de las Amenazas llenado (**Tabla 11**).
    3.4. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimiento.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

4.1. Revisar el Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
4.2. Completar el código identificador de cada activo, asignado en el Formato de Identificación y Clasificación de Activos llenado (**Tabla 04**).
4.3. Completar el nombre del activo relacionado con el código identificador (**Tabla 04**).
4.4. Identificar cuáles son las amenazas (en base a la **Tabla 10**) que impactan sobre los activos críticos de la organización.
4.5. Asignar la frecuencia o probabilidad de ocurrencia de cada amenaza (**Tabla 11**) sobre los activos críticos completados en el Procedimiento 2 y 3.
4.6. Asignar el valor correspondiente por cada frecuencia o probabilidad de ocurrencia asignada a cada activo (**Tabla 11**).
4.7. Definir por quién será elaborado el formato y colocar su firma respectiva.
4.8. Definir por quién será revisado el formato y colocar su firma respectiva.
4.9. Definir por quién será aprobado el formato y colocar su firma respectiva.
4.10. Completar los datos obtenidos en el formato de Identificación y Valoración de Amenazas (**Tabla 13**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de amenazas identificadas sobre cada activo, con su respectiva frecuencia (o probabilidad de ocurrencia) y oportunidades disponibles.

En consecuencia, se determinó el siguiente formato:

Tabla 13: Formato de Identificación y Valoración de Amenazas

<table>
<tr><td colspan="2" rowspan="2">INSERTAR LOGO DE LA INSTITUCIÓN</td><td colspan="4">FORMATO DE IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS</td></tr>
<tr><td colspan="2">Código del Formato: CF N° _____</td><td colspan="2">Fecha: ____/____/20___</td></tr>
<tr><td colspan="4">Fase: III – Evaluación del Riesgo</td><td colspan="2">Proceso: 5 – Identificación y Valoración de Amenazas</td></tr>
<tr><td colspan="2">Objetivos:</td><td colspan="4">- La alta gerencia debe identificar cuáles son los distintos tipos de amenazas que se efectúan sobre los activos críticos y determinar la probabilidad con la que se reiteran estas amenazas.</td></tr>
<tr><td colspan="2">Personal Involucrado:</td><td colspan="4">- Alta gerencia.
- Otros.</td></tr>
<tr><td colspan="2">Entradas:</td><td colspan="4">- Catálogo de Amenazas sobre los activos.
- Otros.</td></tr>
<tr><td colspan="6">Salidas:</td></tr>
<tr><td>CÓDIGO</td><td>ACTIVO</td><td colspan="2">TIPO DE AMENAZA</td><td>FRECUENCIA O PROBABILIDAD</td><td>VALOR</td></tr>
<tr><td rowspan="2">D - RPD</td><td rowspan="2">Copias de Respaldo</td><td colspan="2">[E.2] Errores del administrador</td><td>MB</td><td>1</td></tr>
<tr><td colspan="2">[A.15] Modificación deliberada de la información</td><td>B</td><td>2</td></tr>
<tr><td rowspan="2">Otros …</td><td rowspan="2">Otros …</td><td colspan="2">Otros …</td><td>Otros …</td><td>Otros …</td></tr>
<tr><td colspan="2">Otros …</td><td>Otros …</td><td>Otros …</td></tr>
<tr><td colspan="3">Responsables</td><td colspan="3">Firmas</td></tr>
<tr><td colspan="2">Elaborado por:</td><td>Alta gerencia</td><td colspan="3"></td></tr>
<tr><td colspan="2">Revisado por:</td><td>Equipo analista</td><td colspan="3"></td></tr>
<tr><td colspan="2">Aprobado por:</td><td>Equipo analista</td><td colspan="3"></td></tr>
</table>

Fuente: Elaboración propia

Proceso 6: Identificación, Análisis y Valoración del Riesgo

a) Identificación y Análisis del Riesgo.- Con el fin de estimar el riesgo emplearemos la siguiente formula:

RIESGO = PROBABILIDAD x IMPACTO

Para ello, usaremos como cimiento los valores obtenidos en el análisis respecto al "impacto" de cada activo (**Tabla 09**) y los valores de la

"probabilidad" obtenidos en la identificación y valoración de amenazas (**Tabla 13**).

Teniendo claro que valores usaremos para calcular el riesgo, nos basaremos en la siguiente tabla para poder estimar el riesgo:

Tabla 14: Estimación del Riesgo

RIESGO		PROBABILIDAD				
		MB	**B**	**M**	**A**	**MA**
IMPACTO	**MA**	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: MAGERIT v3.0 – Libro III [39, p. 7]

Ahora que ya se cuenta con los valores de Probabilidad (**Tabla 13**) e Impacto (**Tabla 09**), se asumirán una serie de pasos con el propósito de calcular el nivel del riesgo:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. La alta gerencia debe identificar los niveles del riesgo que puede sufrir cada activo crítico de la organización.
    1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que serán los encargados de calcular el nivel del riesgo:

    2.1. Director de la organización.
    2.2. Administrador de la organización.

2.3. Jefe de TI.
2.4. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

3.1. Formato de Valoración de Activos respecto al Impacto llenado (**Tabla 09**).
3.2. Frecuencia o Probabilidad de ocurrencia de las Amenazas sugerido (**Tabla 12**).
3.3. Formato de Identificación y Valoración de Amenazas llenado (**Tabla 13**).
3.4. Estimación del Riesgo (**Tabla 14**).
3.5. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para lograr los objetivos establecidos:

4.1. Revisar el Formato de Valoración de Activos respecto al Impacto para obtener el impacto por cada activo crítico.
4.2. Revisar el Formato de Identificación y Valoración de Amenazas para obtener la Probabilidad por cada activo crítico.
4.3. Completar el código identificador de cada activo, asignado en el Formato de Valoración de Activos respecto al Impacto llenado (**Tabla 09**).
4.4. Completar el nombre del activo relacionado con el código identificador (**Tabla 09**).
4.5. Completar el Impacto asignado a cada activo crítico (**Tabla 09**).
4.6. Completar la Probabilidad asignada a cada activo crítico (**Tabla 13**).
4.7. Completar la nomenclatura de los diferentes tipos de Amenazas asignadas a cada activo crítico (**Tabla 13**).
4.8. Asignar un ID para el riego, anteponiendo “R -” al código identificador de cada activo.

4.9. Se determina el Riesgo respecto a la Probabilidad y el Impacto de cada activo crítico usando como guía la Estimación del Riesgo (**Tabla 14**).

4.10. Asignar un valor para cada riesgo calculado (se sugiere usar los valores de la **Tabla 12**).

4.11. Definir por quién será elaborado el formato y colocar su firma respectiva.

4.12. Definir por quién será revisado el formato y colocar su firma respectiva.

4.13. Definir por quién será aprobado el formato y colocar su firma respectiva.

4.14. Completar los datos obtenidos en el Formato de Identificación y Análisis del Riesgo (**Tabla 15**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de Riegos identificados por cada Activo crítico.

En consecuencia, se determinó el siguiente formato:

Tabla 15: Formato de Identificación y Análisis del Riesgo

INSERTAR LOGO DE LA INSTITUCIÓN	**FORMATO DE IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO**						
	Código del Formato: CF N° _____					**Fecha: ____/____/20___**	
Fase: III – Evaluación del Riesgo						**Proceso: 6 – Identificación, Análisis y Valoración del Riesgo**	
Objetivos:	- La alta gerencia debe identificar los niveles del riesgo que puede sufrir cada activo crítico de la organización.						
Personal Involucrado:	- Alta gerencia. - Otros.						
Entradas:	- Formato de Valoración de Activos respecto al Impacto llenado. - Otros.						
Salidas:							
CÓDIGO	**ACTIVO**	**IMPACTO**	**PROBABILIDAD**	**AMENAZA**	**ID RIESGO**	**RIESGO**	**VALOR**
D - RPD	Copias de Respaldo	M	B	[A]	R - D - RPD	M	3
…	**…**	**…**	**…**	**…**	**…**	**…**	**…**
Otros …	**Otros …**	**Otros …**	**Otros …**	**Otros …**	**Otros …**	**Otros …**	**Otros …**
Responsables					**Firmas**		
Elaborado por:	Alta gerencia						
Revisado por:	Equipo analista						
Aprobado por:	Equipo analista						

Fuente: Elaboración propia

b) Valoración del Riesgo.- La valoración permite evaluar los riesgos identificados para luego determinar cuál será el tratamiento adecuado.

COBIT 5 para Riesgos evalúa los riesgos en base a:

Apetito de riesgo:

> … Se considera así cuando la institución, en base a un previo análisis, establece que es un porcentaje aceptable para ser asumido, y que puede llegar consigo al cumplimiento de los planes de una entidad, plasmados tanto en su misión como visión. [25, p. 51]

Tolerancia al riesgo: "Se considera así cuando la alta gerencia, asume dicha variación como aceptable, cabe señalar que esta tolerancia es aplicada para un riesgo especifico o particular. Lo cual permitirá el cumplimento de las metas de la institución". [25, p. 85]

Capacidad del riesgo:

> … Corresponde a la variación objetiva que una institución puede tolera o soportar en base a las pérdidas que pueda obtener, sin comprometer la existencia de la misma. Cabe señalar que este punto se diferencia del apetito de riesgo, ya que en ese proceso se compromete a la decisión de la alta gerencia, puesto que ellos dan la aceptación del riesgo deseable a tener. [25, p. 176]

Así también, COBIT 5 para Riegos utiliza un «mapa de riesgos» con el fin de mostrar gráficamente los riesgos y priorizar la toma de decisiones.

En consecuencia, se asumirán una serie de pasos con el propósito de completar el mapa de riesgos:

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

   1.1. Situar los riesgos identificados (**Tabla 15**) en el mapa de riesgos con el propósito de mejorar la toma de decisiones mediante una vista gráfica.

1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que serán los encargados de asignar los riesgos identificados en el «mapa de riesgos» para su posterior valoración:

   2.1. Director de la organización.
   2.2. Administrador de la organización.
   2.3. Jefe de TI.
   2.4. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

   3.1. Formato de Identificación y Análisis del Riesgo (**Tabla 15**).
   3.2. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimiento.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

   4.1. Revisar el Formato de Identificación y Análisis del Riesgo (**Tabla 15**).
   4.2. Ubicar cada riesgo identificado (**Tabla 15**) en el Mapa de Riesgos (**Tabla 16**) utilizando solo el Id del Riesgo.
   4.3. Definir por quién será elaborado el formato y colocar su firma respectiva.
   4.4. Definir por quién será revisado el formato y colocar su firma respectiva.
   4.5. Definir por quién será aprobado el formato y colocar su firma respectiva.
   4.6. Llenar la información obtenida en el Mapa de Riesgos (**Tabla 16**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Vista gráfica de los Riesgos identificados.

En consecuencia, se determinó el siguiente mapa:

Tabla 16: Mapa de Riesgos

INSERTAR LOGO DE LA INSTITUCIÓN	**MAPA DE RIESGOS**				
	Código del Formato: CF N° _____			**Fecha: ____/____/20___**	
Fase: III – Evaluación del Riesgo				**Proceso: 6 – Identificación, Análisis y Valoración del Riesgo**	
Objetivos:	- Situar los riesgos identificados en el mapa de riesgos con el propósito de mejorar la toma de decisiones mediante una vista gráfica.				
Personal Involucrado:	- Alta gerencia. - Otros.				
Entradas:	- Formato de Identificación y Análisis del Riesgo. - Otros.				
Salidas:					
RIESGO		**INTENSIDAD**			
		MÍNIMA (1)	**MENOR (2)**	**MEDIA (3)**	**CRÍTICA (4)**	**CATASTRÓFICA (5)**
PROBABILIDAD	**FRECUENTE (81 - 100 %)**					
	PROBABLE (61 - 80 %)					
	OCASIONAL (41 - 60 %)					
	IMPROBABLE (21 - 40 %)			**R -D - RPD**		
	ESCASO (0 - 20 %)					
Responsables					**Firmas**	
Elaborado por:		Alta gerencia				
Revisado por:		Equipo analista				
Aprobado por:		Equipo analista				

Leyenda:

Insuficiente	Tolerable	Moderado	Importante	Intolerable

Fuente: Elaboración propia

Continuando con la valoración del Riesgo, se asumirán una serie de pasos con el propósito de Valorar los Riesgos identificados anteriormente (**Tabla 15**):

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. Determinar la capacidad de riesgo en base al establecimiento del apetito y la tolerancia de riesgos con el propósito de valorar los riesgos.
    1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que serán los encargados realizar la valoración del riesgo:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de TI.
    2.4. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

    3.1. Formato de Identificación y Valoración de Amenazas (**Tabla 13**).
    3.2. Formato de Identificación y Análisis del Riesgo (**Tabla 15**).
    3.3. Mapa de Riesgos (**Tabla 16**).
    3.4. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

   4.1. Revisar el Formato de Identificación y Análisis del Riesgo.
   4.2. Analizar el Mapa de Riesgos.
   4.3. Completar el código identificador de cada activo (**Tabla 15**).
   4.4. Completar el nombre de cada activo, en concordancia con el código del activo (**Tabla 15**).
   4.5. Completar el tipo de amenaza identificada con mayor probabilidad o mayor frecuencia de ocurrencia por cada activo (**Tabla 13**).
   4.6. Completar el ID del riesgo en concordancia con los activos (**Tabla 15**).
   4.7. Completar el tipo de riesgo por cada activo (**Tabla 15**).
   4.8. Completar el valor del riesgo por cada activo (**Tabla 15**).
   4.9. La alta gerencia debe asignar el apetito por cada riesgo identificado.
   4.10. La alta gerencia debe asignar la tolerancia por cada riesgo identificado.
   4.11. Establecer el tipo de Valoración de riesgo en base a la leyenda del Mapa de riesgos (**Tabla 16**).
   4.12. Definir por quién será elaborado el formato y colocar su firma respectiva.
   4.13. Definir por quién será revisado el formato y colocar su firma respectiva.
   4.14. Definir por quién será aprobado el formato y colocar su firma respectiva.
   4.15. Completar los datos obtenidos en el Formato de Valoración del Riesgo (**Tabla 17**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

   5.1. Lista de riesgos con su respectiva valoración.

   En consecuencia, se determinó el siguiente formato:

Tabla 17: Formato de Valoración del Riesgo

INSERTAR LOGO DE LA INSTITUCIÓN	**FORMATO DE VALORACIÓN DEL RIESGO**							
	Código del Formato: CF N° _____						**Fecha: ____/____/20___**	
Fase: III – Evaluación del Riesgo							**Proceso: 6 – Identificación, Análisis y Valoración del Riesgo**	
Objetivos:	- Determinar la capacidad de riesgo en base al establecimiento del apetito y la tolerancia de riesgos con el propósito de valorar los riesgos.							
Personal Involucrado:	- Alta gerencia. - Otros.							
Entradas:	- Formato de Identificación y Análisis del Riesgo.							
Salidas:								
CÓDIGO	**ACTIVO**	**TIPO DE AMENAZA**	**ID RIESGO**	**RIESGO**	**VALOR RIESGO**	**APETITO**	**TOLERANCIA**	**VALOR ACIÓN**
D - RPD	Copias de Respaldo	5.4.13. [A.15] Modificación deliberada de la información	R - D - RPD	M	3	1	2	Intolerable
…	….	….	…	…	…	…	…	…
Otros …	**Otros …**	**Otros …**	**Otros …**	**Otros …**	**Otros …**	**Otros …**	**Otros …**	**Otros …**

Responsables		**Firmas**
Elaborado por:	Alta gerencia	
Revisado por:	Equipo analista	
Aprobado por:	Equipo analista	

Fuente: Elaboración propia

Fase IV: Tratamiento del Riesgo

ISO 31000 [32, p. 21] define esta fase como: "aquella que se encarga de establecer los procedimientos que permitan seleccionar y a su vez ejecutar los diversas acciones o procesos que ayuden a ocuparse de los riesgos".

ISO 27005 [33, p. 20] propone esta fase a través de la "selección de procesos de control para reducir, retener (aceptar), prevenir o compartir los riesgos; adicionalmente recomienda establecer un plan donde se enmarquen los diversos procesos a ejecutar para lograr un adecuado tratamiento de los diversos riesgos que se puedan presentar".

Para MAGERIT v3.0 [22, p. 10]

> … Hay una variedad formas para manejar de forma óptima un riesgo: se podría evitar aquellas situaciones que son factibles para la manifestación del riesgo, logrando minimizar la ejecución del mismo, delimitando su efecto, compartiéndolo con diversos entes corporativos, o en última instancia, aceptando que el riesgo existe, pudiéndose desarrollar en cualquier momento, y prever con los recursos o procesos necesarios para su debida actuación.

OCTAVE Allegro [28, p. 58] recomienda a las organizaciones que tienen el propósito de hacer frente a los riesgos utilizar las siguientes opciones: Aceptar, Mitigar o Diferir.

COBIT 5 para Riesgos [25, pp. 85 - 87] establece esta fase a través de opciones de respuesta a riesgo, sugiriendo las siguientes opciones:

> … Primero se debe evitar el riesgo, estableciendo diversos procesos para evitar la ejecución del mismo. Segundo, una vez que se tiene claro que contamos con un riesgo existente es necesario Aceptarlo; es lo que llamamos la aceptación del riesgo. Tercero, debemos de compartir y transferir toda la información recolectada referente al riesgo. Y por último, cuatro, establecer procesos eficaces que permitan mitigar los riesgos significativos.

En conclusión, el objetivo de esta fase es seleccionar las opciones de respuesta al riesgo y definir qué controles o salvaguardas están más acorde para contrarrestar las amenazas que acechan a los activos críticos, logrando la mitigación de los riesgos.

Proceso 7: Opciones de Tratamiento del Riesgo

La finalidad de este proceso es definir cuáles son las opciones de tratamiento, las mismas que servirán para decidir cómo enfrentar cada uno de los riesgos y amenazas que afectan a los activos críticos hasta el punto de volverlos tolerables o aceptables para la organización.

Para este proceso se tomará como referencia las opciones de respuesta al riesgo que establece COBIT 5 (para Riesgos) con la finalidad de afrontar los riesgos analizados en el Formato de Valoración del Riesgo (**Tabla 17**).

Tabla 18: Opciones de Tratamiento del riesgo

NOMENCLATURA	DESCRIPCIÓN	DEFINICIÓN
ER	Evitar el Riesgo	Se refiere al hecho de evadir acciones o escapar de aquellas situaciones donde el riesgo es concurrente. La opción de «evitar» es usada solo cuando las demás alternativas de tratamiento son las menos convenientes.
AR	Aceptar el Riesgo	Está enfocada al hecho de admitir cierta cantidad de pérdida en un rango de exposición, omitiendo las posibles respuestas hacia los riesgos (en caso de manifiesten) por lo que es aceptada la pérdida que se genere.
C/TR	Compartir/Transferir el riesgo	Esta opción de tratamiento se basa en el hecho de minimizar el impacto del riesgo mediante la transferencia de un fragmento del riesgo. Entre los procedimientos más frecuentes se encuentra la adquisición de seguros y la subcontratación.
MR	Mitigar el Riesgo	Se enfoca al hecho de escoger actividades para mitigar y disminuir el impacto y la frecuencia del riesgo.

Fuente: COBIT 5 para Riesgos [25, pp. 85 - 87]

Proceso 8: Implementar Planes de Tratamiento del Riesgo

Con el objetivo de escoger las opciones de tratamiento adecuadas (para cada riesgo en particular), se establece el proceso de implementar los planes de tratamiento; basándose en los datos conseguidos a través de la fase de evaluación del riesgo (Fase III) con el fin de mitigar los riesgos y amenazas. Dichos Planes de Tratamiento pueden tomarse en consideración basándose en las Salvaguardas que propone MAGERIT v3.0 - Libro II [38, pp. 53 - 57] (**ANEXO N° 08**); para lo cual se seleccionaran solo aquellos que estén relacionados con los activos y los riesgos identificados (**Tabla 17**).

En consecuencia, se asumirán una serie de pasos con la finalidad de Implementar los Planes de Tratamiento del Riesgo (**Tabla 19**):

1. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

    1.1. Implementar los Planes establecidos en los procesos de Tratamiento del Riesgo empleando a la vez las diversas alternativas de ejecución (**Tabla 18**) de los riesgos seleccionados en el Proceso 7, con la finalidad de mitigar los riesgos y amenazas.
    1.2. Se pueden agregar otros objetivos que se crean convenientes.

2. Personal involucrado.- Conjunto de actores o participantes que serán los encargados de implementar y ejecutar los planes elaborados para un adecuado procedimiento en tratamiento de los procesos de riesgo:

    2.1. Director de la organización.
    2.2. Administrador de la organización.
    2.3. Jefe de TI.
    2.4. Se pueden agregar otros involucrados que se crean convenientes.

3. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

3.1. Formato de Valoración del Riesgo (**Tabla 17**).
3.2. Opciones de Tratamiento del Riesgo (**Tabla 18**).
3.3. Catálogo de Salvaguardas (**ANEXO N° 08**).
3.4. Se pueden agregar otras entradas que se crean convenientes.

4. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos::

4.1. Revisar el Formato de Valoración del Riesgo.
4.2. Analizar las diversas opciones que se puedan presentar al momento de Tratar los Riesgo.
4.3. Analizar el Catálogo de Salvaguardas.
4.4. Completar el código identificador de cada activo (**Tabla 18**).
4.5. Completar el nombre de cada activo, en concordancia con el código del activo (**Tabla 17**).
4.6. Completar los tipos de amenazas identificados por cada activo (**Tabla 17**).
4.7. Completar el ID del riesgo en concordancia con los activos (**Tabla 17**).
4.8. Completar el tipo de riesgo por cada activo (**Tabla 17**).
4.9. Completar la valoración del riesgo por cada activo (**Tabla 17**).
4.10. Usar la nomenclatura para designar el tipo de tratamiento que debe recibir cada riesgo (**Tabla 18**).
4.11. La alta gerencia debe designar las salvaguardas más adecuadas con el propósito de mitigar los riesgos (**ANEXO N° 08**).
4.12. Definir por quién será elaborado el formato y colocar su firma respectiva.
4.13. Definir por quién será revisado el formato y colocar su firma respectiva.
4.14. Definir por quién será aprobado el formato y colocar su firma respectiva.
4.15. Completar los datos obtenidos en el Formato de Implementación de Planes de Tratamiento del Riesgo (**Tabla 19**).

5. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

5.1. Lista de riesgos con su respectivo tratamiento y salvaguardas más apropiados.

En consecuencia, se determinó el siguiente formato:

Tabla 19: Formato de Selección e Implementación de Planes de Tratamiento del Riesgo

<table>
<tr><td colspan="2">INSERTAR LOGO DE LA INSTITUCIÓN</td><td colspan="6">FORMATO DE SELECCIÓN E IMPLEMENTACIÓN DE PLANES DE TRATAMIENTO DEL RIESGO</td></tr>
<tr><td colspan="5">Código del Formato: CF N° _____</td><td colspan="3">Fecha: ____/____/20___</td></tr>
<tr><td colspan="6">Fase: IV – Tratamiento del Riesgo</td><td colspan="2">Proceso: 8 – Implementar Planes de Tratamiento del Riesgo</td></tr>
<tr><td colspan="2">Objetivos:</td><td colspan="6">- Implementar los Planes de Tratamiento del Riesgo empleando a la vez las opciones de tratamiento del riesgo seleccionadas (Tabla 18) en el Proceso 7, con la finalidad de mitigar los riesgos y amenazas.</td></tr>
<tr><td colspan="2">Personal Involucrado:</td><td colspan="6">- Alta gerencia.
- Otros.</td></tr>
<tr><td colspan="2">Entradas:</td><td colspan="6">- Catálogo de Salvaguardas.
- Otros.</td></tr>
<tr><td colspan="8">Salidas:</td></tr>
<tr><td>CÓDIGO</td><td>ACTIVO</td><td>TIPO DE AMENAZA</td><td>ID RIESGO</td><td>RIESGO</td><td>VALORACIÓN</td><td>TRATAMIENTO</td><td>SALVAGUARDA</td></tr>
<tr><td>D - RPD</td><td>Copias de Respaldo</td><td>[A.15] Modificación intencionada de información</td><td>R - D - RPD</td><td>M</td><td>3</td><td>MR</td><td>✓ H.IA Identificación y autenticación.
✓ H.tools.AV Herramienta contra código dañino.
✓ D.I Aseguramiento de la integridad.</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td><td>…</td></tr>
<tr><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td><td>Otros …</td></tr>
<tr><td colspan="6">Responsables</td><td colspan="2">Firmas</td></tr>
<tr><td colspan="2">Elaborado por:</td><td colspan="4">Alta gerencia</td><td colspan="2"></td></tr>
<tr><td colspan="2">Revisado por:</td><td colspan="4">Equipo analista</td><td colspan="2"></td></tr>
<tr><td colspan="2">Aprobado por:</td><td colspan="4">Equipo analista</td><td colspan="2"></td></tr>
</table>

Fuente: Elaboración propia

Fase V: Seguimiento y Evaluación

Para la ISO 31000 [32, p. 23], el Seguimiento y Evaluación "debe estar presente en todas etapas del proceso de gestión de riesgos, incluyendo la planificación, el análisis y la compilación de información, el registro de los resultados y la proporción de retroalimentación".

La ISO 27005 [33, p. 25] declara que "todos los riesgos incluidos sus factores, donde podemos mencionar el valor de los activos, la amenazas encontradas, la colisión de las mismas y la posibilidad que estos ocurran, no son constantes", por lo que pueden cambiar repentinamente sin ningún precedente, en consecuencia:

> … se debe monitorear y revisar los riesgos periódicamente con el fin de determinar e identificar la mayor parte de los cambios que se puedan presentar dentro del entorno de una entidad, desde una fase inicial, logrando así sostener una percepción en forma general y actualizada del riesgo.

NIST SP 800-30 [34, p. 38] establece esta fase con la finalidad de que "las instituciones tengan los conocimientos del riesgo actualizados", proporcionando los medios para: Establecer la eficiencia y eficacia de respuesta al riesgo, identificar el impacto del riesgo, analizar los cambios que sufre los sistemas que proporcionan información y los diversos ambientes en que se desarrollan los mismos.

COBIT 5 para Riesgos [25, p. 97] a través de sus procesos clave de supervisión, evaluación y valoración (MEA01, MEA02 y MEA03), propone un conjunto de metas y métricas que sirven como procesos internos con el propósito de establecer el nivel de desempeño o rendimiento, así mismo propone un modelo de madurez que permitirá mejorar los procesos para una adecuada gestión del riesgo dentro de la entidad.

Proceso 9: Monitorear y Revisar los Riesgos

Para este proceso se han establecido los siguientes objetivos:

- Optimizar y garantizar la efectividad y calidad del proceso de gestión de riesgos.

- Evaluar constantemente las actualizaciones en las fases y procesos del modelo que involucran directamente la alteración o anulación de la evaluación de riesgos.
- Mantener actualizado los conocimientos acerca de los riesgos existentes que comprometen a los activos críticos de la organización.
- Evaluar los posibles cambios en el contexto interno y externo que repercuten de manera favorable o perjudicial a las circunstancias del riesgo, a tal punto que sea indispensable llevar a cabo actualizaciones al proceso de monitoreo y revisión de los riesgos.

Es recomendable que se elabore una programación para poder reexaminar el proceso de Gestión de Riesgos, para lo cual se recomienda que dicha evaluación se ejecuten de manera trimestral o cuando la situación u organización crean convenientes, llegando a involucrar los contextos, procesos y los activos con el fin de conocer la situación real de la institución.

En consecuencia, se asumirán un conjunto de pasos con la finalidad de Monitorear y Revisar los Riesgos (**Tabla 20**):

1. Nombre del Proyecto:

   1.1. Asignar un código y nombre al proyecto.

2. Objetivos.- Conjunto de metas establecidas que serán logradas siguiendo una serie procedimientos:

   2.1. Establecer un proyecto con el propósito de ejecutar el monitoreo y revisión de riesgos mediante indicadores.
   2.2. Se pueden agregar otros objetivos que se crean convenientes.

3. Personal involucrado.- Conjunto de actores o participantes que serán los encargados de supervisar el Monitoreo y Revisión de los Riesgos:

3.1. Director del Hospital.
3.2. Administrador del Hospital.
3.3. Jefe de TI.
3.4. Se pueden agregar otros involucrados que se crean convenientes.

4. Entradas.- Conjunto de herramientas que serán usadas en el transcurso de los procedimientos:

4.1. Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**Tabla 19**).
4.2. Se pueden agregar otras entradas que se crean convenientes.

5. Procedimientos.- Serie o conjunto de pasos a seguir ordenadamente para cumplir con los objetivos propuestos:

5.1. Revisar el Formato de Implementación de Planes de Tratamiento del Riesgo.
5.2. Completar el nombre del Activo involucrado (**Tabla 19**).
5.3. Completar el ID del riesgo (**Tabla 19**).
5.4. Completar la categoría de cada riesgo (respecto a la intensidad) según el Mapa de Riesgos (**Tabla 16**).
5.5. Completar los tipos de amenazas existentes por cada riesgo (**Tabla 19**).
5.6. Completar las Salvaguardas por cada riesgo (**Tabla 19**).
5.7. Recurso de profesional interno o externo requerido para la ejecución del proyecto.
5.8. Detallar la cantidad de profesionales requeridos para llevar a cabo la ejecución del proyecto.
5.9. Detallar la cantidad de horas necesarias para el desarrollo del proyecto.
5.10. Detallar el precio del costo por horas de desarrollo del proyecto.
5.11. Detallar el costo total de la inversión del proyecto.
5.12. Detallar el tiempo total invertido en el desarrollo del proyecto.
5.13. Describir los indicadores involucrados con el proyecto.

5.14. Establecer un conjunto de sugerencias como medidas correctivas para mejorar el proyecto.
5.15. Definir por quién será elaborado el formato y colocar su firma respectiva.
5.16. Definir por quién será revisado el formato y colocar su firma respectiva.
5.17. Definir por quién será aprobado el formato y colocar su firma respectiva.
5.18. Completar los datos obtenidos en el Formato de Monitoreo y Revisión (**Tabla 20**).

6. Salidas.- Resultados obtenidos después de aplicar los procedimientos, cumpliendo con los objetivos trazados:

   6.1. Lista de proyectos con sus respectivos indicadores.

   En consecuencia, se determinó el siguiente formato:

Tabla 20: Formato de Monitoreo y Revisión

<table>
<tr><td rowspan="2">INSERTAR LOGO DE LA INSTITUCIÓN</td><td colspan="5">FORMATO DE MONITOREO Y REVISIÓN</td></tr>
<tr><td colspan="3">Código del Formato: CF N° _____</td><td colspan="2">Fecha: ____/____/20___</td></tr>
<tr><td colspan="4">Fase: V - Seguimiento y Evaluación</td><td colspan="2">Proceso: 9 - Monitorear y Revisar los Riesgos</td></tr>
<tr><td colspan="2">Nombre del Proyecto:</td><td colspan="4">PRY 01: MANTENIMIENTO Y ACTUALIZACIÓN DE SIGA (Sistema Integrado de Gestión Administrativa)</td></tr>
<tr><td colspan="2">Objetivos:</td><td colspan="4">- Solucionar errores que se muestran en SIGA al momento de procesar devengados y giros de la organización.
- Actualizar el sistema a la última versión para evitar más inconvenientes.</td></tr>
<tr><td colspan="2">Personal Involucrado:</td><td colspan="4">- Jefe de TI.</td></tr>
<tr><td colspan="2">Entradas:</td><td colspan="4">- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (Tabla 19).
- Otros.</td></tr>
<tr><td colspan="6">Salidas:</td></tr>
<tr><td>ACTIVO INVOLUCRADO</td><td>ID RIESGO</td><td>CATEGORIA DEL RIESGO</td><td colspan="2">TIPO DE AMENAZA</td><td>SALVAGUARDAS</td></tr>
<tr><td>Copias de Respaldo</td><td>R - D - RPD</td><td>Media</td><td colspan="2">[A.15] Modificación intencionada de la información</td><td>✓ H.IA Identificación y autenticación.
✓ H.tools.AV Herramienta contra código dañino.
✓ D.I Aseguramiento de la integridad.</td></tr>
<tr><td>…</td><td>…</td><td>…</td><td colspan="2">…</td><td>…</td></tr>
<tr><td>Otros …</td><td>Otros …</td><td>Otros …</td><td colspan="2">Otros …</td><td>Otros …</td></tr>
<tr><td colspan="2">RECURSOS:</td><td colspan="4">Residente SIGA asignado a la organización.</td></tr>
<tr><td colspan="2" rowspan="2">IMPORTE:</td><td>CANTIDAD DE ESPECIALISTAS</td><td>CANTIDAD DE HORAS</td><td>COSTO POR HORA</td><td>TOTAL (S/)</td></tr>
<tr><td>1</td><td>40</td><td>0.00</td><td>0.00</td></tr>
<tr><td colspan="2">DETALLE DEL TIEMPO DE EJECUCIÓN:</td><td colspan="4">40 horas (5 días hábiles x 8hrs)</td></tr>
<tr><td colspan="2">INDICADORES:</td><td colspan="4">- Fallo de mantenimiento, por motivo que algunos usuarios no finalizaron sesión en el sistema.
- Pérdida de información contable por fallo del mantenimiento.</td></tr>
</table>

MEDIDAS CORRECTIVAS:	- Establecer un cronograma para el mantenimiento y las actualizaciones del SIGA.	
Responsables		**Firmas**
Elaborado por:	Jefe de TI	
Revisado por:	Equipo analista	
Aprobado por:	Equipo analista	

Fuente: Elaboración propia

3.4. Discusión

Para el presente trabajo de tesis se estableció como objetivo general desarrollar un modelo de gestión de gestión de riesgos de TI que contribuye en la protección de los activos de información en los hospitales de nivel II - I de la región Amazonas. Después de comparar y analizar los distintos marcos de trabajo relacionados con la gestión de riesgos de TI, se logró establecer un modelo de gestión de riesgos de TI, adaptado para las instituciones sanitarias.

El proceso para validar el modelo fue ejecutado mediante una matriz, la cual fue aprobada por 5 magíster expertos en gestión de riesgos de TI, dando por aprobado las fases y procesos que conforman la estructura del modelo propuesto (**ANEXO N° 10**).

El proceso de calcular la confiabilidad y establecer el nivel de conformidad en relación con los profesionales expertos, respecto al contenido y estructura del modelo, se realizó empleando los siguientes instrumentos:

Alfa de Cronbach:

Los resultados obtenidos mediante la matriz de validación de expertos, han sido ingresados y procesados en el aplicativo estadístico informático SPSS para determinar el Alfa de Cronbach, alcanzando un nivel de confiabilidad de 0.829.

Tabla 21: Estadística de Confiabilidad

ESTADÍSTICA DE CONFIABILIDAD	
ALFA DE CRONBACH	**NÚMERO DE ITEMS**
0.829	15

Fuente: SPSS

Ruíz [40, p. 12] proporciona la magnitud de los coeficientes de confiabilidad mediante la siguiente escala:

Tabla 22: Interpretación del Coeficiente de Confiabilidad

ESCALAS	NIVEL DE CONFIABILIDAD
0.81 – 1.00	**Muy Alta**
0.61 – 0.80	**Alta**
0.41 – 0.60	**Moderada**
0.21 – 0.40	**Baja**
0,01 – 0.20	**Muy Baja**

Fuente: Ruíz – Confiablidad [40, p. 12]

Llegando a la conclusión que el nivel de Confiabilidad del Modelo de Gestión de Riegos de TI planteado es "Muy Alta".

Coeficiente de Concordancia W de Kendall:

Según Escobar y Cuervo [41, p. 32], este coeficiente es utilizado para descubrir nivel de asociación entre un grupo de rangos.

Para determinar la concordancia entre los expertos, se presentaron 2 hipótesis:

H_0: Los rangos no coinciden, por lo tanto son independientes.
H_1: Entre los rangos existe una coincidencia relevante.

Interpretación:

> … Si el valor observado sobrepasa el nivel crítico (α de 0.05), H_0 es rechazado. A través del SPSS se puede obtener el nivel de significancia; se rechaza la hipótesis H_0 cuando el nivel de significancia es menor a 0.05, llegando a la conclusión de que existe una concordancia relevante entre los rangos establecidos por los expertos. Adicionalmente la concordancia adquiere valor cuando W se aproxima a 1. [41, p. 33]

Después de analizar los valores proporcionados por los expertos mediante la matriz de validación, la hipótesis H1 es aceptada; en conclusión, existe una coincidencia relevante entre las respuestas de los expertos basado en las dimensiones de medición ($p < 0.05$).

En la siguiente tabla se muestran los resultados obtenidos por cada dimensión en el programa estadístico informático SPSS:

Tabla 23: Resultados del Coeficiente de Concordancia de Kendall

	SUFICIENCIA	CLARIDAD	COHERENCIA	RELEVANCIA
N	15	15	15	15
W de Kendall (α)	0,400	0,287	0,324	0,296
Chi-Cuadrado	24,000	17,231	19,429	17,778
Grado de libertad (gl)	4	4	4	4
Valor de significancia (p)	0,000	0,002	0,001	0,001

Fuente: SPSS

Por último, de acuerdo a los resultados alcanzados en la evaluación del Coeficiente de Concordancia de Kendall, se concluye:

- La hipótesis H_0 queda excluida.
- Existen un acuerdo entre los expertos.
- El modelo propuesto tiene un nivel aceptable demostrando la concordancia en relación a las respuestas de los 5 expertos.

Después de validar el modelo propuesto mediante el juicio de expertos, el siguiente paso es la contrastación de la hipótesis en base al análisis de los siguientes indicadores:

Para la revisión del cumplimiento del primer objetivo específico: "Identificar y analizar comparativamente los marcos de trabajo adecuados que permitan determinar un modelo de gestión de riesgos de TI", se analizó el siguiente indicador:

Indicador: Número de marcos de trabajo analizados comparativamente para proponer el modelo de gestión de riesgos de TI.

Previamente no se había llevado a cabo ningún análisis sobre las metodologías de gestión de riesgos de TI en los hospitales de nivel II – I de la región Amazonas; por ende, se realizó

una evaluación de estas metodologías. En consecuencia, procedemos analizar el siguiente cuadro con los resultados:

INDICADOR	TOTAL	PORCENTAJE DE CUMPLIMIENTO
Números de marcos de trabajo analizados comparativamente antes de implantar parcialmente el modelo de gestión de riesgos de TI.	0	0%
Números de marcos de trabajo analizados comparativamente después de implantar parcialmente el modelo de gestión de riesgos de TI.	6	100%

En los resultados mostrados en el cuadro anterior, se puede observar una variación en el porcentaje de cumplimiento respecto al número de marcos de trabajo analizados antes y después de establecer parcialmente el modelo de gestión de riesgos de TI, donde se contempla que el porcentaje de cumplimiento se elevó en un 100%.

Para la revisión del cumplimiento del segundo objetivo específico: "Proponer el Modelo de Gestión de Riesgos de TI basado en los diferentes marcos de trabajo, con el propósito de contribuir en la protección de los activos de información", se analizó el siguiente indicador:

Indicador: Números de riesgos que pueden afectar a los activos de la organización y el impacto que puede tener.

Para evaluar este indicador, se implantó parcialmente el modelo de gestión de riesgos de TI propuesto mediante un caso de estudio (**ANEXO N° 09**), donde se pudieron identificar un total de 258 riesgos, siendo 24 (9.3%) de estos categorizados como "Muy Altos" y otros 113 (43.8%) catalogados como "Altos". Asimismo se formularon 11 proyectos con la finalidad de monitorear y revisar constantemente la gestión de riesgos de TI.

Para la revisión del cumplimiento del tercer objetivo específico: "Validar el modelo propuesto con la finalidad de garantizar su aplicación y contribución a los hospitales de nivel II – I de la región Amazonas", se analizó el siguiente indicador:

Indicador: Niveles de medición aceptables para determinar que el modelo de gestión de riesgos de TI propuesto está apto para ser aplicado.

Con el propósito de medir la confiabilidad y la concordancia del modelo propuesto se elaboró una matriz (**ANEXO N° 10**) con la finalidad de obtener una validación por expertos en la materia, obteniendo los siguientes resultados:

Alfa de Cronbach: 0.829 – Equivalente a un nivel de confiabilidad "Muy Alto".

Coeficiente de concordancia de Kendall: el valor de significancia ($p<0.05$) en todas las dimensiones de medición, demostrando que existe una conformidad entre los 5 expertos respecto a las procesos y actividades del modelo propuesto, adaptado para el sector salud.

Para la revisión del cumplimiento del cuarto objetivo específico: "Implementar parcialmente el Modelo de Gestión de Riesgos de TI, acondicionado para proteger los activos de información en hospitales de nivel II - I de la región Amazonas", se analizó el siguiente indicador:

Indicador: Porcentaje de implementación parcial con validez suficiente por parte de la organización para demostrar la utilidad del modelo de gestión de riesgos de TI.

A causa de la coyuntura que se vive actualmente por la pandemia del Covid-19, se propuso como objetivo la implementación parcial del modelo; seleccionando en un acuerdo previo (la Alta Gerencia designo al Jefe de TI para la selección de áreas y procesos críticos), la implantación de las 5 Fases que contiene el Modelo de Gestión de Riesgos de TI a la Unidad de Estadística e Informática (TI) del caso de estudio, por la justificación de tener más del 75% de los activos de información críticos bajo su responsabilidad.

En el **ANEXO N° 12**, se evidencia la conformidad de la implementación parcial por parte del caso de estudio.

CONCLUSIONES

1. Se elaboró el análisis comparativo de 6 marcos de trabajo basados en la gestión de riesgos de TI, con el propósito de adaptarlos a las organizaciones del sector salud. Esta propuesta de adaptación se elaboró para las instituciones sanitarias, no obstante, no se hallaron precedentes de una proposición semejante ejecutada en los hospitales de nivel II – I de la región Amazonas.

2. El modelo de gestión de riesgos de TI fue propuesto con el objetivo de proteger los activos de información en los hospitales de nivel II - I de la región Amazonas. Por tal motivo, después examinar el diagnóstico del sector y analizar los marcos de trabajo sobre gestión de riesgos de TI, se lograron establecer 5 fases las cuales servirán de base para cumplir con el objetivo general; dichas fases son las siguientes: Definir el Alcance y Contexto de la Organización, Identificación de Activos, Evaluación del Riesgo, Tratamiento del Riesgo y por último el Seguimiento y Evaluación.

3. El modelo de gestión de riesgos de TI propuesto, fue validado por 5 expertos mediante una matriz de consistencia para los nosocomios de la región Amazonas. A través del Alfa de Cronbach se determinó el nivel de confiabilidad, obteniendo un resultado de 0.829, catalogando el modelo con un nivel “Muy Alto”; seguidamente se analizó la concordancia de los resultados brindados por los expertos por medio del Coeficiente de Concordancia W de Kendall; como resultado el valor de significancia obtenido se situó por debajo de 0.05; en conclusión, el modelo es apto para ser aplicado a los hospitales de nivel II - I de la región Amazonas.

4. Se seleccionó un hospital de nivel II – I como caso de estudio para realizar la implementación parcial del modelo de gestión de riesgos de TI, obteniendo los siguientes resultados: se localizaron un total de 258 riesgos (75%), los cuales ponen en peligro constante a los activos de información críticos, siendo 24 (9.3%) de estos categorizados como “Muy Altos” y otros 113 (43.8%) catalogados como “Altos”. Además se formularon 11 proyectos con la finalidad de monitorear y revisar constantemente la gestión de riesgos de TI.

REFERENCIAS BIBLIOGRÁFICAS

[1] BSA | The Software Alliance, «¿Por qué son tan importantes los datos?,» 2015. [En línea]. Available: https://data.bsa.org/wp-content/uploads/2015/10/BSADataStudy_es.pdf. [Último acceso: 18 Mayo 2020].

[2] Instituto del Sur, «TI: Un Rol Indispensable en las Organizaciones,» 23 Julio 2018. [En línea]. Available: https://www.isur.edu.pe/es/articulo/ua-de-tecnologias-de-informacion/ti-un-rol-indispensable-en-las-organizaciones. [Último acceso: 18 Mayo 2020].

[3] World Economic Forum®, «The Global Risks (Report 2018),» *The Global Risks*, vol. 13th Edition, p. 6, 2018.

[4] British Broadcasting Corporation (BBC), «Hollywood hospital pays ransom to hackers,» 18 Febrero 2016. [En línea]. Available: https://www.bbc.com/news/technology-35602527. [Último acceso: 08 Mayo 2020].

[5] El Tiempo, «Multa de $ 840 millones a Bancolombia por fallas técnicas,» 24 Febrero 2017. [En línea]. Available: https://www.eltiempo.com/economia/empresas/multa-a-bancolombia-por-fallas-tecnicas-61496. [Último acceso: 19 Mayo 2020].

[6] La Prensa Gráfica, «5 datos claves para entender el "error humano" de Smartmatic en las Elecciones 2018,» 06 Marzo 2018. [En línea]. Available: https://www.laprensagrafica.com/techlife/Esto-es-un-error-de-estudiante-de-primer-ano-de-informatica-5-datos-claves-para-entender-el-error-humano-de-Smartmatic-en-las-Elecciones-2018-20180306-0049.html. [Último acceso: 19 Mayo 2020].

[7] British Broadcasting Corporation (BBC), «Filtración de datos en Ecuador: la "grave falla informática" que expuso la información personal de casi toda la población del país sudamericano,» 16 Septiembre 2019. [En línea]. Available: https://www.bbc.com/mundo/noticias-america-latina-49721456. [Último acceso: 20 Mayo 2020].

[8] Andina, «Andina. Agencia peruana de noticias,» 31 Agosto 2018. [En línea]. Available: https://portal.andina.pe/edpespeciales/2018/ciberataques-peru/index.html. [Último acceso: 16 Julio 2019].

[9] Gestión, «Empresas peruanas dedican el 20% de su presupuesto de TI en

ciberseguridad,» 28 Febrero 2019. [En línea]. Available: https://gestion.pe/economia/empresas/70-empresas-peruanas-desconoce-vulnerabilidad-sistemas-informaticos-259962-noticia/?ref=gesr. [Último acceso: 08 Mayo 2020].

[10] Congreso de la República del Perú, «Ley de Protección de Datos Personales,» 03 Julio 2011.

[11] J. C. Alfaro Campos, Metodología para la gestión de riesgos de TI basada en COBIT 5, Cartago, 2017.

[12] Y. E. Dugarte Coll, Diseño del Proceso de Gestión de Riesgos de TI de la Multinacional "La Compañía" e Implementación en el Área de Operaciones Colombia, Barranquilla, 2017.

[13] L. P. Rudas Tayo, Modelo de Gestión de Riesgos para Proyectos de Desarrollo Tecnológico, Santiago de Queretaro, 2017.

[14] R. Chambi Choque, Modelo de Gestión de Riesgos de TI Bajo COBIT 5, La Paz, 2018.

[15] G. C. Llontop Díaz, Gestión de riesgos de Tecnologías de Información de las empresas de Nephila Networks, Lima, 2018.

[16] L. A. Moscoso Anaya, E. E. Peña Núñez y M. d. C. Soto Castrillón, Modelo de Gestión de Riesgos de TI que Contribuye a la Operación de los Procesos de Gestión Comercial de las Empresas del Sector de Saneamiento del Norte del Perú, Chiclayo, 2018.

[17] J. C. Banda Santisteban, Modelo Basado en Metodologías de Gestión de Riesgos de TI para Contribuir en la Mejora de la Seguridad de los Activos de Información en Empresas del Sector Agroindustrial de la Región Lambayeque, Chiclayo, 2019.

[18] J. M. Rodríguez Castro, Modelo de Gestión de Riesgos de Tecnologías de la Información como Apoyo en la Continuidad del Negocio en una Empresa que Brinda Software como Servicio, Chiclayo, 2019.

[19] J. C. García Porras y S. C. Huamani Pastor, Modelo de Gestión de Riesgos de Seguridad de la Información para pymes en el Perú, Lima, 2019.

[20] F. B. Vásquez Velásquez y J. D. P. Alva Zapata, Modelo de Gestión de Riesgos de TI para Contribuir en la Continuidad del Negocio de las Microfinancieras de la Región Lambayeque, Chiclayo, 2018.

[21] Information Systems Audit and Control Association (ISACA), «COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa,» Rolling Meadows,

Illinois, 2012.

[22] Consejo Superior de Administración Electrónica, «MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Libro I - Método),» Madrid, © Ministerio de Hacienda y Administraciones Públicas, 2012.

[23] National Institute of Standards and Technology (NIST), «Managing Information Security Risk (Organization, Mission, and Information System View),» de *NIST Special Publication 800-39*, Gaithersburg, 2011.

[24] Consejo Superior de Administración Electrónica, «MAGERIT - versión 1. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» Madrid, © Ministerio de Hacienda y Administraciones Públicas, 1997.

[25] Information Systems Audit and Control Association (ISACA), «COBIT 5: para Riesgos,» Rolling Meadows, Illinois, 2013.

[26] Comités Técnicos de Normalización, «UNE 71504 - Metodología de análisis y gestión de riesgos para los sistemas de información,» Madrid, Asociación Española de Normalización, 2008.

[27] Central Computer and Telecommunications Agency, «CCTA Risk Analysis and Management Method (CRAMM),» vol. Version 5.0, 2003.

[28] R. A. Caralli, J. F. Stevens Lisa y R. Y. William R. Wilson, «La introducción de OCTAVE Allegro: Mejorar el Proceso de Evaluación de Riesgos de Seguridad,» Pittsburgh, Carnegie Mellon University, 2007.

[29] Instituto Nacional de Ciberseguridad, «Gestión de Riesgos: Una Guía de Aproximación para el Empresario. Versión 1,» León, 2015.

[30] Organización Mundial de la Salud, «Función de los hospitales en los programas de protección de la salud.,» Ginebra, 1957.

[31] Miniterio de Salud (MINSA), *Categorías de Establecimientos del Sector Salud*, Lima, 2011.

[32] UNE - International Organization for Standardization (ISO) 31000, «Gestión del riesgo,» de *Directrices*, Génova, Madrid: AENOR INTERNACIONAL S.A.U., 2018.

[33] International Organization for Standardization, «ISO/IEC 27005,» de *Risk Management of Information Security*, Vernier, Ginebra, Index House, 2018.

[34] National Institute of Standards and Technology (NIST), «Guide for Coducting Risk

Assesments,» de *NIST Special Publication 800-30 (Revision 1)*, Gaithersburg, 2012.

[35] R. Hernández Sampieri, C. Fernández Collado y P. Baptista Lucio, «Metodología de la Investigación,» Sexta ed., Ciudad de México, McGRAW-HILL, 2014.

[36] SUSALUD, «Listado de establecimientos registrados en el renipress,» 2019. [En línea]. Available: http://app20.susalud.gob.pe:8080/registro-renipress-webapp/listadoEstablecimientosRegistrados.htm?action=mostrarBuscar#no-back-button. [Último acceso: 15 Septiembre 2019].

[37] Asociación Colombiana de Facultades de Psicología, Colegio Colombiano de Psicólogos y la Universidad del Rosario, «Ética Psicológica,» 17 Julio 2018. [En línea]. Available: http://eticapsicologica.org/index.php/documentos/articulos/item/16-que-son-los-principios-eticos. [Último acceso: 05 Agosto 2019].

[38] Consejo Superior de Administración Electrónica, «MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Libro II - Catálogo de Elementos),» Madrid, © Ministerio de Hacienda y Administraciones Públicas, 2012.

[39] Consejo Superior de Administración Electrónica, «MAGERIT - versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Libro III - Guía de Técnicas),» Madrid, © Ministerio de Hacienda y Administraciones Públicas, 2012.

[40] C. Ruíz Bolivar, «Programa Interinstitucional Doctorado en Educación - CONFIABILIDAD,» [En línea]. Available: http://200.11.208.195/blogRedDocente/alexisduran/wp-content/uploads/2015/11/CONFIABILIDAD.pdf. [Último acceso: 27 Julio 2020].

[41] J. Escobar Pérez y Á. Cuervo Martínez, «Validez de Contenido y Juicio de Expertos: Una Aproximación a su Utilización,» 2008. [En línea]. Available: https://pdfs.semanticscholar.org/0736/455b135cfa8e5fc192d6bd526d1546b4528d.pdf. [Último acceso: 28 Julio 2020].

ANEXOS

ANEXO Nº 01: CUESTIONARIO DE EVALUACIÓN SITUACIONAL REALIZADA A LOS ENCARGADOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LOS HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

Objetivos:

- Diagnosticar si la alta dirección facilita los recursos necesarios para apoyar de manera efectiva al área de TI.
- Constatar si en la organización se tiene una cultura para la gestión de riesgos.
- Corroborar si el área de TI cuenta un plan estratégico y políticas de seguridad para gestionar los riesgos a los que están expuestos los activos de información.
- Identificar si se cuenta con un inventario de los activos y riesgos de TI.
- Verificar si tiene un registro de los riesgos que se han materializado en la organización.

PREGUNTAS

NOMBRE: _____ FECHA: _____

INSTITUCIÓN: _____

CARGO: _____

Instrucciones:

Marque con una "X" la respuesta que considere más conveniente y de ser posible sustente la justificación de su respuesta.

PREGUNTAS	SI	NO	JUSTIFICACIÓN
1. ¿Se ha establecido un plan estratégico para el área de TI?			
2. ¿Usted cuenta con políticas de seguridad informática?			
3. ¿Usted realiza capacitaciones o brinda nociones acerca de "Seguridad de la Información" en la organización?			
4. ¿Existe algún reglamento interno donde se hace mención a la correcta de utilización de activos de información de la organización?			
5. ¿Los usuarios tienen conocimiento de cuáles son los			

activos de información más relevantes de la organización?			
6. ¿La organización cuenta con un inventario de activos de información?			
7. ¿Existe alguna categorización para los activos de información según su valor, requisitos legales, sensibilidad y criticidad para la organización?			
8. ¿Existe alguna asignación de activos de información a los usuarios de acuerdo a las responsabilidades y roles?			
9. ¿Se tiene establecido un cronograma o automatización de copias de seguridad de los datos más relevantes de la organización?			
10. ¿Se han implementado políticas y procedimientos de seguridad para salvaguardar los activos de información?			
11. ¿Se ha establecido alguna metodología para la identificación y análisis de los riesgos internos y externos de la organización relacionados con los activos de información de TI?			
12. ¿Existe alguna bitácora donde se registren los riesgos que hayan causado un impacto comprometiendo los activos de información de la organización?			
13. ¿La organización cuenta con una filosofía de riesgos (Apetito de riesgo, Tolerancia de riesgo y Capacidad de riesgo)?			
14. ¿La cultura existente en la organización requiere cambiar o mejorar para poder enfrentar de manera efectiva la gestión de riesgos?			
15. ¿Se ha elaborado una tasación de las posibles pérdidas económicas que se asumirán si un probable escenario de riesgo de TI se manifiesta?			
16. ¿Se hizo un estudio o investigación de los daños experimentados a raíz de la materialización de los riesgos de TI?			
17. ¿La organización cuenta con alguna clasificación de los escenarios de riesgos?			
18. ¿Se han implantado actividades de control que se deben ejecutar para mitigar los riesgos?			
19. ¿Se ha elaborado una guía de procedimientos si es que la materialización de un riesgo causa un impacto significativo en la organización?			
20. ¿Se realiza alguna supervisión del perfil de riesgo de la organización?			
21. ¿La alta dirección es notificada sobre los riesgos a los que se encuentran comprometidos los activos de información?			

MARCO DE REFERENCIA: COBIT® 2019 Framework Governance and Management Objectives

OBJETIVOS DE GOBIERNO Y GESTIÓN			
PROCESOS DE COBIT		**CUESTIONARIO**	**OBJETIVO DEL INSTRUMENTO**
PRÁCTICA DE GESTIÓN	**ACTIVIDADES**		
CONOCIMIENTO DE LA ORGANIZACIÓN Y SU CONTEXTO			
APO01.04	Definir el alcance, foco, mandato y responsabilidades de cada función dentro de la organización de I&T, en línea con la dirección de gobierno.	¿Se ha establecido un plan estratégico para el área de TI?	Corroborar si el área de TI cuenta con un plan estratégico o utiliza políticas de seguridad para salvaguardar los activos de información que están expuestos a riesgos.
	Establecer un comité de dirección de I&T (o equivalente) compuesto por directores ejecutivos, de negocio y de I&T para hacer un seguimiento del estado de los proyectos, resolver los conflictos de recursos y monitorizar los niveles y mejoras del servicio.		
APO02.03	Definir objetivos y metas de I&T de alto nivel y especificar su contribución a los objetivos empresariales.		
	Determinar las estrategias en cuanto a capacidades, metodologías y enfoques organizativos de I&T requeridas para lograr el portafolio definido de productos y servicios de I&T. Considerar distintas metodologías de desarrollo (Agile, Scrum, Waterfall, Bimodal IT), dependiendo de los requisitos del negocio. Considerar como cada uno de ellos puede contribuir a lograr los objetivos de I&T.		
APO01.09	Crear una serie de políticas para mejorar las expectativas de control de IT en temas clave relevantes, como la calidad, la seguridad, la privacidad, los controles internos, el uso de activos de I&T, la ética y los derechos de propiedad intelectual.	¿Usted cuenta con políticas de seguridad informática?	

APO11.01	Definir roles, tareas y derechos de decisión y responsabilidades para la gestión de la calidad en la estructura organizativa.		
APO11.03	Definir los estándares, prácticas y procedimientos de gestión de la calidad en línea con los requisitos del marco de control de I&T y los criterios y políticas de gestión de la calidad empresariales.		
	Comunicar de forma eficaz el enfoque de gestión de la calidad (p. ej., a través de programas de capacitación de calidad formales y regulares).	¿Usted realiza capacitaciones o brinda nociones acerca de "Seguridad de la Información" en la organización?	Verificar si se concientiza al personal de la organización sobre la cultura de Seguridad de la Información
APO11.05	Establecer una plataforma para compartir buenas prácticas y captar información sobre los defectos y errores para permitir el aprendizaje a partir de ellos.		
EDM03	Promover una cultura consciente de los riesgos de I&T en todos los niveles de la organización y facultar proactivamente a la empresa para que identifique, comunique y escale el riesgo, oportunidad y posibles impactos del negocio en I&T.		
BAI08.03	Transmitir los recursos de conocimiento disponibles a las partes interesadas correspondientes y comunicar cómo estos recursos pueden utilizarse para abordar diferentes necesidades (p. ej., resolución de problemas, aprendizaje, planificación estratégica y toma de decisiones).		
DSS05.01	Comunicar acerca de concienciación sobre software malicioso y hacer cumplir los procedimientos y responsabilidades de prevención. Impartir formación periódica sobre malware en el uso de correo electrónico e Internet. Formar a los usuarios para que no abran e informen sobre correos electrónicos sospechosos y no instalen software compartido o no aprobado.		

DSS05.05	Realizar formación sobre concienciación de la seguridad de la información física de forma regular.		
CLASIFICACIÓN DE ACTIVOS			
APO01.05	Establecer, acordar y comunicar los roles y responsabilidades relacionadas con I&T a todo el personal de la empresa, de acuerdo con las necesidades y objetivos de la empresa. Delinear claramente las responsabilidades y la rendición de cuentas, especialmente para la toma de decisiones y aprobaciones.	¿Existe algún reglamento interno donde se hace mención a la correcta de utilización de activos de información de la organización?	Constatar si se han establecido políticas de protección de los activos de información
		¿Los usuarios tienen conocimiento de cuáles son los activos de información más relevantes de la organización?	
BAI09.03	Obtener, recibir, verificar, probar y registrar todos los activos de forma controlada, incluyendo etiquetas físicas, cuando se requiera.	¿La organización cuenta con un inventario de activos de información?	Determinar si la organización tiene catalogados los activos de información para la gestión de TI
BAI08.01	Considerar los tipos de contenido (procedimientos, procesos, estructuras, conceptos, políticas, reglas, hechos, clasificaciones), artefactos (documentos, registros, vídeo, voz) e información estructurada y no estructurada (expertos, redes sociales, correo electrónico, mensajes de voz, canales RSS (Rich Site Summary)).		
	Clasificar las fuentes de información con base en el esquema de clasificación de contenidos (p. ej. el modelo de arquitectura de la información). Correlacionar las fuentes de información con el esquema de clasificación.	¿Existe alguna categorización para los activos de información según su valor, requisitos legales, sensibilidad y criticidad para la organización?	
	Recopilar, cotejar y validar las fuentes de información con base en los criterios de validación de la información (p. ej., comprensión, relevancia, importancia, integridad, precisión, consistencia, confidencialidad, vigencia y confiabilidad).		

BAI09.01	Identificar todos los activos adquiridos en un registro de activos que recoja el estado actual. Los activos se reportan en la hoja del balance; se compran o crean para aumentar el valor de una compañía o beneficiar las operaciones de la empresa (p. ej. hardware y software).		
BAI09.02	Identificar activos que son críticos para proporcionar la capacidad de servicio mediante la referencia a los requisitos en las definiciones de servicio, los SLA y el sistema de gestión de la configuración.		
APO01.07	Evaluar y distinguir entre datos, información y sistemas críticos (de alto valor) y no críticos. Asegurar la protección adecuada para cada categoría.		
	Crear y mantener un inventario de información (sistemas y datos) que incluyan una lista de Dueños, custodios y clasificaciones. Incluir sistemas que sean externalizados y aquellos cuya propiedad debería estar dentro de la empresa.	¿Existe alguna asignación de activos de información a los usuarios de acuerdo a las responsabilidades y roles?	Cerciorarse si la distribución de los activos está acorde a las necesidades del negocio.
APO14.01	Establecer una función de gestión de los datos con responsabilidad de gestionar las actividades que respalden los objetivos de gestión de los datos.		
	Especificar roles y responsabilidades para respaldar la gestión de los datos y la interacción entre el gobierno y la función de gestión de datos.		
BAI09.03	Asignar los activos a usuarios, con responsabilidades de aceptación y confirmación, como corresponda.		
	Siempre que sea posible, reasignar los activos cuando ya no se necesiten debido a un cambio de rol del usuario, redundancia en un servicio o retirada de un servicio.		
GESTIONAR ACTIVOS			
APO14.10	Definir una programación para garantizar una copia de seguridad (backup) correcta de todos los datos críticos.	¿Se tiene establecido un cronograma o automatización de	Comprobar si se resguardan los activos con políticas de

DSS05.01	Instalar y activar herramientas de protección contra software malicioso en todas las instalaciones de procesamiento, con archivos de definición de software malicioso que se actualizan según sea necesario (automáticamente o semiautomáticamente).	copias de seguridad de los datos más relevantes de la organización?	información bajo los lineamientos del negocio.
DSS06.06	Aplicar las políticas y procedimientos de seguridad para la clasificación y uso aceptable de datos y para proteger los activos de información que están bajo control del negocio.	¿Se han implementado políticas y procedimientos de seguridad para salvaguardar los activos de información?	
BAI09.02	Establecer un plan de mantenimiento preventivo para todo el hardware considerando un análisis de coste beneficio, las recomendaciones de los proveedores, el riesgo de suspensión del servicio, el personal calificado y otros factores relevantes.		
IDENTIFICAR EL RIESGO			
APO12.01	Establecer y mantener un método para la recogida, clasificación y análisis de datos relacionados con el riesgo de I&T.	¿Se ha establecido alguna metodología para la identificación y análisis de los riesgos internos y externos de la organización relacionados con los activos de información de TI?	Evidenciar si la organización es consciente de los riegos a los que se encuentran expuestos los activos de información.
	Registrar datos relevantes y significativos relacionados con los riesgos de I&T en el entorno operativo interno y externo de la empresa.		
	Registrar datos de eventos de riesgo que han causado o podrían causar impacto en el negocio conforme a las categorías de impacto definidas en la taxonomía de riesgo. Capturar datos relevantes de cuestiones, incidentes, problemas e investigaciones.	¿Existe alguna bitácora donde se registren los riesgos que hayan causado un impacto comprometiendo los activos de información de la organización?	Analizar si los eventos que ocasionan perjuicio en la organización, son considerados para una futura toma de decisiones.
	Realizar un análisis periódico de eventos y factores de riesgo para identificar riesgos nuevos o emergentes y para mejorar el entendimiento de los factores de riesgo internos y externos asociados.		
ANALIZAR EL RIESGO			

<table>
<tr><td rowspan="1">APO12.02</td><td>Definir el alcance adecuado de los esfuerzos en análisis de riesgos, considerando todos los factores de riesgo y/o la criticidad de los activos para el negocio.</td><td rowspan="2">¿La organización cuenta con una filosofía de riesgos (Apetito de riesgo, Tolerancia de riesgo y Capacidad de riesgo)?</td><td rowspan="5">Diagnosticar si la organización posee una cultura para la gestión de riesgos y analizar hasta qué punto la empresa es capaz de un cambio organizacional para proteger los activos de información.</td></tr>
<tr><td rowspan="3">EDM03.01</td><td>Determinar el apetito al riesgo de la organización, es decir, el nivel de riesgo relacionado con I&T que la empresa está dispuesta a tomar en la búsqueda de sus objetivos empresariales.</td></tr>
<tr><td>Determinar los niveles de tolerancia al riesgo frente al apetito al riesgo, es decir, las desviaciones aceptables temporalmente del apetito al riesgo.</td></tr>
<tr><td>Determinar el grado de alineamiento de la estrategia de riesgos en I&T de la empresa y garantizar que el apetito al riesgo se sitúe por debajo de la capacidad de riesgo de la organización.</td><td rowspan="3">¿La cultura existente en la organización requiere cambiar o mejorar para poder enfrentar de manera efectiva la gestión de riesgos?</td></tr>
<tr><td>Evaluar las actividades de gestión de riesgos para asegurar que se alineen con la capacidad de la empresa para las pérdidas relacionadas con I&T y la tolerancia correspondiente por parte de la dirección.</td></tr>
<tr><td rowspan="3">APO12.02</td><td>Comparar el riesgo actual (exposición a pérdidas de I&T) con el apetito al riesgo y la tolerancia de riesgo aceptable. Identificar el riesgo inaceptable o elevado.</td></tr>
<tr><td>Proponer respuestas al riesgo para riesgos que excedan el apetito al riesgo y los niveles de tolerancia.</td></tr>
<tr><td>Estimar la frecuencia (o probabilidad) y la magnitud de la pérdida o ganancia asociada con escenarios de riesgos de I&T. Tener en cuenta todos los factores de riesgo aplicables y evaluar controles operativos conocidos.</td><td>¿Se ha elaborado una tasación de las posibles pérdidas económicas que se asumirán si un probable escenario de riesgo de TI se manifiesta?</td><td>Establecer una proyección de los gastos económicos que se ocasionarían por la materialización de los riesgos</td></tr>
<tr><td colspan="4">VALORAR EL RIESGO</td></tr>
</table>

APO12.01	Estudiar y analizar los datos históricos de riesgo de I&T y de pérdidas experimentadas a partir de datos y tendencias externos disponibles, homólogos de la industria a través de logs de eventos de la industria, bases de datos, y acuerdos de la industria, para la publicación común de eventos.	¿Se hizo un estudio o investigación de los daños experimentados a raíz de la materialización de los riesgos de TI?	Comprobar si se analizan los percances ocasionados a causa de los riesgos manifestados.
APO12.03	Agregar los escenarios de riesgos actuales por categoría, línea de negocio y área funcional.	¿La organización cuenta con alguna clasificación de los escenarios de riesgos?	Determinar si la organización tiene catalogados los escenarios de riesgos
APO12.06	Clasificar los incidentes y comparar las exposiciones a pérdidas relacionadas con I&T con los umbrales de tolerancia al riesgo. Comunicar los impactos de negocio a los responsables de la toma de decisiones como parte del reporte y actualización del perfil de riesgo.		
TRATAMIENTO DEL RIESGO			
APO12.05	Mantener un inventario de las actividades de control que se han implantado para mitigar el riesgo y que permiten que se tomen riesgos alineados con el apetito y la tolerancia al riesgo. Clasificar las actividades de control y asignarlas a escenarios de riesgos de I&T específicos y escenarios de riesgos de I&T agregados.	¿Se han implantado actividades de control que se deben ejecutar para mitigar los riesgos?	Constatar si en la organización se han establecido actividades, políticas y procedimientos para el tratamiento de riesgos.
APO12.06	Preparar, mantener y probar planes que documenten los pasos específicos que deben darse cuando un evento de riesgo pudiera causar un incidente significativo de desarrollo u operativo con un impacto grave para el negocio. Asegurar que los planes incluyan vías de escalamiento en la empresa.	¿Se ha elaborado una guía de procedimientos si es que la materialización de un riesgo causa un impacto significativo en la organización?	
SUPERVISAR LA GESTION DE RIESGO			
EDM03.03	Supervise hasta qué punto se gestiona el perfil de riesgo dentro de los umbrales de tolerancia y apetito de riesgo de la empresa.	¿Se realiza alguna supervisión del perfil de riesgo de la organización?	Comprobar si se actualiza frecuentemente el perfil de riesgo alienado a los umbrales de tolerancia y objetivos de la organización.

COMUNICAR EL RIESGO			
APO12.04	Informar sobre los resultados del análisis de riesgo a todas las partes interesadas afectadas en términos y formatos útiles para soportar las decisiones empresariales. Siempre que sea posible, incluir las probabilidades y rangos de pérdidas o ganancias, junto con los niveles de confianza, para permitir que la gerencia haga balance del retorno del riesgo.	¿La alta dirección es notificada sobre los riesgos a los que se encuentran comprometidos los activos de información?	Asegurarse que la alta dirección sea participe de los análisis y resultados de la gestión de riesgos.
EDM03.02	Ordenar que el riesgo, oportunidades, problemas o preocupaciones puedan identificarse y comunicarse por cualquier persona a la parte correspondiente en cualquier momento. El riesgo debe gestionarse conforme a las políticas y procedimientos publicados y comunicados a los responsables de la toma de decisiones.		
EDM03.03	Comunicar cualquier problema de gestión de riesgos al consejo de administración o comité ejecutivo.		

ANEXO Nº 02: RESULTADOS DEL CUESTIONARIO DE EVALUACIÓN SITUACIONAL REALIZADA A LOS ENCARGADOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LOS HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

CUESTIONARIO	HOSPITAL 01	HOSPITAL 02	HOSPITAL 03
1. ¿Se ha establecido un plan estratégico para el área de TI?	NO	NO	NO
2. ¿Usted cuenta con políticas de seguridad informática?	SI	NO	NO
3. ¿Usted realiza capacitaciones o brinda nociones acerca de "Seguridad de la Información" en la organización?	NO	NO	NO
4. ¿Existe algún reglamento interno donde se hace mención a la correcta de utilización de activos de información de la organización?	NO	NO	NO
5. ¿Los usuarios tienen conocimiento de cuáles son los activos de información más relevantes de la organización?	SI	NO	SI
6. ¿La organización cuenta con un inventario de activos de información?	NO	SI	SI
7. ¿Existe alguna categorización para los activos de información según su valor, requisitos legales, sensibilidad y criticidad para la organización?	NO	NO	NO
8. ¿Existe alguna asignación de activos de información a los usuarios de acuerdo a las responsabilidades y roles?	NO	NO	SI
9. ¿Se tiene establecido un cronograma o automatización de copias de seguridad de los datos más relevantes de la organización?	SI	NO	SI
10. ¿Se han implementado políticas y procedimientos de seguridad para salvaguardar los activos de información?	NO	NO	SI
11. ¿Se ha establecido alguna metodología para la identificación y análisis de los riesgos internos y externos de la organización relacionados con los activos de información de TI?	NO	NO	NO
12. ¿Existe alguna bitácora donde se registren los riesgos que hayan causado un impacto comprometiendo los activos de información de la organización?	NO	NO	NO
13. ¿La organización cuenta con una filosofía de riesgos (Apetito de riesgo, Tolerancia de riesgo y Capacidad de riesgo)?	NO	NO	NO
14. ¿La cultura existente en la organización requiere cambiar o mejorar para poder enfrentar	NO	NO	SI

de manera efectiva la gestión de riesgos?			
15. ¿Se ha elaborado una tasación de las posibles pérdidas económicas que se asumirán si un probable escenario de riesgo de TI se manifiesta?	NO	NO	NO
16. ¿Se hizo un estudio o investigación de los daños experimentados a raíz de la materialización de los riesgos de TI?	NO	NO	NO
17. ¿La organización cuenta con alguna clasificación de los escenarios de riesgos?	NO	NO	NO
18. ¿Se han implantado actividades de control que se deben ejecutar para mitigar los riesgos?	NO	NO	NO
19. ¿Se ha elaborado una guía de procedimientos si es que la materialización de un riesgo causa un impacto significativo en la organización?	NO	NO	NO
20. ¿Se realiza alguna supervisión del perfil de riesgo de la organización?	NO	NO	NO
21. ¿La alta dirección es notificada sobre los riesgos a los que se encuentran comprometidos los activos de información?	NO	NO	NO

ENCUESTA

Cuestionario de evaluación situacional de los hospitales de nivel II – I de la región Amazonas.

Estimado profesional, usted ha sido invitado a formar parte del proceso de evaluación de un instrumento para la tesis de maestría que tiene por nombre: "Modelo de Gestión de Riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas."; para optar el grado de Magíster en Ingeniería de Sistemas y Computación con Mención en Dirección Estratégica de TI. Por tal motivo se le otorga el instrumento de evaluación que será indispensable para que pueda hacerme llegar su perspectiva en cada ítem del instrumento de investigación.

NOMBRE: Jaime Izquierdo Cabrera FECHA: 29/11/19
INSTITUCIÓN: Hospital de Apoyo Bagua
CARGO: Jefe de informatica

Instrucciones:
Marque con una "X" la respuesta que considere más conveniente y de ser posible sustente la justificación de su respuesta.

PREGUNTAS	SI	NO	JUSTIFICACIÓN
1. ¿Se ha establecido un plan estratégico para el área de TI?		X	
2. ¿Usted cuenta con políticas de seguridad informática?	X		Pero no está documentado
3. ¿Usted realiza capacitaciones o brinda nociones acerca de "Seguridad de la Información" en la organización?		X	
4. ¿Existe algún reglamento interno donde se hace mención a la correcta de utilización de activos de información de la organización?		X	
5. ¿Los usuarios tienen conocimiento de cuáles son los activos de información más relevantes de la organización?	X		
6. ¿La organización cuenta con un inventario de activos de información?		X	
7. ¿Existe alguna categorización para los activos de información según su valor, requisitos legales, sensibilidad y criticidad para la organización?		X	
8. ¿Existe alguna asignación de activos de información a los usuarios de acuerdo a las responsabilidades y roles?		X	
9. ¿Se tiene establecido un cronograma o	X		

automatización de copias de seguridad de los datos más relevantes de la organización?			
10. ¿Se han implementado políticas y procedimientos de seguridad para salvaguardar los activos de información?		X	
11. ¿Se ha establecido alguna metodología para la identificación y análisis de los riesgos internos y externos de la organización relacionados con los activos de información de TI?		X	
12. ¿Existe alguna bitácora donde se registren los riesgos que hayan causado un impacto comprometiendo los activos de información de la organización?		X	
13. ¿La organización cuenta con una filosofía de riesgos (Apetito de riesgo, Tolerancia de riesgo y Capacidad de riesgo)?		X	
14. ¿La cultura existente en la organización requiere cambiar o mejorar para poder enfrentar de manera efectiva la gestión de riesgos?		X	
15. ¿Se ha elaborado una tasación de las posibles pérdidas económicas que se asumirán si un probable escenario de riesgo de TI se manifiesta?		X	
16. ¿Se hizo un estudio o investigación de los daños experimentados a raíz de la materialización de los riesgos de TI?		X	
17. ¿La organización cuenta con alguna clasificación de los escenarios de riesgos?		X	
18. ¿Se han implantado actividades de control que se deben ejecutar para mitigar los riesgos?		X	
19. ¿Se ha elaborado una guía de procedimientos si es que la materialización de un riesgo causa un impacto significativo en la organización?		X	
20. ¿Se realiza alguna supervisión del perfil de riesgo de la organización?		X	
21. ¿La alta dirección es notificada sobre los riesgos a los que se encuentran comprometidos los activos de información?		X	

MINISTERIO DE SALUD
GOBIERNO REGIONAL AMAZONAS
HOSPITAL DE APOYO BAGUA
Ing. Jaime Izquierdo Cabrera
DNI N° 40888472
JEFE DE INFORMÁTICA

FIRMA RESPONSABLE DE TI

FIRMA RESPONSABLE DE TESIS
César A. Villegas Rivera

ENCUESTA

Cuestionario de evaluación situacional de los hospitales de nivel II – I de la región Amazonas.

Estimado profesional, usted ha sido invitado a formar parte del proceso de evaluación de un instrumento para la tesis de maestría que tiene por nombre: "Modelo de Gestión de Riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas."; para optar el grado de Magíster en Ingeniería de Sistemas y Computación con Mención en Dirección Estratégica de TI. Por tal motivo se le otorga el instrumento de evaluación que será indispensable para que pueda hacerme llegar su perspectiva en cada ítem del instrumento de investigación.

NOMBRE: DANTE L.E. DELGADO SIRLOPU FECHA: 04/12/2019
INSTITUCIÓN: HOSPITAL SANTIAGO APOSTOL - UTCUBAMBA
CARGO: RESP. ESTADISTICA E INFORMATICA

Instrucciones:
Marque con una "X" la respuesta que considere más conveniente y de ser posible sustente la justificación de su respuesta.

PREGUNTAS	SI	NO	JUSTIFICACIÓN
1. ¿Se ha establecido un plan estratégico para el área de TI?		X	
2. ¿Usted cuenta con políticas de seguridad informática?		X	
3. ¿Usted realiza capacitaciones o brinda nociones acerca de "Seguridad de la Información" en la organización?		X	Se les hace hincapié al personal sobre los riesgos q pueden conllevar a que los activos de información sufran algún daño o pérdidas de datos.
4. ¿Existe algún reglamento interno donde se hace mención a la correcta de utilización de activos de información de la organización?		X	
5. ¿Los usuarios tienen conocimiento de cuáles son los activos de información más relevantes de la organización?		X	
6. ¿La organización cuenta con un inventario de activos de información?	X		
7. ¿Existe alguna categorización para los activos de información según su valor, requisitos legales, sensibilidad y criticidad para la organización?		X	

8. ¿Existe alguna asignación de activos de información a los usuarios de acuerdo a las responsabilidades y roles?		X	
9. ¿Se tiene establecido un cronograma o automatización de copias de seguridad de los datos más relevantes de la organización?		X	
10. ¿Se han implementado políticas y procedimientos de seguridad para salvaguardar los activos de información?		X	
11. ¿Se ha establecido alguna metodología para la identificación y análisis de los riesgos internos y externos de la organización relacionados con los activos de información de TI?		X	
12. ¿Existe alguna bitácora donde se registren los riesgos que hayan causado un impacto comprometiendo los activos de información de la organización?		X	
13. ¿La organización cuenta con una filosofía de riesgos (Apetito de riesgo, Tolerancia de riesgo y Capacidad de riesgo)?		X	
14. ¿La cultura existente en la organización requiere cambiar o mejorar para poder enfrentar de manera efectiva la gestión de riesgos?		X	
15. ¿Se ha elaborado una tasación de las posibles pérdidas económicas que se asumirán si un probable escenario de riesgo de TI se manifiesta?		X	
16. ¿Se hizo un estudio o investigación de los daños experimentados a raíz de la materialización de los riesgos de TI?		X	
17. ¿La organización cuenta con alguna clasificación de los escenarios de riesgos?		X	
18. ¿Se han implantado actividades de control que se deben ejecutar para mitigar los riesgos?		X	
19. ¿Se ha elaborado una guía de procedimientos si es que la materialización de un riesgo causa un impacto significativo en la organización?		X	
20. ¿Se realiza alguna supervisión del perfil de riesgo de la organización?		X	
21. ¿La alta dirección es notificada sobre los riesgos a los que se encuentran comprometidos los activos de información?		X	

REGION DE SALUD AMAZONAS
Hospital de Apoyo I SANTIAGO APOSTOL
DANTE E. DELGADO SIRLOSI
DNI 42705269
TEC. EN COMPUTACION E INFORMATICA

FIRMA RESPONSABLE DE TI

FIRMA RESPONSABLE DE TESIS
César A. Villegas Rivera

ENCUESTA

Cuestionario de evaluación situacional de los hospitales de nivel II – I de la región Amazonas.

Estimado profesional, usted ha sido invitado a formar parte del proceso de evaluación de un instrumento para la tesis de maestría que tiene por nombre: "Modelo de Gestión de Riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas"; para optar el grado de Magíster en Ingeniería de Sistemas y Computación con Mención en Dirección Estratégica de TI. Por tal motivo se le otorga el instrumento de evaluación que será indispensable para que pueda hacerme llegar su perspectiva en cada ítem del instrumento de investigación.

NOMBRE: Nancy del Carmen Jaramillo Ypanaqui FECHA: 25/11/2019
INSTITUCIÓN: Hospital María Auxiliadora de Rod. de Mendoza
CARGO: Responsable de Estadística e Informática

Instrucciones:
Marque con una "X" la respuesta que considere más conveniente y de ser posible sustente la justificación de su respuesta.

PREGUNTAS	SI	NO	JUSTIFICACIÓN
1. ¿Se ha establecido un plan estratégico para el área de TI?		X	
2. ¿Usted cuenta con políticas de seguridad informática?		X	
3. ¿Usted realiza capacitaciones o brinda nociones acerca de "Seguridad de la Información" en la organización?		X	
4. ¿Existe algún reglamento interno donde se hace mención a la correcta de utilización de activos de información de la organización?		X	
5. ¿Los usuarios tienen conocimiento de cuáles son los activos de información más relevantes de la organización?	X		
6. ¿La organización cuenta con un inventario de activos de información?	X		
7. ¿Existe alguna categorización para los activos de información según su valor, requisitos legales, sensibilidad y criticidad para la organización?		X	
8. ¿Existe alguna asignación de activos de información a los usuarios de acuerdo a las responsabilidades y roles?	X		
9. ¿Se tiene establecido un cronograma o	X		

automatización de copias de seguridad de los datos más relevantes de la organización?	X		
10. ¿Se han implementado políticas y procedimientos de seguridad para salvaguardar los activos de información?	X		
11. ¿Se ha establecido alguna metodología para la identificación y análisis de los riesgos internos y externos de la organización relacionados con los activos de información de TI?		X	
12. ¿Existe alguna bitácora donde se registren los riesgos que hayan causado un impacto comprometiendo los activos de información de la organización?		X	
13. ¿La organización cuenta con una filosofia de riesgos (Apetito de riesgo, Tolerancia de riesgo y Capacidad de riesgo)?		X	
14. ¿La cultura existente en la organización requiere cambiar o mejorar para poder enfrentar de manera efectiva la gestión de riesgos?	X		
15. ¿Se ha elaborado una tasación de las posibles pérdidas económicas que se asumirán si un probable escenario de riesgo de TI se manifiesta?		X	
16. ¿Se hizo un estudio o investigación de los daños experimentados a raíz de la materialización de los riesgos de TI?		X	
17. ¿La organización cuenta con alguna clasificación de los escenarios de riesgos?		X	
18. ¿Se han implantado actividades de control que se deben ejecutar para mitigar los riesgos?		X	
19. ¿Se ha elaborado una guía de procedimientos si es que la materialización de un riesgo causa un impacto significativo en la organización?		X	
20. ¿Se realiza alguna supervisión del perfil de riesgo de la organización?		X	
21. ¿La alta dirección es notificada sobre los riesgos a los que se encuentran comprometidos los activos de información?		X	

DIRECCION REGIONAL DE SALUD AMAZONAS
HOSPITAL MARIA AUXILIADORA - RDO MENDOZA

Ing. Nancy del Caramillo Tupanqui

FIRMA RESPONSABLE DE TI

FIRMA RESPONSABLE DE TESIS
César A. Villegas Rivera

ANEXO Nº 03: GRÁFICOS DE LOS RESULTADOS DEL CUESTIONARIO DE EVALUACIÓN SITUACIONAL REALIZADA A LOS ENCARGADOS DE TECNOLOGÍAS DE LA INFORMACIÓN DE LOS HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

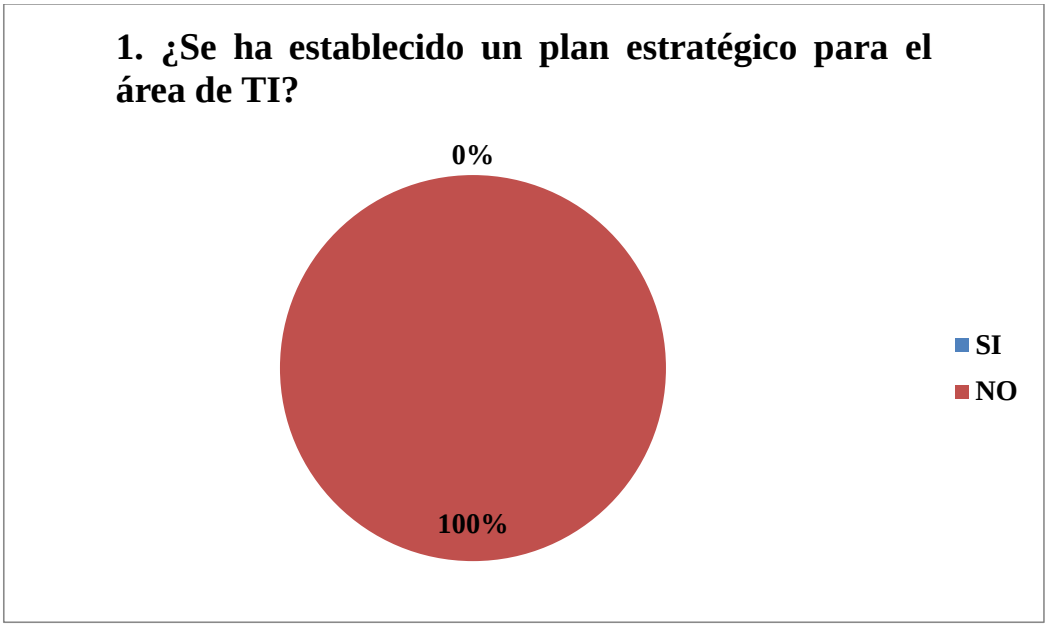


Gráfico 1: ¿Se ha establecido un plan estratégico para el área de TI?

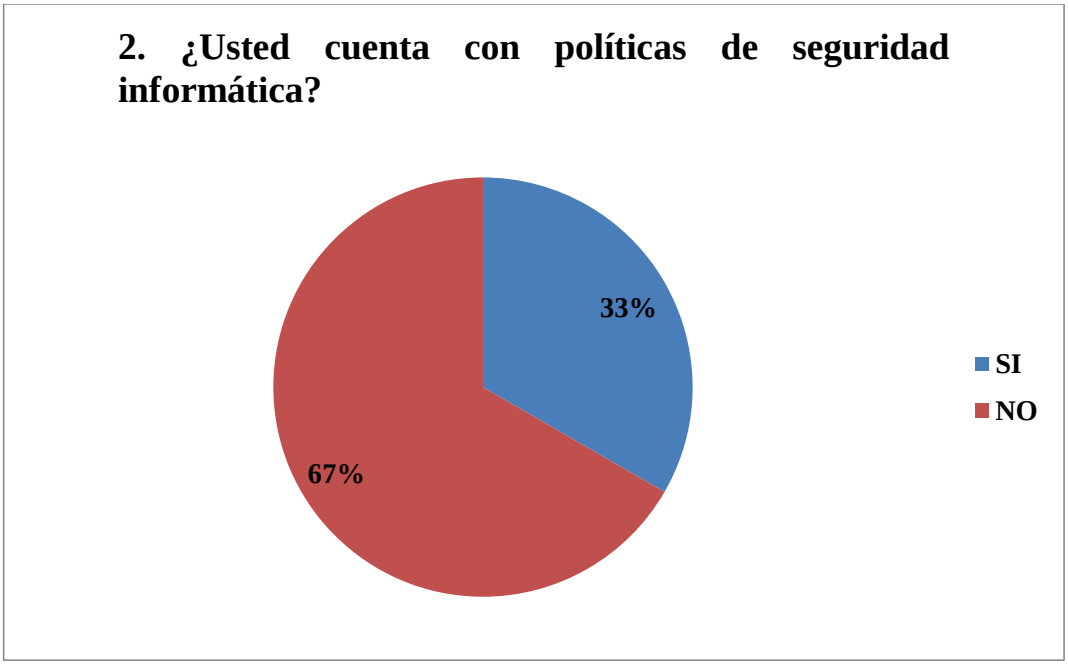


Gráfico 2: ¿Usted cuenta con políticas de seguridad informática?

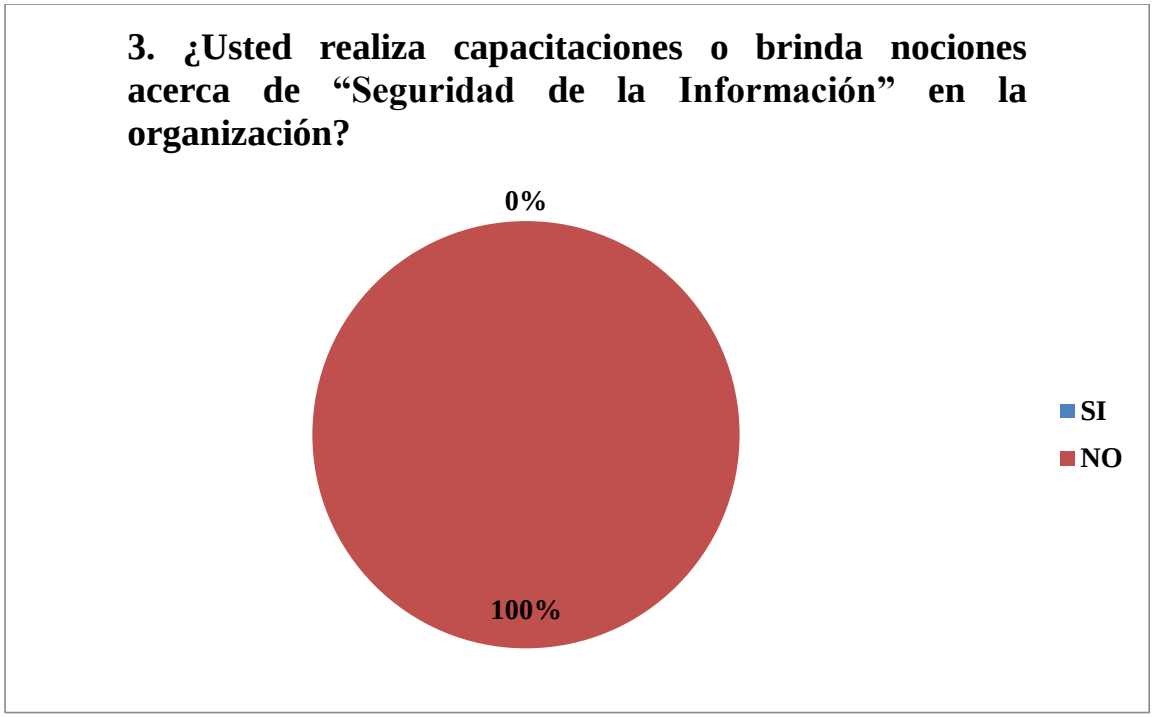


Gráfico 3: ¿Usted realiza capacitaciones o brinda nociones acerca de "Seguridad de la Información" en la organización?

Gráfico 4: ¿Existe algún reglamento interno donde se hace mención a la correcta de utilización de activos de información de la organización?

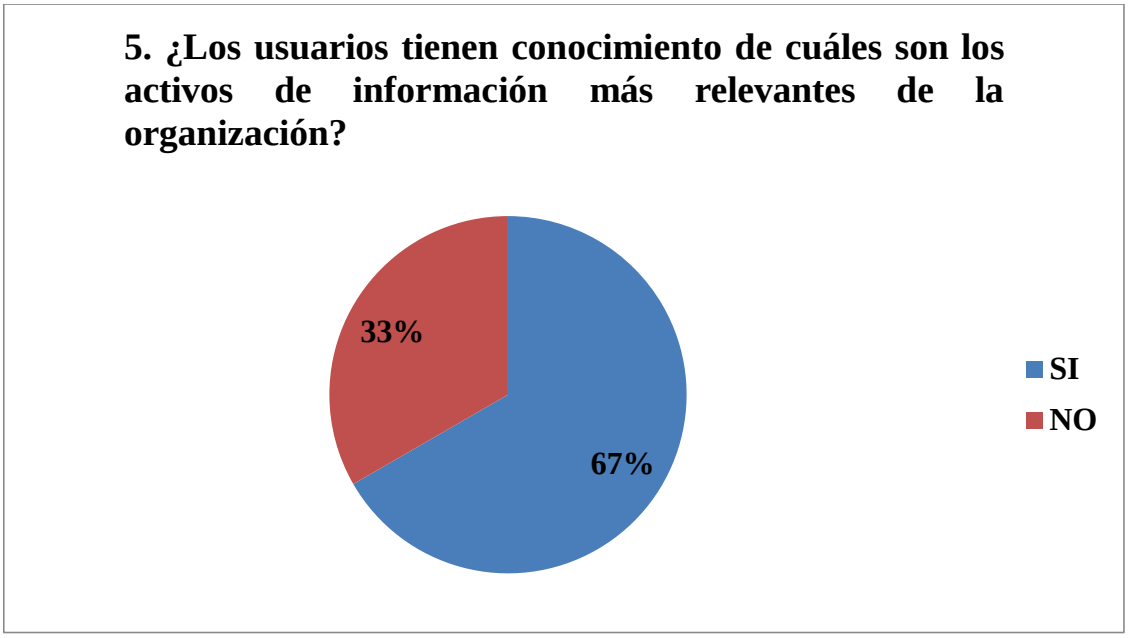


Gráfico 5: ¿Los usuarios tienen conocimiento de cuáles son los activos de información más relevantes de la organización?

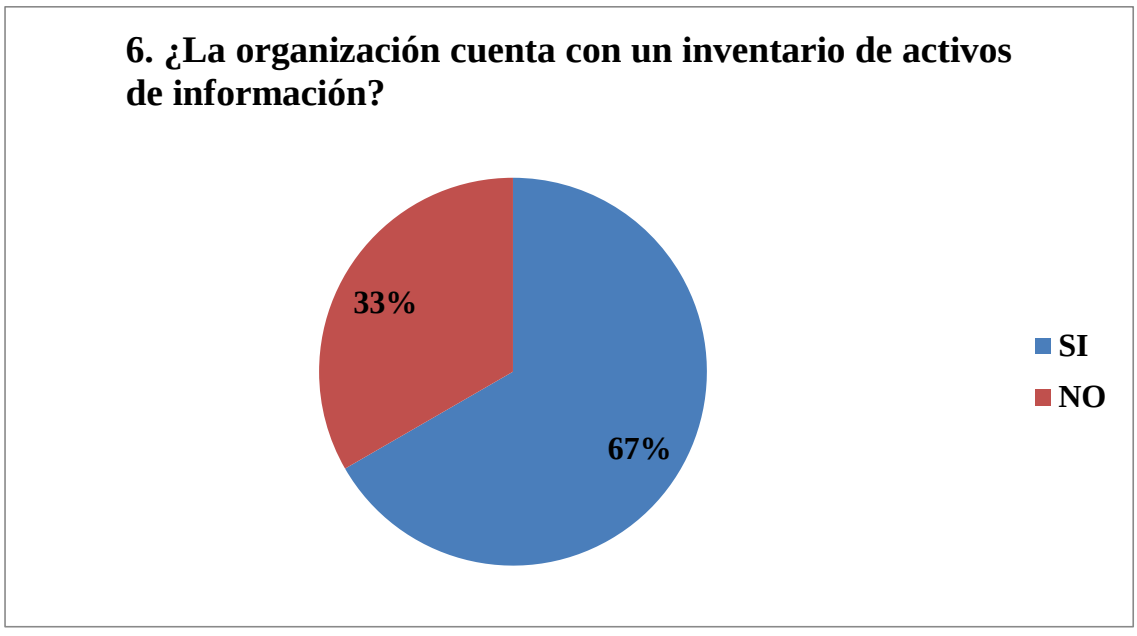


Gráfico 6: ¿La organización cuenta con un inventario de activos de información?

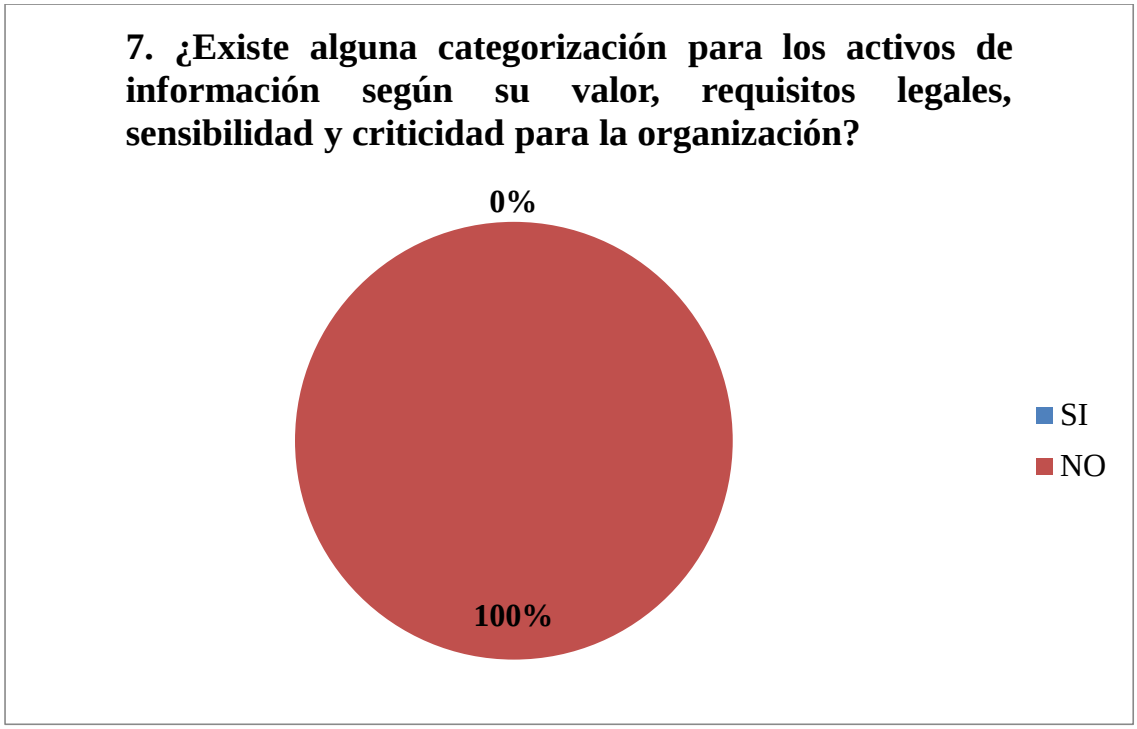


Gráfico 7: ¿Existe alguna categorización para los activos de información según su valor, requisitos legales, sensibilidad y criticidad para la organización?

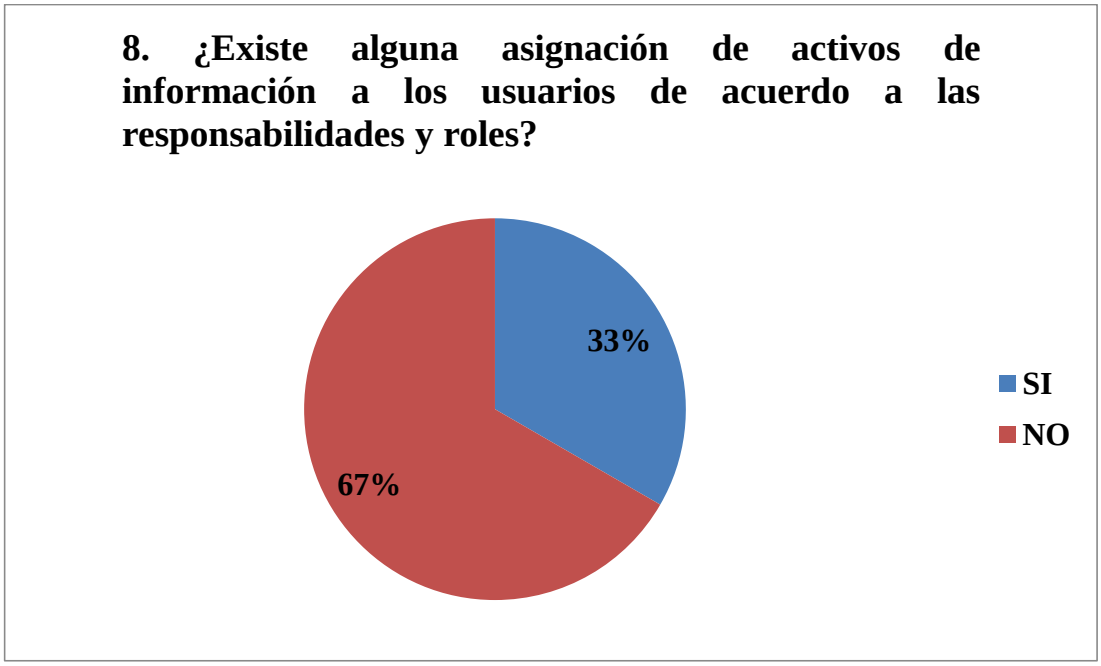


Gráfico 8: ¿Existe alguna asignación de activos de información a los usuarios de acuerdo a las responsabilidades y roles?

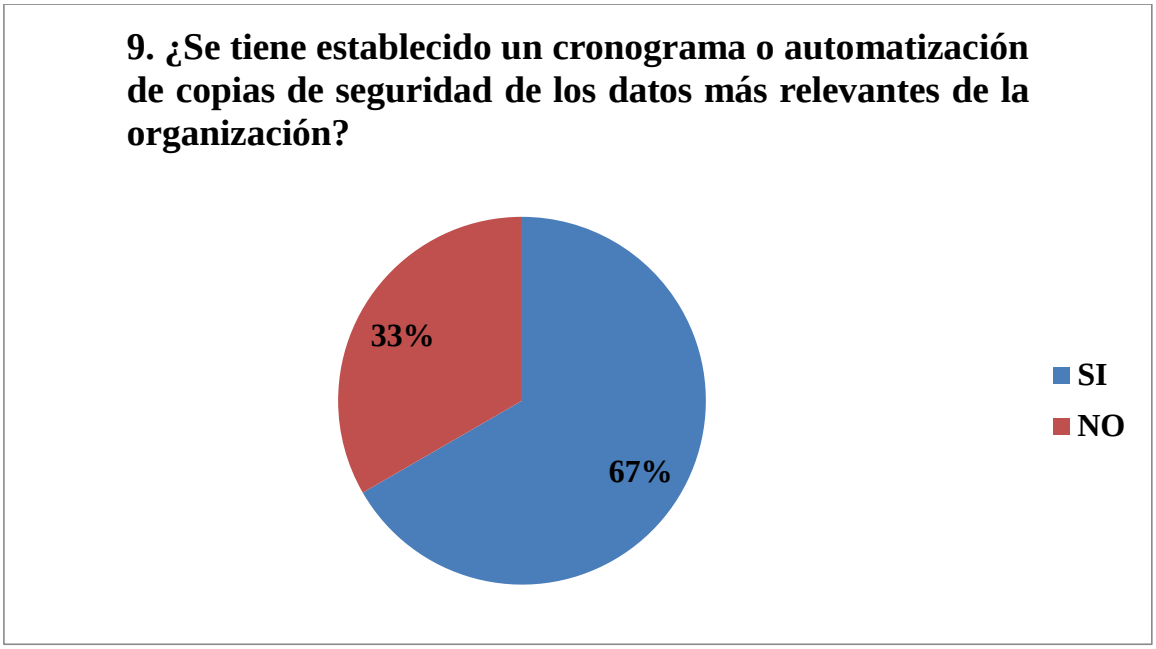


Gráfico 9: ¿Se tiene establecido un cronograma o automatización de copias de seguridad de los datos más relevantes de la organización?

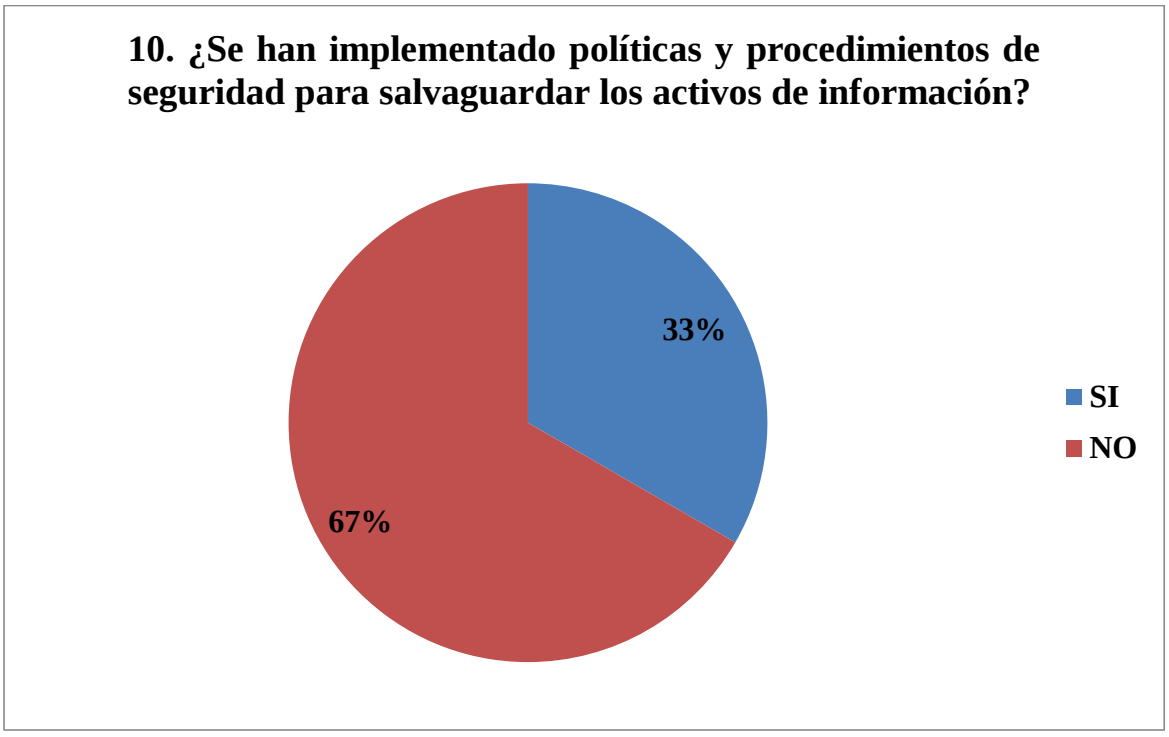


Gráfico 10: ¿Se han implementado políticas y procedimientos de seguridad para salvaguardar los activos de información?

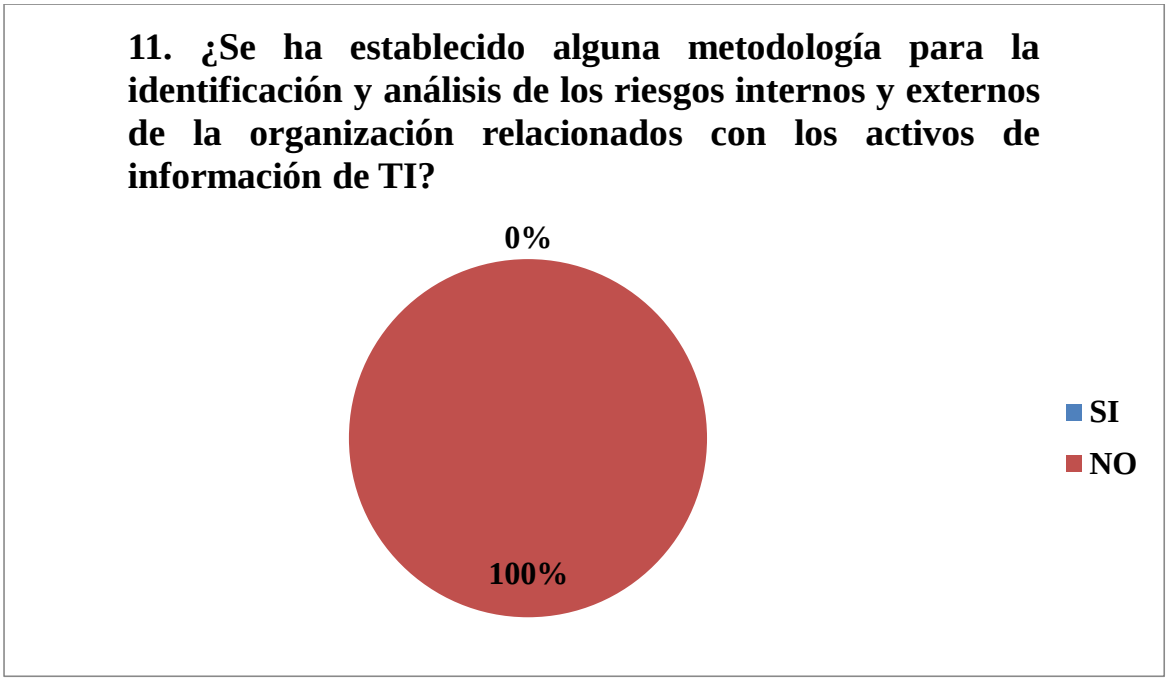


Gráfico 11: ¿Se ha establecido alguna metodología para la identificación y análisis de los riesgos internos y externos de la organización relacionados con los activos de información de TI?

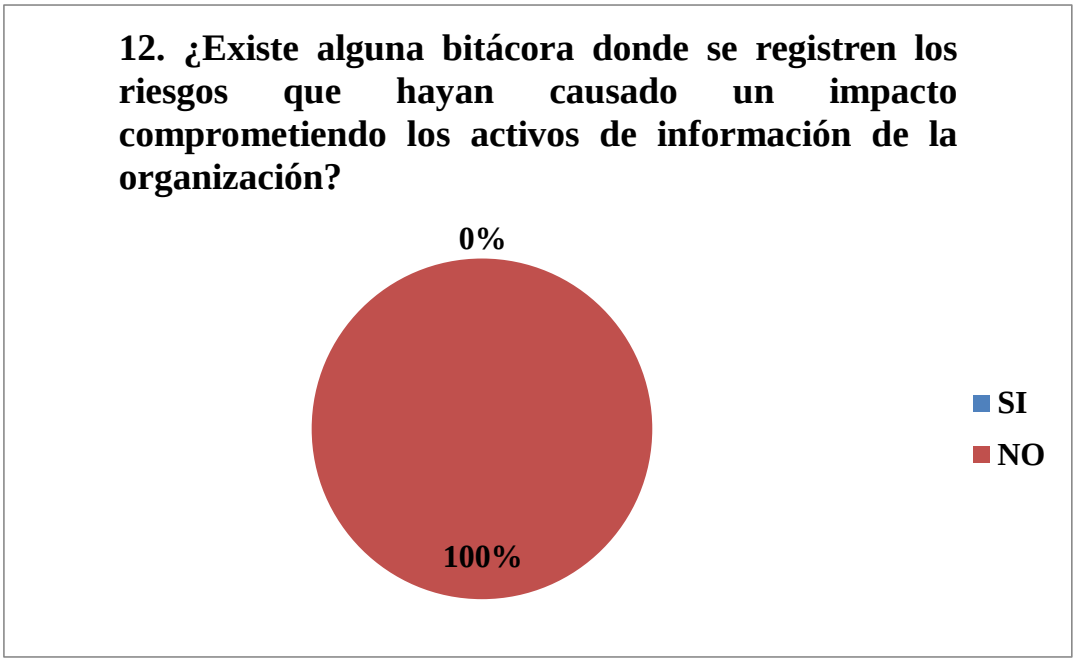


Gráfico 12: ¿Existe alguna bitácora donde se registren los riesgos que hayan causado un impacto comprometiendo los activos de información de la organización?

Gráfico 13: ¿La organización cuenta con una filosofía de riesgos (Apetito de riesgo, Tolerancia de riesgo y Capacidad de riesgo)?

Gráfico 14: ¿La cultura existente en la organización requiere cambiar o mejorar para poder enfrentar de manera efectiva la gestión de riesgos?

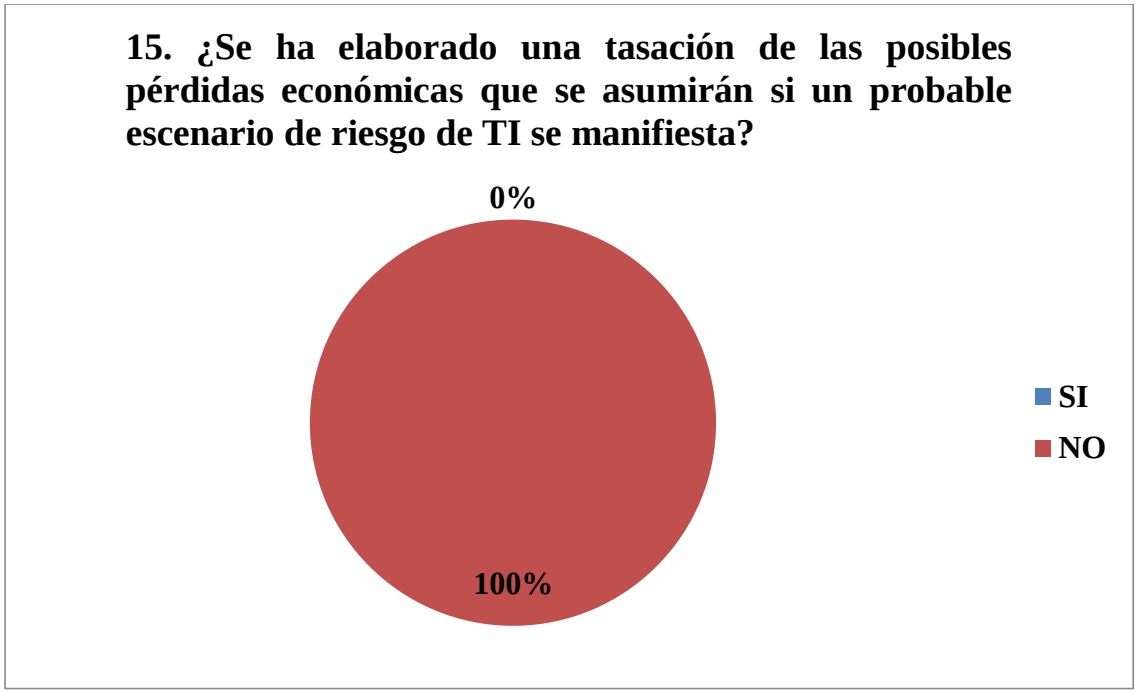


Gráfico 15: ¿Se ha elaborado una tasación de las posibles pérdidas económicas que se asumirán si un probable escenario de riesgo de TI se manifiesta?

Gráfico 16: ¿Se hizo un estudio o investigación de los daños experimentados a raíz de la materialización de los riesgos de TI?

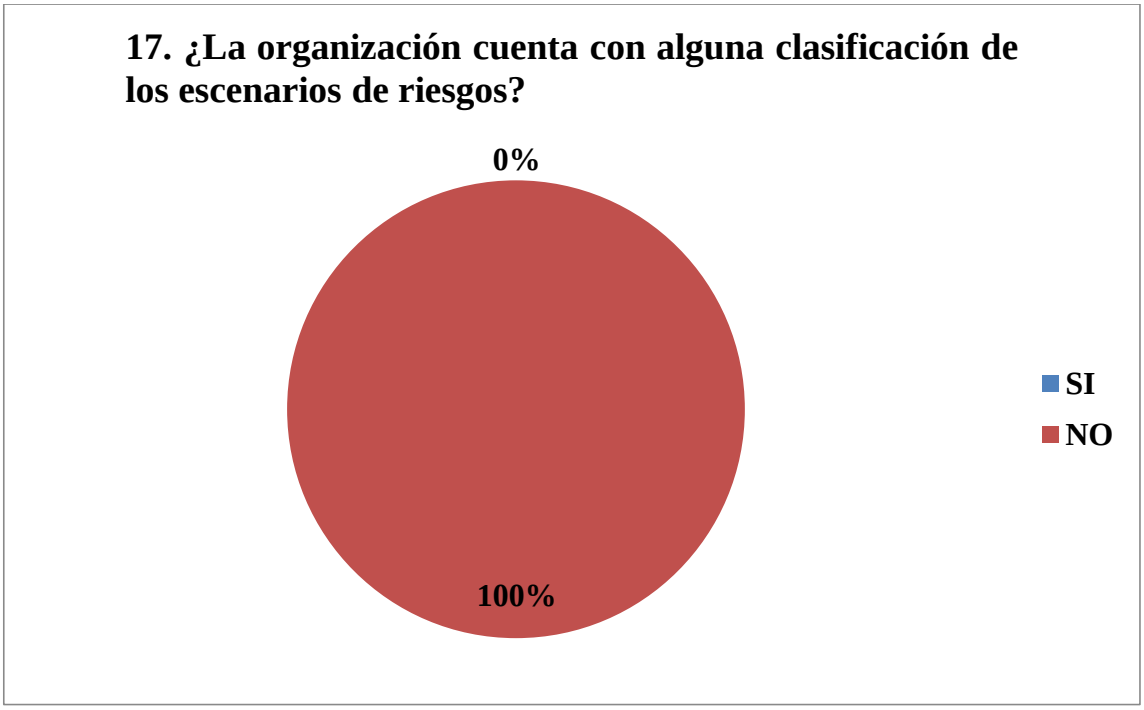


Gráfico 17: ¿La organización cuenta con alguna clasificación de los escenarios de riesgos?

Gráfico 18: ¿Se han implantado actividades de control que se deben ejecutar para mitigar los riesgos?

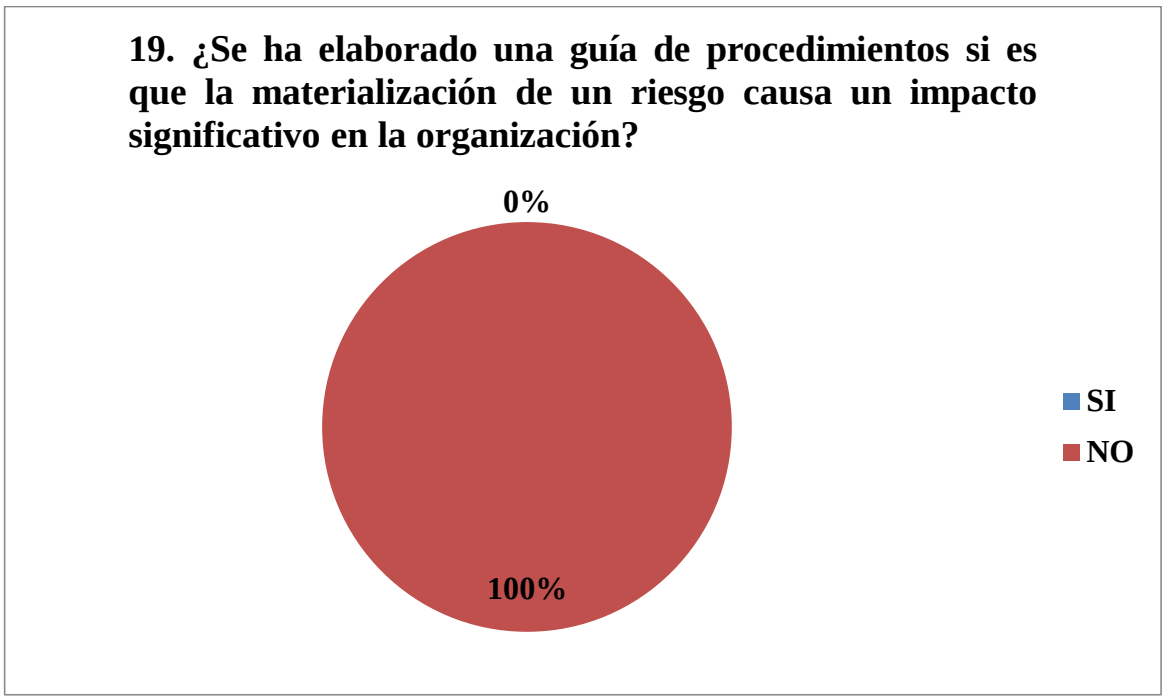


Gráfico 19: ¿Se ha elaborado una guía de procedimientos si es que la materialización de un riesgo causa un impacto significativo en la organización?

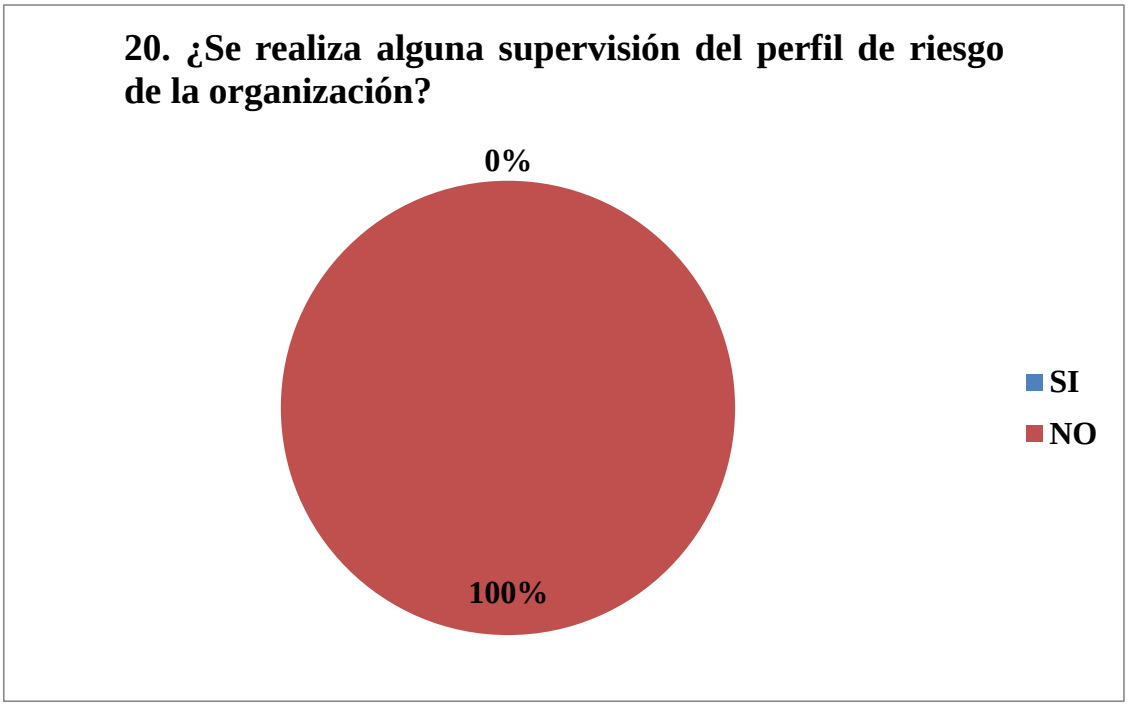


Gráfico 20: ¿Se realiza alguna supervisión del perfil de riesgo de la organización?

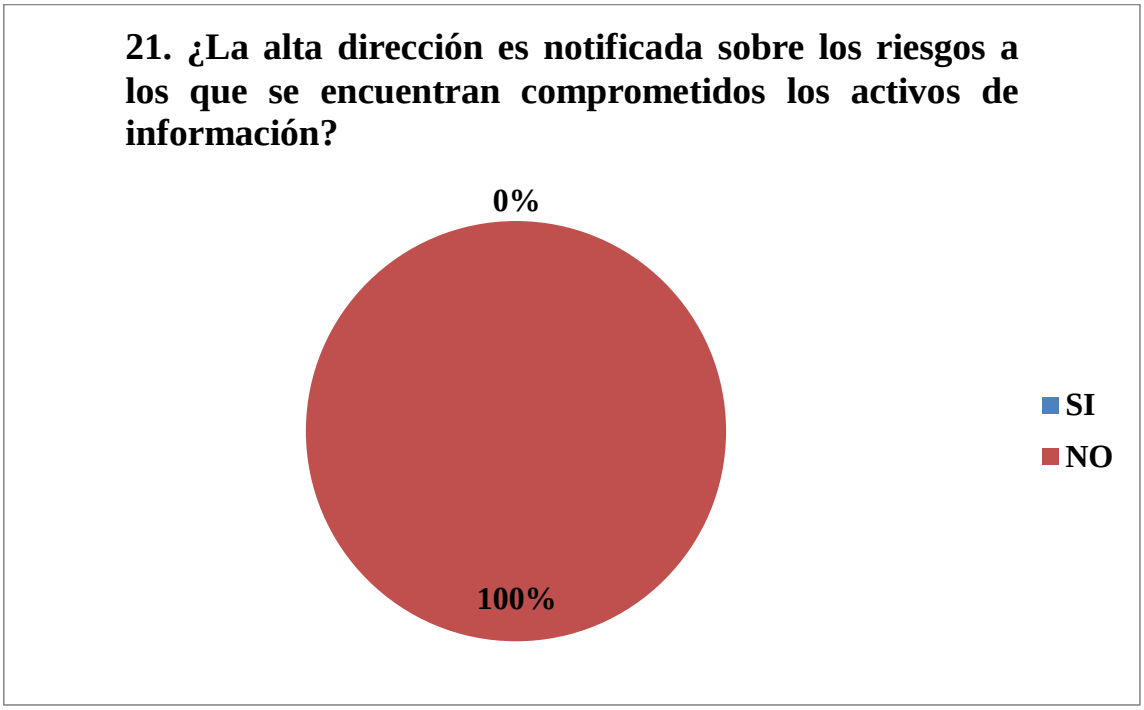


Gráfico 21: ¿La alta dirección es notificada sobre los riesgos a los que se encuentran comprometidos los activos de información?

ANEXO Nº 04: ANÁLISIS DE MARCOS DEL TRABAJO, METODOLOGÍAS Y ESTÁNDARES RELACIONADOS

		ANÁLISIS DE MARCOS DE TRABAJO, METODOLOGÍAS Y ESTÁNDARES					
FASES		**ISO / IEC 31000:2018**	**ISO / IEC 27005:2018**	**MAGERIT 3.0**	**NIST SP 800-30**	**OCTAVE ALLEGRO**	**COBIT 5 para Riesgos**
I	**DEFINIR EL ALCANCE Y CONTEXTO DE LA ORGANIZACIÓN**	**Definir el Alcance:** - Objetivos y decisiones que necesitan ser tomadas. - Resultados esperados de los pasos a ser seguidos en el proceso. - Tiempo, ubicación, inclusiones y exclusiones específicas. - Herramientas y técnicas apropiadas de evaluación del riesgo. - Recursos requeridos, responsabilidades y registros a conservar. - Relaciones con otros proyectos, procesos y actividades.	**Alcance y Límites:** - Los objetivos, estrategias y políticas comerciales estratégicas de la organización. - Procesos comerciales. - Las funciones y la estructura de la organización. - Requisitos legales, reglamentarios y contractuales aplicables a la organización. - La política de seguridad de la información de la organización. - El enfoque general de la organización		**Identificar el Alcance:** - Niveles que son abordados en la evaluación. - Partes de la organización que son afectados por la evaluación y como son afectados. - Decisiones que son apoyadas por los resultados de la evaluación. - Cantidad de tiempo que los resultados de la evaluación son relevantes. - Lo que influye en la necesidad de actualizar la evaluación.		**Alcance de COBIT 5 para Riesgos:** - Se focaliza en la aplicación de los catalizadores de COBIT 5 hacia el riesgo, a través de la perspectiva de la función de riesgos. - Ofrece una guía de alto nivel sobre cómo identificar, analizar y responder al riesgo, a través de la aplicación de los procesos principales de gestión de riesgos en COBIT 5 y mediante el uso de escenarios de riesgos. - Está alineada con fuentes de referencia de ERM en el mercado (estándares, marcos de referencia y guías prácticas) y con

			para la gestión de riesgos. - Activos de información. - Ubicaciones de la organización y sus características geográficas. - Limitaciones que afectan a la organización. - Expectativa de las partes interesadas. - Entorno sociocultural. - Interfaces (es decir, intercambio de información con el entorno).				las iniciativas ERM. COBIT 5 para Riesgos incluye vínculos y comparaciones con las (mayores fuentes de referencia del mercado. - Ofrece un vínculo entre los escenarios de riesgos y los catalizadores de COBIT 5 que pueden ser utilizados para mitigar los riesgos.
		Contexto Interno: - Visión, misión y valores. - La gobernanza, la estructura de la organización, los roles y la rendición de cuentas. - Estrategia, objetivos y políticas. - Cultura de la organización.	**Contexto Interno:** - Gobierno, estructura organizacional, roles y responsabilidades. - Políticas, objetivos y las estrategias que existen para lograrlos. - Las capacidades, entendidas en términos de recursos y conocimiento. - Sistemas de información, flujos de información y procesos de toma de	**Contexto:** - Cultural			**Contexto Interno:** - Metas y objetivos de la empresa. - Importancia estratégica de TI en la empresa. - Complejidad de TI. - Complejidad de la empresa.

			decisiones (tanto formales como informales).				
		- Normas, directrices y modelos adoptados por la organización.	- Relaciones y percepciones y valores de las partes interesadas internas.				- Grado de cambio.
		- Capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, propiedad intelectual, procesos, sistemas y tecnologías).	- Cultura de la organización.	- Social			- Capacidad de gestión del cambio.
		- Datos, sistemas de información y flujos de información.	- Estándares, pautas y modelos adoptados por la organización.				- Filosofía de la gestión de riesgos.
		- Las relaciones con las partes interesadas internas, teniendo en cuenta sus percepciones y valores.	- Forma y alcance de las relaciones contractuales.				- Modelo operativo.
		- Relaciones contractuales y compromisos.	**Contexto Externo:**	- Político			- Prioridades estratégicas.
		- Interdependencias e interconexiones.	- Lo cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y entorno competitivo, ya sea internacional, nacional, regional o				- Cultura empresarial.
		Contexto Externo:		- Obligaciones, legales, reglamentarias y contractuales			- Capacidad financiera.

			local. - Impulsores y tendencias clave que tienen impacto en los objetivos de la organización. - Relaciones y percepciones y valores de partes interesadas externas.				**Contexto Externo:** - Factores de mercado y económicos. - Tasa de cambio del mercado en el que opera la empresa / ciclo de vida del producto. - Ambiente competitivo. - Situación geopolítica. - Ambiente regulatorio. - Estado tecnológico y evolución. - Escenario de amenazas.
		- Factores sociales, culturales, políticos, legales, regulatorios, financieros, tecnológicos, económicos y ambientales ya sea a nivel internacional, nacional, regional o local. - Impulsores clave y las tendencias que afectan los objetivos de la organización. - Relaciones, percepciones, valores, necesidades y expectativas de las partes interesadas externas. - Relaciones contractuales y compromisos. - Complejidad de redes y dependencias.		- Competencia			
		Definir Criterios del Riesgo: - La naturaleza y los tipos de las incertidumbres que	**Criterios Básicos:** - Enfoque de Gestión de Riesgos		**Factores de Riesgo:** - Amenaza - Vulnerabilidad	**Actividad 1:** Defina un conjunto de medidas cualitativas (criterios de medición	**Capacidades de la gestión de riesgos:** - Gobierno del riesgo. - Gestión del riesgo.

		pueden afectar a los resultados y objetivos (tanto tangibles como intangibles). - Cómo se van a definir y medir las consecuencias (tanto positivas como negativas) y la probabilidad. - Factores relacionados con el tiempo. - Coherencia en el uso de mediciones. - Cómo se va determinar el nivel de riesgo. - Cómo se tendrán en cuenta las combinaciones y secuencias de riesgos múltiples. - Capacidad de la organización.	- Criterios de Evaluación de Riesgos - Criterios de Impacto - Criterios de Aceptación de Riesgos		- Impacto - Probabilidad - Condición predisponente **Enfoque de Evaluación:** - Cuantitativo - Cualitativo - Semicuantitativo **Enfoque de Análisis:** - Orientado a la amenaza - Orientado al activo / impacto - Orientado a la vulnerabilidad	de riesgo) contra las cuales podrá evaluar el efecto de un riesgo en la misión y los objetivos comerciales de su organización. Como mínimo, considere las siguientes áreas de impacto: - Reputación / Confianza del cliente - Financiero - Productividad - Seguridad y salud - Multas / Sanciones legales - Área de impacto definida por el usuario. **Actividad 2:** Priorizar las áreas de impacto de la más importante a la menos importante. La categoría más importante debe recibir la puntuación más alta y la menos importante la más baja.	**Capacidades relacionadas con TI:** - Evaluar, dirigir y supervisar (EDM). - Alinear, planificar y organizar (APO). - Construir, adquirir e implementar (BAI). - Entregar, dar servicio y soporte (DSS). - Supervisar, evaluar y valorar (MEA).

II	**IDENTIFICACIÓN DE ACTIVOS**		**IDENTIFICACIÓN DE ACTIVOS** **Entrada:** - Alcance y límites para la evaluación de riesgos a realizar, lista de componentes con los propietarios, ubicación, función, etc. **Acción:** - Deben identificarse los activos dentro del alcance establecido. **Guía de Implementación** **Salida:** - Una lista de activos para gestionar los riesgos y una lista de procesos empresariales relacionados con los activos y su relevancia. **Valoración de Activos:** - Confidencialidad - Integridad	**Identificación de los Activos:** - Activos esenciales: La información que maneja y los servicios que presta. - Activos relevantes: Datos, Servicios auxiliares, Aplicaciones informáticas, Equipos Informáticos, Soportes de Información, Equipamiento auxiliar, Redes de Comuniación, Instalaciones y Personas. **Caracterización de los Activos:** - Valoración de los Activos **Dependencias entre Activos:** - Activos esenciales. - Servicios internos. - Equipamiento informático. - Activos del entorno. - Servicios subcontratados a terceros.	**Valoración de Activos:** - Confidencialidad - Integridad - Disponibilidad - - - - - - - -	**Establecer Perfiles de Activos:** - Desarrollo de Perfiles de Activos de Información. - Identificación de Contenedores de Activos de Información. -	**Activo / recurso:** - Personas y habilidades. - Estructuras organizativas. - Procesos de TI. - Infraestructura física, instalaciones, equipo, etc. - Infraestructura de TI, incluyendo hardware, infraestructura de redes y middleware. - Otros componentes de arquitectura de la empresa, incluyendo información y aplicaciones.

			- Disponibilidad - No Repudio - Responsabilidad - Autenticidad - Confiabilidad	- Instalaciones físicas. - Personal. **Valoración de Activos:** - Disponibilidad - Integridad - Confidencialidad - Autenticidad - Trazabilidad	-		
III	**EVALUACIÓN DEL RIESGO**	**Identificación del Riesgo:** - Fuentes de riesgos tangibles e intangibles. - Causas y eventos. - Amenazas y oportunidades. - Vulnerabilidades y capacidades. - Cambios en el contexto externo e interno. - Indicadores de riesgos emergentes. - Naturaleza y valor de los activos y recursos. - Consecuencias y su impacto en los objetivos.	**Identificación del Riesgo:** - Identificación de Amenazas. - Identificación de Controles Existentes. - Identificación de Vulnerabilidades. - Identificación de Consecuencias.	**Caracterización de las Amenazas:** - Identificación de las Amenazas **Caracterización de las Salvaguardas:** -Identificación de las Salvaguardas Pertinentes.	**Realizar la Evaluación:** - - Identificar Fuentes de Amenaza - Identificar Eventos de Amenaza - Identificar Vulnerabilidades y Condiciones predisponentes. -	**Identificar Riesgos:** - - Identificación de Riesgos. - Análisis de Riesgos. - **Identificar Amenazas:** - Identificación de Áreas de Preocupación. - Identificación de Escenarios de Amenaza. -	**Identificar el Riesgo:** - Consta de los siguientes elementos: Control, Valor y Condición de Amenaza que impone un nivel notable de riesgo de TI. - Incluye prácticas de gestión para identificar los riesgos asociados con los productos y servicios clave de la organización que dependen de TI, y para identificar factores de riesgo que contribuyen a los incidentes y eventos históricos.

		- Limitaciones de conocimiento y confiabilidad de la información. - Factores relacionados con el tiempo. - Sesgos, suposiciones y creencias de las personas involucradas.			- - - - - -		- Incluye técnicas específicas para identificar escenarios basados en un actor, tipo de amenaza, evento, recursos / activos y una dimensión de tiempo. - COBIT 5 para Riesgos también utiliza el desarrollo de escenarios para identificar riesgos.
		Análisis del Riesgo: - Probabilidad de eventos y de las consecuencias. - Naturaleza y magnitud de las consecuencias. - Complejidad y la interconexión. - Factores relacionados con el tiempo y la volatilidad. - Eficacia de los controles existentes. - Niveles de sensibilidad y de confianza.	**Análisis del Riesgo:** - Metodologías de Análisis de Riesgos. - Evaluación de consecuencias. - Evaluación de Probabilidad de Incidentes. - Nivel de Determinación del Riesgo.	**Estimación del Estado de Riesgo:** - Estimación del Impacto - Estimación del Riesgo	**Realizar la Evaluación:** - Determinar la Probabilidad - Determinar el Impacto - Determinar el Riesgo	**ANALIZAR EL RIESGO** **Metodología:** - Cualitativo **Valor de Impacto** **Requerimientos de Seguridad**	**Analizar el Riesgo:** - El análisis del riesgo es el proceso que estima la frecuencia y el impacto de los escenarios de riesgo de TI.
		Valoración del	**Evaluación del**	**Caracterización de**			**Valorar el Riesgo:**

		Riesgo: - No hacer nada más. - Considerar opciones de tratamiento de riesgo. - Emprender un análisis adicional para comprender mejor el riesgo. - Mantener los controles existentes. - Reconsiderar objetivos.	**Riesgo:** - Entrada: Una lista de riesgos con niveles de valor asignados y criterios de evaluación de riesgos. - Acción: El nivel de riesgos debe compararse con los criterios de evaluación de riesgos y los criterios de aceptación de riesgos. - Guía de Implementación. - Salida: Una lista de riesgos priorizados de acuerdo con los criterios de evaluación de riesgos en relación con los escenarios de incidentes que conducen a esos riesgos.	**las Amenazas:** - Valoración de las Amenazas **Caracterización de las Salvaguardas:** - Valoración de las Salvaguardas			- Aborda esta fase del proceso en forma intrínseca. - Evalúa los riesgos de acuerdo a "la tolerancia al riesgo de la gerencia con respecto al apetito de riesgo del consejo directivo". - Utiliza un mapa de riesgos para priorizar y mostrar gráficamente los riesgos por rangos definidos de frecuencia e impacto.
IV	**TRATAMIENTO DEL RIESGO**	**Seleccionar Opciones de Tratamiento del Riesgo** - Evitar el riesgo decidiendo no iniciar o continuar con la actividad que genera el riesgo. - Aceptar o aumentar el riesgo en busca de una oportunidad.	**Tratamiento del Riesgo:** - Descripción general del tratamiento de riesgo - Modificación del Riesgo. - Retención de Riesgos. - Evitación de Riesgos.	**Opciones de Tratamiento del Riesgo:** - Aceptación - Eliminación - Mitigación - Compartición		**IDENTIFICAR Y MITIGAR RIESGOS** **Selección de Enfoque de Mitigación:** - Aceptar - Postergar - Mitigar	**Seleccionar Opciones de Tratamiento del Riesgo:** - Incluye una guía sobre las opciones comunes de respuesta y cómo se aplican en un contexto de TI. - La sección 2B describe los tratamientos de los

		- Eliminar la fuente del riesgo. - Modificar la probabilidad. - Modificar las consecuencias. - Compartir el riesgo (por ejemplo, a través de contratos, compra de seguros). - Retener el riesgo con base en una decisión informada.	- Riesgo Compartido.	- Financiación		- Transferir	riesgos identificados. Estos son: • Evitar los riesgos. • Reducir/mitigar los riesgos. • Compartir/transferir los riesgos. • Aceptar los riesgos.
		Preparar e Implementar Planes de Tratamiento del Riesgo - El fundamento de la selección de las opciones para el tratamiento, incluyendo los beneficios esperados. - Las personas que rinden cuentas y aquellas responsables de la aprobación e implementación del plan. - Acciones propuestas.	**Aceptación del Riesgo:** - Entrada: El plan de tratamiento de riesgos y la evaluación de riesgos residuales están sujetos a la decisión de aceptación de los gerentes de la organización. - Acción: La decisión de aceptar los riesgos y las responsabilidades de la decisión debe tomarse y registrarse formalmente.				**Preparar e Implementar Planes de Tratamiento del Riesgo:** - Define respuestas específicas al riesgo para abordar diferentes tratamientos del riesgo (sección 2B, subsección 5.2). - Utiliza desarrollo de escenarios para la identificación de riesgos.

		- Recursos necesarios, incluyendo las contingencias. - Medidas de rendimiento desempeño. - Restricciones. - Informes y seguimiento requeridos. - Plazos previstos para la realización y la finalización de las acciones.	- Guía de Implementación. - Salida: Una lista de riesgos aceptados con justificación para aquellos que no cumplen con los criterios normales de aceptación de riesgos de la organización.				
V	**SEGUIMIENTO Y EVALUACIÓN**	**Seguimiento y Revisión**	**Comunicación y Consulta de Riesgos:** - Entrada: Toda la información de riesgos obtenida de las actividades de gestión de riesgos. - Acción: La información sobre el riesgo debe intercambiarse y / o compartirse entre el tomador de decisiones y otras partes interesadas. - Guía de Implementación. - Salida: Comprensión continua del proceso y los resultados de la gestión de riesgos de seguridad de la información de la		**Mantener la Evaluación:** - Monitorear los Factores de Riesgo - Actualizar la Evaluación del Riesgo		**Comunicación y Consulta de Riesgos:** - Principio 1: Satisfacer las necesidades de las partes interesadas. - El habilitador "Información" incluye información específica para ser comunicada entre las partes interesadas. **Supervisión y Revisión:** - Incluye metas y métricas que pueden ser utilizadas para medir el desempeño, y un modelo de madurez para establecer una hoja de ruta para mejorar el

			organización. **<u>Monitoreo y Revisión de Riesgos:</u>** - Seguimiento y revisión de los factores de riesgo. - Seguimiento, revisión y mejora de la gestión de riesgos.				proceso de gestión de riesgos.

ANEXO Nº 05: PROPUESTA DE MODELO

MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS											
FASES		**PROCESOS**	**SUB PROCESO**	**ISO / IEC 31000:2018**	**ISO / IEC 27005:2018**	**MAGERIT 3.0**	**NIST SP 800-30**	**OCTAVE ALLEGRO**	**COBIT 5 para Riesgos**	**METODOLOGÍA SELECCIONADA**	**JUSTIFICACIÓN**
I	**DEFINIR EL ALCANCE Y CONTEXTO DE LA ORGANIZACIÓN**	**1. DEFINIR EL ALCANCE**		CUMPLE	CUMPLE	NO CONTIENE INFORMACIÓN	CUMPLE	NO CONTIENE INFORMACIÓN	CUMPLE	COBIT 5 para Riegos	Determina que el Alcance "debe estar integrado en los procesos normales para formar parte de las prácticas de gestión diaria logrando proporcionar la seguridad necesaria a las partes interesadas".
		2. IDENTIFICACIÓN DEL CONTEXTO INTERNO Y EXTERNO		CUMPLE	CUMPLE	CUMPLE	NO CONTIENE INFORMACIÓN	NO CONTIENE INFORMACIÓN	CUMPLE	ISO 31000	El contexto del proceso de la gestión del riesgo se debería establecer a partir de la comprensión de los entornos externo e interno en los cuales opera la organización y debería reflejar el entorno específico de la actividad en la cual se va a aplicar el proceso de la gestión del riesgo.
II	**IDENTIFICACIÓN DE ACTIVOS**	**3. IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS**		NO CONTIENE INFORMACIÓN	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	MAGERIT	Ofrece un catálogo de los distintos tipos de activos, que puede ser utilizado como guía para clasificar los activos que son críticos para los hospitales.
		4. VALORACIÓN DE ACTIVOS	**De acuerdo a las Dimensiones de Valoración y Escalas Estándar**	NO CONTIENE INFORMACIÓN	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	MAGERIT	A diferencia de otras metodologías, establece un conjunto de dimensiones con sus respectivas escalas estándar para complementar un buena valoración de activos
			De acuerdo al Impacto	NO CONTIENE INFORMACIÓN	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	Definición propia	Después de analizar las distintas metodologías, se elaboró una tabla (para la valoración de acuerdo al impacto) que se ajuste más al contexto del sector salud.
III	**EVALUACION DEL RIESGO**	**5. IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS**	**Identificación de Amenazas**	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	MAGERIT	Ofrece un catálogo de los distintos tipos de amenazas, que puede ser utilizado como guía para la identificación de Amenazas en los hospitales.
			Valoración de Amenazas	NO CONTIENE INFORMACIÓN	NO CONTIENE INFORMACIÓN	CUMPLE	NO CONTIENE INFORMACIÓN	NO CONTIENE INFORMACIÓN	NO CONTIENE INFORMACIÓN	Definición propia	Después de analizar las distintas metodologías, se elaboró una tabla (para determinar la frecuencia o probabilidad de ocurrencia de las amenazas) que se ajuste más al contexto del sector salud.
		6. IDENTIFICACIÓN, ANÁLISIS Y VALORACIÓN DEL RIESGO	**Identificación y Análisis del Riesgo**	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	CUMPLE	MAGERIT	Ofrece una tabla sencilla e intuitiva que sirve para calcular el riesgo mediante la probabilidad y el impacto.
			Valoración del Riesgo	CUMPLE	CUMPLE	NO CONTIENE INFORMACIÓN	CUMPLE	CUMPLE	CUMPLE	COBIT 5 para Riegos	Establece la evaluación de los riesgos mediante el uso de un mapa de riesgos y la definición del apetito, la tolerancia y la capacidad del riesgo en la organización.
IV	**TRATAMIENTO DEL RIESGO**	**7. OPCIONES DE TRATAMIENTO DEL RIESGO**		CUMPLE	CUMPLE	CUMPLE	NO CONTIENE INFORMACIÓN	CUMPLE	CUMPLE	COBIT 5 para Riegos	Establece un conjunto de opciones para el tratamiento de los riesgos más adecuados para los hospitales.
		8. IMPLEMENTAR PLANES DE TRATAMIENTO DEL RIESGO		CUMPLE	CUMPLE	PARCIAL	NO CONTIENE INFORMACIÓN	NO CONTIENE INFORMACIÓN	CUMPLE	MAGERIT	Ofrece un catálogo de los distintos tipos de salvaguardas, que puede ser utilizado como guía para la implementación del tratamiento de los riesgos.
V	**SEGUIMIENTO Y EVALUACIÓN**	**9. MONITOREAR Y REVISAR LOS RIESGOS**		CUMPLE	CUMPLE	CUMPLE	CUMPLE	NO CONTIENE INFORMACIÓN	CUMPLE	ISO 27005	Declara que los riesgos y sus factores (el valor de los activos, los impactos, las amenazas, las vulnerabilidades y la probabilidad de ocurrencia) se deben monitorear y revisar periódicamente con el objetivo de identificar los cambios que sufre la organización desde una etapa inicial,

ANEXO Nº 06: CATÁLOGO SEGÚN LOS TIPOS DE ACTIVOS PROPUESTO POR MAGERIT

CATÁLOGO DE TIPOS DE ACTIVO		
TIPO	**DESCRIPCIÓN**	**ACTIVOS**
[D] Datos / Información	Los datos son los fundamentos que permite a una organización prestar sus servicios. La información es un activo abstracto que será almacenado en equipos o soportes de información (normalmente agrupado como ficheros o bases de datos) o será transferido de un lugar a otro por los medios de transmisión de datos.	[files] ficheros. [backup] copias de respaldo. [conf] datos de configuración. [int] datos de gestión interna. [password] credenciales (ej. contraseñas) [auth] datos de validación de credenciales. [acl] datos de control de acceso. [log] registro de actividad. [source] código fuente. [exe] código ejecutable. [test] datos de prueba.
[S] Servicios	Función que satisface una necesidad de los usuarios (del servicio). Esta sección contempla servicios prestados por el sistema.	[anon] anónimo (sin requerir identificación del usuario) [pub] al público en general (sin relación contractual). [ext] a usuarios externos (bajo una relación contractual). [int] interno (a usuarios de la propia organización).
[SW] Software - Aplicaciones informáticas	Con múltiples denominaciones (programas, aplicativos, desarrollos, etc.) este epígrafe se refiere a tareas que han sido automatizadas para su desempeño por un equipo informático. Las aplicaciones gestionan, analizan y transforman los datos permitiendo la explotación de la información para la prestación de los servicios.	[prp] desarrollo propio (in house). [sub] desarrollo a medida (subcontratado). [std] estándar (off the shelf). [browser] navegador web. [www] servidor de presentación. [app] servidor de aplicaciones. [email_client] cliente de correo electrónico. [email_server] servidor de correo electrónico. [file] servidor de ficheros. [dbms] sistema de gestión de bases de datos. [tm] monitor transaccional. [office] ofimática. [av] anti virus. [os] sistema operativo. [hypervisor] gestor de máquinas virtuales. [ts] servidor de terminales. [backup] sistema de backup.

CATÁLOGO DE TIPOS DE ACTIVO		
TIPO	**DESCRIPCIÓN**	**ACTIVOS**
[HW] Equipamiento informático (hardware)	Dícese de los medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización, siendo pues depositarios temporales o permanentes de los datos, soporte de ejecución de las aplicaciones informáticas o responsables del procesado o la transmisión de datos.	[host] grandes equipos. [mid] equipos medios. [pc] informática personal. [mobile] informática móvil. [pda] agendas electrónicas. [vhost] equipo virtual. [backup] equipamiento de respaldo. [peripheral] periféricos. [print] medios de impresión. [scan] escáneres. [crypto] dispositivos criptográficos. [bp] dispositivo de frontera. [network] soporte de la red. [modem] módems. [hub] concentradores. [switch] conmutadores. [router] encaminadores. [bridge] pasarelas. [firewall] cortafuegos. [wap] punto de acceso inalámbrico. [pabx] centralita telefónica. [ipphone] teléfono IP.
[COM] Redes de comunicaciones	Incluyendo tanto instalaciones dedicadas como servicios de comunicaciones contratados a terceros; pero siempre centrándose en que son medios de transporte que llevan datos de un sitio a otro.	[PSTN] red telefónica. [ISDN] rdsi (red digital). [X25] X25 (red de datos). [ADSL] ADSL. [pp] punto a punto. [radio] comunicaciones radio. [wifi] red inalámbrica. [mobile] telefonía móvil. [sat] por satélite. [LAN] red local. [MAN] red metropolitana. [Internet] Internet.
[Media] Soportes de información	En este epígrafe se consideran dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo.	[electronic] electrónicos. [disk] discos. [vdisk] discos virtuales. [san] almacenamiento en red. [disquette] disquetes. [cd] cederrón (CD-ROM). [usb] memorias USB. [dvd] DVD. [tape] cinta magnética. [mc] tarjetas de memoria. [ic] tarjetas inteligentes.

CATÁLOGO DE TIPOS DE ACTIVO		
TIPO	**DESCRIPCIÓN**	**ACTIVOS**
		[non_electronic] no electrónicos. [printed] material impreso. [tape] cinta de papel. [film] microfilm. [cards] tarjetas perforadas.
[AUX] Equipamiento auxiliar	En este epígrafe se consideran otros equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos.	[power] fuentes de alimentación. [ups] sistemas de alimentación ininterrumpida. [gen] generadores eléctricos. [ac] equipos de climatización. [cabling] cableado. [wire] cable eléctrico. [fiber] fibra óptica. [robot] robots. [tape] ... de cintas. [disk] ... de discos. [supply] suministros esenciales. [destroy] equipos de destrucción de soportes de información. [furniture] mobiliario: armarios, etc. [safe] cajas fuertes.
[L] Instalaciones	En este epígrafe entran los lugares donde se hospedan los sistemas de información y comunicaciones.	[site] recinto. [building] edificio. [local] cuarto. [mobile] plataformas móviles. [car] vehículo terrestre: coche, camión, etc. [plane] vehículo aéreo: avión, etc. [ship] vehículo marítimo: buque, lancha, etc. [shelter] contenedores. [channel] canalización. [backup] instalaciones de respaldo
[P] Personal	En este epígrafe aparecen las personas relacionadas con los sistemas de información.	[ue] usuarios externos. [ui] usuarios internos. [op] operadores. [adm] administradores de sistemas. [com] administradores de comunicaciones. [dba] administradores de BBDD. [sec] administradores de seguridad. [des] desarrolladores / programadores. [sub] subcontratas. [prov] proveedores.

ANEXO Nº 07: ESCALAS ESTÁNDAR PROPUESTAS POR MAGERIT

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo
[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad		
10	10.si	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u

		organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas
[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	9.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización
[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales
[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] Administración y gestión		
9	9.adm	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre

7	7.adm	probablemente impediría la operación efectiva de la Organización
5	5.adm	probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	pudiera impedir la operación efectiva de una parte de la Organización
[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

ANEXO Nº 08: CATÁLOGO DE SALVAGUARDAS PROPUESTO POR MAGERIT

CATÁLOGO DE SALVAGUARDAS		
TIPO	**NOMENCLATURA**	**DESCRIPCIÓN**
Protecciones Generales	H	Protecciones generales
	H.IA	Identificación y autenticación
	H.IR	Gestión de incidencias
	H.tools	Herramientas de seguridad
	H.tools.AV	Herramienta contra código dañino
	H.tools.IDS	IDS/IPS: Herramienta de detección / prevención de intrusión
	H.tools.VA	Herramienta de análisis de vulnerabilidades
	H.tools.SFV	Verificación de las funciones de seguridad
	H.VM	Gestión de vulnerabilidades
Protección de los datos / información	D	Protección de la Información
	D.A	Copias de seguridad de los datos (backup)
	D.I	Aseguramiento de la integridad
	D.C	Cifrado de la información
Protección de los servicios	S	Protección de los Servicios
	S.A	Aseguramiento de la disponibilidad
	S.start	Aceptación y puesta en operación
	S.SC	Se aplican perfiles de seguridad
	S.CM	Gestión de cambios (mejoras y sustituciones)
	S.end	Terminación
	S.www	Protección de servicios y aplicaciones web
	S.dns	Protección del servidor de nombres de dominio (DNS)
	S.TW	Teletrabajo
Protección de las aplicaciones (software)	SW	Protección de las Aplicaciones Informáticas
	SW.A	Copias de seguridad (backup)
	SW.SC	Se aplican perfiles de seguridad
	SW.CM	Cambios (actualizaciones y mantenimiento)
Protección de los equipos (hardware)	HW	Protección de los Equipos Informáticos
	HW.SC	Se aplican perfiles de seguridad
	HW.A	Aseguramiento de la disponibilidad
	HW.CM	Cambios (actualizaciones y mantenimiento)
	HW.print	Reproducción de documentos
Protección de las comunicaciones	COM	Protección de las Comunicaciones
	COM.SC	Se aplican perfiles de seguridad

CATÁLOGO DE SALVAGUARDAS		
TIPO	**NOMENCLATURA**	**DESCRIPCIÓN**
	COM.A	Aseguramiento de la disponibilidad
	COM.I	Protección de la integridad de los datos intercambiados
	COM.CM	Cambios (actualizaciones y mantenimiento)
	COM.internet	Internet: uso de acceso
Seguridad física – Protección de las instalaciones	L	Protección de las Instalaciones
	L.depth	Defensa en profundidad
	L.AC	Control de los accesos físicos
	L.A	Aseguramiento de la disponibilidad
Salvaguardas relativas al personal	PS	Gestión del Personal
	PS.AT	Formación y concienciación
	PS.A	Aseguramiento de la disponibilidad
Continuidad de operaciones	BC	Continuidad del negocio
	BC.BIA	Análisis de impacto (BIA)
	BC.DRP	Plan de Recuperación de Desastres (DRP)
Externalización	E	Relaciones Externas
	E.2	Acceso externo
	E.3	Servicios proporcionados por otras organizaciones
Adquisición y desarrollo	NEW	Adquisición / desarrollo
	NEW.S	Servicios: Adquisición o desarrollo
	NEW.SW	Aplicaciones: Adquisición o desarrollo
	NEW.HW	Equipos: Adquisición o desarrollo
	NEW.COM	Comunicaciones: Adquisición o contratación
	NEW.MP	Soportes de Información: Adquisición
	NEW.C	Productos certificados o acreditados

ANEXO Nº 09: IMPLANTACIÓN DEL MODELO DE GESTIÓN DE RIESGOS TI - CASO DE ESTUDIO HOSPITAL II - I "HHH"

Fase I: Definir el Alcance y Contexto de la Organización

Proceso 1: Definir el Alcance

	FORMATO DE DEFINICIÓN DEL ALCANCE	
	Código del Formato: CF N° 01	**Fecha: ____/____/2020**
Fase: I - Definir el Alcance y Contexto de la Organización		**Proceso: 1 - Definir el Alcance**
Objetivos:	- Definir el Alcance por medio de la identificación de los procesos críticos y áreas involucradas de la organización con el fin de ser considerados en el transcurso del proceso de gestión de riesgos de TI.	
Personal Involucrado:	- Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.	
Entradas:	- Reglamento de Organización y Funciones (ROF). - Manual de Organización y Funciones (MOF). - Organigrama institucional.	

Salidas:	
PROCESOS CRÍTICOS	**ÁREAS INVOLUCRADAS**
Mantenimiento de los servidores.	Unidad de Estadística e Informática (TI)
Mantenimiento de los sistemas informáticos.	
(SIGA, SIAF, SISMED y Sistema de Control de Asistencias).	
Monitoreo del estado de la red externa.	

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

Proceso 2: Identificación del Contexto Interno y Externo

HOSPITAL II - I "HHH"	**FORMATO DE IDENTIFICACIÓN DEL CONTEXTO INTERNO**	
	Código del Formato: CF N° 02	**Fecha: ____/____/2020**
Fase: I - Definir el Alcance y Contexto de la Organización		**Proceso: 2 - Identificación del Contexto Interno y Externo**
Objetivos:	- Identificar los parámetros del contexto interno que influyen en el impacto de la organización para cumplir con los objetivos estratégicos. - Tomar en consideración los parámetros identificados para la revisión periódica del proceso de gestión de riesgos de TI.	
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de Recursos Humanos. - Jefe de Asesoría Legal. - Jefe de Patrimonio. - Personal Analista.	
Entradas:	- Plan Estratégico de la organización, - Reglamento de Organización y Funciones (ROF). - Manual de Organización y Funciones (MOF). - Misión, Visión, Valores y Objetivos Estratégicos. - Organigrama de la institución.	
Salidas:		
PARÁMETROS	**DESCRIPCIÓN**	
Objetivos Estratégicos	Ayudan a proporcionar la dirección de cómo la organización pretende alcanzar o trasladarse hacia las metas desarrolladas a nivel estratégico en un determinado periodo de tiempo basándose en la misión, visión y valores de la organización.	
Política Interna	Responde a una serie de fundamentos establecidos y que es necesario que sean difundidos, comprendidos y aceptados por los trabajadores de la organización.	
Cultura Organizacional	Es el conjunto de percepciones, actitudes, tradiciones, hábitos, valores y formas de interacción entre los grupos existentes de la organización.	
Infraestructura Tecnológica	Está conformada por el hardware y software sobre el que se asientan los diferentes servicios que la organización necesita tener en funcionamiento para poder llevar a cabo todas sus actividades por parte de la administración o gestión interna.	
Estructura Organizacional	Es la metodología a través de la cual la organización planifica su trabajo y reparte formalmente sus responsabilidades, en la que cada usuario asume un papel que se espera que cumpla con el mayor rendimiento posible, para trabajar en conjunto y de forma óptima, logrando así que se alcancen las metas fijadas en la planificación.	
Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	ALTA GERENCIA	
Aprobado por:	ALTA GERENCIA	

HOSPITAL II - I "HHH"	**FORMATO DE IDENTIFICACIÓN DEL CONTEXTO EXTERNO**	
	Código del Formato: CF N° 03	**Fecha: ____/____/2020**
Fase: I - Definir el Alcance y Contexto de la Organización		**Proceso: 2 - Identificación del Contexto Interno y Externo**
Objetivos:	- Identificar los parámetros del contexto externo que influyen en el impacto de la organización para cumplir con los objetivos estratégicos. - Tomar en consideración los parámetros identificados para la revisión periódica del proceso de gestión de riesgos de TI.	
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de Recursos Humanos. - Jefe de Asesoría Legal. - Jefe de Contabilidad. - Jefe de la Unidad de Estadística e Informática (TI). - Jefe de Estadística. - Personal Analista.	
Entradas:	- Lista de entidades que forman parte del entorno económico. - Reportes estadísticos de los diferentes factores socio-culturales. - Reporte de activos de información que forma parte del entorno tecnológico y las Políticas internas impuestas por TI, respecto a las diferentes tecnologías que se manejan en la organización. - Lista de instituciones que conforman el contexto político. - Lista de entidades que forman parte del entorno legal. - Reporte de Senamhi de los diferentes fenómenos climatológicos en la región Amazonas. - Lista de instituciones que brindan servicios similares a los de la organización. - Lista de proveedores que ofrecen servicios a la organización.	
Salidas:		
PARÁMETROS	**ENTIDADES/ACTIVIDADES QUE FORMAN PARTE DEL PARÁMETRO**	
Económico	- Banco de la Nación (BN). - Banco Central de Reserva del Perú (BCRP). - Rimac Seguros. - Caja Trujillo. - Caja Piura. - Cooperativa El Tumi.	
Socio-Culturales	- Información estadística INEI. - Censos. - Evolución de la pirámide poblacional. - Reportes de Gobiernos Regionales - Reportes de Redes de Salud. - Valores sociales, morales y éticos.	
Tecnológicos	- Reporte de activos de información.	

	- Políticas establecidas por TI.
Políticos	- Constitución Política del Perú. - Gobiernos regionales. - Redes de Salud.
Legales	- Ministerio de Salud (MINSA). - Superintendencia Nacional de Salud (SUSALUD). - Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI). - Instituto Nacional de Defensa Civil (INDECI). - Superintendencia Nacional de Registros Públicos (SUNARP). - Ministerio de Economía y Finanzas (MEF).
Medioambientales	- Tormentas eléctricas. - Lluvias torrenciales. - Inundaciones. - Sequías.
Competitivo	- Hospitales o clínicas que brindan servicios similares o mejorados. - Hospitales o clínicas que cuentan con la misma tecnología o superior. - Hospitales o clínicas que cuentan con la misma calidad de productos o superior.

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	ALTA GERENCIA	
Aprobado por:	ALTA GERENCIA	

Fase II: Identificación de Activos

Proceso 3: Identificación y Clasificación de Activos

HOSPITAL II - 1 "HHH"	**FORMATO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS**		
	Código del Formato: CF N° 04		**Fecha: ____/____/2020**
Fase: II – Identificación de Activos			**Proceso: 3 - Identificación y Clasificación de Activos**
Objetivos:	- Identificar los activos críticos para la institución; aquellos que al ser afectados generan un impacto negativo en la prestación de sus servicios o el desarrollo de sus actividades. - Clasificar los activos identificados respecto al catálogo de tipos de activos ofrecido por MAGERIT.		
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Responsables de los procesos críticos. - Personal Analista.		
Entradas:	- Reporte de activos de información. - Manual de Organización y Funciones (MOF).		
Salidas:			
CÓDIGO	**CLASIFICACIÓN**	**ACTIVO**	**DESCRIPCIÓN**
D - CRPD	[backup]	Copias de Respaldo	Ficheros de copias de respaldo de los distintos sistemas y aplicaciones.
D - HCL	[files]	Historias Clínicas	Información clínica de los pacientes con sus beneficios.
SW - AVS	[av]	Antivirus	Software para detectar y eliminar virus informáticos.
SW - BDCA	[dbms]	Base de datos Access - Control de Asistencia	Usado para la gestión y administración de los datos del hospital involucrados con el Control de Asistencia, brindando el soporte necesario a todas las actividades manejadas en el software y colaborando con los procesos involucrados.
SW - BDSIAF	[dbms]	Base de datos MVFP - SIAF	Usado para la gestión y administración de los datos del hospital involucrados con el Sistema Integrado de Administración Financiera, brindando el soporte necesario a todas las actividades manejadas en el software y colaborando con los procesos involucrados.
SW - BDSIGA	[dbms]	Base de datos SQL - SIGA	Usado para la gestión y administración de los datos del hospital involucrados con el Sistema Integrado de Gestión Administrativa, brindando el soporte necesario a todas las actividades

			manejadas en el software y colaborando con los procesos involucrados.
SW - BDSISMED	[dbms]	Base de datos MVFP - SISMED	Usado para la gestión y administración de los datos del hospital involucrados con el Sistema de Información de Precios de Medicamentos, brindando el soporte necesario a todas las actividades manejadas en el software y colaborando con los procesos involucrados.
SW - OFM	[office]	Ofimática	Conjunto de aplicaciones necesarias para la realización de las actividades, así como la producción de recursos.
HW - LPT	[mobile]	Laptop	Permiten la realización de tareas del personal administrativo conectadas a través de la red interna.
SW - SOP	[os]	Sistemas Operativos	Software que administra los recursos de las computadoras de uso organizacional.
SW - SCA	[sub]	Sistema de Control y Asistencia	Permiten controlar y gestionar las horas trabajadas de los empleados.
HW - SVD	[host]	Servidor.	Computadoras especializadas en proveer los recursos, almacenar datos y ejecutar el software de diferentes aplicaciones a través de la red.
HW - MDM	[modem]	Módem	Dispositivo que permite la comunicación entre computadoras del hospital a través de la línea telefónica.
HW - SWT	[switch]	Switch para Red	Administra las VLANS que permite realizar la segmentación de la red de datos, gestionar y optimizar el ancho de banda, así como expandir la conexión de las computadoras de uso organizacional.
HW - UPS	[peripheral]	Acumulador de Energía - UPS	Provee energía temporal a los Servidores y demás dispositivos vitales en caso de fallas eléctricas inesperadas.
COM - REN	[radio]	Radio Enlace	Usada como medio de contingencia en caso las 2 fibras ópticas caigan, permitiendo la comunicación de internet dentro del hospital.
AUX - FOC	[fiber]	Fibra Óptica Claro	Usada como medio de contingencia ante las caídas repentinas y constantes de la red, permitiendo que el servicio de internet mantenga su continuidad.
AUX - FOM	[fiber]	Fibra Óptica Movistar	Usada como medio de principal para proveer internet a todas las oficinas del Hospital, permitiendo trabajar con rapidez.
P - JTI	[adm]/[com]/[dba]/	Jefe de TI	Personal encargado de administrar los

	[sec]		sistemas, las comunicaciones, bases de datos, soporte técnico y la seguridad informática en general.
L - SSVD	[site]	Sala de Servidores	Estructura física que acoge a los servidores que contienen los sistemas informáticos del Hospital.
Media - DDE	[disk]	Disco Duro Externo	Usado principalmente para guardar y trasladar información importante.

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

Proceso 4: Valoración de Activos

a) Respecto a las Dimensiones de Valoración y Escalas Estándar

HOSPITAL II - I "HHH"	**FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO A LAS DIMENSIONES DE VALORACIÓN**	
	Código del Formato: CF N° 05	**Fecha: ____/____/2020**
Fase: II – Identificación de Activos		**Proceso: 4 - Valoración de Activos**
Objetivos:	- La alta gerencia debe valorar (respecto a las Dimensiones de Valoración y Escalas Estándar) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos (Tabla 04) con el propósito de medir los efectos de una amenaza cuando se materializa.	
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.	
Entradas:	- Formato de Identificación y Clasificación de Activos llenado (**CF N° 04**). - Dimensiones de Valoración (**MAGERIT v3.0 – Libro II [pp. 15, 16]**). - Escalas Estándar (**ANEXO N° 07**).	

Salidas:

CÓDIGO	ACTIVO	DIMENSIONES DE VALORACIÓN				
		DISPONIBILIDAD [D]	INTEGRIDAD [I]	CONFIDENCIALIDAD [C]	AUTENTICIDAD [A]	TRAZABILIDAD [T]
D - CRPD	Copias de Respaldo	5.adm	1.si	10.si		
D - HCL	Historias Clínicas	1.adm	6.pi2	7.lro	6.pi2	6.pi2
SW - AVS	Antivirus	2.lg		7.si		
SW - BDCA	Base de datos Access - Control de Asistencia	7.adm	7.adm	10.si	7.adm	
SW - BDSIAF	Base de datos MVFP - SIAF	7.adm	7.adm	10.si	7.adm	
SW -	Base de datos SQL - SIGA	7.adm	7.adm	10.si	7.adm	

BDSIGA						
SW - BDSISMED	Base de datos MVFP - SISMED	7.adm	7.adm	10.si	7.adm	
SW - OFM	Ofimática	1.adm				
HW - LPT	Laptop	1.adm				
SW - SOP	Sistemas Operativos	5.adm	7.si	9.si		
SW - SCA	Sistema de Control y Asistencia	1.pi1				
HW - SVD	Servidor.	5.adm		10.si	7.si	
HW - MDM	Módem	5.adm				7.si
HW - SWT	Switch para Red	5.adm				7.si
HW - UPS	Acumulador de Energía - UPS	5.adm				
COM - REN	Radio Enlace	5.adm				
AUX - FOC	Fibra Óptica Claro	5.adm				
AUX - FOM	Fibra Óptica Movistar	5.adm				
P - JTI	Jefe de Estadística e Informática (TI)	5.adm				
L - SSVD	Sala de Servidores	7.adm				
Media - DDE	Disco Duro Externo	1.adm		1.si		

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - I "HHH"	**FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO A LAS ESCALAS ESTÁNDAR**	
	Código del Formato: CF N° 06	**Fecha: ____/____/2020**
Fase: II - Identificación de Activos		**Proceso: 4 - Valoración de Activos**
Objetivos:	- La alta gerencia debe valorar (respecto a las Dimensiones de Valoración y Escalas Estándar) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos con el propósito de medir los efectos de una amenaza cuando se materializa.	
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.	
Entradas:	- Formato de Identificación y Clasificación de Activos llenado (**CF N° 04**). - Dimensiones de Valoración (**MAGERIT v3.0 – Libro II [pp. 15, 16]**). - Escalas Estándar (**ANEXO N° 07**).	

Salidas:		
CÓDIGO	**DIMENSIÓN DE SEGURIDAD**	**DESCRIPCIÓN**
D - CRPD	[D]	5.adm: probablemente impediría la operación efectiva de más de una parte de la Organización.
	[I]	1.si: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
	[C]	10.si: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
D - HCL	[D]	1.adm: pudiera impedir la operación efectiva de una parte de la Organización.
	[I][A][T]	6.pi2: probablemente quebrante seriamente la ley o algún reglamento de protección de información personal.
	[C]	7.lro: probablemente cause un incumplimiento grave de una ley o regulación.
SW - AVS	[D]	2.lg: Probablemente cause una pérdida menor de la confianza dentro de la Organización.
	[C]	7.si: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
SW - BDCA/ SW - BDSIAF/ SW - BDSIGA/ SW - BDSISMED	[D][I][A]	7.adm: probablemente impediría la operación efectiva de la Organización.
	[C]	10.si: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
SW - OFM HW - LPT	[D]	1.adm: pudiera impedir la operación efectiva de una parte de la Organización.
SW - SOP	[D]	5.adm: probablemente impediría la operación

		efectiva de más de una parte de la Organización.
	[I]	7.si: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
	[C]	9.si: probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios.
SW - SCA	[D]	1.pi1: pudiera causar molestias a un individuo.
HW - SVD	[D]	5.adm: probablemente impediría la operación efectiva de más de una parte de la Organización.
	[C]	10.si: probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios.
	[A]	7.si: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
HW – MDM/ HW - SWT	[D]	5.adm: probablemente impediría la operación efectiva de más de una parte de la Organización.
	[T]	7.si: probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
HW - UPS/ COM - REN/ AUX - FOC/ AUX - FOM/ P - JTI	[D]	5.adm: probablemente impediría la operación efectiva de más de una parte de la Organización.
L - SSVD	[D]	7.adm: probablemente impediría la operación efectiva de la Organización.
Media - DDE	[D]	1.adm: pudiera impedir la operación efectiva de una parte de la Organización.
	[C]	1.si: pudiera causar una merma en la seguridad o dificultar la investigación de un incidente.

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

b) Respecto al Impacto

HOSPITAL II - I "HHH"	**FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO AL IMPACTO**	
	Código del Formato: CF N° 07	**Fecha: ____/____/2020**
Fase: II – Identificación de Activos		**Proceso: 4 - Valoración de Activos**
Objetivos:	- La alta gerencia debe valorar (respecto al impacto) los activos críticos identificados en el Formato de Identificación y Clasificación de Activos con el propósito de medir los efectos de una amenaza cuando se materializa.	
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.	
Entradas:	- Formato de Identificación y Clasificación de Activos llenado (**CF N° 04**). - Formato de Valoración de Activos respecto a las Dimensiones de Valoración llenado (**CF N° 05**). - Formato de Valoración de Activos respecto a las Escalas Estándar llenado (**CF N° 06**). - Valoración de Activos respecto al Impacto (**Tabla 08 del informe [p. 81]**).	

Salidas:				
CÓDIGO	**ACTIVO**	**VALOR**	**IMPACTO**	**JUSTIFICACIÓN**
D - CRPD	Copias de Respaldo	10	MA	Las copias de respaldo son determinantes para la recuperación de archivos ante un desastre.
D - HCL	Historias Clínicas	7	A	Archivos de historial clínico contienen información de enfermedades, tratamientos y suministros de medicamentos a los pacientes del hospital.
SW - AVS	Antivirus	7	A	Utilizado para la prevención y eliminación de software malintencionado, así como evitar la propagación de malware por la red.
SW - BDCA	Base de datos Access - Control de Asistencia	10	MA	Almacena toda la información del Sistema de Control de Asistencia, así como el soporte para el desarrollo normal de los procesos de la misma aplicación.
SW - BDSIAF	Base de datos MVFP - SIAF	10	MA	Almacena toda la información del SIAF, así como el soporte para el desarrollo normal de los procesos de la misma aplicación.
SW - BDSIGA	Base de datos SQL - SIGA	10	MA	Almacena toda la información del SIGA, así como el soporte para el desarrollo normal de los procesos de la misma aplicación.
SW -	Base de	10	MA	Almacena toda la información del

BDSISMED	datos MVFP - SISMED			SISMED, así como el soporte para el desarrollo normal de los procesos de la misma aplicación.
SW - OFM	Ofimática	1	MB	Utilizado para la ejecución de tareas informáticas.
HW - LPT	Laptop	1	MB	Dispositivo portátil usado para la ejecución de tareas propias de la oficina.
SW - SOP	Sistemas Operativos	9	A	Gestiona los recursos de software y hardware de las diferentes computadoras del Hospital.
SW - SCA	Sistema de Control y Asistencia	1	MB	Usado para controlar y gestionar las horas trabajadas de los empleados.
HW - SVD	Servidor.	10	MA	Dispositivo esencial para el correcto funcionamiento de los diferentes Sistemas de Información que soportan los procesos del Hospital.
HW - MDM	Módem	7	A	Dispositivo que permite la comunicación entre las computadoras del Hospital a través del cable módem.
HW - SWT	Switch para Red	7	A	Dispositivo esencial para direccionar el tráfico de datos interno, administración de VLAN y segmentar el ancho de banda con el fin de optimizarla.
HW - UPS	Acumulador de Energía - UPS	5	M	Equipo fundamental para mantener el funcionando a los dispositivos en caso de una eventual falla en el suministro eléctrico, así como evitar el daño parcial o total del hardware.
COM - REN	Radio Enlace	5	M	Usada como medio de contingencia en caso las 2 fibras ópticas de respaldo caigan, permitiendo la comunicación continua de internet dentro del hospital.
AUX - FOC	Fibra Óptica Claro	5	M	Usada como medio de contingencia ante las caídas repentinas y constantes de la red, permitiendo trabajar con rapidez.
AUX - FOM	Fibra Óptica Movistar	5	M	Usada como medio de contingencia ante las caídas repentinas y constantes de la red, permitiendo trabajar con rapidez.
P - JTI	Jefe de TI	5	M	Persona encargada de administrar los diferentes sistemas, configurar y optimizar el rendimiento de las bases de datos que contienen los

				datos de los diferentes Sistemas de Información, así como velar por la seguridad de que éstos se mantengan confidenciales, disponibles e íntegros.
L - SSVD	Sala de Servidores	7	A	Esencial para el funcionamiento correcto de todos los Sistemas informáticos que soportan los procesos del Hospital.
Media - DDE	Disco Duro Externo	1	MB	Usado principalmente para guardar y trasladar información importante como bases de datos o copias de respaldo.

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

Fase III: Evaluación del Riesgo

Proceso 5: Identificación y Valoración de Amenazas

HOSPITAL II - I "HHH"	**FORMATO DE IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS**	
	Código del Formato: CF N° 08	**Fecha: ____/____/2020**
Fase: III – Evaluación del Riesgo		**Proceso: 5 – Identificación y Valoración de Amenazas**
Objetivos:	- La alta gerencia debe identificar cuáles son los distintos tipos de amenazas que se efectúan sobre los activos críticos y determinar la probabilidad con la que se reiteran estas amenazas.	
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.	
Entradas:	- Formato de Identificación y Clasificación de Activos llenado (**CF N° 04**). - Catálogo de Amenazas posibles sobre los activos (**MAGERIT v3.0 – Libro II [pp. 25 - 47]**). - Formato de Frecuencia o Probabilidad de ocurrencia de las Amenazas sugerido (**Tabla 12 del informe [p. 88]**).	

Salidas:

CÓDIGO	ACTIVO	TIPO DE AMENAZA	FRECUENCIA O PROBABILIDAD	VALOR
D - CRPD	Copias de Respaldo	[E.1] Errores de los usuarios	MB	1
		[E.2] Errores del administrador	B	2
		[E.15] Alteración accidental de la información	MB	1
		[E.18] Destrucción de información	MB	1
		[E.19] Fugas de información	MB	1
		[A.6] Abuso de privilegios de acceso	MB	1
		[A.11] Acceso no autorizado	MB	1
		[A.15] Modificación deliberada de la información	MB	1
		[A.18] Destrucción de información	MB	1
		[A.19] Divulgación de información	MB	1
D - HCL	Historias Clínicas	[E.2] Errores del administrador	MB	1

		[E.15] Alteración accidental de la información	B	2
		[E.18] Destrucción de información	MB	1
		[E.19] Fugas de información	M	3
		[A.5] Suplantación de identidad del usuario	MB	1
		[A.6] Abuso de privilegios de acceso	M	3
		[A.11] Acceso no autorizado	MB	1
		[A.15] Modificación deliberada de la información	B	2
		[A.18] Destrucción de información	MB	1
		[A.19] Divulgación de información	B	2
SW - AVS	Antivirus	[I.5] Avería de origen físico o lógico	MB	1
		[E.1] Errores de los usuarios	M	3
		[E.8] Difusión de software dañino	M	3
		[E.20] Vulnerabilidades de los programas (software)	B	2
		[E.21] Errores de mantenimiento / actualización de programas (software)	MB	1
		[A.7] Uso no previsto	B	2
		[A.8] Difusión de software dañino	MB	1
		[A.11] Acceso no autorizado	MB	1
SW - BDCA/ SW- BDSIAF/ SW- BDSIGA/ SW - BDSISMED	Base de datos Access - Control de Asistencia/ Base de datos MVFP - SIAF/ Base de datos SQL - SIGA/ Base de datos MVFP - SISMED	[I.5] Avería de origen físico o lógico	MB	1
		[E.2] Errores del administrador	B	2
		[E.8] Difusión de software dañino	MB	1
		[E.15] Alteración accidental de la información	MB	1
		[E.18] Destrucción de información	MB	1
		[E.19] Fugas de	MB	1

		información		
		[E.20] Vulnerabilidades de los programas (software)	B	2
		[E.21] Errores de mantenimiento / actualización de programas (software)	MB	1
		[A.5] Suplantación de identidad del usuario	B	2
		[A.6] Abuso de privilegios de acceso	B	2
		[A.7] Uso no previsto	MB	1
		[A.8] Difusión de software dañino	MB	1
		[A.9] [Re-]encaminamiento de mensajes	MB	1
		[A.10] Alteración de secuencia	MB	1
		[A.11] Acceso no autorizado	MB	1
		[A.15] Modificación deliberada de la información	MB	1
		[A.18] Destrucción de información	MB	1
		[A.19] Divulgación de la información	MB	1
		[A.22] Manipulación de programas	MB	1
SW - OFM	Ofimática	[I.5] Avería de origen físico o lógico	B	2
		[E.1] Errores de los usuarios	M	3
		[E.8] Difusión de software dañino	B	2
		[E.18] Destrucción de información	M	3
		[E.20] Vulnerabilidades de los programas (software)	M	3
		[A.7] Uso no previsto	A	4
		[A.8] Difusión de software dañino	MB	1
		[A.11] Acceso no autorizado	MB	1
HW - LPT	Laptop	[N.*] Desastres naturales	B	2
		[I.1] Fuego	MB	1
		[I.2] Daños por agua	MB	1
		[I.5] Avería de origen	MB	1

		físico o lógico		
		[I.6] Corte del suministro eléctrico	M	3
		[I.7] Condiciones inadecuadas de temperatura o humedad	B	2
		[E.2] Errores del administrador	B	2
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	2
		[E.24] Caída del sistema por agotamiento de recursos	MB	1
		[E.25] Pérdida de equipos	MB	1
		[A.6] Abuso de privilegios de acceso	B	2
		[A.7] Uso no previsto	A	4
		[A.24] Denegación de servicio	MB	1
		[A.25] Robo	MB	1
SW - SOP	Sistemas Operativos	[I.5] Avería de origen físico o lógico	B	2
		[E.1] Errores de los usuarios	B	2
		[E.2] Errores del administrador	B	2
		[E.8] Difusión de software dañino	M	3
		[E.15] Alteración accidental de la información	B	2
		[E.18] Destrucción de información	B	2
		[E.19] Fugas de información	MB	1
		[E.20] Vulnerabilidades de los programas (software)	B	2
		[E.21] Errores de mantenimiento / actualización de programas (software)	MB	1
		[A.5] Suplantación de identidad del usuario	MB	1
		[A.6] Abuso de privilegios de acceso	B	2
		[A.7] Uso no previsto	M	3
		[A.8] Difusión de software	MB	1

		dañino		
		[A.9] [Re-]encaminamiento de mensajes	MB	1
		[A.10] Alteración de secuencia	MB	1
		[A.11] Acceso no autorizado	B	2
		[A.15] Modificación deliberada de la información	MB	1
		[A.18] Destrucción de información	B	2
		[A.19] Divulgación de la información	MB	1
		[A.22] Manipulación de programas	B	2
SW - SCA	Sistema de Control y Asistencia	[I.5] Avería de origen físico o lógico	MB	1
		[E.1] Errores de los usuarios	MB	1
		[E.2] Errores del administrador	B	2
		[E.15] Alteración accidental de la información	MB	1
		[E.18] Destrucción de información	MB	1
		[E.19] Fugas de información	MB	1
		[E.20] Vulnerabilidades de los programas (software)	MB	1
		[A.5] Suplantación de la identidad del usuario	B	2
		[A.6] Abuso de privilegios de acceso	B	2
		[A.15] Modificación deliberada de la información	M	3
HW - SVD	Servidor	[N.*] Desastres naturales	B	2
		[I.1] Fuego	MB	1
		[I.2] Daños por agua	B	2
		[I.5] Avería de origen físico o lógico	MB	1
		[I.6] Corte del suministro eléctrico	M	3
		[I.7] Condiciones inadecuadas de temperatura o humedad	B	2

		[E.2] Errores del administrador	B	2
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	2
		[E.24] Caída del sistema por agotamiento de recursos	MB	1
		[E.25] Pérdida de equipos	MB	1
		[A.6] Abuso de privilegios de acceso	B	2
		[A.7] Uso no previsto	MB	1
		[A.11] Acceso no autorizado	MB	1
		[A.23] Manipulación de los equipos	MB	1
		[A.24] Denegación de servicio	MB	1
		[A.25] Robo	MB	1
HW - MDM/ HW - SWT	Módem/ Switch para Red	[N.*] Desastres naturales	B	2
		[I.1] Fuego	MB	1
		[I.2] Daños por agua	B	2
		[I.5] Avería de origen físico o lógico	MB	1
		[I.6] Corte del suministro eléctrico	M	3
		[I.7] Condiciones inadecuadas de temperatura o humedad	B	2
		[E.2] Errores del administrador	B	2
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	B	2
		[E.24] Caída del sistema por agotamiento de recursos	MB	1
		[E.25] Pérdida de equipos	MB	1
		[A.6] Abuso de privilegios de acceso	MB	1
		[A.7] Uso no previsto	MB	1
		[A.11] Acceso no autorizado	MB	1
		[A.23] Manipulación de los equipos	MB	1
		[A.24] Denegación de servicio	MB	1

		[A.25] Robo	MB	1
HW - UPS	Acumulador de Energía - UPS	[N.*] Desastres naturales	B	2
		[I.1] Fuego	MB	1
		[I.2] Daños por agua	B	2
		[I.5] Avería de origen físico o lógico	MB	1
		[I.6] Corte del suministro eléctrico	MB	1
		[I.7] Condiciones inadecuadas de temperatura o humedad	B	2
		[A.25] Robo	B	2
COM – REN	Radio Enlace	[I.8] Fallo de servicios de comunicaciones	MB	1
		[E.2] Errores del administrador	MB	1
		[E.9] Errores de [re-] encaminamiento	MB	1
		[E.24] Caída del sistema por agotamiento de recursos	B	2
		[A.24] Denegación de servicio	B	2
AUX - FOC/ AUX - FOM	Fibra Óptica Claro/ Fibra Óptica Movistar	[N.*] Desastres naturales	B	2
		[I.1] Fuego	MB	1
		[I.2] Daños por agua	MB	1
		[I.5] Avería de origen físico o lógico	MB	1
		[I.6] Corte del suministro eléctrico	M	3
		[I.7] Condiciones inadecuadas de temperatura o humedad	M	3
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	MB	1
		[A.7] Uso no previsto	MB	1
P - JTI	Jefe de TI	[E.7] Deficiencias en la organización	M	3
		[E.19] Fugas de información	MB	1
		[E.28] Indisponibilidad del personal	M	3
		[A.28] Indisponibilidad del personal	MB	1
		[A.30] Ingeniería social (picaresca)	M	3

L - SSVD	Sala de Servidores	[N.*] Desastres Naturales	B	2
		[I.2] Daños por agua	B	2
		[I.11] Emanaciones electromagnéticas	MB	1
		[E.15] Alteración accidental de la información	MB	1
		[E.18] Destrucción de información	MB	1
		[E.19] Fugas de información	MB	1
		[A.7] Uso no previsto	MB	1
Media - DDE	Disco Duro Externo	[N.2] Daños por agua	MB	1
		[N.*] Desastres naturales	B	2
		[I.5] Avería de origen físico o lógico	MB	1
		[I.6] Corte del suministro eléctrico	M	3
		[I.7] Condiciones inadecuadas de temperatura o humedad	M	3
		[I.10] Degradación de los soportes de almacenamiento de la información	MB	1
		[E.1] Errores de los usuarios	B	2
		[E.2] Errores del administrador	MB	1
		[E.15] Alteración accidental de la información	B	2
		[E.18] Destrucción de información	MB	1
		[E.19] Fugas de información	MB	1
		[E.25] Pérdida de equipos	MB	1
		[A.7] Uso no previsto	A	4
		[A.25] Robo	MB	1

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

Proceso 6: Identificación, Análisis y Valoración del Riesgo

a) Identificación y Análisis del Riesgo

HOSPITAL II - I "HHH"	**FORMATO DE IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO**						
	Código del Formato: CF N° 09				**Fecha: ____/____/2020**		
Fase: III – Evaluación del Riesgo					**Proceso: 6 – Identificación, Análisis y Valoración del Riesgo**		
Objetivos:	- La alta gerencia debe identificar los niveles del riesgo que puede sufrir cada activo crítico de la organización.						
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.						
Entradas:	- Formato de Valoración de Activos respecto al Impacto llenado (**CF N° 07**). - Frecuencia o Probabilidad de ocurrencia de las Amenazas sugerido (**Tabla 12 del informe [p. 88]**). - Formato de Identificación y Valoración de Amenazas llenado (**CF N° 08**). - Estimación del Riesgo (**Tabla 14 del informe [p. 92]**).						
Salidas:							
CÓDIGO	**ACTIVO**	**IMPACTO**	**PROBABILIDAD**	**AMENAZA**	**ID RIESGO**	**RIESGO**	**VALOR**
D - CRPD	Copias de Respaldo	MA	MB	[E.1]	R - D - CRPD - 1	A	4
			B	[E.2]	R - D - CRPD - 2	MA	5
			MB	[E.15]	R - D - CRPD - 3	A	4
			MB	[E.18]	R - D - CRPD - 4	A	4
			MB	[E.19]	R - D - CRPD - 5	A	4
			MB	[A.6]	R - D - CRPD - 6	A	4
			MB	[A.11]	R - D - CRPD - 7	A	4
			MB	[A.15]	R - D - CRPD - 8	A	4
			MB	[A.18]	R - D - CRPD - 9	A	4
			MB	[A.19]	R - D - CRPD - 10	A	4

D - HCL	Historias Clínicas	A	MB	[E.2]	R - D - HCL - 1	M	3
			B	[E.15]	R - D - HCL - 2	A	4
			MB	[E.18]	R - D - HCL - 3	M	3
			M	[E.19]	R - D - HCL - 4	A	4
			MB	[A.5]	R - D - HCL - 5	M	3
			M	[A.6]	R - D - HCL - 6	A	4
			MB	[A.11]	R - D - HCL - 7	M	3
			B	[A.15]	R - D - HCL - 8	A	4
			MB	[A.18]	R - D - HCL - 9	M	3
			B	[A.19]	R - D - HCL - 10	A	4
SW - AVS	Antivirus	A	MB	[I.5]	R - SW - AVS - 1	M	3
			M	[E.1]	R - SW - AVS - 2	A	4
			M	[E.8]	R - SW - AVS - 3	A	4
			B	[E.20]	R - SW - AVS - 4	A	4
			MB	[E.21]	R - SW - AVS - 5	M	3
			B	[A.7]	R - SW - AVS - 6	A	4
			MB	[A.8]	R - SW - AVS - 7	M	3
			MB	[A.11]	R - SW - AVS - 8	M	3
SW - BDCA	Base de datos Access - Control de Asistencia	MA	MB	[I.5]	R - SW – BDCA - 1	A	4
			B	[E.2]	R - SW – BDCA - 2	MA	5
			MB	[E.8]	R - SW – BDCA - 3	A	4
			MB	[E.15]	R - SW – BDCA - 4	A	4
			MB	[E.18]	R - SW – BDCA - 5	A	4
			MB	[E.19]	R - SW – BDCA - 6	A	4
			B	[E.20]	R - SW – BDCA - 7	MA	5
			MB	[E.21]	R - SW – BDCA - 8	A	4
			B	[A.5]	R - SW – BDCA - 9	MA	5
			B	[A.6]	R - SW – BDCA - 10	MA	5
			MB	[A.7]	R - SW – BDCA - 11	A	4
			MB	[A.8]	R - SW – BDCA - 12	A	4
			MB	[A.9]	R - SW – BDCA - 13	A	4

			MB	[A.10]	R - SW – BDCA - 14	A	4
			MB	[A.11]	R - SW – BDCA - 15	A	4
			MB	[A.15]	R - SW – BDCA - 16	A	4
			MB	[A.18]	R - SW – BDCA - 17	A	4
			MB	[A.19]	R - SW – BDCA - 18	A	4
			MB	[A.22]	R - SW – BDCA - 19	A	4
SW - BDSIAF	Base de datos MVFP - SIAF	MA	MB	[I.5]	R - SW - BDSIAF - 1	A	4
			B	[E.2]	R - SW - BDSIAF - 2	MA	5
			MB	[E.8]	R - SW - BDSIAF - 3	A	4
			MB	[E.15]	R - SW - BDSIAF - 4	A	4
			MB	[E.18]	R - SW - BDSIAF - 5	A	4
			MB	[E.19]	R - SW - BDSIAF - 6	A	4
			B	[E.20]	R - SW - BDSIAF - 7	MA	5
			MB	[E.21]	R - SW - BDSIAF - 8	A	4
			B	[A.5]	R - SW - BDSIAF - 9	MA	5
			B	[A.6]	R - SW - BDSIAF - 10	MA	5
			MB	[A.7]	R - SW - BDSIAF - 11	A	4
			MB	[A.8]	R - SW - BDSIAF - 12	A	4
			MB	[A.9]	R - SW - BDSIAF - 13	A	4
			MB	[A.10]	R - SW - BDSIAF - 14	A	4
			MB	[A.11]	R - SW - BDSIAF - 15	A	4
			MB	[A.15]	R - SW - BDSIAF - 16	A	4
			MB	[A.18]	R - SW - BDSIAF - 17	A	4
			MB	[A.19]	R - SW - BDSIAF - 18	A	4
			MB	[A.22]	R - SW - BDSIAF - 19	A	4
SW - BDSIGA	Base de datos SQL - SIGA	MA	MB	[I.5]	R - SW - BDSIGA - 1	A	4
			B	[E.2]	R - SW - BDSIGA - 2	MA	5
			MB	[E.8]	R - SW - BDSIGA - 3	A	4
			MB	[E.15]	R - SW - BDSIGA - 4	A	4
			MB	[E.18]	R - SW - BDSIGA - 5	A	4
			MB	[E.19]	R - SW - BDSIGA – 6	A	4

			B	[E.20]	R - SW - BDSIGA - 7	MA	5
			MB	[E.21]	R - SW - BDSIGA - 8	A	4
			B	[A.5]	R - SW - BDSIGA - 9	MA	5
			B	[A.6]	R - SW -BDSIGA - 10	MA	5
			MB	[A.7]	R - SW -BDSIGA - 11	A	4
			MB	[A.8]	R - SW -BDSIGA - 12	A	4
			MB	[A.9]	R - SW -BDSIGA - 13	A	4
			MB	[A.10]	R - SW -BDSIGA - 14	A	4
			MB	[A.11]	R - SW -BDSIGA - 15	A	4
			MB	[A.15]	R - SW -BDSIGA - 16	A	4
			MB	[A.18]	R - SW -BDSIGA - 17	A	4
			MB	[A.19]	R - SW -BDSIGA - 18	A	4
			MB	[A.22]	R - SW -BDSIGA - 19	A	4
SW - BDSISMED	Base de datos MVFP - SISMED	MA	MB	[I.5]	R-SW-BDSISMED-1	A	4
			B	[E.2]	R-SW-BDSISMED-2	MA	5
			MB	[E.8]	R-SW-BDSISMED-3	A	4
			MB	[E.15]	R-SW-BDSISMED-4	A	4
			MB	[E.18]	R-SW-BDSISMED-5	A	4
			MB	[E.19]	R-SW-BDSISMED-6	A	4
			B	[E.20]	R-SW-BDSISMED-7	MA	5
			MB	[E.21]	R-SW-BDSISMED-8	A	4
			B	[A.5]	R-SW-BDSISMED-9	MA	5
			B	[A.6]	R-SW-BDSISMED-10	MA	5
			MB	[A.7]	R-SW-BDSISMED-11	A	4
			MB	[A.8]	R-SW-BDSISMED-12	A	4
			MB	[A.9]	R-SW-BDSISMED-13	A	4
			MB	[A.10]	R-SW-BDSISMED-14	A	4
			MB	[A.11]	R-SW-BDSISMED-15	A	4
			MB	[A.15]	R-SW-BDSISMED-16	A	4
			MB	[A.18]	R-SW-BDSISMED-17	A	4
			MB	[A.19]	R-SW-BDSISMED-18	A	4

			MB	[A.22]	R-SW-BDSISMED-19	A	4
SW - OFM	Ofimática	MB	B	[I.5]	R - SW - OFM - 1	MB	1
			M	[E.1]	R - SW - OFM - 2	MB	1
			B	[E.8]	R - SW - OFM - 3	MB	1
			M	[E.18]	R - SW - OFM - 4	MB	1
			M	[E.20]	R - SW - OFM - 5	MB	1
			A	[A.7]	R - SW - OFM - 6	B	2
			MB	[A.8]	R - SW - OFM - 7	MB	1
			MB	[A.11]	R - SW - OFM - 8	MB	1
HW - LPT	Laptop	MB	B	[N*]	R - HW - LPT - 1	MB	1
			MB	[I.1]	R - HW - LPT - 2	MB	1
			MB	[I.2]	R - HW - LPT - 3	MB	1
			MB	[I.5]	R - HW - LPT - 4	MB	1
			M	[I.6]	R - HW - LPT - 5	MB	1
			B	[I.7]	R - HW - LPT - 6	MB	1
			B	[E.2]	R - HW - LPT - 7	MB	1
			B	[E.23]	R - HW - LPT - 8	MB	1
			MB	[E.24]	R - HW - LPT - 9	MB	1
			MB	[E.25]	R - HW - LPT - 10	MB	1
			B	[A.6]	R - HW - LPT - 11	MB	1
			A	[A.7]	R - HW - LPT - 12	B	2
			MB	[A.24]	R - HW - LPT - 13	MB	1
			MB	[A.25]	R - HW - LPT - 14	MB	1
SW - SOP	Sistemas Operativos	A	B	[I.5]	R - SW - SOP - 1	A	4
			B	[E.1]	R - SW - SOP - 2	A	4
			B	[E.2]	R - SW - SOP - 3	A	4
			M	[E.8]	R - SW - SOP - 4	A	4
			B	[E.15]	R - SW - SOP - 5	A	4
			B	[E.18]	R - SW - SOP - 6	A	4
			MB	[E.19]	R - SW - SOP - 7	M	3
			B	[E.20]	R - SW - SOP - 8	A	4

			MB	[E.21]	R - SW - SOP - 9	M	3
			MB	[A.5]	R - SW - SOP - 10	M	3
			B	[A.6]	R - SW - SOP - 11	A	4
			M	[A.7]	R - SW - SOP - 12	A	4
			MB	[A.8]	R - SW - SOP - 13	M	3
			MB	[A.9]	R - SW - SOP - 14	M	3
			MB	[A.10]	R - SW - SOP - 15	M	3
			B	[A.11]	R - SW - SOP - 16	A	4
			MB	[A.15]	R - SW - SOP - 17	M	3
			B	[A.18]	R - SW - SOP - 18	A	4
			MB	[A.19]	R - SW - SOP - 19	M	3
			B	[A.22]	R - SW - SOP - 20	A	4
SW - SCA	Sistema de Control y Asistencia	MB	MB	[I.5]	R - SW - SCA - 1	MB	1
			MB	[E.1]	R - SW - SCA - 2	MB	1
			B	[E.2]	R - SW - SCA - 3	MB	1
			MB	[E.15]	R - SW - SCA - 4	MB	1
			MB	[E.18]	R - SW - SCA - 5	MB	1
			MB	[E.19]	R - SW - SCA - 6	MB	1
			MB	[E.20]	R - SW - SCA - 7	MB	1
			B	[A.5]	R - SW - SCA - 8	MB	1
			B	[A.6]	R - SW - SCA - 9	MB	1
			M	[A.15]	R - SW - SCA - 10	MB	1
HW - SVD	Servidor	MA	B	[N.*]	R - HW - SVD - 1	MA	5
			MB	[I.1]	R - HW - SVD - 2	A	4
			B	[I.2]	R - HW - SVD - 3	MA	5
			MB	[I.5]	R - HW - SVD - 4	A	4
			M	[I.6]	R - HW - SVD - 5	MA	5
			B	[I.7]	R - HW - SVD - 6	MA	5
			B	[E.2]	R - HW - SVD - 7	MA	5
			B	[E.23]	R - HW - SVD - 8	MA	5
			MB	[E.24]	R - HW - SVD - 9	A	4

			MB	[E.25]	R - HW - SVD - 10	A	4
			B	[A.6]	R - HW - SVD - 11	MA	5
			MB	[A.7]	R - HW - SVD - 12	A	4
			MB	[A.11]	R - HW - SVD - 13	A	4
			MB	[A.23]	R - HW - SVD - 14	A	4
			MB	[A.24]	R - HW - SVD - 15	A	4
			MB	[A.25]	R - HW - SVD - 16	A	4
HW - MDM	Módem	A	B	[N.*]	R - HW - MDM - 1	A	4
			MB	[I.1]	R - HW - MDM - 2	M	3
			B	[I.2]	R - HW - MDM - 3	A	4
			MB	[I.5]	R - HW - MDM - 4	M	3
			M	[I.6]	R - HW - MDM - 5	A	4
			B	[I.7]	R - HW - MDM - 6	A	4
			B	[E.2]	R - HW - MDM - 7	A	4
			B	[E.23]	R - HW - MDM - 8	A	4
			MB	[E.24]	R - HW - MDM - 9	M	3
			MB	[E.25]	R - HW - MDM - 10	M	3
			MB	[A.6]	R - HW - MDM - 11	M	3
			MB	[A.7]	R - HW - MDM - 12	M	3
			MB	[A.11]	R - HW - MDM - 13	M	3
			MB	[A.23]	R - HW - MDM - 14	M	3
			MB	[A.24]	R - HW - MDM - 15	M	3
			MB	[A.25]	R - HW - MDM - 16	M	3
HW - SWT	Switch para Red	A	B	[N.*]	R - HW - SWT - 1	A	4
			MB	[I.1]	R - HW - SWT - 2	M	3
			B	[I.2]	R - HW - SWT - 3	A	4
			MB	[I.5]	R - HW - SWT - 4	M	3
			M	[I.6]	R - HW - SWT - 5	A	4
			B	[I.7]	R - HW - SWT - 6	A	4
			B	[E.2]	R - HW - SWT - 7	A	4
			B	[E.23]	R - HW - SWT - 8	A	4

			MB	[E.24]	R - HW - SWT - 9	M	3
			MB	[E.25]	R - HW - SWT - 10	M	3
			MB	[A.6]	R - HW - SWT - 11	M	3
			MB	[A.7]	R - HW - SWT - 12	M	3
			MB	[A.11]	R - HW - SWT - 13	M	3
			MB	[A.23]	R - HW - SWT - 14	M	3
			MB	[A.24]	R - HW - SWT - 15	M	3
			MB	[A.25]	R - HW - SWT - 16	M	3
HW - UPS	Acumulador de Energía - UPS	M	B	[N.*]	R - HW - UPS - 1	M	3
			MB	[I.1]	R - HW - UPS - 2	B	2
			B	[I.2]	R - HW - UPS - 3	M	3
			MB	[I.5]	R - HW - UPS - 4	B	2
			MB	[I.6]	R - HW - UPS - 5	B	2
			B	[I.7]	R - HW - UPS - 6	M	3
			B	[A.25]	R - HW - UPS - 7	M	3
COM - REN	Radio Enlace	M	MB	[I.8]	R - COM - REN - 1	B	2
			MB	[E.2]	R - COM - REN - 2	B	2
			MB	[E.9]	R - COM - REN - 3	B	2
			B	[E.24]	R - COM - REN - 4	M	3
			B	[A.24]	R - COM - REN - 5	M	3
AUX - FOC	Fibra Óptica Claro	M	B	[N.*]	R - AUX - FOC - 1	M	3
			MB	[I.1]	R - AUX - FOC - 2	B	2
			MB	[I.2]	R - AUX - FOC - 3	B	2
			MB	[I.5]	R - AUX - FOC - 4	B	2
			M	[I.6]	R - AUX - FOC - 5	M	3
			M	[I.7]	R - AUX - FOC - 6	M	3
			MB	[E.23]	R - AUX - FOC - 7	B	2
			MB	[A.7]	R - AUX - FOC - 8	B	2
AUX - FOM	Fibra Óptica Movistar	M	B	[N.*]	R - AUX - FOM - 1	M	3
			MB	[I.1]	R - AUX - FOM - 2	B	2
			MB	[I.2]	R - AUX - FOM - 3	B	2

			MB	[I.5]	R - AUX - FOM - 4	B	2
			M	[I.6]	R - AUX - FOM - 5	M	3
			M	[I.7]	R - AUX - FOM - 6	M	3
			MB	[E.23]	R - AUX - FOM - 7	B	2
			MB	[A.7]	R - AUX - FOM - 8	B	2
P - JTI	Jefe de TI	M	M	[E.7]	R - P - JTI - 1	M	3
			MB	[E.19]	R - P - JTI - 2	B	2
			M	[E.28]	R - P - JTI - 3	M	3
			MB	[A.28]	R - P - JTI - 4	B	2
			M	[A.30]	R - P - JTI - 5	M	3
L - SSVD	Sala de Servidores	A	B	[N.*]	R - L - SSVD - 1	A	4
			B	[I.2]	R - L - SSVD - 2	A	4
			MB	[I.11]	R - L - SSVD - 3	M	3
			MB	[E.15]	R - L - SSVD - 4	M	3
			MB	[E.18]	R - L - SSVD - 5	M	3
			MB	[E.19]	R - L - SSVD - 6	M	3
			MB	[A.7]	R - L - SSVD - 7	M	3
Media - DDE	Disco Duro Externo	MB	MB	[N.2]	R - Media - DDE - 1	MB	1
			B	[N*]	R - Media - DDE - 2	MB	1
			MB	[I.5]	R - Media - DDE - 3	MB	1
			M	[I.6]	R - Media - DDE - 4	MB	1
			M	[I.7]	R - Media - DDE - 5	MB	1
			MB	[I.10]	R - Media - DDE - 6	MB	1
			B	[E.1]	R - Media - DDE - 7	MB	1
			MB	[E.2]	R - Media - DDE - 8	MB	1
			B	[E.15]	R - Media - DDE - 9	MB	1
			MB	[E.18]	R - Media - DDE - 10	MB	1
			MB	[E.19]	R - Media - DDE - 11	MB	1
			MB	[E.25]	R - Media - DDE - 12	MB	1
			A	[A.7]	R - Media - DDE - 13	B	2
			MB	[A.25]	R - Media - DDE - 14	MB	1

Responsables		Firmas
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

b) Valoración del Riesgo

	MAPA DE RIESGOS				
	Código del Formato: CF N° 10				**Fecha: ____/____/2020**
Fase: III – Evaluación del Riesgo					**Proceso: 6 – Identificación, Análisis y Valoración del Riesgo**
Objetivos:	- Situar los riesgos identificados en el mapa de riesgos con el propósito de mejorar la toma de decisiones mediante una vista gráfica.				
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.				
Entradas:	- Formato de Identificación y Análisis del Riesgo (**CF N° 09**).				
Salidas:					
RIESGO	**INTENSIDAD**				
	MÍNIMA (1)	**MENOR (2)**	**MEDIA (3)**	**CRÍTICA (4)**	**CATASTRÓFICA (5)**

PROBABILIDAD	**FRECUENTE (81 - 100 %)**	R-D-CRPD-1/R-D-CRPD-3/R-D-CRPD-4/R-D-CRPD-5/ R-D-CRPD-6/R-D-CRPD-7/R-D-CRPD-8/R-D-CRPD-9/ R-D-CRPD-10/R-SW-BDCA-1/R-SW-BDCA-3/R-SW-BDCA-4/R-SW-BDCA-5/R-SW-BDCA-6/R-SW-BDCA-8/R-SW-BDCA-11/R-SW-BDCA-12/R-SW-BDCA-13/R-SW-BDCA-14/R-SW-BDCA-15/R-SW-BDCA-16/R-SW-BDCA-17/R-SW-BDCA-18/R-SW-BDCA-19/R-SW-BDSIAF-1/R-SW-BDSIAF-3/R-SW-BDSIAF-4/R-SW-BDSIAF-5/R-SW-BDSIAF-6/R-SW-BDSIAF-8/R-SW-BDSIAF-11/R-SW-BDSIAF-12/R-SW-BDSIAF-13/R-SW-BDSIAF-14/R-SW-BDSIAF-15/R-SW-BDSIAF-16/R-SW-BDSIAF-17/R-SW-BDSIAF-18/R-SW-BDSIAF-19/R-SW-BDSIGA-1/R-SW-BDSIGA-3/R-SW-BDSIGA-4/R-SW-BDSIGA-5/R-SW-BDSIGA-6/R-SW-BDSIGA-8/R-SW-BDSIGA-11/R-SW-BDSIGA-12/R-SW-BDSIGA-13/R-SW-BDSIGA-14/R-SW-BDSIGA-15/R-SW-BDSIGA-16/R-SW-BDSIGA-17/R-SW-BDSIGA-18/R-SW-BDSIGA-19/R-SW-BDSISMED-1/R-SW-BDSISMED-3/R-SW-BDSISMED-4/R-SW-BDSISMED-5/R-SW-BDSISMED-6/R-SW-BDSISMED-8/R-SW-BDSISMED-11/R-SW-BDSISMED-12/R-SW-BDSISMED-13/R-SW-BDSISMED-14/R-SW-BDSISMED-15/R-SW-BDSISMED-16/R-SW-BDSISMED-17/R-SW-BDSISMED-18/R-SW-BDSISMED-19/R-HW-SVD-2/R-HW-SVD-4/R-HW-SVD-9/R-HW-SVD-10/R-HW-SVD-12/R-HW-SVD-13/R-HW-SVD-14/R-HW-SVD-15/R-HW-SVD-16	R - D - CRPD - 2/ R - SW – BDCA - 2/ R - SW – BDCA - 7/ R - SW – BDCA - 9/ R - SW – BDCA - 10/ R - SW – BDSIAF - 2/ R - SW – BDSIAF - 7/ R - SW – BDSIAF - 9/ R - SW – BDSIAF - 10/ R - SW – BDSIGA - 2/ R - SW – BDSIGA - 7/ R - SW – BDSIGA - 9/ R - SW – BDSIGA - 10/ R – SW - BDSISMED – 2/ R - SW - BDSISMED – 7/ R - SW – BDSISMED - 9/ R - SW - BDSISMED -10/ R - HW - SVD – 1/ R - HW - SVD – 3/ R - HW - SVD – 6/ R - HW - SVD – 7/ R - HW - SVD – 8/ R - HW - SVD - 11	R - HW - SVD - 5		
	PROBABLE (61 - 80 %)	R-D-HCL-1/R-D-HCL-3/R-D-HCL-5/R-D-HCL-7/ R-D-HCL-9/R-SW-AVS-1/R-SW-AVS-5/R-SW-AVS-7/ R-SW-AVS-8/R-SW-SOP-7/R-SW-SOP-9/R-SW-SOP-10/ R-SW-SOP-13/R-SW-SOP-14/R-SW-SOP-15/R-SW-SOP-17/R-SW-SOP-19/R-HW-MDM-2/R-HW-MDM-4/R-HW-MDM-9/R-HW-MDM-10/R-HW-MDM-11/R-HW-MDM-12/R-HW-MDM-13/R-HW-MDM-14/R-HW-MDM-15/R-HW-MDM-16/R-HW-SWT-2/R-HW-SWT-4/R-HW-SWT-9/R-HW-SWT-10/R-HW-SWT-11/R-HW-SWT-12/R-HW-SWT-13/R-HW-SWT-14/R-HW-SWT-15/R-HW-SWT-16/R-L-SSVD-3/R-L-SSVD-4/R-L-SSVD-5/R-L-SSVD-6/R-L-SSVD-7	R-D-HCL-2/R-D-HCL-8/R-D-HCL-10/ R-SW-AVS-4/R-SW-AVS-6/R-SW-SOP-1/ R-SW-SOP-2/R-SW-SOP-3/R-SW-SOP-5/ R-SW-SOP-6/R-SW-SOP-8/R-SW-SOP-11/ R-SW-SOP-16/R-SW-SOP-18/R-SW-SOP-20/ R-HW-MDM-1/R-HW-MDM-3/R-HW-MDM-6/R-HW-MDM-7/R-HW-MDM-8/R-HW-SWT-1/R-HW-SWT-3/R-HW-SWT-6/ R-HW-SWT-7/R-HW-SWT-8/R-L-SSVD-1/R-L-SSVD-2	R-D-HCL-4/R-D-HCL-6/ R-SW-AVS-2/R-SW-AVS-3/ R-SW-SOP-4/ R-SW-SOP-12/ R-HW-MDM-5/R-HW-SWT-5		
	OCASIONAL (41 - 60 %)	R-HW-UPS-2/R-HW-UPS-4/R-HW-UPS-5/R-COM-REN-1/R-COM-REN-2/R-COM-REN-3/R-AUX-FOC-2/R-AUX-FOC-3/R-AUX-FOC-4/R-AUX-FOC-7/R-AUX-FOC-8/R-AUX-FOM-2/R-AUX-FOM-3/R-AUX-FOM-4/R-AUX-FOM-7/R-AUX-FOM-8/R-P-JTI-2/R-P-JTI-4	R-HW-UPS-1/R-HW-UPS-3/R-HW-UPS-6/R-HW-UPS-7/R-COM-REN-4/R-AUX-FOC-1/ R-AUX-FOM-1	R-AUX-FOC-5/R-AUX-FOC-6/R-AUX-FOM-5/R-AUX-FOM-6/R-P-JTI-1/R-P-JTI-3/R-P-JTI-5		

	IMPROBABLE (21 - 40 %)					
	ESCASO (0 - 20 %)	R-SW-OFM-7/R-SW-OFM-8/R-HW-LPT-2/R-HW-LPT-3/ R-HW-LPT-4/R-HW-LPT-9/R-HW-LPT-10/R-HW-LPT-13/R-HW-LPT-14/R-SW-SCA-1/R-SW-SCA-2/R-SW-SCA-4/R-SW-SCA-5/R-SW-SCA-6/R-SW-SCA-7/R-Media-DDE-1/R-Media-DDE-3/R-Media-DDE-6/R-Media-DDE-8/R-Media-DDE-10/R-Media-DDE-11/R-Media-DDE-12/R-Media-DDE-14	R-SW-OFM-1/R-SW-OFM-3/R-HW-LPT-1/R-HW-LPT-6/R-HW-LPT-7/R-HW-LPT-8/R-HW-LPT-11/R-SW-SCA-3/R-SW-SCA-8/R-SW-SCA-9/R-Media-DDE-2/R-Media-DDE-7/R-Media-DDE-9	R - SW - OFM - 2/ R - SW - OFM - 4/ R - SW - OFM - 5/ R - HW - LPT - 5/ R - SW - SCA - 10/ R - Media-DDE-4/ R - Media-DDE- 5	R - SW - OFM - 6/ R - HW - LPT - 12/ R - Media – DDE - 13	

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

Leyenda:

Insuficiente	**Tolerable**	**Moderado**	**Importante**	**Intolerable**

HOSPITAL II - I "HHH"	**FORMATO DE VALORACIÓN DEL RIESGO**	
	Código del Formato: CF N° 11	**Fecha: ____/____/2020**
Fase: III – Evaluación del Riesgo		**Proceso: 6 – Identificación, Análisis y Valoración del Riesgo**
Objetivos:	- Determinar la capacidad de riesgo en base al establecimiento del apetito y la tolerancia de riesgos con el propósito de valorar los riesgos.	
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.	
Entradas:	- Formato de Identificación y Valoración de Amenazas (**CF N° 08**). - Formato de Identificación y Análisis del Riesgo (**CF N° 09**). - Mapa de Riesgos (**CF N° 10**).	

Salidas:

CÓDIGO	ACTIVO	TIPO DE AMENAZA	ID RIESGO	RIESGO	VALOR RIESGO	APETITO	TOLERANCIA	VALORACIÓN
D - CRPD	Copias de Respaldo	[E.1] Errores de los usuarios	R-D-CRPD-1	A	4	3	4	Importante
		[E.2] Errores del administrador	R-D-CRPD-2	MA	5	3	4	Intolerable
		[E.15] Alteración accidental de la información	R-D-CRPD-3	A	4	3	4	Importante
		[E.18] Destrucción de información	R-D-CRPD-4	A	4	3	4	Importante
		[E.19] Fugas de información	R-D-CRPD-5	A	4	3	4	Importante
		[A.6] Abuso de privilegios de acceso	R-D-CRPD-6	A	4	3	4	Importante
		[A.11] Acceso no autorizado	R-D-CRPD-7	A	4	3	4	Importante
		[A.15] Modificación deliberada de la información	R-D-CRPD-8	A	4	3	4	Importante

		[A.18] Destrucción de información	R-D-CRPD-9	A	4	3	4	Importante
		[A.19] Divulgación de información	R-D-CRPD-10	A	4	3	4	Importante
D - HCL	Historias Clínicas	[E.2] Errores del administrador	R-D-HCL-1	M	3	3	4	Moderado
		[E.15] Alteración accidental de la información	R-D-HCL-2	A	4	3	4	Importante
		[E.18] Destrucción de información	R-D-HCL-3	M	3	3	4	Moderado
		[E.19] Fugas de información	R-D-HCL-4	A	4	3	4	Importante
		[A.5] Suplantación de identidad del usuario	R-D-HCL-5	M	3	3	4	Moderado
		[A.6] Abuso de privilegios de acceso	R-D-HCL-6	A	4	3	4	Importante
		[A.11] Acceso no autorizado	R-D-HCL-7	M	3	3	4	Moderado
		[A.15] Modificación deliberada de la información	R-D-HCL-8	A	4	3	4	Importante
		[A.18] Destrucción de información	R-D-HCL-9	M	3	3	4	Moderado
		[A.19] Divulgación de información	R-D-HCL-10	A	4	3	4	Importante
SW - AVS	Antivirus	[I.5] Avería de origen físico o lógico	R-SW-AVS-1	M	3	3	4	Moderado
		[E.1] Errores de los usuarios	R-SW-AVS-2	A	4	3	4	Importante
		[E.8] Difusión de software dañino	R-SW-AVS-3	A	4	3	4	Importante
		[E.20] Vulnerabilidades de los programas (software)	R-SW-AVS-4	A	4	3	4	Importante
		[E.21] Errores de mantenimiento / actualización	R-SW-AVS-5	M	3	3	4	Moderado

		de programas (software)						
		[A.7] Uso no previsto	R-SW-AVS-6	A	4	3	4	Importante
		[A.8] Difusión de software dañino	R-SW-AVS-7	M	3	3	4	Moderado
		[A.11] Acceso no autorizado	R-SW-AVS-8	M	3	3	4	Moderado
SW - BDCA	Base de datos Access - Control de Asistencia	[I.5] Avería de origen físico o lógico	R-SW-BDCA-1	A	4	3	4	Importante
		[E.2] Errores del administrador	R-SW-BDCA-2	MA	5	3	4	Intolerable
		[E.8] Difusión de software dañino	R-SW-BDCA-3	A	4	3	4	Importante
		[E.15] Alteración accidental de la información	R-SW-BDCA-4	A	4	3	4	Importante
		[E.18] Destrucción de información	R-SW-BDCA-5	A	4	3	4	Importante
		[E.19] Fugas de información	R-SW-BDCA-6	A	4	3	4	Importante
		[E.20] Vulnerabilidades de los programas (software)	R-SW-BDCA-7	MA	5	3	4	Intolerable
		[E.21] Errores de mantenimiento / actualización de programas (software)	R-SW-BDCA-8	A	4	3	4	Importante
		[A.5] Suplantación de identidad del usuario	R-SW-BDCA-9	MA	5	3	4	Intolerable
		[A.6] Abuso de privilegios de acceso	R-SW-BDCA-10	MA	5	3	4	Intolerable
		[A.7] Uso no previsto	R-SW-BDCA-11	A	4	3	4	Importante
		[A.8] Difusión de software dañino	R-SW-BDCA-12	A	4	3	4	Importante
		[A.9] [Re-]encaminamiento de mensajes	R-SW-BDCA-13	A	4	3	4	Importante
		[A.10] Alteración de	R-SW-BDCA-14	A	4	3	4	Importante

		secuencia						
		[A.11] Acceso no autorizado	R-SW-BDCA-15	A	4	3	4	Importante
		[A.15] Modificación deliberada de la información	R-SW-BDCA-16	A	4	3	4	Importante
		[A.18] Destrucción de información	R-SW-BDCA-17	A	4	3	4	Importante
		[A.19] Divulgación de la información	R-SW-BDCA-18	A	4	3	4	Importante
		[A.22] Manipulación de programas	R-SW-BDCA-19	A	4	3	4	Importante
SW - BDSIAF	Base de datos MVFP - SIAF	[I.5] Avería de origen físico o lógico	R-SW-BDSIAF-1	A	4	3	4	Importante
		[E.2] Errores del administrador	R-SW-BDSIAF-2	MA	5	3	4	Intolerable
		[E.8] Difusión de software dañino	R-SW-BDSIAF-3	A	4	3	4	Importante
		[E.15] Alteración accidental de la información	R-SW-BDSIAF-4	A	4	3	4	Importante
		[E.18] Destrucción de información	R-SW-BDSIAF-5	A	4	3	4	Importante
		[E.19] Fugas de información	R-SW-BDSIAF-6	A	4	3	4	Importante
		[E.20] Vulnerabilidades de los programas (software)	R-SW-BDSIAF-7	MA	5	3	4	Intolerable
		[E.21] Errores de mantenimiento / actualización de programas (software)	R-SW-BDSIAF-8	A	4	3	4	Importante
		[A.5] Suplantación de identidad del usuario	R-SW-BDSIAF-9	MA	5	3	4	Intolerable
		[A.6] Abuso de privilegios de acceso	R-SW-BDSIAF-10	MA	5	3	4	Intolerable
		[A.7] Uso no previsto	R-SW-BDSIAF-	A	4	3	4	Importante

			11					
		[A.8] Difusión de software dañino	R-SW-BDSIAF-12	A	4	3	4	Importante
		[A.9] [Re-]encaminamiento de mensajes	R-SW-BDSIAF-13	A	4	3	4	Importante
		[A.10] Alteración de secuencia	R-SW-BDSIAF-14	A	4	3	4	Importante
		[A.11] Acceso no autorizado	R-SW-BDSIAF-15	A	4	3	4	Importante
		[A.15] Modificación deliberada de la información	R-SW-BDSIAF-16	A	4	3	4	Importante
		[A.18] Destrucción de información	R-SW-BDSIAF-17	A	4	3	4	Importante
		[A.19] Divulgación de la información	R-SW-BDSIAF-18	A	4	3	4	Importante
		[A.22] Manipulación de programas	R-SW-BDSIAF-19	A	4	3	4	Importante
SW - BDSIGA	Base de datos SQL - SIGA	[I.5] Avería de origen físico o lógico	R-SW-BDSIGA-1	A	4	3	4	Importante
		[E.2] Errores del administrador	R-SW-BDSIGA-2	MA	5	3	4	Intolerable
		[E.8] Difusión de software dañino	R-SW-BDSIGA-3	A	4	3	4	Importante
		[E.15] Alteración accidental de la información	R-SW-BDSIGA-4	A	4	3	4	Importante
		[E.18] Destrucción de información	R-SW-BDSIGA-5	A	4	3	4	Importante
		[E.19] Fugas de información	R-SW-BDSIGA-6	A	4	3	4	Importante
		[E.20] Vulnerabilidades de los programas (software)	R-SW-BDSIGA-7	MA	5	3	4	Intolerable

		[E.21] Errores de mantenimiento / actualización de programas (software)	R-SW-BDSIGA-8	A	4	3	4	Importante
		[A.5] Suplantación de identidad del usuario	R-SW-BDSIGA-9	MA	5	3	4	Intolerable
		[A.6] Abuso de privilegios de acceso	R-SW-BDSIGA-10	MA	5	3	4	Intolerable
		[A.7] Uso no previsto	R-SW-BDSIGA-11	A	4	3	4	Importante
		[A.8] Difusión de software dañino	R-SW-BDSIGA-12	A	4	3	4	Importante
		[A.9] [Re-]encaminamiento de mensajes	R-SW-BDSIGA-13	A	4	3	4	Importante
		[A.10] Alteración de secuencia	R-SW-BDSIGA-14	A	4	3	4	Importante
		[A.11] Acceso no autorizado	R-SW-BDSIGA-15	A	4	3	4	Importante
		[A.15] Modificación deliberada de la información	R-SW-BDSIGA-16	A	4	3	4	Importante
		[A.18] Destrucción de información	R-SW-BDSIGA-17	A	4	3	4	Importante
		[A.19] Divulgación de la información	R-SW-BDSIGA-18	A	4	3	4	Importante
		[A.22] Manipulación de programas	R-SW-BDSIGA-19	A	4	3	4	Importante
SW - BDSISMED	Base de datos MVFP - SISMED	[I.5] Avería de origen físico o lógico	R-SW-BDSISMED-1	A	4	3	4	Importante
		[E.2] Errores del administrador	R-SW-BDSISMED-2	MA	5	3	4	Intolerable
		[E.8] Difusión de software dañino	R-SW-BDSISMED-3	A	4	3	4	Importante

		[E.15] Alteración accidental de la información	R-SW-BDSISMED-4	A	4	3	4	Importante
		[E.18] Destrucción de información	R-SW-BDSISMED-5	A	4	3	4	Importante
		[E.19] Fugas de información	R-SW-BDSISMED-6	A	4	3	4	Importante
		[E.20] Vulnerabilidades de los programas (software)	R-SW-BDSISMED-7	MA	5	3	4	Intolerable
		[E.21] Errores de mantenimiento / actualización de programas (software)	R-SW-BDSISMED-8	A	4	3	4	Importante
		[A.5] Suplantación de identidad del usuario	R-SW-BDSISMED-9	MA	5	3	4	Intolerable
		[A.6] Abuso de privilegios de acceso	R-SW-BDSISMED-10	MA	5	3	4	Intolerable
		[A.7] Uso no previsto	R-SW-BDSISMED-11	A	4	3	4	Importante
		[A.8] Difusión de software dañino	R-SW-BDSISMED-12	A	4	3	4	Importante
		[A.9] [Re-]encaminamiento de mensajes	R-SW-BDSISMED-13	A	4	3	4	Importante
		[A.10] Alteración de secuencia	R-SW-BDSISMED-14	A	4	3	4	Importante
		[A.11] Acceso no autorizado	R-SW-BDSISMED-15	A	4	3	4	Importante
		[A.15] Modificación deliberada de la información	R-SW-BDSISMED-16	A	4	3	4	Importante
		[A.18] Destrucción de información	R-SW-BDSISMED-17	A	4	3	4	Importante
		[A.19] Divulgación de la información	R-SW-BDSISMED-18	A	4	3	4	Importante

		[A.22] Manipulación de programas	R-SW-BDSISMED-19	A	4	3	4	Importante
SW - OFM	Ofimática	[I.5] Avería de origen físico o lógico	R - SW - OFM - 1	MB	1	3	4	Insuficiente
		[E.1] Errores de los usuarios	R - SW - OFM - 2	MB	1	3	4	Insuficiente
		[E.8] Difusión de software dañino	R - SW - OFM - 3	MB	1	3	4	Insuficiente
		[E.18] Destrucción de información	R - SW - OFM - 4	MB	1	3	4	Insuficiente
		[E.20] Vulnerabilidades de los programas (software)	R - SW - OFM - 5	MB	1	3	4	Insuficiente
		[A.7] Uso no previsto	R - SW - OFM - 6	B	2	3	4	Tolerable
		[A.8] Difusión de software dañino	R - SW - OFM - 7	MB	1	3	4	Insuficiente
		[A.11] Acceso no autorizado	R - SW - OFM - 8	MB	1	3	4	Insuficiente
HW - LPT	Laptop	[N.*] Desastres naturales	R - HW - LPT - 1	MB	1	3	4	Insuficiente
		[I.1] Fuego	R - HW - LPT - 2	MB	1	3	4	Insuficiente
		[I.2] Daños por agua	R - HW - LPT - 3	MB	1	3	4	Insuficiente
		[I.5] Avería de origen físico o lógico	R - HW - LPT - 4	MB	1	3	4	Insuficiente
		[I.6] Corte del suministro eléctrico	R - HW - LPT - 5	MB	1	3	4	Insuficiente
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - HW - LPT - 6	MB	1	3	4	Insuficiente
		[E.2] Errores del administrador	R - HW - LPT - 7	MB	1	3	4	Insuficiente
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R - HW - LPT - 8	MB	1	3	4	Insuficiente
		[E.24] Caída del sistema por agotamiento de recursos	R - HW - LPT - 9	MB	1	3	4	Insuficiente

		[E.25] Pérdida de equipos	R- HW - LPT - 10	MB	1	3	4	Insuficiente
		[A.6] Abuso de privilegios de acceso	R - HW - LPT - 11	MB	1	3	4	Insuficiente
		[A.7] Uso no previsto	R- HW - LPT - 12	B	2	3	4	Tolerable
		[A.24]Denegación de servicio	R- HW - LPT - 13	MB	1	3	4	Insuficiente
		[A.25] Robo	R- HW - LPT - 14	MB	1	3	4	Insuficiente
SW - SOP	Sistemas Operativos	[I.5] Avería de origen físico o lógico	R - SW - SOP - 1	A	4	3	4	Importante
		[E.1] Errores de los usuarios	R - SW - SOP - 2	A	4	3	4	Importante
		[E.2] Errores del administrador	R - SW - SOP - 3	A	4	3	4	Importante
		[E.8] Difusión de software dañino	R - SW - SOP - 4	A	4	3	4	Importante
		[E.15] Alteración accidental de la información	R - SW - SOP - 5	A	4	3	4	Importante
		[E.18] Destrucción de información	R - SW - SOP - 6	A	4	3	4	Importante
		[E.19] Fugas de información	R - SW - SOP - 7	M	3	3	4	Moderado
		[E.20] Vulnerabilidades de los programas (software)	R - SW - SOP - 8	A	4	3	4	Importante
		[E.21] Errores de mantenimiento / actualización de programas (software)	R - SW - SOP - 9	M	3	3	4	Moderado
		[A.5] Suplantación de identidad del usuario	R - SW - SOP - 10	M	3	3	4	Moderado
		[A.6] Abuso de privilegios de acceso	R - SW - SOP - 11	A	4	3	4	Importante
		[A.7] Uso no previsto	R- SW - SOP - 12	A	4	3	4	Importante
		[A.8] Difusión de software dañino	R - SW - SOP - 13	M	3	3	4	Moderado
		[A.9] [Re-]encaminamiento	R - SW - SOP -	M	3	3	4	Moderado

		de mensajes	14					
		[A.10] Alteración de secuencia	R - SW - SOP - 15	M	3	3	4	Moderado
		[A.11] Acceso no autorizado	R- SW - SOP - 16	A	4	3	4	Importante
		[A.15] Modificación deliberada de la información	R - SW - SOP - 17	M	3	3	4	Moderado
		[A.18] Destrucción de información	R - SW - SOP - 18	A	4	3	4	Importante
		[A.19] Divulgación de la información	R - SW - SOP - 19	M	3	3	4	Moderado
		[A.22] Manipulación de programas	R - SW - SOP - 20	A	4	3	4	Importante
SW - SCA	Sistema de Control y Asistencia	[I.5] Avería de origen físico o lógico	R - SW - SCA - 1	MB	1	3	4	Insuficiente
		[E.1] Errores de los usuarios	R - SW - SCA - 2	MB	1	3	4	Insuficiente
		[E.2] Errores del administrador	R - SW - SCA - 3	MB	1	3	4	Insuficiente
		[E.15] Alteración accidental de la información	R - SW - SCA - 4	MB	1	3	4	Insuficiente
		[E.18] Destrucción de información	R - SW - SCA - 5	MB	1	3	4	Insuficiente
		[E.19] Fugas de información	R - SW - SCA - 6	MB	1	3	4	Insuficiente
		[E.20] Vulnerabilidades de los programas (software)	R - SW - SCA - 7	MB	1	3	4	Insuficiente
		[A.5] Suplantación de la identidad del usuario	R - SW - SCA - 8	MB	1	3	4	Insuficiente
		[A.6] Abuso de privilegios de acceso	R - SW - SCA - 9	MB	1	3	4	Insuficiente
		[A.15] Modificación deliberada de la información	R - SW - SCA - 10	MB	1	3	4	Insuficiente
HW - SVD	Servidor	[N.*] Desastres naturales	R - HW - SVD - 1	MA	5	3	4	Intolerable

		[I.1] Fuego	R - HW - SVD - 2	A	4	3	4	Importante
		[I.2] Daños por agua	R - HW - SVD - 3	MA	5	3	4	Intolerable
		[I.5] Avería de origen físico o lógico	R - HW - SVD - 4	A	4	3	4	Importante
		[I.6] Corte del suministro eléctrico	R - HW - SVD - 5	MA	5	3	4	Intolerable
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - HW - SVD - 6	MA	5	3	4	Intolerable
		[E.2] Errores del administrador	R - HW - SVD - 7	MA	5	3	4	Intolerable
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R - HW - SVD - 8	MA	5	3	4	Intolerable
		[E.24] Caída del sistema por agotamiento de recursos	R - HW - SVD - 9	A	4	3	4	Importante
		[E.25] Pérdida de equipos	R-HW - SVD - 10	A	4	3	4	Importante
		[A.6] Abuso de privilegios de acceso	R - HW - SVD - 11	MA	5	3	4	Intolerable
		[A.7] Uso no previsto	R-HW - SVD - 12	A	4	3	4	Importante
		[A.11] Acceso no autorizado	R-HW - SVD - 13	A	4	3	4	Importante
		[A.23] Manipulación de los equipos	R - HW - SVD - 14	A	4	3	4	Importante
		[A.24]Denegación de servicio	R-HW - SVD - 15	A	4	3	4	Importante
		[A.25] Robo	R-HW - SVD - 16	A	4	3	4	Importante
HW - MDM	Módem	[N.*] Desastres naturales	R-HW - MDM - 1	A	4	3	4	Importante
		[I.1] Fuego	R-HW - MDM - 2	M	3	3	4	Moderado
		[I.2] Daños por agua	R-HW - MDM - 3	A	4	3	4	Importante
		[I.5] Avería de origen físico o lógico	R - HW - MDM - 4	M	3	3	4	Moderado
		[I.6] Corte del suministro eléctrico	R - HW - MDM - 5	A	4	3	4	Importante

		[I.7]Condiciones inadecuadas de temperatura o humedad	R - HW - MDM - 6	A	4	3	4	Importante
		[E.2] Errores del administrador	R - HW - MDM - 7	A	4	3	4	Importante
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R - HW - MDM - 8	A	4	3	4	Importante
		[E.24] Caída del sistema por agotamiento de recursos	R - HW - MDM - 9	M	3	3	4	Moderado
		[E.25] Pérdida de equipos	R-HW-MDM - 10	M	3	3	4	Moderado
		[A.6] Abuso de privilegios de acceso	R - HW - MDM - 11	M	3	3	4	Moderado
		[A.7] Uso no previsto	R-HW-MDM - 12	M	3	3	4	Moderado
		[A.11] Acceso no autorizado	R-HW-MDM - 13	M	3	3	4	Moderado
		[A.23] Manipulación de los equipos	R - HW - MDM - 14	M	3	3	4	Moderado
		[A.24]Denegación de servicio	R-HW-MDM - 15	M	3	3	4	Moderado
		[A.25] Robo	R-HW-MDM - 16	M	3	3	4	Moderado
HW - SWT	Switch para Red	[N.*] Desastres naturales	R- HW - SWT - 1	A	4	3	4	Importante
		[I.1] Fuego	R- HW - SWT - 2	M	3	3	4	Moderado
		[I.2] Daños por agua	R- HW - SWT - 3	A	4	3	4	Importante
		[I.5] Avería de origen físico o lógico	R - HW - SWT - 4	M	3	3	4	Moderado
		[I.6] Corte del suministro eléctrico	R - HW - SWT - 5	A	4	3	4	Importante
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - HW - SWT - 6	A	4	3	4	Importante
		[E.2] Errores del administrador	R - HW - SWT - 7	A	4	3	4	Importante
		[E.23] Errores de mantenimiento / actualización	R - HW - SWT - 8	A	4	3	4	Importante

		de equipos (hardware)						
		[E.24] Caída del sistema por agotamiento de recursos	R - HW - SWT - 9	M	3	3	4	Moderado
		[E.25] Pérdida de equipos	R-HW- SWT - 10	M	3	3	4	Moderado
		[A.6] Abuso de privilegios de acceso	R - HW - SWT - 11	M	3	3	4	Moderado
		[A.7] Uso no previsto	R-HW- SWT - 12	M	3	3	4	Moderado
		[A.11] Acceso no autorizado	R-HW- SWT - 13	M	3	3	4	Moderado
		[A.23] Manipulación de los equipos	R - HW - SWT - 14	M	3	3	4	Moderado
		[A.24]Denegación de servicio	R-HW- SWT - 15	M	3	3	4	Moderado
		[A.25] Robo	R-HW- SWT - 16	M	3	3	4	Moderado
HW - UPS	Acumulador de Energía - UPS	[N.*] Desastres naturales	R - HW - UPS - 1	M	3	3	4	Moderado
		[I.1] Fuego	R - HW - UPS - 2	B	2	3	4	Tolerable
		[I.2] Daños por agua	R - HW - UPS - 3	M	3	3	4	Moderado
		[I.5] Avería de origen físico o lógico	R - HW - UPS - 4	B	2	3	4	Tolerable
		[I.6] Corte del suministro eléctrico	R - HW - UPS - 5	B	2	3	4	Tolerable
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - HW - UPS - 6	M	3	3	4	Moderado
		[A.25] Robo	R - HW - UPS - 7	M	3	3	4	Moderado
COM - REN	Radio Enlace	[I.8] Fallo de servicios de comunicaciones	R - COM - REN - 1	B	2	3	4	Tolerable
		[E.2] Errores del administrador	R - COM - REN - 2	B	2	3	4	Tolerable
		[E.9] Errores de [re-] encaminamiento	R - COM - REN - 3	B	2	3	4	Tolerable
		[E.24] Caída del sistema por agotamiento de recursos	R - COM - REN - 4	M	3	3	4	Moderado
		[A.24]Denegación de servicio	R-COM- REN - 5	M	3	3	4	Moderado

AUX - FOC	Fibra Óptica Claro	[N.*] Desastres naturales	R-AUX - FOC - 1	M	3	3	4	Moderado
		[I.1] Fuego	R-AUX - FOC - 2	B	2	3	4	Tolerable
		[I.2] Daños por agua	R-AUX - FOC - 3	B	2	3	4	Tolerable
		[I.5] Avería de origen físico o lógico	R - AUX - FOC - 4	B	2	3	4	Tolerable
		[I.6] Corte del suministro eléctrico	R - AUX - FOC - 5	M	3	3	4	Moderado
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - AUX - FOC - 6	M	3	3	4	Moderado
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R - AUX - FOC - 7	B	2	3	4	Tolerable
		[A.7] Uso no previsto	R-AUX - FOC - 8	B	2	3	4	Tolerable
AUX - FOM	Fibra Óptica Movistar	[N.*] Desastres naturales	R-AUX-FOM - 1	M	3	3	4	Moderado
		[I.1] Fuego	R-AUX- FOM - 2	B	2	3	4	Tolerable
		[I.2] Daños por agua	R-AUX- FOM - 3	B	2	3	4	Tolerable
		[I.5] Avería de origen físico o lógico	R - AUX - FOM - 4	B	2	3	4	Tolerable
		[I.6] Corte del suministro eléctrico	R - AUX - FOM - 5	M	3	3	4	Moderado
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - AUX - FOM - 6	M	3	3	4	Moderado
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R - AUX - FOM - 7	B	2	3	4	Tolerable
		[A.7] Uso no previsto	R-AUX- FOM - 8	B	2	3	4	Tolerable
P - JTI	Jefe de TI	[E.7] Deficiencias en la organización	R - P - JTI - 1	M	3	3	4	Moderado
		[E.19] Fugas de información	R - P - JTI - 2	B	2	3	4	Tolerable
		[E.28] Indisponibilidad del personal	R - P - JTI - 3	M	3	3	4	Moderado

		[A.28] Indisponibilidad del personal	R - P - JTI - 4	B	2	3	4	Tolerable
		[A.30] Ingeniería social (picaresca)	R - P - JTI - 5	M	3	3	4	Moderado
L - SSVD	Sala de Servidores	[N.*] Desastres Naturales	R - L - SSVD - 1	A	4	3	4	Importante
		[I.2] Daños por agua	R - L - SSVD - 2	A	4	3	4	Importante
		[I.11] Emanaciones electromagnéticas	R - L - SSVD - 3	M	3	3	4	Moderado
		[E.15] Alteración accidental de la información	R - L - SSVD - 4	M	3	3	4	Moderado
		[E.18] Destrucción de información	R - L - SSVD - 5	M	3	3	4	Moderado
		[E.19] Fugas de información	R - L - SSVD - 6	M	3	3	4	Moderado
		[A.7] Uso no previsto	R - L - SSVD - 7	M	3	3	4	Moderado
Media - DDE	Disco Duro Externo	[N.2] Daños por agua	R-Media-DDE-1	MB	1	3	4	Insuficiente
		[N.*] Desastres naturales	R - Media- DE - 2	MB	1	3	4	Insuficiente
		[I.5] Avería de origen físico o lógico	R-Media-DDE - 3	MB	1	3	4	Insuficiente
		[I.6] Corte del suministro eléctrico	R-Media-DDE - 4	MB	1	3	4	Insuficiente
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - Media - DDE - 5	MB	1	3	4	Insuficiente
		[I.10] Degradación de los soportes de almacenamiento de la información	R - Media - DDE - 6	MB	1	3	4	Insuficiente
		[E.1] Errores de los usuarios	R-Media-DDE-7	MB	1	3	4	Insuficiente
		[E.2] Errores del administrador	R - Media - DDE - 8	MB	1	3	4	Insuficiente
		[E.15] Alteración accidental de la información	R - Media - DDE - 9	MB	1	3	4	Insuficiente
		[E.18] Destrucción de	R - Media - DDE	MB	1	3	4	Insuficiente

		información	- 10					
		[E.19] Fugas de información	R-Media-DDE-11	MB	1	3	4	Insuficiente
		[E.25] Pérdida de equipos	R-Media-DDE-12	MB	1	3	4	Insuficiente
		[A.7] Uso no previsto	R-Media-DDE-13	B	2	3	4	Tolerable
		[A.25] Robo	R-Media-DDE-14	MB	1	3	4	Insuficiente

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

Fase IV: Tratamiento del Riesgo

Proceso 8: Implementar Planes de Tratamiento del Riesgo

HOSPITAL II - I "HHH"	**FORMATO DE SELECCIÓN E IMPLEMENTACIÓN DE PLANES DE TRATAMIENTO DEL RIESGO**	
	Código del Formato: CF N° 12	**Fecha: ____/____/2020**
Fase: IV – Tratamiento del Riesgo		**Proceso: 8 – Implementar Planes de Tratamiento del Riesgo**
Objetivos:	- Implementar los Planes de Tratamiento del Riesgo empleando a la vez las opciones de tratamiento del riesgo seleccionadas en el Proceso 7, con la finalidad de mitigar los riesgos y amenazas.	
Personal Involucrado:	- Director del Hospital. - Administrador del Hospital. - Jefe de la Unidad de Estadística e Informática (TI). - Personal Analista.	
Entradas:	- Formato de Valoración del Riesgo (**CF N° 11**). - Opciones de Tratamiento del Riesgo (**Tabla 18 del informe [p. 103]**). - Catálogo de Salvaguardas (**ANEXO N° 08**).	

Salidas:

CÓDIGO	ACTIVO	TIPO DE AMENAZA	ID RIESGO	RIESGO	VALORACIÓN	TRATAMIENTO	SALVAGUARDA
D - CRPD	Copias de Respaldo	[E.2] Errores del administrador	R-D-CRPD-2	MA	Intolerable	MR	✓ H Protecciones Generales. ✓ H.IA Identificación y autenticación. ✓ H.AC Control de acceso lógico. ✓ H.tools Herramientas de seguridad. ✓ H.tools.IDS
		[E.1] Errores de los usuarios	R-D-CRPD-1	A	Importante		
		[E.15] Alteración accidental de la información	R-D-CRPD-3				
		[E.18] Destrucción de información	R-D-CRPD-4				
		[E.19] Fugas de información	R-D-CRPD-5				
		[A.6] Abuso de privilegios de acceso	R-D-CRPD-6				

		[A.11] Acceso no autorizado	R-D-CRPD-7				IDS/IPS: Herramienta de detección / prevención de intrusión ✓ D Protección de la Información. ✓ D.A Copias de seguridad de los datos (backup). ✓ D.I Aseguramiento de la integridad. ✓ D.C Cifrado de la información.
		[A.15] Modificación deliberada de la información	R-D-CRPD-8				
		[A.18] Destrucción de información	R-D-CRPD-9				
		[A.19] Divulgación de información	R-D-CRPD-10				
D - HCL	Historias Clínicas	[E.15] Alteración accidental de la información	R-D-HCL-2	A	Importante	MR	✓ H.tools Herramientas de seguridad ✓ D Protección de la Información. ✓ D.I Aseguramiento de la integridad. ✓ D.C Cifrado de la información.
		[E.19] Fugas de información	R-D-HCL-4				
		[A.6] Abuso de privilegios de acceso	R-D-HCL-6				
		[A.15] Modificación deliberada de la información	R-D-HCL-8				
		[A.19] Divulgación de información	R-D-HCL-10				
		[E.2] Errores del administrador	R-D-HCL-1	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[E.18] Destrucción de información	R-D-HCL-3				
		[A.5] Suplantación de identidad del usuario	R-D-HCL-5				
		[A.11] Acceso no autorizado	R-D-HCL-7				
		[A.18] Destrucción de información	R-D-HCL-9				

SW - AVS	Antivirus	[E.1] Errores de los usuarios	R-SW-AVS-2	A	Importante	MR	✓ H.tools.AV Herramienta contra código dañino. ✓ SW Protección de las Aplicaciones Informáticas. ✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican perfiles de seguridad.
		[E.8] Difusión de software dañino	R-SW-AVS-3				
		[E.20] Vulnerabilidades de los programas (software)	R-SW-AVS-4				
		[A.7] Uso no previsto	R-SW-AVS-6				
		[I.5] Avería de origen físico o lógico	R-SW-AVS-1	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[E.21] Errores de mantenimiento/actualización de programas (software)	R-SW-AVS-5				
		[A.8] Difusión de software dañino	R-SW-AVS-7				
		[A.11] Acceso no autorizado	R-SW-AVS-8				
SW - BDCA	Base de datos Access - Control de Asistencia	[E.2] Errores del administrador	R-SW-BDCA-2	MA	Intolerable	MR	✓ H.IA Identificación y autenticación. ✓ H.tools Herramientas de seguridad. ✓ H.tools.AV Herramienta contra código dañino. ✓ H.tools.IDS IDS/IPS: Herramienta de detección /
		[E.20] Vulnerabilidades de los programas (software)	R-SW-BDCA-7				
		[A.5] Suplantación de identidad del usuario	R-SW-BDCA-9				
		[A.6] Abuso de privilegios de acceso	R-SW-BDCA-10				
		[I.5] Avería de origen físico o lógico	R-SW-BDCA-1	A	Importante		
		[E.8] Difusión de software dañino	R-SW-BDCA-3				

		[E.15] Alteración accidental de la información	R-SW-BDCA-4				prevención de intrusión. ✓ H.tools.VA Herramienta de análisis de vulnerabilidades. ✓ SW Protección de las Aplicaciones Informáticas. ✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican perfiles de seguridad.
		[E.18] Destrucción de información	R-SW-BDCA-5				
		[E.19] Fugas de información	R-SW-BDCA-6				
		[E.21] Errores de mantenimiento / actualización de programas (software)	R-SW-BDCA-8				
		[A.7] Uso no previsto	R-SW-BDCA-11				
		[A.8] Difusión de software dañino	R-SW-BDCA-12				
		[A.9] [Re-]encaminamiento de mensajes	R-SW-BDCA-13				
		[A.10] Alteración de secuencia	R-SW-BDCA-14				
		[A.11] Acceso no autorizado	R-SW-BDCA-15				
		[A.15] Modificación deliberada de la información	R-SW-BDCA-16				
		[A.18] Destrucción de información	R-SW-BDCA-17				
		[A.19] Divulgación de la información	R-SW-BDCA-18				
		[A.22] Manipulación de programas	R-SW-BDCA-19				
SW - BDSIAF	Base de datos MVFP - SIAF	[E.2] Errores del administrador	R-SW-BDSIAF-2	MA	Intolerable	MR	✓ H.IA Identificación y autenticación. ✓ H.tools Herramientas de seguridad. ✓ H.tools.AV Herramienta contra
		[E.20] Vulnerabilidades de los programas (software)	R-SW-BDSIAF-7				
		[A.5] Suplantación de identidad del usuario	R-SW-BDSIAF-9				
		[A.6] Abuso de privilegios de	R-SW-BDSIAF-				

		acceso	10				código dañino. ✓ H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión. ✓ H.tools.VA Herramienta de análisis de vulnerabilidades. ✓ SW Protección de las Aplicaciones Informáticas. ✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican perfiles de seguridad.
		[I.5] Avería de origen físico o lógico	R-SW-BDSIAF-1	A	Importante		
		[E.8] Difusión de software dañino	R-SW-BDSIAF-3				
		[E.15] Alteración accidental de la información	R-SW-BDSIAF-4				
		[E.18] Destrucción de información	R-SW-BDSIAF-5				
		[E.19] Fugas de información	R-SW-BDSIAF-6				
		[E.21] Errores de mantenimiento / actualización de programas (software)	R-SW-BDSIAF-8				
		[A.7] Uso no previsto	R-SW-BDSIAF-11				
		[A.8] Difusión de software dañino	R-SW-BDSIAF-12				
		[A.9] [Re-]encaminamiento de mensajes	R-SW-BDSIAF-13				
		[A.10] Alteración de secuencia	R-SW-BDSIAF-14				
		[A.11] Acceso no autorizado	R-SW-BDSIAF-15				
		[A.15] Modificación deliberada de la información	R-SW-BDSIAF-16				
		[A.18] Destrucción de información	R-SW-BDSIAF-17				
		[A.19] Divulgación de la información	R-SW-BDSIAF-18				
		[A.22] Manipulación de programas	R-SW-BDSIAF-19				

SW - BDSIGA	Base de datos SQL - SIGA	[E.2] Errores del administrador	R-SW-BDSIGA-2	MA	Intolerable	MR	✓ H.IA Identificación y autenticación. ✓ H.tools Herramientas de seguridad. ✓ H.tools.AV Herramienta contra código dañino. ✓ H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión. ✓ H.tools.VA Herramienta de análisis de vulnerabilidades. ✓ SW Protección de las Aplicaciones Informáticas. ✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican perfiles de seguridad.
		[E.20] Vulnerabilidades de los programas (software)	R-SW-BDSIGA-7				
		[A.5] Suplantación de identidad del usuario	R-SW-BDSIGA-9				
		[A.6] Abuso de privilegios de acceso	R-SW-BDSIGA-10				
		[I.5] Avería de origen físico o lógico	R-SW-BDSIGA-1	A	Importante		
		[E.8] Difusión de software dañino	R-SW-BDSIGA-3				
		[E.15] Alteración accidental de la información	R-SW-BDSIGA-4				
		[E.18] Destrucción de información	R-SW-BDSIGA-5				
		[E.19] Fugas de información	R-SW-BDSIGA-6				
		[E.21] Errores de mantenimiento / actualización de programas (software)	R-SW-BDSIGA-8				
		[A.7] Uso no previsto	R-SW-BDSIGA-11				
		[A.8] Difusión de software dañino	R-SW-BDSIGA-12				
		[A.9] [Re-]encaminamiento de mensajes	R-SW-BDSIGA-13				
		[A.10] Alteración de secuencia	R-SW-BDSIGA-14				
		[A.11] Acceso no autorizado	R-SW-BDSIGA-15				
		[A.15] Modificación	R-SW-BDSIGA-				

		deliberada de la información	16				
		[A.18] Destrucción de información	R-SW-BDSIGA-17				
		[A.19] Divulgación de la información	R-SW-BDSIGA-18				
		[A.22] Manipulación de programas	R-SW-BDSIGA-19				
SW - BDSISMED	Base de datos MVFP - SISMED	[E.2] Errores del administrador	R-SW-BDSISMED-2	MA	Intolerable	MR	✓ H.IA Identificación y autenticación. ✓ H.tools Herramientas de seguridad. ✓ H.tools.AV Herramienta contra código dañino. ✓ H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión. ✓ H.tools.VA Herramienta de análisis de vulnerabilidades. ✓ SW Protección de las Aplicaciones Informáticas. ✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican
		[E.20] Vulnerabilidades de los programas (software)	R-SW-BDSISMED-7				
		[A.5] Suplantación de identidad del usuario	R-SW-BDSISMED-9				
		[A.6] Abuso de privilegios de acceso	R-SW-BDSISMED-10				
		[I.5] Avería de origen físico o lógico	R-SW-BDSISMED-1	A	Importante		
		[E.8] Difusión de software dañino	R-SW-BDSISMED-3				
		[E.15] Alteración accidental de la información	R-SW-BDSISMED-4				
		[E.18] Destrucción de información	R-SW-BDSISMED-5				
		[E.19] Fugas de información	R-SW-BDSISMED-6				
		[E.21] Errores de mantenimiento / actualización de programas (software)	R-SW-BDSISMED-8				
		[A.7] Uso no previsto	R-SW-BDSISMED-11				
		[A.8] Difusión de software	R-SW-				

		dañino	BDSISMED-12				perfiles de seguridad.
		[A.9] [Re-]encaminamiento de mensajes	R-SW-BDSISMED-13				
		[A.10] Alteración de secuencia	R-SW-BDSISMED-14				
		[A.11] Acceso no autorizado	R-SW-BDSISMED-15				
		[A.15] Modificación deliberada de la información	R-SW-BDSISMED-16				
		[A.18] Destrucción de información	R-SW-BDSISMED-17				
		[A.19] Divulgación de la información	R-SW-BDSISMED-18				
		[A.22] Manipulación de programas	R-SW-BDSISMED-19				
SW - OFM	Ofimática	[A.7] Uso no previsto	R-SW-OFM-6	B	Tolerable	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[I.5] Avería de origen físico o lógico	R - SW - OFM - 1	MB	Insuficiente		
		[E.1] Errores de los usuarios	R - SW - OFM - 2				
		[E.8] Difusión de software dañino	R - SW - OFM - 3				
		[E.18]nDestrucción de información	R - SW - OFM - 4				
		[E.20] Vulnerabilidades de los programas (software)	R - SW - OFM - 5				
		[A.8] Difusión de software dañino	R - SW - OFM - 7				
		[A.11] Acceso no autorizado	R - SW - OFM - 8				
HW - LPT	Laptop	[A.7] Uso no previsto	R-HW-LPT-12	B	Tolerable	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este
		[N.*] Desastres naturales	R - HW - LPT - 1	MB	Insuficiente		
		[I.1] Fuego	R - HW - LPT - 2				

		[I.2] Daños por agua	R - HW - LPT - 3				se manifiesta.
		[I.5] Avería de origen físico o lógico	R - HW - LPT - 4				
		[I.6] Corte del suministro eléctrico	R - HW - LPT - 5				
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - HW - LPT - 6				
		[E.2] Errores del administrador	R - HW - LPT - 7				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R - HW - LPT - 8				
		[E.24] Caída del sistema por agotamiento de recursos	R - HW - LPT - 9				
		[E.25] Pérdida de equipos	R - HW - LPT - 10				
		[A.6] Abuso de privilegios de acceso	R - HW - LPT - 11				
		[A.24]Denegación de servicio	R- HW - LPT - 13				
		[A.25] Robo	R - HW - LPT – 14				
SW - SOP	Sistemas Operativos	[I.5] Avería de origen físico o lógico	R-SW-SOP-1	A	Importante	MR	✓ H.IA Identificación y autenticación. ✓ H.tools Herramientas de seguridad. ✓ H.tools.AV Herramienta contra código dañino. ✓ SW Protección de las Aplicaciones
		[E.1] Errores de los usuarios	R-SW-SOP-2				
		[E.2] Errores del administrador	R-SW-SOP-3				
		[E.8] Difusión de software dañino	R-SW-SOP-4				
		[E.15] Alteración accidental de la información	R-SW-SOP-5				
		[E.18] Destrucción de	R-SW-SOP-6				

		información					Informáticas. ✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican perfiles de seguridad.
		[E.20] Vulnerabilidades de los programas (software)	R-SW-SOP-8				
		[A.6] Abuso de privilegios de acceso	R-SW-SOP-11				
		[A.7] Uso no previsto	R-SW-SOP-12				
		[A.11] Acceso no autorizado	R-SW-SOP-16				
		[A.18] Destrucción de información	R-SW-SOP-18				
		[A.22] Manipulación de programas	R-SW-SOP-20				
		[E.19] Fugas de información	R - SW - SOP - 7	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[E.21] Errores de mantenimiento / actualización de programas (software)	R - SW - SOP - 9				
		[A.5] Suplantación de identidad del usuario	R - SW - SOP - 10				
		[A.8] Difusión de software dañino	R - SW - SOP - 13				
		[A.9] [Re-]encaminamiento de mensajes	R - SW - SOP - 14				
		[A.10] Alteración de secuencia	R-SW-SOP-15				
		[A.15] Modificación deliberada de la información	R - SW - SOP - 17				
		[A.19] Divulgación de la información	R - SW - SOP - 19				
SW - SCA	Sistema de Control y Asistencia	[I.5] Avería de origen físico o lógico	R - SW - SCA - 1	MB	Insuficiente	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[E.1] Errores de los usuarios	R - SW - SCA - 2				
		[E.2] Errores del	R - SW - SCA - 3				

		administrador					
		[E.15] Alteración accidental de la información	R - SW - SCA - 4				
		[E.18] Destrucción de información	R - SW - SCA - 5				
		[E.19] Fugas de información	R - SW - SCA - 6				
		[E.20] Vulnerabilidades de los programas (software)	R - SW - SCA - 7				
		[A.5] Suplantación de la identidad del usuario	R - SW - SCA - 8				
		[A.6] Abuso de privilegios de acceso	R - SW - SCA - 9				
		[A.15] Modificación deliberada de la información	R-SW-SCA-10				
HW - SVD	Servidor	[N.*] Desastres naturales	R-HW-SVD-1	MA	Intolerable	MR	✓ H Protecciones Generales. ✓ HW Protección de los Equipos Informáticos. ✓ HW.start Puesta en producción. ✓ Se aplican perfiles de seguridad. ✓ HW.A Aseguramiento de la disponibilidad. ✓ HW.CM Cambios (actualizaciones y mantenimiento)
		[I.2] Daños por agua	R-HW-SVD-3				
		[I.6] Corte del suministro eléctrico	R-HW-SVD-5				
		[I.7]Condiciones inadecuadas de temperatura o humedad	R-HW-SVD-6				
		[E.2] Errores del administrador	R-HW-SVD-7				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R-HW-SVD-8				
		[A.6] Abuso de privilegios de acceso	R-HW-SVD-11				
		[I.1] Fuego	R - HW - SVD - 2	A	Importante		
		[I.5] Avería de origen físico o lógico	R - HW - SVD - 4				
		[E.24] Caída del sistema por	R - HW - SVD - 9				

		agotamiento de recursos					
		[E.25] Pérdida de equipos	R-HW - SVD - 10				
		[A.7] Uso no previsto	R-HW - SVD - 12				
		[A.11] Acceso no autorizado	R-HW - SVD - 13				
		[A.23] Manipulación de los equipos	R - HW - SVD - 14				
		[A.24] Denegación de servicio	R - HW - SVD - 15				
		[A.25] Robo	R-HW - SVD - 16				
HW - MDM	Módem	[N.*] Desastres naturales	R-HW-MDM-1	A	Importante	MR	✓ H Protecciones Generales. ✓ HW Protección de los Equipos Informáticos. ✓ HW.start Puesta en producción. ✓ HW.A Aseguramiento de la disponibilidad. ✓ HW.CM Cambios (actualizaciones y mantenimiento)
		[I.2] Daños por agua	R-HW-MDM-3				
		[I.6] Corte del suministro eléctrico	R-HW-MDM-5				
		[I.7]Condiciones inadecuadas de temperatura o humedad	R-HW-MDM-6				
		[E.2] Errores del administrador	R-HW-MDM-7				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R-HW-MDM-8				
		[I.1] Fuego	R-HW - MDM - 2	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[I.5] Avería de origen físico o lógico	R - HW - MDM - 4				
		[E.24] Caída del sistema por agotamiento de recursos	R - HW - MDM - 9				
		[E.25] Pérdida de equipos	R-HW-MDM-10				
		[A.6] Abuso de privilegios de acceso	R - HW - MDM - 11				
		[A.7] Uso no previsto	R-HW-MDM-12				

		[A.11] Acceso no autorizado	R-HW-MDM-13				
		[A.23] Manipulación de los equipos	R - HW - MDM – 14				
		[A.24] Denegación de servicio	R-HW-MDM-15				
		[A.25] Robo	R-HW-MDM-16				
HW - SWT	Switch para Red	[N.*] Desastres naturales	R-HW-SWT-1	A	Importante	MR	✓ H Protecciones Generales. ✓ HW Protección de los Equipos Informáticos. ✓ HW.start Puesta en producción. ✓ HW.A Aseguramiento de la disponibilidad. ✓ HW.CM Cambios (actualizaciones y mantenimiento).
		[I.2] Daños por agua	R-HW-SWT-3				
		[I.6] Corte del suministro eléctrico	R-HW-SWT-5				
		[I.7]Condiciones inadecuadas de temperatura o humedad	R-HW-SWT-6				
		[E.2] Errores del administrador	R-HW-SWT-7				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R-HW-SWT-8				
		[I.1] Fuego	R - HW - SWT - 2	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[I.5] Avería de origen físico o lógico	R - HW - SWT - 4				
		[E.24] Caída del sistema por agotamiento de recursos	R - HW - SWT - 9				
		[E.25] Pérdida de equipos	R-HW-SWT-10				
		[A.6] Abuso de privilegios de acceso	R - HW - SWT - 11				
		[A.7] Uso no previsto	R-HW-SWT-12				
		[A.11] Acceso no autorizado	R-HW-SWT-13				
		[A.23] Manipulación de los equipos	R-HW - SWT - 14				

		[A.24] Denegación de servicio	R-HW-SWT-15				
		[A.25] Robo	R-HW-SWT-16				
HW - UPS	Acumulador de Energía – UPS	[N.*] Desastres naturales	R-HW-UPS-1	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[I.2] Daños por agua	R-HW-UPS-3				
		[I.7] Condiciones inadecuadas de temperatura o humedad	R-HW-UPS-6				
		[A.25] Robo	R-HW-UPS-7				
		[I.1] Fuego	R - HW - UPS - 2	B	Tolerable		
		[I.5] Avería de origen físico o lógico	R - HW - UPS - 4				
		[I.6] Corte del suministro eléctrico	R - HW - UPS - 5				
COM - REN	Radio Enlace	[E.24] Caída del sistema por agotamiento de recursos	R-COM-REN-4	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[A.24] Denegación de servicio	R-COM-REN-5				
		[I.8] Fallo de servicios de comunicaciones	R - COM - REN - 1	B	Tolerable		
		[E.2] Errores del administrador	R-COM-REN-2				
		[E.9] Errores de [re-] encaminamiento	R - COM - REN - 3				
AUX - FOC	Fibra Óptica Claro	[N.*] Desastres naturales	R-AUX-FOC-1	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[I.6] Corte del suministro eléctrico	R-AUX-FOC-5				
		[I.7]Condiciones inadecuadas de temperatura o humedad	R-AUX-FOC-6				
		[I.1] Fuego	R-AUX - FOC - 2	B	Tolerable		
		[I.2] Daños por agua	R-AUX - FOC - 3				
		[I.5] Avería de origen físico o	R - AUX - FOC -				

		lógico	4				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R - AUX - FOC - 7				
		[A.7] Uso no previsto	R-AUX - FOC - 8				
AUX - FOM	Fibra Óptica Movistar	[N.*] Desastres naturales	R-AUX-FOM-1	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[I.6] Corte del suministro eléctrico	R-AUX-FOM-5				
		[I.7] Condiciones inadecuadas de temperatura o humedad	R-AUX-FOM-6				
		[I.1] Fuego	R-AUX- FOM - 2	B	Tolerable		
		[I.2] Daños por agua	R-AUX- FOM - 3				
		[I.5] Avería de origen físico o lógico	R - AUX - FOM - 4				
		[E.23] Errores de mantenimiento / actualización de equipos (hardware)	R - AUX - FOM - 7				
		[A.7] Uso no previsto	R-AUX- FOM - 8				
P - JTI	Jefe de TI	[E.7] Deficiencias en la organización	R-P-JTI-1	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[E.28] Indisponibilidad del personal	R-P-JTI-3				
		[A.30] Ingeniería social (picaresca)	R-P-JTI-5				
		[E.19] Fugas de información	R - P - JTI - 2	B	Tolerable		
		[A.28] Indisponibilidad del personal	R - P - JTI - 4				
L - SSVD	Sala de Servidores	[N.*] Desastres Naturales	R-L-SSVD-1	A	Importante	MR	✓ H Protecciones Generales.

		[I.2] Daños por agua	R-L-SSVD-2				✓ L Protección de las Instalaciones. ✓ L.AC Control de los accesos físicos. ✓ L.A Aseguramiento de la disponibilidad.
		[I.11] Emanaciones electromagnéticas	R - L - SSVD - 3	M	Moderado	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[E.15] Alteración accidental de la información	R - L - SSVD - 4				
		[E.18] Destrucción de información	R - L - SSVD - 5				
		[E.19] Fugas de información	R - L - SSVD - 6				
		[A.7] Uso no previsto	R - L - SSVD - 7				
Media - DDE	Disco Duro Externo	[A.7] Uso no previsto	R-Media-DDE-13	B	Tolerable	AR	✓ Se acepta el riesgo y la pérdida que se genere si es que este se manifiesta.
		[N.2] Daños por agua	R-Media-DDE - 1	MB	Insuficiente		
		[N.*] Desastres naturales	R-Media-DDE - 2				
		[I.5] Avería de origen físico o lógico	R - Media - DDE - 3				
		[I.6] Corte del suministro eléctrico	R - Media - DDE - 4				
		[I.7]Condiciones inadecuadas de temperatura o humedad	R - Media - DDE - 5				
		[I.10] Degradación de los soportes de almacenamiento de la información	R - Media - DDE - 6				
		[E.1] Errores de los usuarios	R-Media-DDE - 7				
		[E.2] Errores del administrador	R-Media DDE - 8				
		[E.15] Alteración accidental de la información	R - Media - DDE – 9				

		[E.18] Destrucción de información	R - Media - DDE - 10				
		[E.19] Fugas de información	R-Media-DDE-11				
		[E.25] Pérdida de equipos	R-Media-DDE-12				
		[A.25] Robo	R-Media-DDE-14				

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

Fase V: Seguimiento y Evaluación

Proceso 9: Monitorear y Revisar los Riesgos

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**			
	Código del Formato: CF N° 13			**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación				**Proceso: 9 - Monitorear y Revisar los Riesgos**
Nombre del Proyecto:	**PRY 01: Establecer controles para minimizar los errores provocados por el administrador del sistema.**			
Objetivos:	- Reducir el número de errores causados por el administrador del sistema.			
Personal Involucrado:	- Jefe de la Unidad de Estadística e Informática (TI).			
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).			
Salidas:				
ACTIVO INVOLUCRADO	**ID RIESGO**	**CATEGORIA DEL RIESGO**	**TIPO DE AMENAZA**	**SALVAGUARDAS**
Copias de Respaldo	R-D-CRPD-2	Muy Alto	[E.2] Errores del administrador	✓ D Protección de la Información. ✓ D.A Copias de seguridad de los datos (backup). ✓ D.C Cifrado de la información.
Base de datos Access - Control de Asistencia	R-SW-BDCA-2			✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican perfiles de seguridad.
Base de datos MVFP - SIAF	R-SW-BDSIAF-2			
Base de datos SQL - SIGA	R-SW-BDSIGA-2			
Base de datos MVFP - SISMED	R-SW-BDSISMED-2			
Servidor	R-HW-SVD-7			✓ HW Protección de los Equipos Informáticos.
Sistemas Operativos	R-SW-SOP-3	Alto		✓ SW.A Copias de seguridad

				(backup). ✓ SW.SC Se aplican perfiles de seguridad.
Módem	R-HW-MDM-7			✓ HW Protección de los Equipos Informáticos.
Switch para Red	R-HW-SWT-7			

RECURSOS:	- Jefe de la Unidad de Estadística e Informática (TI).			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**
	1	30	0.00	0.00
DETALLE DEL TIEMPO DE EJECUCIÓN:	2 hrs x 15 días hábiles = 30 horas			
INDICADORES:	- Número de incidencias relacionadas con el uso de las copias de respaldo. - Número de incidencias relacionadas con el uso de la base de datos (Control de asistencia, SIAF, SIGA, y SISMED). - Número de incidencias relacionadas con el uso del servidor. - Número de incidencias relacionadas con el uso de los sistemas operativos. - Número de incidencias relacionadas con el uso del Módem y el Switch para red,			
MEDIDAS CORRECTIVAS:	- Implementar políticas que hagan mención al uso correcto de las Copias de Respaldo. - Implementar políticas que hagan mención al uso correcto de las bases de datos (Control de asistencia, SIAF, SIGA, y SISMED). - Implementar políticas que hagan mención al uso correcto del servidor. - Implementar políticas que hagan mención al uso correcto de los sistemas operativos. - Implementar políticas que hagan mención al uso correcto del Módem y el Switch para red. - Evaluar los resultados obtenidos de forma periódica para corroborar la disminución de las incidencias que involucran a las copias de respaldo.			

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**			
	Código del Formato: CF N° 14			**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación				**Proceso: 9 - Monitorear y Revisar los Riesgos**
Nombre del Proyecto:	**PRY 02: Programar capacitaciones para concientizar el uso de información sensible.**			
Objetivos:	- Disminuir los casos identificados en relación a las fugas de información. - Minimizar el uso indebido de los privilegios de acceso.			
Personal Involucrado:	- Personal que labora en la Oficina de Admisión.			
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).			
Salidas:				
ACTIVO INVOLUCRADO	**ID RIESGO**	**CATEGORIA DEL RIESGO**	**TIPO DE AMENAZA**	**SALVAGUARDAS**
Historias Clínicas	R-D-HCL-4	Alto	[E.19] Fugas de información	✓ D Protección de la Información. ✓ D.I Aseguramiento de la integridad. ✓ D.C Cifrado de la información.
RECURSOS:	- Jefe de la Unidad de Estadística e Informática (TI).			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**
	1	20	10.00	200.00
DETALLE DEL TIEMPO DE EJECUCIÓN:	2 hrs x 10 días hábiles = 20 horas			
INDICADORES:	- Número de casos registrados donde se hizo uso indebido o no solicitado de las historias clínicas			
MEDIDAS CORRECTIVAS:	- Programar capacitaciones constantes para concientizar al personal que maneja las historias clínicas de los pacientes del hospital. - Establecer políticas que restrinjan en acceso no autorizado a la información de las historias clínicas. - Evaluar los resultados obtenidos de forma periódica para corroborar la disminución de las incidencias que involucran la fuga de información de las historias clínicas del hospital.			

Responsables		Firmas
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**	
	Código del Formato: CF N° 15	**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación		**Proceso: 9 - Monitorear y Revisar los Riesgos**
Nombre del Proyecto:	**PRY 03: Establecer capacitaciones a los usuarios que hacen uso del software de antivirus y los sistemas operativos.**	
Objetivos:	- Reducir el número de errores causados por los usuarios. - Contrarrestar la propagación de software dañino.	
Personal Involucrado:	- Usuarios que hacen uso de los diferentes equipos informáticos del Hospital.	
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).	

Salidas:

ACTIVO INVOLUCRADO	ID RIESGO	CATEGORIA DEL RIESGO	TIPO DE AMENAZA	SALVAGUARDAS
Antivirus	R-SW-AVS-2	Alto	[E.1] Errores de los usuarios	✓ SW Protección de las Aplicaciones Informáticas. ✓ SW.A Copias de seguridad (backup).
Sistemas Operativos	R-SW-SOP-2			
Antivirus	R-SW-AVS-3		[E.8] Difusión de software dañino	✓ H.tools.AV Herramienta contra código dañino. ✓ SW.SC Se aplican perfiles de seguridad.
Sistemas Operativos	R-SW-SOP-4			

RECURSOS:	- Jefe de la Unidad de Estadística e Informática (TI).			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**
	1	15	0.00	0.00
DETALLE DEL TIEMPO DE EJECUCIÓN:	3 hrs x 5 días hábiles = 15 horas			
INDICADORES:	- Número de incidentes asociados con los errores causados por los usuarios al momento de hacer uso del software de antivirus. - Número de incidentes asociados con los errores causados por los usuarios al momento de hacer uso del sistema operativo.			

	- Número de incidentes relacionados a la difusión de software dañino.	
MEDIDAS CORRECTIVAS:	- Programar capacitaciones constantes para concientizar al personal que maneja el software de antivirus y los sistemas operativos en los equipos informáticos del Hospital. - Establecer políticas relacionadas al uso de dispositivos o medios que trasmitan la difusión de software dañino. - Evaluar los resultados obtenidos de forma regular para corroborar la disminución de las incidencias por parte de los usuarios. - Evaluar los resultados obtenidos de forma regular para corroborar la disminución de las incidencias relacionadas con la propagación del software dañino.	
Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**	
	Código del Formato: CF N° 16	**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación		**Proceso: 9 - Monitorear y Revisar los Riesgos**
Nombre del Proyecto:	**PRY 04: Implementación de políticas para minimizar la suplantación de identidad, el abuso de privilegios y sus respectivas vulnerabilidades en los distintos activos de información del Hospital.**	
Objetivos:	- Reducir el número de Vulnerabilidades detectadas en los activos críticos. - Contrarrestar la suplantación de identidad. - Minimizar el abuso excesivo de los privilegios de acceso.	
Personal Involucrado:	- Usuarios que manejan los distintos sistemas informáticos (Control de Asistencia, SIAF, SIGA y SISMED) del Hospital.	
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).	

Salidas:

ACTIVO INVOLUCRADO	ID RIESGO	CATEGORIA DEL RIESGO	TIPO DE AMENAZA	SALVAGUARDAS
Base de datos Access - Control de Asistencia	R-SW-BDCA-7	Muy Alto	[E.20] Vulnerabilidades de los programas (software). [A.5] Suplantación de identidad del usuario. [A.6] Abuso de privilegios de acceso.	✓ H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión. ✓ H.tools.VA Herramienta de análisis de vulnerabilidades. ✓ SW Protección de las Aplicaciones Informáticas. ✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican perfiles de seguridad.
	R-SW-BDCA-9			
	R-SW-BDCA-10			
Base de datos MVFP - SIAF	R-SW-BDSIAF-7			
	R-SW-BDSIAF-9			
	R-SW-BDSIAF-10			
Base de datos SQL - SIGA	R-SW-BDSIGA-7			
	R-SW-BDSIGA-9			
	R-SW-BDSIGA-10			
Base de datos MVFP - SISMED	R-SW-BDSISMED-7			
	R-SW-BDSISMED-9			
	R-SW-BDSISMED-10			
Sistemas Operativos	R - SW - SOP - 8	Alto		
	R - SW - SOP - 11			

Antivirus	R-SW-AVS-4			
Historias Clínicas	R-D-HCL-6			✓ D.I Aseguramiento de la integridad. ✓ D.C Cifrado de la información.
Servidor	R-HW-SVD-11	Muy Alto		✓ HW Protección de los Equipos Informáticos. ✓ HW.A Aseguramiento de la disponibilidad.

RECURSOS:	- Jefe de la Unidad de Estadística e Informática (TI). - Residente SIAF asignado al Hospital. - Residente SIGA asignado al Hospital.			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**
	3	75	0.00	0.00
DETALLE DEL TIEMPO DE EJECUCIÓN:	5 hrs x 15 días hábiles = 75 horas			
INDICADORES:	- Número de Vulnerabilidades detectadas. - Número de incidencias registradas respecto a la suplantación de identidad de los usuarios. - Número de incidencias registradas respecto al uso excesivo de privilegios en los accesos.			
MEDIDAS CORRECTIVAS:	- Programar un cronograma con el fin de actualizar constantemente los sistemas informáticos que hacen uso de las distintas bases de datos, mediante los residentes SIAF y SIGA asignados al Hospital. - Establecer políticas de seguridad relacionadas con la identificación de usuarios. - Establecer políticas que limiten el uso de privilegios y accesos según los tipos de usuarios que hacen usos de los distintos activos de información. - Evaluar constantemente los resultados obtenidos con el fin de corroborar la disminución en los acontecimientos que involucran las vulnerabilidades y las incidencias registradas respecto a suplantación de identidad y el abuso de privilegios por usuarios			

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**	
	Código del Formato: CF N° 17	**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación		**Proceso: 9 - Monitorear y Revisar los Riesgos**

Nombre del Proyecto:	**PRY 05: Establecer controles para minimizar el uso no previsto de equipos informáticos y Sistemas operativos.**
Objetivos:	- Minimizar el uso no previsto en el antivirus, los equipos informáticos, el sistema operativo de estos y los medios de almacenamiento de información.
Personal Involucrado:	- Usuarios que hacen uso de los diferentes equipos informáticos del Hospital.
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).

Salidas:

ACTIVO INVOLUCRADO	ID RIESGO	CATEGORIA DEL RIESGO	TIPO DE AMENAZA	SALVAGUARDAS
Laptop	R - HW - LPT - 12	Bajo	[A.7] Uso no previsto	✓ HW Protección de los Equipos Informáticos. ✓ HW.SC Se aplican perfiles de seguridad.
Disco Duro Externo	R - Media - DDE - 13			✓ MP Protección de los Soportes de Información. ✓ MP.IC Protección criptográfica del contenido.
Sistemas Operativos	R - SW - SOP - 12	Alto		✓ SW Protección de las Aplicaciones Informáticas. ✓ SW.A Copias de seguridad (backup). ✓ SW.SC Se aplican perfiles de seguridad.
Antivirus	R-SW-AVS-6			

RECURSOS:	- Jefe de la Unidad de Estadística e Informática (TI).			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**

	1	20	0.00	0.00
DETALLE DEL TIEMPO DE EJECUCIÓN:	2 hrs x 10 días hábiles = 20 horas			
INDICADORES:	- Número de incidencias respecto al uso no previsto de los equipos informáticos y los medios de almacenamiento de información. - Número de incidencias respecto al uso no previsto en el antivirus. - Número de incidencias respecto al uso no previsto del sistema operativo que usan los equipos informáticos.			
MEDIDAS CORRECTIVAS:	- Implementar políticas que limiten el uso del antivirus, los equipos informáticos y los medios de almacenamiento de información sólo para ocasiones laborales o en beneficio del Hospital. - Evaluar constantemente los resultados obtenidos con el fin de disminuir las incidencias que involucran al antivirus, los equipos informáticos del Hospital, el sistema operativo de estos y los medios de almacenamiento de información.			
Responsables			**Firmas**	
Elaborado por:	CVILLEGASR			
Revisado por:	JIZQUIERDOC			
Aprobado por:	JIZQUIERDOC			

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**	
	Código del Formato: CF N° 18	**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación		**Proceso: 9 - Monitorear y Revisar los Riesgos**

Nombre del Proyecto:	**PRY 06: Determinar lineamientos para asegurar la continuidad de funcionamiento así como la vida útil de los equipos en casos de corte de energía eléctrica.**
Objetivos:	- Resguardar la vida útil de los servidores, y componentes que aseguran el suministro de internet en el Hospital, así como la continuidad funcional de los mismos en casos de corte de energía eléctrica.
Personal Involucrado:	- Personal que hace uso de los sistemas informáticos almacenados en los servidores del Hospital. - Personal que hace uso del servicio de internet para cumplir con sus labores asignadas.
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).

Salidas:

ACTIVO INVOLUCRADO	ID RIESGO	CATEGORIA DEL RIESGO	TIPO DE AMENAZA	SALVAGUARDAS
Servidor	R-HW-SVD-5	Muy Alto	[I.6] Corte del suministro eléctrico	✓ HW Protección de los Equipos Informáticos. ✓ HW.start Puesta en producción. ✓ HW.A Aseguramiento de la disponibilidad.
Módem	R-HW-MDM-5	Alto		
Switch para Red	R-HW-SWT-5			
Fibra Óptica Claro	R-AUX-FOC-5	Medio		✓ AUX.A Aseguramiento de la disponibilidad. ✓ AUX.power Suministro eléctrico.
Fibra Óptica Movistar	R-AUX-FOM-5			

RECURSOS:	- Jefe de la Unidad de Estadística e Informática (TI).			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**
	1	21	0.00	0.00
DETALLE DEL TIEMPO DE EJECUCIÓN:	3 hrs x 7 días hábiles = 21 horas			

INDICADORES:	- Número de incidencias provocadas a causa del corte de energía eléctrica relacionadas con el uso de los servidores. - Número de incidencias provocadas a causa de la interrupción del servicio eléctrico relacionado con el servicio de internet.
MEDIDAS CORRECTIVAS:	- Establecer lineamientos donde se haga mención de los pasos o procedimientos a seguir para que el corte de energía eléctrica no interrumpa de manera crítica los procesos que se ejecutan en los servidores. - Determinar medidas para asegurar que el servicio de internet se ejecute con normalidad una vez restablecido el servicio de energía eléctrica. - Evaluar los resultados obtenidos de manera periódica para garantizar no solo el restablecimiento oportuno de las actividades asociadas con los servidores y los componentes que suministran internet en el Hospital; si no también para asegurar la vida útil de los activos ya mencionados.

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - 1 "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**	
	Código del Formato: CF N° 19	**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación		**Proceso: 9 - Monitorear y Revisar los Riesgos**
Nombre del Proyecto:	**PRY 07: Establecer estrategias para enfrentar los inconvenientes causados por los desastres naturales e industriales.**	
Objetivos:	- Proteger los activos antes los casos frecuentes desastres naturales (movimientos sísmicos) que presenta la región Amazonas. - Proteger los activos frente de los acontecimientos suscitados a causa de inundaciones.	
Personal Involucrado:	- Personal que utiliza los sistemas informáticos alojados en la Sala de servidores.	
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).	

Salidas:

ACTIVO INVOLUCRADO	ID RIESGO	CATEGORIA DEL RIESGO	TIPO DE AMENAZA	SALVAGUARDAS
Sala de Servidores	R-L-SSVD-1	Alto	[N.*] Desastres naturales. [I.2] Daños por agua.	✓ H Protecciones Generales. ✓ L Protección de las Instalaciones. ✓ L.AC Control de los accesos físicos. ✓ L.A Aseguramiento de la disponibilidad.
	R-L-SSVD-2			
Módem	R-HW-MDM-1			✓ H Protecciones Generales. ✓ HW Protección de los Equipos Informáticos. ✓ HW.start Puesta en producción. ✓ HW.A Aseguramiento de la disponibilidad. ✓ HW.end Terminación.
	R-HW-MDM-3			
Switch para Red	R-HW-SWT-1			
	R-HW-SWT-3			
Servidor	R-HW-SVD-1	Muy Alto		
	R-HW-SVD-3			
Acumulador de Energía – UPS	R-HW-UPS-1	Medio		
	R-HW-UPS-3			
Fibra Óptica Claro	R-AUX-FOC-1		[N.*] Desastres naturales.	✓ AUX.A Aseguramiento de la

<table>
<tr><td>Fibra Óptica Movistar</td><td>R-AUX-FOM-1</td><td></td><td></td><td colspan="2">disponibilidad.
✓ AUX.start Instalación.
✓ AUX.wires Protección del cableado.</td></tr>
<tr><td>RECURSOS:</td><td colspan="5">- Director del Hospital.
- Administrador del Hospital.
- Jefe de la Unidad de Estadística e Informática (TI).</td></tr>
<tr><td rowspan="2">IMPORTE:</td><td>CANTIDAD DE ESPECIALISTAS</td><td colspan="2">CANTIDAD DE HORAS</td><td>COSTO POR HORA</td><td>TOTAL (S/)</td></tr>
<tr><td>3</td><td colspan="2">18</td><td>0.00</td><td>0.00</td></tr>
<tr><td>DETALLE DEL TIEMPO DE EJECUCIÓN:</td><td colspan="5">3 hrs x 6 días hábiles = 18 horas</td></tr>
<tr><td>INDICADORES:</td><td colspan="5">- Número de incidentes causados por los distintos desastres naturales en la región Amazonas.
- Número de incidentes de origen industrial que perjudican la ejecución de procesos críticos del Hospital.</td></tr>
<tr><td>MEDIDAS CORRECTIVAS:</td><td colspan="5">- Establecer planes de acción frente a los inconvenientes que puedan causar desastres naturales (sismos o lluvias torrenciales) e industriales (inundaciones), provocando la detención de los servicios o el deterioro de los activos de TI.
- Evaluar los resultados obtenidos de manera periódica para garantizar la protección de los activos involucrados.</td></tr>
<tr><td colspan="3">Responsables</td><td colspan="3">Firmas</td></tr>
<tr><td>Elaborado por:</td><td colspan="2">CVILLEGASR</td><td colspan="3"></td></tr>
<tr><td>Revisado por:</td><td colspan="2">JIZQUIERDOC</td><td colspan="3"></td></tr>
<tr><td>Aprobado por:</td><td colspan="2">JIZQUIERDOC</td><td colspan="3"></td></tr>
</table>

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**	
	Código del Formato: CF N° 20	**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación		**Proceso: 9 - Monitorear y Revisar los Riesgos**

Nombre del Proyecto:	**PRY 08: Definir planes de acción frente a las condiciones inadecuadas de temperatura que afectan a los activos.**
Objetivos:	- Proteger los activos que se ven perjudicados por las diversas condiciones climáticas, poniendo en peligro la continuidad de las operaciones y la duración de la vida útil de estos activos.
Personal Involucrado:	- Personal que dispone de UPS para la ejecución normal de sus actividades. - Personal que requiere del servicio de internet para realizar funciones asignadas como parte de su trabajo.
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).

Salidas:

ACTIVO INVOLUCRADO	ID RIESGO	CATEGORIA DEL RIESGO	TIPO DE AMENAZA	SALVAGUARDAS
Servidor	R-HW-SVD-6	Alto	[I.7] Condiciones inadecuadas de temperatura o humedad	✓ H Protecciones Generales. ✓ HW Protección de los Equipos Informáticos. ✓ HW.A Aseguramiento de la disponibilidad.
Acumulador de Energía – UPS	R-HW-UPS-6	Medio		
Fibra Óptica Claro	R-AUX-FOC-6			✓ H Protecciones Generales. ✓ AUX.A Aseguramiento de la disponibilidad. ✓ AUX.AC Climatización. ✓ AUX.wires Protección del cableado
Fibra Óptica Movistar	R-AUX-FOM-6			

RECURSOS:	- Empresa distribuidora de aire acondicionado (Reparación de 5 aires acondicionados).			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**
	3	10	100.00	3 000.00
DETALLE DEL TIEMPO	2 hrs x 5 días hábiles = 10 horas			

DE EJECUCIÓN:		
INDICADORES:	- Número de procesos interrumpidos a causa de las condiciones climáticas inadecuadas que afectan a los activos involucrados.	
MEDIDAS CORRECTIVAS:	- Contratar un empresa distribuidora de aire acondicionado que se encargue de dar mantenimiento (reparaciones de goteo) al aire acondicionado necesario el buen rendimiento de los activos involucrados. - Evaluar los resultados obtenidos de manera periódica para garantizar la diminución de los procesos interrumpidos.	
Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**				
	Código del Formato: CF N° 21				**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación					**Proceso: 9 - Monitorear y Revisar los Riesgos**
Nombre del Proyecto:	**PRY 09: Implementar políticas y planes de acción para proteger los activos en casos de hurto.**				
Objetivos:	- Proteger los activos que por su condición física o ubicación son fáciles de extraer o robar.				
Personal Involucrado:	- Personal que dispone de UPS para la ejecución normal de sus actividades.				
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).				
Salidas:					
ACTIVO INVOLUCRADO	**ID RIESGO**	**CATEGORIA DEL RIESGO**	**TIPO DE AMENAZA**	**SALVAGUARDAS**	
Acumulador de Energía – UPS	R - HW - UPS	Medio	[A.25] Robo	✓ H Protecciones Generales. ✓ HW Protección de los Equipos Informáticos. ✓ HW.SC Se aplican perfiles de seguridad. ✓ HW.A Aseguramiento de la disponibilidad	
RECURSOS:	- Jefe de la Unidad de Estadística e Informática (TI). - Empresa especialista en video vigilancia (5 cámaras de video vigilancia más el sistema de grabación y almacenamiento).				
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**	
	3	15	100.00	4 500.00	
DETALLE DEL TIEMPO DE EJECUCIÓN:	5 hrs x 3 días hábiles = 15 horas				
INDICADORES:	- Número de activos reportados como robo. - Número de procesos interrumpidos por falta de los activos robados, siendo estos indispensables para el funcionamiento de las actividades que se realizan en las distintas áreas del Hospital.				
MEDIDAS	- Establecer políticas de seguridad donde se haga mención o estén relacionados con la protección física de los				

CORRECTIVAS:	activos en riesgo. - Implementar un sistema de video vigilancia para mejorar la protección de los activos involucrados. - Evaluar los resultados obtenidos de manera periódica para minimizar los incidentes de los procesos interrumpidos a causa del robo de los activos.	
Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**	
	Código del Formato: CF N° 22	**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación		**Proceso: 9 - Monitorear y Revisar los Riesgos**

Nombre del Proyecto:	**PRY 10: Establecer planes de contingencia ante las caídas del servicio de internet.**
Objetivos:	- Asegurar que el servicio de internet esté disponible la mayor parte del tiempo.
Personal Involucrado:	- Personal que requiere del servicio de internet para realizar funciones asignadas como parte de sus labores diarias.
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).

Salidas:

ACTIVO INVOLUCRADO	ID RIESGO	CATEGORIA DEL RIESGO	TIPO DE AMENAZA	SALVAGUARDAS
Radio Enlace	R -COM-REN	Medio	[E.24] Caída del sistema por agotamiento de recursos [A.24] Denegación de servicio	✓ COM Protección de las Comunicaciones. ✓ COM.A Aseguramiento de la disponibilidad.

RECURSOS:	- Proveedor de Radio Enlace (mejorar el servicio del ancho de banda).			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**
	2	5	300.00	3 000.00
DETALLE DEL TIEMPO DE EJECUCIÓN:	5 hrs x 1 día hábil = 5 horas			
INDICADORES:	- Número de procesos interrumpidos a causa de las caías de las 2 fibras ópticas.			
MEDIDAS CORRECTIVAS:	- Mejor el servicio de banda ancha del radio enlace, en caso que las 2 fibras ópticas caigan el Radio Enlace podrá soportar sin problemas todos los procesos que se llevan a cabo en las distintas áreas del Hospital. * Es importante mencionar que este servicio genera el gasto mensual al ser indispensable para la comunicación continua de internet. - Evaluar los resultados obtenidos de manera periódica para reducir el número de procesos interrumpidos a causa de las caídas de las fibras ópticas.			

Responsables		Firmas
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

HOSPITAL II - I "HHH"	**FORMATO DE MONITOREO Y REVISIÓN**	
	Código del Formato: CF N° 23	**Fecha: ____/____/2020**
Fase: V - Seguimiento y Evaluación		**Proceso: 9 - Monitorear y Revisar los Riesgos**

Nombre del Proyecto:	**PRY 11: Establecer capacitaciones para concientizar al personal sobre el uso consiente del ROF.**
Objetivos:	- Reasignar funciones con el fin de disminuir la sobrecarga laboral. - Establecer un personal de respaldo para cubrir las tareas por indisposición de los usuarios.
Personal Involucrado:	- Jefaturas de las principales áreas que componen el sector administrativo y asistencial del hospital.
Entradas:	- Formato de Selección e Implementación de Planes de Tratamiento del Riesgo (**CF N° 12**).

Salidas:

ACTIVO INVOLUCRADO	ID RIESGO	CATEGORIA DEL RIESGO	TIPO DE AMENAZA	SALVAGUARDAS
Jefe de TI	R - P - JTI	Medio	[E.7] Deficiencias en la organización [E.28] Indisponibilidad del personal [A.30] Ingeniería social (picaresca)	✓ PS Gestión del Personal. ✓ PS.AT Formación y concienciación. ✓ PS.A Aseguramiento de la disponibilidad.

RECURSOS:	- Capacitador de Gestión del Recurso Humano.			
IMPORTE:	**CANTIDAD DE ESPECIALISTAS**	**CANTIDAD DE HORAS**	**COSTO POR HORA**	**TOTAL (S/)**
	1	18	150.00	2 700.00
DETALLE DEL TIEMPO DE EJECUCIÓN:	3 hrs x 6 días hábiles = 18 horas			
INDICADORES:	- Porcentaje de sobrecarga laboral a los usuarios por el desconocimiento de la Alta Gerencia sobre las funciones asignadas a cada personal. - Porcentaje de retraso laboral por la ausencia del personal.			
MEDIDAS CORRECTIVAS:	- Programar capacitaciones constantes con el fin de concientizar al personal y explicar los protocolos establecidos en el ROF.			

	- Hacer uso frecuente del ROF para distribuir correctamente las funciones asignadas a cada usuario según las políticas determinadas por la Alta Gerencia del Hospital. - Establecer un personal de respaldo para la continuidad de labores establecidas en caso el usuario principal esté indispuesto. - Evaluar los resultados obtenidos de manera periódica para disminuir el porcentaje de sobrecarga laboral a los usuarios. - Evaluar los resultados obtenidos de manera periódica para minimizar el porcentaje de retraso laboral o incumplimiento de funciones por indisposición del personal a cargo.

Responsables		**Firmas**
Elaborado por:	CVILLEGASR	
Revisado por:	JIZQUIERDOC	
Aprobado por:	JIZQUIERDOC	

ANEXO Nº 10: MATRIZ DE VALIDACIÓN DE EXPERTOS

DR. GILBERTO CARRIÓN BARCO

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS. Para tal fin, se anexa la matriz de consistencia para la validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : GILBERTO CARRIÓN BARCO

FORMACIÓN ACADÉMICA : DR EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS

ÁREAS DE EXPERIENCIA PROFESIONAL : - INFRAESTRUCTURA TECNOLOGICA
- SEGURIDAD INFORMÁTICA

TIEMPO DE EXPERIENCIA : 15 AÑOS

CARGO ACTUAL : CATEDRÁTICO

INSTITUCIÓN : UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Objetivo de la investigación : Contribuir en la protección de los activos de información en hospitales de nivel II – I de la región Amazonas mediante el desarrollo de un modelo de gestión de riesgos de TI.

Objetivo del juicio de expertos : Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba : Determinar la utilidad del modelo propuesto para los hospitales de nivel II – I de la región Amazonas.

PROFESIONAL EXPERTO

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORÍA	CLASIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

MODELO DE GESTIÓN DE RIESGOS DE TI PARA HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

FASE I: DEFINIR EL ALCANCE Y CONTEXTO DE LA ORGANIZACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 1: Definir el alcance	Identificar los procesos críticos de la organización.	4	4	4	4	
	Identificar las áreas fundamentales para el proceso de gestión de riegos de TI.	4	4	4	4	
Proceso 2: Identificación del Contexto Interno y Externo	Identificar los factores internos que impactan en el comportamiento de la organización.	3	3	4	4	como entradas, tambien se debe considerar al TUPA
	Identificar los factores externos que impactan en el comportamiento de la organización.	4	4	4	4	
FASE II: IDENTIFICACIÓN DE ACTIVOS						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 3: Identificación y Clasificación de Activos.	Identificar y clasificar (mediante un catálogo) los activos que deben ser incluidos en el proceso de gestión de riesgos de TI.	4	4	4	4	
Proceso 4: Valoración de Activos	Determinar la valoración de los activos respecto a las dimensiones de valoración y escalas estándar.	4	4	4	4	
	Valorar el grado de importancia de los activos de acuerdo al impacto.	4	4	4	4	
FASE III: EVALUACIÓN DEL RIESGO						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 5: Identificación y Valoración de Amenazas	Identificar (mediante un catálogo) los tipos de amenazas que podrían causar daño a la organización.	3	3	3	4	- Considerar amenazas tipo la Pandemia - covid 19 - Considerar amenazas económicas
	Determinar la valoración de las amenazas.	4	4	4	4	

Proceso 6: Identificación, Análisis y Valoración del riesgo	Identificar y analizar el nivel del riesgo mediante la probabilidad y el impacto.	4	4	4	4	
	Valorar los riesgos respecto al resultado entre el impacto y la probabilidad de ocurrencia.	4	4	4	4	
FASE IV: TRATAMIENTO DEL RIESGO						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 7: Opciones de Tratamiento del Riesgo	Determinar si las opciones para el tratamiento son las más adecuadas para enfrentar los riesgos.	4	4	4	4	
Proceso 8: Implementar planes de Tratamiento del Riesgo	Establecer tipos de Tratamiento y Salvaguardas adecuados (mediante un catálogo) para ejecutar las opciones de tratamiento.	4	4	4	4	
FASE V: SEGUIMIENTO Y EVALUACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 9: Monitorear y Revisar los Riesgos	Identificar la medida de lo logrado en la aplicación del procesamiento.	4	4	4	4	
	Identificar medidas correctivas para mejorar los resultados obtenidos.	4	4	4	4	

ACEPTACIÓN	✓
OBSERVADO	
DISCONFORMIDAD	

EL MODELO PROPUESTO CONTIENE LOS PROCESOS Y ACTIVIDADES SUFICIENTES Y NECESARIOS PARA SER CONSIDERADOS VALIDOS, POR LO TANTO, APTOS PARA SER APLICADAS EN EL LOGRO DE LOS OBJETIVOS QUE SE PLANTEAN EN LA INVESTIGACIÓN.

PROFESIONAL EXPERTO

DRA. JESSIE LEILA BRAVO JAICO

Modelo de Gestión de Riesgos de TI - César Villegas Rivera

Translate message to: English | Never translate from: Spanish

César Villegas Rivera
Tue 2020-07-21 17:49
To: jbravo@unprg.edu.pe

MGR TI QUE CONTRIBUYE EN... 3 MB
MGR TI QUE CONTRIBUYE EN... 7 MB
MATRIZ DE CONSISTENCIA P... 20 KB

3 attachments (10 MB) Download all Save all to OneDrive

Ing. Jessie le adjunto mi tesis "Modelo de Gestión de Riesgos de TI que contribuye en la protección de los activos de información en hospitales de nivel II - I de la región Amazonas". Y la Matriz para la validación de expertos.

De antemano muchas gracias.

Atte.

César A. Villegas Rivera

Re: Modelo de Gestión de Riesgos de TI - César Villegas Rivera

Jessie Leila Bravo Jaico <jbravo@unprg.edu.pe>
Wed 2020-07-29 00:08
To: You

MATRIZ DE CONSISTENCIA P... 47 KB

César:
Disculpa la demora, remito la matriz de validación.

Saludos.

Jessie Bravo

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS. Para tal fin, se anexa la matriz de consistencia para la validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS	**:** JESSIE LEILA BRAVO JAICO
FORMACIÓN ACADÉMICA	**:** DRA. EN CIENCIAS DE LA COMPUTACIÓN Y SISTEMAS
ÁREAS DE EXPERIENCIA PROFESIONAL	**:** SEGURIDAD INFORMÁTICA, AUDITORÍA INFORMÁTICA, GESTIÓN DE RIESGOS DE TI
TIEMPO DE EXPERIENCIA	**:** 20 AÑOS
CARGO ACTUAL	**:** CATEDRÁTICA PRE Y POSGRADO
INSTITUCIÓN	**:** UNPRG, USAT, USS
Objetivo de la investigación	**:** Contribuir en la protección de los activos de información en hospitales de nivel II – I de la región Amazonas mediante el desarrollo de un modelo de gestión de riesgos de TI.
Objetivo del juicio de expertos	**:** Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.
Objetivo de la prueba	**:** Determinar la utilidad del modelo propuesto para los hospitales de nivel II – I de la región Amazonas.

PROFESIONAL EXPERTO

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORÍA	CLASIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

MODELO DE GESTIÓN DE RIESGOS DE TI PARA HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

FASE I: DEFINIR EL ALCANCE Y CONTEXTO DE LA ORGANIZACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 1: Definir el alcance	Identificar los procesos críticos de la organización.	**4**	**4**	**4**	**4**	
	Identificar las áreas fundamentales para el proceso de gestión de riegos de TI.	**4**	**4**	**4**	**4**	
Proceso 2: Identificación del Contexto Interno y Externo	Identificar los factores internos que impactan en el comportamiento de la organización.	**4**	**4**	**4**	**4**	
	Identificar los factores externos que impactan en el comportamiento de la organización.	**3**	**4**	**4**	**3**	Verificar este aspecto, en la Tabla 3 no se observa el control importante que ejerce el MINSA y los documentos como decretos y resoluciones que se han dado por ejemplo en esta época de la pandemia (manejo de prioridades).
FASE II: IDENTIFICACIÓN DE ACTIVOS						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 3: Identificación y Clasificación de Activos.	Identificar y clasificar (mediante un catálogo) los activos que deben ser incluidos en el proceso de gestión de riesgos de TI.	**4**	**4**	**4**	**4**	Verificar los activos de la ciberseguridad (ISO 27032)
Proceso 4: Valoración de Activos	Determinar la valoración de los activos respecto a las dimensiones de valoración y escalas estándar.	**4**	**4**	**4**	**4**	

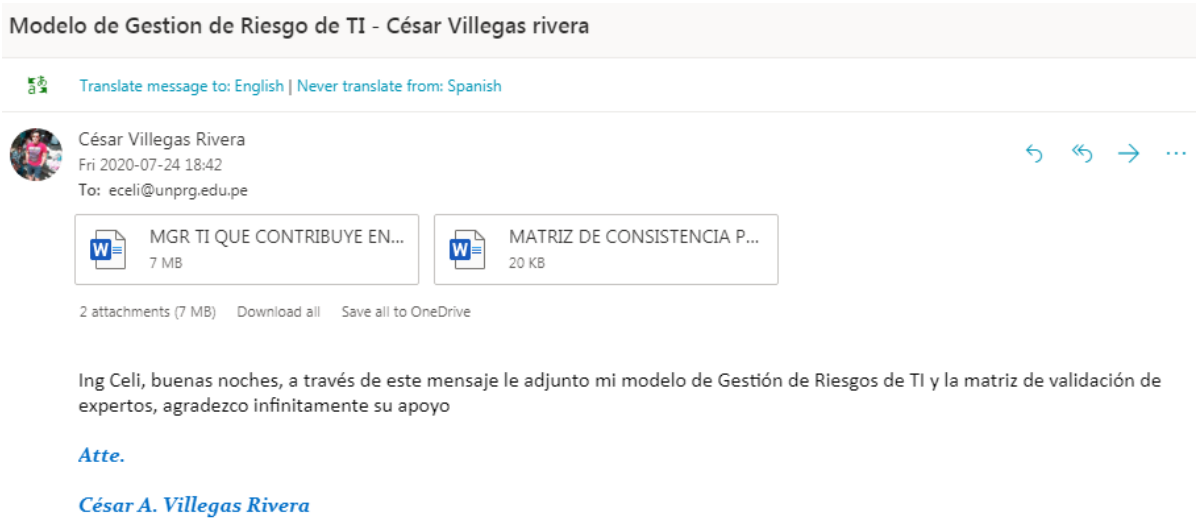
	Valorar el grado de importancia de los activos de acuerdo al impacto.	**4**	**4**	**4**	**4**	
FASE III: EVALUACIÓN DEL RIESGO						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 5: Identificación y Valoración de Amenazas	Identificar (mediante un catálogo) los tipos de amenazas que podrían causar daño a la organización.	**3**	**4**	**4**	**4**	Evaluar la situación actual de pandemia que estamos viviendo
	Determinar la valoración de las amenazas.	**4**	**4**	**4**	**4**	
Proceso 6: Identificación, Análisis y Valoración del riesgo	Identificar y analizar el nivel del riesgo mediante la probabilidad y el impacto.	**4**	**4**	**4**	**4**	
	Valorar los riesgos respecto al resultado entre el impacto y la probabilidad de ocurrencia.	**4**	**4**	**4**	**4**	
FASE IV: TRATAMIENTO DEL RIESGO						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 7: Opciones de Tratamiento del Riesgo	Determinar si las opciones para el tratamiento son las más adecuadas para enfrentar los riesgos.	**4**	**4**	**4**	**4**	
Proceso 8: Implementar planes de Tratamiento del Riesgo	Establecer tipos de Tratamiento y Salvaguardas adecuados (mediante un catálogo) para ejecutar las opciones de tratamiento.	**4**	**4**	**4**	**4**	
FASE V: SEGUIMIENTO Y EVALUACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**

Proceso 9: Monitorear y Revisar los Riesgos	Identificar la medida de lo logrado en la aplicación del procesamiento.	**4**	**4**	**4**	**4**	
	Identificar medidas correctivas para mejorar los resultados obtenidos.	**4**	**4**	**4**	**4**	

ACEPTACIÓN	**X**
OBSERVADO	
DISCONFORMIDAD	

PROFESIONAL EXPERTO

DR. ERNESTO KARLO CELI ARÉVALO



Modelo de Gestion de Riesgo de TI - César Villegas rivera

Translate message to: English | Never translate from: Spanish

César Villegas Rivera
Fri 2020-07-24 18:42
To: eceli@unprg.edu.pe

MGR TI QUE CONTRIBUYE EN...
7 MB

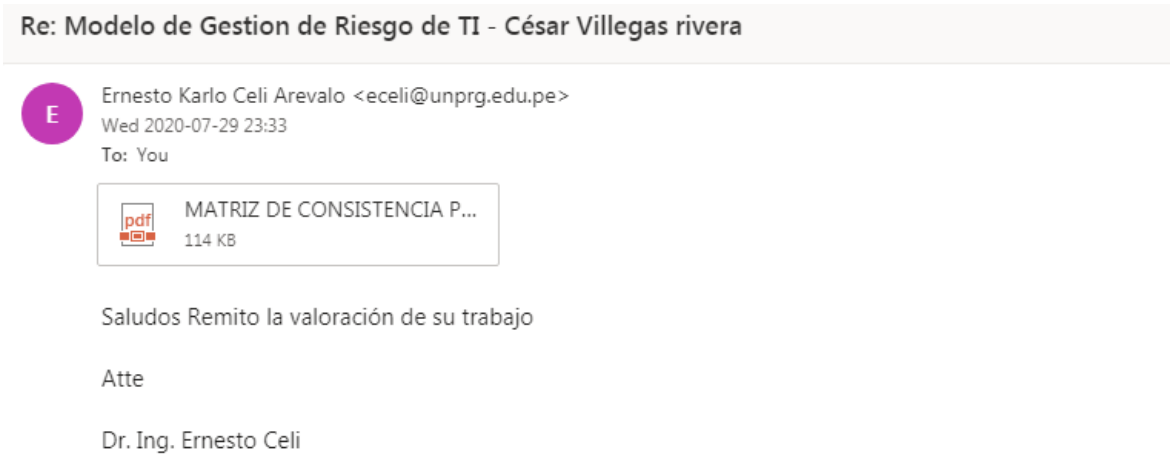
MATRIZ DE CONSISTENCIA P...
20 KB

2 attachments (7 MB) Download all Save all to OneDrive

Ing Celi, buenas noches, a través de este mensaje le adjunto mi modelo de Gestión de Riesgos de TI y la matriz de validación de expertos, agradezco infinitamente su apoyo

Atte.

César A. Villegas Rivera



Re: Modelo de Gestion de Riesgo de TI - César Villegas rivera

Ernesto Karlo Celi Arevalo <eceli@unprg.edu.pe>
Wed 2020-07-29 23:33
To: You

MATRIZ DE CONSISTENCIA P...
114 KB

Saludos Remito la valoración de su trabajo

Atte

Dr. Ing. Ernesto Celi

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS. Para tal fin, se anexa la matriz de consistencia para la validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS :

ERNESTO KARLO CELI ARÉVALO

FORMACIÓN ACADÉMICA :

INGENIERO DE COMPUTACIÓN Y SISTEMAS

ÁREAS DE EXPERIENCIA PROFESIONAL :

SEGURIDAD DE TI, GESTIÓN DE RIESGOS DE TI Y CONTINUIDAD DEL NEGOCIO

TIEMPO DE EXPERIENCIA :

27 AÑOS

CARGO ACTUAL :

DIRECTOR DE LA ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

INSTITUCIÓN :

UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO

Objetivo de la investigación : Contribuir en la protección de los activos de información en hospitales de nivel II – I de la región Amazonas mediante el desarrollo de un modelo de gestión de riesgos de TI.

Objetivo del juicio de expertos : Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba : Determinar la utilidad del modelo propuesto para los hospitales de nivel II – I de la región Amazonas.

PROFESIONAL EXPERTO

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORÍA	CLASIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

MODELO DE GESTIÓN DE RIESGOS DE TI PARA HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

FASE I: DEFINIR EL ALCANCE Y CONTEXTO DE LA ORGANIZACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 1: Definir el alcance	Identificar los procesos críticos de la organización.	**3**	**4**	**3**	**4**	
	Identificar las áreas fundamentales para el proceso de gestión de riegos de TI.	**3**	**3**	**3**	**4**	
Proceso 2: Identificación del Contexto Interno y Externo	Identificar los factores internos que impactan en el comportamiento de la organización.	**4**	**4**	**4**	**4**	
	Identificar los factores externos que impactan en el comportamiento de la organización.	**4**	**4**	**4**	**4**	
FASE II: IDENTIFICACIÓN DE ACTIVOS						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 3: Identificación y Clasificación de Activos.	Identificar y clasificar (mediante un catálogo) los activos que deben ser incluidos en el proceso de gestión de riesgos de TI.	**4**	**3**	**4**	**4**	
Proceso 4: Valoración de Activos	Determinar la valoración de los activos respecto a las dimensiones de valoración y escalas estándar.	**4**	**4**	**4**	**4**	

FASE V: SEGUIMIENTO Y EVALUACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 9: Monitorear y Revisar los Riesgos	Identificar la medida de lo logrado en la aplicación del procesamiento.	**3**	**4**	**3**	**4**	
	Identificar medidas correctivas para mejorar los resultados obtenidos.	**3**	**4**	**3**	**4**	

ACEPTACIÓN	**X**
OBSERVADO	
DISCONFORMIDAD	

PROFESIONAL EXPERTO

MTRO. LUIS MONTENEGRO CAMACHO

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS. Para tal fin, se anexa la matriz de consistencia para la validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : Luis Montenegro Camacho

FORMACIÓN ACADÉMICA : Licenciado en Educación Secundaria (Especialidad Matemática)
Maestro en Ciencias con mención en Tecnologías de la Información

AREAS DE EXPERIENCIA PROFESIONAL : Seguridad de TI Educativo

TIEMPO DE EXPERIENCIA : 25 años

CARGO ACTUAL : Docente de Post Grado

INSTITUCIÓN : Universidad César Vallejo

Objetivo de la investigación:	Contribuir en la protección de los activos de información en hospitales de nivel II – I de la región Amazonas mediante el desarrollo de un modelo de gestión de riesgos de TI.
Objetivo del juicio de expertos:	Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

Objetivo de la prueba: Determinar la utilidad del modelo propuesto para los hospitales de nivel II – I de la región Amazonas.

PROFESIONAL EXPERTO

16672474

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORÍA	CLASIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero

		otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS

MODELO DE GESTIÓN DE RIESGOS DE TI PARA HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

FASE I: DEFINIR EL ALCANCE Y CONTEXTO DE LA ORGANIZACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 1: Definir el alcance	Identificar los procesos críticos de la organización.	4	4	4	4	
	Identificar las áreas fundamentales para el proceso de gestión de riegos de TI.	4	4	4	4	
Proceso 2: Identificación del Contexto Interno y Externo	Identificar los factores internos que impactan en el comportamiento de la organización.	4	3	4	4	
	Identificar los factores externos que impactan en el comportamiento de la organización.	4	4	4	3	
FASE II: IDENTIFICACIÓN DE ACTIVOS						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 3: Identificación y Clasificación de Activos.	Identificar y clasificar (mediante un catálogo) los activos que deben ser incluidos en el proceso de gestión de riesgos de TI.	4	4	4	4	
Proceso 4: Valoración de Activos	Determinar la valoración de los activos respecto a las dimensiones de valoración y escalas estándar.	4	4	4	3	
	Valorar el grado de importancia de los activos de acuerdo al impacto.	4	4	4	4	
FASE III: EVALUACIÓN DEL RIESGO						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 5: Identificación y	Identificar (mediante un catálogo) los tipos de amenazas que podrían causar	4	3	4	3	

Valoración de Amenazas	daño a la organización.					
	Determinar la valoración de las amenazas.	4	4	4	4	
Proceso 6: Identificación, Análisis y Valoración del riesgo	Identificar y analizar el nivel del riesgo mediante la probabilidad y el impacto.	4	4	4	3	
	Valorar los riesgos respecto al resultado entre el impacto y la probabilidad de ocurrencia.	4	4	4	4	
FASE IV: TRATAMIENTO DEL RIESGO						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 7: Opciones de Tratamiento del Riesgo	Determinar si las opciones para el tratamiento son las más adecuadas para enfrentar los riesgos.	4	4	4	3	
Proceso 8: Implementar planes de Tratamiento del Riesgo	Establecer tipos de Tratamiento y Salvaguardas adecuados (mediante un catálogo) para ejecutar las opciones de tratamiento.	4	3	4	3	
FASE V: SEGUIMIENTO Y EVALUACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 9: Monitorear y Revisar los Riesgos	Identificar la medida de lo logrado en la aplicación del procesamiento.	4	3	4	4	
	Identificar medidas correctivas para mejorar los resultados obtenidos.	4	4	4	4	

ACEPTACIÓN	X
OBSERVADO	
DISCONFORMIDAD	

PROFESIONAL EXPERTO
16672474

MTRO. JUDITH KARIM BAUTISTA GONZÁLES

FORMATO PARA VALIDACIÓN DE EXPERTOS DEL MODELO PROPUESTO

Estimado Ingeniero:

A través de la presente me dirijo a usted con el fin de solicitarle su ayuda para la validación de la propuesta realizada en la investigación denominada MODELO DE GESTIÓN DE RIESGOS DE TI QUE CONTRIBUYE EN LA PROTECCIÓN DE LOS ACTIVOS DE INFORMACIÓN EN HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS. Para tal fin, se anexa la matriz de consistencia para la validación.

Agradecemos su valiosa colaboración.

NOMBRES Y APELLIDOS : Judith Karim Bautista Gonzales

FORMACIÓN ACADÉMICA : Licenciada en Educación Matemática, Maestro en Ciencias con mención en Tecnologías de la Información.

AREAS DE EXPERIENCIA PROFESIONAL : Seguridad en TI Educativa

TIEMPO DE EXPERIENCIA : 20 años

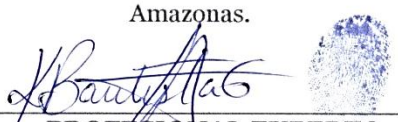
CARGO ACTUAL : Sub-Directora I.E. "Pedro Abel Labarthe"

INSTITUCIÓN : I.E. "Pedro Abel Labarthe"

Objetivo de la investigación:	Contribuir en la protección de los activos de información en hospitales de nivel II – I de la región Amazonas mediante el desarrollo de un modelo de gestión de riesgos de TI.
Objetivo del juicio de expertos:	Verificar la validez del modelo propuesto en relación a la suficiencia, claridad, coherencia y relevancia de los ítems considerados.

J. Bautista G.

Objetivo de la prueba: Determinar la utilidad del modelo propuesto para los hospitales de nivel II – I de la región Amazonas.



PROFESIONAL EXPERTO

16701047

De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

CATEGORÍA	CLASIFICACIÓN	INDICADOR
SUFICIENCIA: Los ítems que pertenecen a una misma dimensión bastan para obtener la medición de ésta.	1. No cumple con el criterio	Los ítems no son suficientes para medir la dimensión.
	2. Bajo Nivel	Los ítems miden algún aspecto de la dimensión pero no corresponden con la dimensión total.
	3. Moderado nivel	Se deben incrementar algunos ítems para poder evaluar la dimensión completamente.
	4. Alto nivel	Los ítems son suficientes.
CLARIDAD: El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de las mismas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA: El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. No cumple con el criterio	El ítem no tiene relación lógica con la dimensión.
	2. Bajo Nivel	El ítem tiene una relación tangencial con la dimensión.
	3. Moderado nivel	El ítem tiene una relación moderada con la dimensión que está midiendo.
	4. Alto nivel	El ítem se encuentra completamente relacionado con la dimensión que está midiendo.
RELEVANCIA: El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

MATRIZ DE CONSISTENCIA PARA JUICIO DE EXPERTOS K. Bautista. G

MODELO DE GESTIÓN DE RIESGOS DE TI PARA HOSPITALES DE NIVEL II - I DE LA REGIÓN AMAZONAS

FASE I: DEFINIR EL ALCANCE Y CONTEXTO DE LA ORGANIZACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 1: Definir el alcance	Identificar los procesos críticos de la organización.	4	4	4	4	
	Identificar las áreas fundamentales para el proceso de gestión de riegos de TI.	4	3	4	4	
Proceso 2: Identificación del Contexto Interno y Externo	Identificar los factores internos que impactan en el comportamiento de la organización.	4	3	4	4	
	Identificar los factores externos que impactan en el comportamiento de la organización.	4	4	4	3	
FASE II: IDENTIFICACIÓN DE ACTIVOS						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 3: Identificación y Clasificación de Activos.	Identificar y clasificar (mediante un catálogo) los activos que deben ser incluidos en el proceso de gestión de riesgos de TI.	4	4	4	4	
Proceso 4: Valoración de Activos	Determinar la valoración de los activos respecto a las dimensiones de valoración y escalas estándar.	4	3	4	3	
	Valorar el grado de importancia de los activos de acuerdo al impacto.	4	4	4	4	
FASE III: EVALUACIÓN DEL RIESGO						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 5: Identificación y	Identificar (mediante un catálogo) los tipos de amenazas que podrían causar	4	3	4	3	

Valoración de Amenazas	daño a la organización.					
	Determinar la valoración de las amenazas.	4	4	4	4	
Proceso 6: Identificación, Análisis y Valoración del riesgo	Identificar y analizar el nivel del riesgo mediante la probabilidad y el impacto.	4	3	4	3	
	Valorar los riesgos respecto al resultado entre el impacto y la probabilidad de ocurrencia.	4	4	4	4	
FASE IV: TRATAMIENTO DEL RIESGO						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 7: Opciones de Tratamiento del Riesgo	Determinar si las opciones para el tratamiento son las más adecuadas para enfrentar los riesgos.	4	3	4	3	
Proceso 8: Implementar planes de Tratamiento del Riesgo	Establecer tipos de Tratamiento y Salvaguardas adecuados (mediante un catálogo) para ejecutar las opciones de tratamiento.	4	3	4	3	
FASE V: SEGUIMIENTO Y EVALUACIÓN						
PROCESO	**ACTIVIDAD**	**SUFICIENCIA**	**CLARIDAD**	**COHERENCIA**	**RELEVANCIA**	**OBSERVACIONES**
Proceso 9: Monitorear y Revisar los Riesgos	Identificar la medida de lo logrado en la aplicación del procesamiento.	4	3	4	4	
	Identificar medidas correctivas para mejorar los resultados obtenidos.	4	3	4	4	

ACEPTACIÓN	X
OBSERVADO	
DISCONFORMIDAD	

PROFESIONAL EXPERTO

16701047

ANEXO Nº 11: PERFIL DE LOS PROFESIONALES EXPERTOS

GILBERTO CARRIÓN BARCO

INFRAESTRUCTURA TECNOLÓGICA Y SEGURIDAD INFORMÁTICA

PERFIL

Doctor en Ciencias de la Computación y Sistemas. Maestro en Ingeniería de Sistemas, Magister en Docencia Universitaria, Maestro en Gestión Pública, Licenciado en Administración Pública e Ingeniero en Computación e Informática con Colegiatura N° 90931 por el Colegio de Ingenieros del Perú, habilitado. Consultor y Asesor en Soluciones de Networking, Gestión de la Información y Transformación Digital para el sector privado y sector público, con más de 15 años de experiencia en docencia universitaria a nivel de pregrado y postgrado en Universidad Nacional Pero Ruiz Gallo (UNPRG), Universidad César Vallejo (UCV), Universidad Señor de Sipán (USS), Universidad Tecnológica del Perú (UTP), Universidad de San Martín de Porres (USMP), Universidad Católica Santo Toribio de Mogrovejo (USAT) e Investigador en la línea Transformación Digital, Tecnologías de la Información para la Educación, Gobierno Electrónico, Gestión por Procesos y Gestión por Resultados. Amplia experiencia como Jurado y Asesor de Investigaciones tanto en pregrado como en postgrado. Comprometido con el trabajo en equipo, proactivo y con vocación de servicio.

Así mimo, he desempeñado cargos públicos como privados entre ellos, Director de Escuela Profesional de Ingeniería en Computación e Informática (UNPRG), Jefe de Laboratorio (UNPRG), secretario del Colegio de Ingenieros del Perú sede Lambayeque, Gerente Administrativo del Centro de Entrenamiento en Tecnología de la Información – CETI.

DATOS ACADÉMICOS

- **Doctor en Ciencias de la Computación y Sistemas**
  Universidad Señor de Sipán
- **Maestro en Gestión Pública**
  Universidad César Vallejo
- **Magister en Ingeniería de Sistemas con mención en Gerencia de Tecnologías de la Información y Gestión de Software**
  Universidad Nacional Pedro Ruíz Gallo
- **Ingeniero en Computación e Informática**
  Universidad Nacional Pedro Ruíz Gallo

EXPERIENCIA LABORAL

- **DOCENTE POSGRADO**
  Universidad César Vallejo
- **CATEDRÁTICO ASOCIADO**
  Universidad Tecnológica del Perú
- **CATEDRÁTICO ASOCIADO**
  Universidad Nacional Pedro Ruiz Gallo
- **CATEDRÁTICO ASOCIADO**
  Universidad Señor De Sipán
- **DIRECTOR DE ESCUELA**

Universidad Nacional Pedro Ruiz Gallo

- **GERENTE ADMINISTRATIVO**
  Centro de Entrenamiento en Tecnologías de la Información – CETI
- **CATEDRÁTICO ASOCIADO**
  Universidad de San Martin de Porres
- **JEFE ÁREA ADMINISTRATIVA RED TELEMÁTICA**
  Universidad Nacional Pedro Ruiz Gallo
- **CATEDRÁTICO ASOCIADO**
  Universidad Católica Santo Toribio de Mogrovejo

JESSIE LEILA BRAVO JAICO

Docente en la UNPRG y en la USAT. Asesora y Consultora en TI. Especialista Redes, Seguridad y Auditoría Informática.

PERFIL

Ing. de Computación y Sistemas. Primera Promoción de la Universidad Privada Antenor Orrego de Trujillo. Doctora en Ciencias de Computación y Sistemas en la USS. Magister en Informática y Multimedia en la Universidad de Los Lagos - Chile. Magister en Administración de empresas con mención en Gerencia Empresarial de la Universidad Nacional Pedro Ruiz Gallo. Especialización en Redes Informáticas, Gestión de proyectos, Auditoría y consultoría de sistemas. Asesora y Consultora de TI en empresas de la región.

DATOS ACADÉMICOS

- **Doctora en Ciencias de la Computación y Sistemas**
  Universidad Señor de Sipán
- **Maestra en Administración con mención en Gerencia Empresaria**
  Universidad Nacional Pedro Ruíz Gallo
- **Magister en Informática y Multimedia**
  Universidad San Pedro
- **Ingeniero de Computación y Sistemas**
  Universidad Privada Antenor Orrego

EXPERIENCIA LABORAL

- **CATEDRÁTICA**
  Universidad Nacional Pedro Ruíz Gallo
- **CATEDRÁTICA**
  Universidad Católica Santo Toribio de Mogrovejo
- **CONSULTORA INFORMÁTICA**
  Clínica Servimédicos – AUNA
- **ASESORA Y CONSUTORA DE TI**
  Clínica Max Salud
- **DIRECTORA DE ESCUELA**
  Universidad Nacional Pedro Ruíz Gallo

ERNESTO KARLO CELI ARÉVALO

Gestión de la Seguridad de Información, Riesgos TI y Continuidad de Procesos

PERFIL

Especialista en Seguridad y Auditoría Informática con COSO, COBIT 5.0, ISO/IEC 27001, ISO/IEC 27002. Especialista en Gestión de Riesgos de TI con ISO/IEC 27005, Magerit. Especialista en Gestión de servicios de TI con ITIL. Docente universitario con más de 22 años de experiencia en diferentes universidades nacionales y particulares a nivel de pregrado y postgrado. Docente en diferentes cursos de especialización en temas relacionados a: Auditoría Informática, Gestión de Riesgos de TI, Seguridad de la Información, Continuidad de negocio, Gobierno de TI y Gestión de servicios de TI. Auditor Informático, especializado en el sector financieras, con experiencia en más de 15 años. Proyectistas de proyectos informáticos a nivel de entidades públicas y privadas con experiencia en más de 20 años. Consultor externo en Gestión de servicios de TI. Cargos ocupados: Director de Escuela Profesional, Decano de Facultad, Presidente de Capítulo de CIP, Jefe de la Unidad de Riesgos de TI.

DATOS ACADÉMICOS

- **Doctor en Administración**
  Universidad Nacional pedro Ruíz Gallo
- **Maestro en Ciencias Informática y Sistemas**
  Universidad Nacional Pedro Ruíz Gallo
- **Ingeniero de Computación y Sistemas**
  Universidad Privada Antenor Orrego

EXPERIENCIA LABORAL

- **DIRECTOR DE ESCUELA**
  Universidad Nacional Pedro Ruíz Gallo
- **DOCENTE UNIVERSITARIO**
  Universidad Nacional Pedro Ruíz Gallo
- **AUDITOR EXTERNO DE TI**
  Caja Rural De Ahorro Y Crédito Cruz De Chalpón (Hoy Caja Sipán)
- **PROYECTISTA PRINCIPAL**
  Consorcio ATA – KUKOVA
- **DECANO**
  Universidad Nacional Pedro Ruíz Gallo
- **LÍDER DE PROYECTO**
  Municipalidad Provincial Condorcanqui
- **ANALISTA DE PROCESOS**
  Ministerio De La Producción
- **SUPERVISOR DE ELABORACIÓN DE EXPEDIENTE TÉCNICO**
  Proyecto Especial Olmos Tinajones
- **JEFE DE OFICINA CENTRAL**
  Universidad Nacional Pedro Ruíz Gallo

LUIS MONTENEGRO CAMACHO
SEGURIDAD DE TI EDUCATIVA

PERFIL

Doctor en Administración, Maestro en Ciencias de la Educación con mención en tecnología de la información e informática educativa, segunda especialidad con mención en tecnología de informática educativa, con 25 años de experiencia en seguridad de TI y docencia de Post Grado.

DATOS ACADÉMICOS

- **Doctor en Administración de la Educación**
  Universidad César Vallejo
- **Maestro en ciencias de la Educación con mención en Tecnología de la Información e Informática Educativa**
  Universidad Nacional Pedro Ruíz Gallo
- **Segunda Especialidad con mención en Tecnología e Informática Educativa**
  Universidad Nacional Pedro Ruíz Gallo
- **Licenciado en Educación Secundaria Especialidad Matemática**
  Universidad Nacional Mayor de San Marcos

CARGO ACTUAL

- **DOCENTE POSGRADO**
  Universidad César Vallejo

JUDITH KARIM GONZÁLES BAUTISTA

SEGURIDAD DE TI EDUCATIVA

PERFIL

Maestro en ciencias de la Educación con mención en Tecnologías de la Información e Informática Educativa, Segunda Especialidad en Gestión Escolar con Liderazgo Pedagógico, Licenciado en Educación Matemática, con 20 años de experiencia en seguridad de TI.

DATOS ACADÉMICOS

- **Maestro en ciencias de la Educación con mención en Tecnologías de la Información e Informática Educativa**
  Universidad Nacional Pedro Ruíz Gallo
- **Segunda Especialidad en Gestión Escolar con Liderazgo Pedagógico**
  Pontificia Universidad Católica del Perú
- **Licenciado en Educación Matemática**
  Universidad Nacional Pedro Ruíz Gallo

CARGO ACTUAL

- **SUB DIRECTORA**
  Colegio Pedro Abel Labarthe Durand

ANEXO Nº 12: EVIDENCIA DE CONFORMIDAD DE LA IMPLEMENTACIÓN PARCIAL POR PARTE DEL CASO DE ESTUDIO

Aceptación del Modelo de Gestión de Riesgos propuesto - César Villegas Rivera

Translate message to: English | Never translate from: Spanish

JC

J[redacted] I[redacted] C[redacted] <jizquierdoc@hab.com>

Sat 2020-07-25 14:06

To: You

Buen día César,

Después de revisar y analizar el modelo de gestión de riesgos que propones para nuestro hospital, tenemos la certeza que cumple con reforzar las debilidades relativas a la gestión de riesgos que forman parte del entorno de nuestra institución, el cual servirá de gran ayuda al momento de realizar la ejecución para analizar futuros riesgos. Estamos a la expectativa de poder llevar a cabo la implementación al 100% cuando la coyuntura actual lo permita.

Saludos cordiales, Atte. Unidad de Estadística e Informática (TI).

Reply | Forward

Documento de Revisión y Conformidad

Yo, **JIC**, en calidad de **Jefe de la Unidad de Estadística e Informática (TI)**, del **HAB**, he verificado la información relativa al Hospital incluida en la tesis denominada como "**Modelo de Gestión de Riesgos de TI que Contribuye en la Protección de los Activos de Información en Hospitales de Nivel II - I de la región Amazonas**", y con la firma de la presente doy conformidad a los valores incluidos en los formatos que se detallan a continuación, debido a que estos se ajustan a la realidad de nuestro hospital, asimismo dejo constancia de conocimiento que los datos incluidos en la tesis en mención solo serán usados con fines educativos.

Por otro lado, con la implementación parcial desarrollada en la tesis, se han logrado identificar más del 75% de los riesgos que ponen en peligro constante a los activos de información críticos de nuestra institución, puesto que dichos activos forman parte de la Unidad de Estadística e Informática (TI).

MINISTERIO DE SALUD GOBIERNO REGIONAL AMAZONAS V° B° INFORMÁTICA HOSPITAL DE APOYO BAGUA

Código	Nombre
CF N° 01	FORMATO DE DEFINICIÓN DEL ALCANCE
CF N° 02	FORMATO DE IDENTIFICACIÓN DEL CONTEXTO INTERNO
CF N° 03	FORMATO DE IDENTIFICACIÓN DEL CONTEXTO EXTERNO
CF N° 04	FORMATO DE IDENTIFICACIÓN Y CLASIFICACIÓN DE ACTIVOS
CF N° 05	FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO A LAS DIMENSIONES DE VALORACIÓN
CF N° 06	FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO A LAS ESCALAS ESTÁNDAR
CF N° 07	FORMATO DE VALORACIÓN DE ACTIVOS RESPECTO AL IMPACTO
CF N° 08	FORMATO DE IDENTIFICACIÓN Y VALORACIÓN DE AMENAZAS
CF N° 09	FORMATO DE IDENTIFICACIÓN Y ANÁLISIS DEL RIESGO
CF N° 10	MAPA DE RIESGOS
CF N° 11	FORMATO DE VALORACIÓN DEL RIESGO
CF N° 12	FORMATO DE SELECCIÓN E IMPLEMENTACIÓN DE PLANES DE TRATAMIENTO DEL RIESGO
CF N° 13	FORMATO DE MONITOREO Y REVISIÓN (PRY 01: Establecer

	controles para minimizar los errores provocados por el administrador del sistema)
CF N° 14	FORMATO DE MONITOREO Y REVISIÓN (PRY 02: Programar capacitaciones para concientizar el uso de información sensible)
CF N° 15	FORMATO DE MONITOREO Y REVISIÓN (PRY 03: Establecer capacitaciones a los usuarios que hacen uso del software de antivirus)
CF N° 16	FORMATO DE MONITOREO Y REVISIÓN (PRY 04: Implementación de políticas para minimizar la suplantación de identidad y el abuso de privilegios de accesos que involucran las bases de datos y sus vulnerabilidades en los distintos sistemas informáticos del Hospital)
CF N° 17	FORMATO DE MONITOREO Y REVISIÓN (PRY 05: Establecer controles para minimizar el uso no previsto de equipos informáticos y Sistemas operativos)
CF N° 18	FORMATO DE MONITOREO Y REVISIÓN (PRY 06: Determinar lineamientos para asegurar la continuidad de funcionamiento así como la vida útil de los equipos en casos de corte de energía eléctrica)
CF N° 19	FORMATO DE MONITOREO Y REVISIÓN (PRY 07: Establecer estrategias para enfrentar los inconvenientes causados por los desastres naturales e industriales)
CF N° 20	FORMATO DE MONITOREO Y REVISIÓN (PRY 08: Definir planes de acción frente a las condiciones inadecuadas de temperatura que afectan a los activos)
CF N° 21	FORMATO DE MONITOREO Y REVISIÓN (PRY 09: Implementar políticas y planes de acción para proteger los activos en casos de hurto)
CF N° 22	FORMATO DE MONITOREO Y REVISIÓN (PRY 10: Establecer planes de contingencia ante las caídas del servicio de internet)
CF N° 23	FORMATO DE MONITOREO Y REVISIÓN (PRY 11: Establecer capacitaciones para concientizar al personal sobre el uso consiente del ROF)

MINISTERIO DE SALUD
V° B°
INFORMÁTICA
HOSPITAL DE APOYO BAGUA

MINISTERIO DE SALUD
GOBIERNO REGIONAL AMAZONAS
HOSPITAL DE APOYO BAGUA
Ing. Jaime Izquierdo Cabrera
DNI. N° 70068472
JEFE DE INFORMÁTICA

Ing Sist. JIC
Jefe de la Unidad de
Estadística e Informática (TI)

César Augusto Villegas Rivera
Autor de Tesis