UNIVERSIDAD DE LAMBAYEQUE

FACULTAD DE CIENCIAS DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

PLAN PARA REDUCIR LOS RIESGOS OPERATIVOS DE TECNOLOGÍAS DE LA INFORMACIÓN BASADA EN METODOLOGIA MAGERIT EN LA CAJA PIURA DE LA CIUDAD DE CHICLAYO

PRESENTADA PARA OPTAR EL TITULO DE INGENIERO DE SISTEMAS

Autor (es):

Wilber Santa María Huamán

Asesor:

Mg. Enrique Santos Nauca Torres

Línea de Investigación:

Desarrollo y gestión de los sistemas de información

Chiclayo – Perú

2020

Firma del asesor y jurado de tesis

_____
Mg. Enrique Santos Nauca Torres
ASESOR

_____
Ing. Jorge Tomás Cumpa Vásquez
PRESIDENTE

_____
Mg. Cilenny Cayotopa Ylatoma
SECRETARIO

_____
Mg. Enrique Santos Nauca Torres
VOCAL

Dedicatoria

La presente investigación está dedicada a mi familia, mis padres y hermana, a mis abuelos, que han sido y seguirán siendo un soporte a mi vida en los años venideros, ellos y las personas que más cercanas son un cimiento importante para mi vida profesional, en ellos tengo un espejo en el cual quiero reflejar sus virtuales y sus grandes corazones, los cuales admiro cada día más.

A Dios también que siempre llena mi vida, llevándome por el camino correcto.

Agradecimientos

A Dios, nuestro padre por brindarme salud y bienestar, inteligencia para poder seguir formándome como un profesional de Ingeniería de Sistemas.

A mis profesores que a lo largo de toda mi carrera universitaria me brindaron sus conocimientos y son la fuente de donde yo he podido seguir aprendiendo y mejorando como profesional

Y a mi padre por ser siempre un el mejor ejemplo de ingeniero y persona.

Resumen

La Caja Piura de la ciudad de Chiclayo es una caja municipal de ahorro y crédito de derecho privado, orientada a promover servicios de intermediación financiera, sujeta a la Ley General del Sistema Financiero, Ley General de Sociedades y directivas que dicten la Superintendencia de Banca y Seguros y Banco Central de Reserva del Perú.

Las empresas que adoptan un criterio equilibrado ante la madurez de la gestión de riesgos operativos de tecnologías de información, tienen menos incidentes en este ámbito y además obtienen mayor rentabilidad del negocio respecto de la competencia.

El objetivo de esta investigación desarrollar la propuesta de un plan basado en la Metodología MagerIT con la finalidad de reducir los riesgos operativos de tecnologías de la información en la Caja Piura; teniendo como objetivos específicos (1) el análisis de los riesgos operativos de TI que existen (2) el diseño de la propuesta de plan basada en la Metodología MagerIT para reducir los riesgos operativos de TI y (3) validar el modelo propuesto.

El proyecto concluyó con la encuesta de tres expertos que aceptaron en un 93% los factores considerados para el diseño de la metodología de análisis y tratamiento de riesgos de Tecnologías de Información propuesto.

Palabras Clave: MagerIT, Riesgos, Tecnología de Información, Valor Residual, Riesgos Operativos

Abstract

Caja Piura of the city of Chiclayo is a municipal savings and credit fund under private law, aimed at promoting financial intermediation services, subject to the General Law of the Financial System, General Companies Law and directives issued by the SBS and Insurance and Central Reserve Bank of Peru.

Companies that adopt a balanced approach to the maturity of information technology operational risk management have fewer incidents in this area and also obtain greater business profitability compared to the competition.

The objective of this research is to develop a proposal for a plan based on the MagerIT Methodology in order to reduce the operational risks of information technology in Caja Piura; having as specific objectives (1) the analysis of the IT operational risks that exist (2) the design of the proposed plan based on the MagerIT Methodology to reduce the IT operational risks and (3) validate the proposed model.

The project concluded with the survey of three experts who accepted 93% of the factors considered for the design of the proposed Information Technology risk analysis and treatment methodology.

Key Words: MagerIT, Risks, Information Technology, Residual Value, Operational risks

Índice

Índice de tablas

Índice de figuras

I. Introducción

Según IBM Company (2016) las empresas que adoptan un criterio equilibrado ante la madurez de la gestión de riesgos operativos de tecnologías de información, tienen menos incidentes en este ámbito y además obtienen mayor rentabilidad del negocio respecto de la competencia. En los últimos años nuevos roles han aparecido en la estructura de empresa relacionados a la gestión de riesgos de TI; los oficiales de seguridad de información tienen como principal función reducir cada vez más las brechas de seguridad de tecnologías de información, las principales preguntas que intentan resolver es si su entorno de tecnologías de información está en situación de riesgo y de ser así cuál es la manera efectiva de mejorar los niveles de madurez de seguridad en tecnologías de información para mitigar el riesgo.

Según Gartner (2017), en su estudio sobre de los patrones de gasto de tecnologías de información de seguridad, señala que en seguridad de tecnologías de información los rangos de gasto están entre el 4% y el 8% del presupuesto total de tecnologías de información, con un ligero aumento, en promedio, al 6,2% del gasto total en TI. Por otro lado, el gasto en seguridad de red sigue siendo la categoría dominante en el presupuesto general de la seguridad de tecnologías de información. También concluye que los programas de seguridad de la información no han madurado durante el último año.

En el Perú, según Max (2016) la Oficina Nacional de Gobierno Electrónico e Informática de la PCM (ONGEI), en la última encuesta realizada sobre seguridad de la información, la cual se aplicó al Poder Legislativo, Poder Judicial, Poder Ejecutivo, Organismos Autónomos (20), Gobiernos Regionales (8), Gobiernos Provinciales (4), Municipalidades (30), se encontraron resultados poco alentadores sobre gestión de riesgos de tecnologías de información.

Respecto de las empresas del sector privado en el Perú, son las empresas del sistema financiero el tipo de organizaciones que buscan generar más ventaja competitiva utilizando tecnologías de información como soporte de sus procesos críticos, relacionados básicamente con los créditos y colocaciones y el recupero de éstos. La Superintendencia de Banco y Seguros (SBS) es la institución responsable de regular y supervisar a éste tipo de entidades, y sus exigencias en relación a la seguridad de la información y la gestión de riesgos operativos de tecnologías de información lo cual está normado en Resolución N° 006-2002, Reglamento para la administración de riesgos de operación y en la Circular N° G-105-2002, lo que constituye criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información.

La Caja Piura de la ciudad de Chiclayo es una caja municipal de ahorro y crédito de derecho privado, orientada a promover servicios de intermediación financiera. Está sujeta a la Ley General del Sistema Financiero, Ley General de Sociedades y directivas que dicten la Superintendencia de Banca y Seguros y Banco Central de Reserva del Perú. Con la finalidad que logre cumplir las exigencias de la SBS relacionadas a la gestión de tecnologías de información, de la seguridad y de riesgos de tecnologías de información, se determina que: Caja Piura tiene dos procesos críticos principales que son: (1) el proceso de crédito, el cual consiste en recopilar y revisar la información de los solicitantes de créditos mediante visitas domiciliarias o a su centro de trabajo para otorgar créditos, normándolos y administrándolos correctamente; y (2) el proceso de operaciones, que consiste en la apertura de cuentas de ahorro, cuentas a plazo, así como también las operaciones que los clientes realizan en sus cuentas.

La SBS exige a Caja Piura contar orgánicamente con una Unidad de Riesgos encargada de la evaluación y tratamiento de los riesgos a nivel de empresa, entre los cuales se incluyen aquellos relacionados con tecnologías. Además la SBS también exige contar con la documentación relacionada a la gestión y gobierno de tecnologías de información, tales como el Plan Estratégico Institucional (PEI), el Plan Estratégico de Tecnologías de Información (PETI) y Plan Operativo del Área de Tecnología de la Información (POTI)

Resultado de la observación de procesos y de la estructura de Caja Piura se identificaron los siguientes problemas relacionados a la gestión de riesgos operativos de tecnologías de información: (a) Las políticas, procedimientos y normativas relacionadas con la seguridad de la información y la gestión de riesgos de tecnologías de información se encuentran desfasadas y en muchos casos no tienen concordancia con las exigencias de la SBS; ocasionando incumplimientos a las normas exigidas lo cual puede dar lugar a multas o sanciones. (b) Los activos de tecnología así como su relación con los procesos no han sido priorizados correctamente, en consecuencia no existe información confiable para tomar decisiones relacionadas a las inversiones en seguridad de la información y gestión de riesgos de tecnologías de información. (c) Con frecuencia se incumplen tiempos en el desarrollo de proyectos de tecnologías de información o en la atención de requerimientos de las áreas usuarias para actualizaciones y modificaciones en los sistemas existentes, lo cual ocasión incremento en costos de producción y desarrollo, pérdida de oportunidades de negocio e impacto negativo en las áreas usuarias por falta de atención de sus necesidades. (d) No existe clasificación de la información para definir niveles de acceso y sus controles de comunicación y divulgación, lo que genera que no exista información confiable y priorizada para la toma de

decisiones en relación a las inversiones en seguridad de la información. (e) Se evidencia la falta de procedimientos adecuados para el registro de incidentes y la atención de problemas; así como la trazabilidad de las transacciones registradas. Ocasionando falta de atención oportuna de incidencias y atención de problemas, aumentando potencialmente sus impactos negativos sobre la seguridad de la información. (f) Según el último informe sobre gestión de riesgos de tecnologías de información se presentan con frecuencia caída en la red interna, intentos de acceso lógicos no autorizados externos e internos y errores negligentes. (g) No existe un proceso de evaluación y de tratamiento de riesgos de tecnologías de información, que analice adecuadamente las amenazas, vulnerabilidades e impactos asociados con cada activo.

El problema de investigación consistió en definir la propuesta de un plan basada en la Metodología MagerIT para reducir los riesgos operativos de tecnologías de la información en la Caja Piura de la ciudad de Chiclayo, teniendo como objetivo principal proponer un plan basado en la metodología MagerIT para reducir los riesgos operativos de tecnologías de información en la Caja Piura de la ciudad de Chiclayo. Se definieron como objetivos específicos (a) Analizar la situación actual de los riesgos operativos de tecnologías de información en la Caja Piura de la ciudad de Chiclayo, (b) Diseñar la propuesta de un plan basado en la metodología MagerIT para reducir los riesgos operativos de tecnologías de información en la Caja Piura de la ciudad de Chiclayo y (c) Validar por juicio de expertos la propuesta de un plan basado en la metodología MagerIT para reducir los riesgos operativos de tecnologías de información en la Caja Piura de la ciudad de Chiclayo

La investigación se justificó desde lo económico, pues con su ejecución se define un modelo que proporciona información a la administración del negocio para la toma de decisiones respecto de la inversión en la implantación de controles como mecanismo de salvaguarda de sus activos tecnológicos, reduciendo así gastos innecesarios y maximizando los beneficios de su inversión en tecnología. Desde el punto de vista social, porque con la ejecución de este proyecto se logra administrar los incidentes de seguridad reduciendo impactos negativos que puedan ocasionar pérdidas de información en los procesos de la caja o caídas de los activos tecnológicos, y por tanto pérdida de imagen institucional.

II. Marco teórico

2.1. Antecedentes del problema

De la revisión literaria, se describe a continuación los antecedentes tomados como referencia para el estudio, los que servirán de guía en el desarrollo de tesis

Antecedentes Internacionales

Paredes (2016) en su investigación *"Análisis de riesgos de la seguridad de la información utilizando la metodología MagerIT"* en la Institución Educativa Domingo Savio en la ciudad de Florencia – Caquetá" plantea el análisis de riesgos relacionado con las tecnologías de la información basado en la metodología MagerIT, como herramienta de la seguridad de la información que permite determinar los factores de riesgo a los que potencialmente podría estar expuestos los activos de información de la Institución Educativa Domingo Savio. Como objetivo general plantea la identificación de los riesgos de seguridad de la información. Finalmente, se logró determinar los activos de información con los cuales se continuó a la etapa de análisis de riesgos donde se determinó que como toda organización, se presentan brechas de seguridad que pueden repercutir negativamente en los activos de información relevantes, por lo tanto se establecieron estrategias de mejora en un informe técnico en donde se presentaron elementos importantes encontrados, así como también se estableció una Política de Seguridad aplicable para la organización, que le permita mitigar el impacto y la probabilidad de ocurrencia que pueda causar una amenaza sobre un activo de información crítico de la institución.

Según Valencia Duque (2016) en su investigación: "*Gobierno y gestión de riesgos de tecnologías de información y aspectos de información y aspectos diferenciadores con el riesgo organizacional*", se tuvo como objetivo es diseñar un modelo integrado de aseguramiento de tecnologías de información y comunicaciones, aplicables a cualquier tipo de organización, se concluye que es necesario acudir a los referentes internacionales de gobierno y gestión de tecnologías de información y a las metodologías de gestión de riesgos de TIC como referentes para incorporar una metodología que se ajuste a las necesidades de la organización y que diferencie dos de los aspectos específicos propios de un contexto tecnológico como son los activos objeto de análisis y los criterios de impacto.

Antecedentes Nacionales

García Porras (2017) en su investigación "*Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú*" consigue implementar un modelo de gestión de riesgos de seguridad de la información para Pymes, integrando la metodología OCTAVE-S y la norma ISO/IEC 27005. Se abarca el análisis de las metodologías y normas de gestión de riesgos, el diseño del modelo de gestión de riesgos de seguridad de la información, la validación del modelo en una Pyme en el proceso de ventas. El trabajo permite identificar los principales riesgos valorizándolos, para luego proceder a un tratamiento de acuerdo a las necesidades de la empresa, teniendo como objetivo que el modelo ayude en la gestión de riesgos de seguridad

de la información dentro de las Pymes, para poder reducir el impacto de riesgos a los que pueden estar expuestas.

Villena Aguilar (2015) en su investigación "*Planteamiento de un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú*" plantea como objetivo establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú, el cual apunte a asegurar que la tecnología de información usada esté alineada con la estrategia de negocio y que los activos de información tengan el nivel de protección acorde con el valor y riesgo que represente para la organización, en base al estándar ISO/IEC 17799. Para lo cual se tomó como referencia el modelo de seguridad de información de Mc Cumber, por ser uno de los más influyentes, dado que abarca los principales estados de la información, características y medidas de seguridad. La relación con esta investigación está en la implantación de una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia dando a conocer la importancia de la seguridad de información en los procesos que manejan.

Zamalloa Pacheco (2018) en su proyecto titulado "*Aplicación de ITIL V3.0 para mejorar la gestión de servicios en área de soporte en Protransporte*" propone mejorar los servicios de TI, para que el personal que labora en esta organización realice su trabajo de forma eficiente. Para ello, adopta la metodología deITIL basada en 10 pasos, a fin de identificar puntos claves en una entidad pública que es objeto de nuestro estudio. Para el modelamiento y diseño de los procesos planeados y puestos en marcha en el área de soporte se empleó el software Bizagi Modeler, orientado a BPMN (Business Process Model and notation) y el método GQM (Goal, Question, metric), para definir las métricas para controlar los procesos a desarrollar y así optimizar tiempos de atención.

Antecedente local

Guevara Chumán (2015) en su investigación "*Aplicación de la metodología MagerIT para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruíz Gallo*" tuvo como objetivo brindar un Plan de Mitigación de riesgos basado en las medidas de seguridad ya implementadas, aplicando la metodología Magerit, Metodología de Análisis y Gestión de riesgos de las tecnologías de Información, la cual abarca dos procesos que son estructurados de la siguiente manera: Método de análisis de riesgos (Identificación, Dependencias y Valoración de los activos; Identificación y Valoración de las amenazas; Identificación y Valoración de las salvaguardas existentes; estimación del

impacto y riesgo). Proceso De Gestión De Riesgos (Toma de decisiones y Plan de Mitigación), y la herramienta Pilar, Procedimiento Informático Lógico de Análisis de Riesgos, aplicación desarrollada en java a medida para la implementación de la metodología MagerIT.

Según Celi Arévalo (2014) en su artículo "*La gestión de riesgos de TI y la efectividad de los sistemas de seguridad de la información: Caso procesos críticos en las pequeñas entidades financieras de Lambayeque, Perú*", tuvo como objetivo proponer un modelo para la gestión de riesgos operativos de TI como parte del Sistema de Gestión de la Seguridad de la Información, desde una perspectiva que integra técnicas cuantitativas y cualitativas para entidades financieras tipo pymes, cajas rurales o municipales. Se concluye en la demostración que la metodología de gestión de riesgos de TI, permite identificar los niveles de riesgos de tal forma que sirve de información para la toma de decisiones en relación la inversión para la implementación de los controles que sirvan de salvaguardas en la protección del proceso contra posibles amenazas y vulnerabilidades.

Galán Santisteban (2015) en su investigación "*Implementación del marco de trabajo ITIL para apoyar la gestión de los servicios del Centro de Sistemas de Información en la Gerencia Regional de Salud*", logra con la implementación de la metodología ITIL aplicada a los procesos de TI mejorar la utilización de recursos, reduciendo y eliminando tareas repetitivas, para reducir los plazos de entrega y tiempo en el desarrollo de proyectos de TI. Para ello, se utilizó técnicas de recolección de datos tales como encuestas y fichas de observación, logrando determinar las deficiencias en los servicios que se brindaban; para luego proponer posibles soluciones para contrarrestar los problemas encontrados. Los resultados obtenidos determinaron que al incorporar herramientas basadas en ITIL, se obtuvo una mejora en la gestión del mantenimiento preventivo y correctivo de TI de 65% en los tiempos de solución de los problemas de TI, teniendo ahora una duración promedio de quince minutos.

2.2. Bases teórico-científicas

2.2.1. Proceso de gestión de riesgos

Según ISO 9001 la gestión del riesgo se define como el proceso de identificar, analizar y cuantificar las probabilidades de pérdidas y efectos secundarios que se desprenden de los desastres, así como de las acciones preventivas, correctivas y reductivas correspondientes que deben emprenderse.

Santos Costas (2012) establece que la Gestión de los Riesgos permite tener control sobre el desarrollo, la implementación y funcionamiento de los procesos, lo cual llevara a lograr de manera eficiente el cumplimiento de sus objetivos estratégicos y estar preparados para enfrentar cualquier incidente que pueda presentarse.

La incertidumbre representa riesgos y oportunidades con el potencial de destruir o crear valor. La gestión de riesgos de la empresa permite a los administradores hacer frente eficazmente a las incertidumbres así como a los riesgos y oportunidades asociados con ellos, con el fin de mejorar la capacidad de generar valor.

El enfoque integral de la gestión del riesgo pone énfasis en las medidas ex-ante y ex-post y depende esencialmente de:

- La identificación y análisis del riesgo.
- La concepción y aplicación de medidas de prevención y mitigación
- La protección financiera mediante la transferencia o retención del riesgo; y
- Los preparativos y acciones para las fases posteriores de atención, rehabilitación y reconstrucción.

Sobre los procesos, se construyen controles con el objetivo de reducir la frecuencia de las amenazas o limitar el daño causado y llevar el nivel de riesgo a un nivel aceptable por la organización. Dependiendo del tipo de riesgo, se puede optar por:

- Evitar el riesgo: por ejemplo eliminando el activo.
- Mitigar el riesgo: implementando controles para reducir la probabilidad y el impacto.
- Transferir el riesgo: por ejemplo contratando un seguro con cobertura para ese riesgo.
- Aceptar el riesgo: reconociendo que el riesgo existe y monitorizarlo.

Una vez que los controles han sido aplicados, el nivel de riesgo que queda es el riesgo residual. Como se establece en los Requerimientos de los Sistemas de Gestión de Seguridad de la Información en la norma ISO 27001; la Dirección debe establecer el nivel de riesgo aceptable para la organización. Los riesgos que excedan de ese nivel deben ser reducidos.

2.2.2. Riesgo de tecnologías de información

Concepto

El Riesgo de Tecnologías de Información es la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información que la empresa dispone para prestar sus servicios. Se asocia con la capacidad de la empresa en que la tecnología disponible satisfaga las necesidades actuales y futuras de la empresa y soporten el cumplimiento de la misión. El concepto de riesgo de TI puede definirse también como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Es el control el que actúa sobre la causa del riesgo para minimizar sus efectos. Cuando se dice

que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos.

Un riesgo es cualquier tipo de hecho que este existir sería una amenaza los objetivos de la organización, estos riesgos tienen una posibilidad de ocurrencia por lo que se miden como la multiplicación de impacto por probabilidad (INDECOPI, 2007). Los riesgos operacionales son activos que afecta a la parte estratégica que están alineados a los objetivos relacionados de la organización (tales como presupuestos, informes, cronogramas y tecnologías).

ISACA (2009) afirma: "Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos." (p. 11)

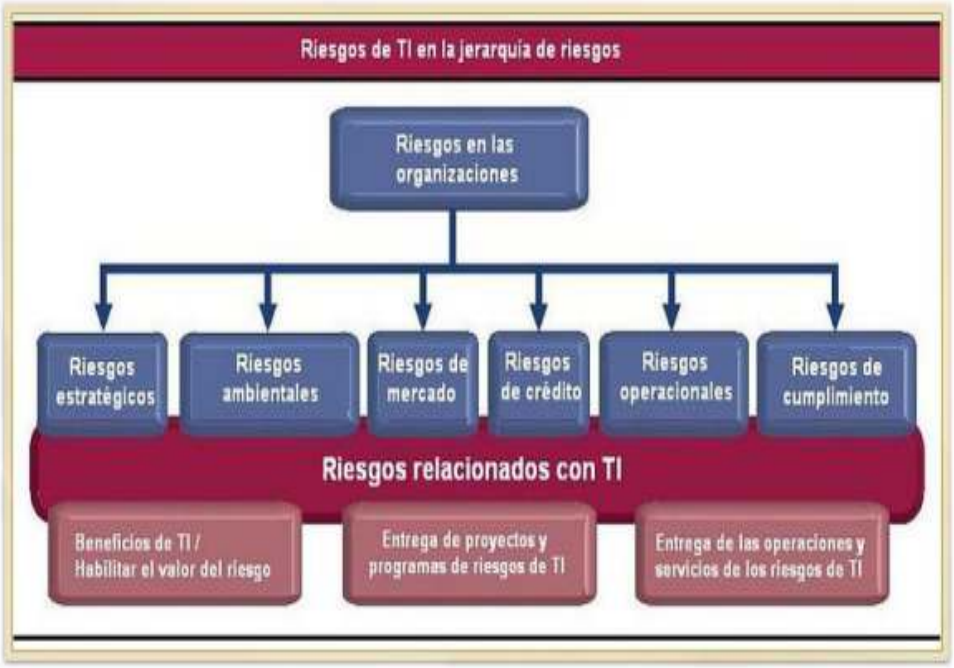


Figura 1: Pasos para implementar un Sistema de Gestión de Riesgos
Fuente: (Caso, 2019)

2.2.3. Gestión eficaz de riesgo

Según Celi Arévalo (2014) nos indica para determinar el perfil de riesgo se debe tener en cuenta las dimensiones del riesgo con los factores de riesgo, con la finalidad de comprender

cuáles son las causas que determinan los valores estimados en cada dimensión de riesgo y, cuáles son los factores que lo originan. La Figura 2 establece esta relación.

La gestión eficaz del riesgo es una combinación lógica de tres disciplinas básicas:

- Proceso de gobernanza del riesgo: políticas completas y eficaces relacionados con el riesgo, combinado con un proceso maduro y consistente para identificar, evaluar, priorizar y supervisar los riesgos oportunamente.
- Cultura consciente sobre riesgos: personas cualificadas que saben cómo identificar y evaluar las amenazas e implementar la mitigación efectiva del riesgo.
- Implantación eficaz de TI: infraestructura y las aplicaciones de TI que tienen riesgos inherentemente inferiores a los tolerables, debido a que están bien gestionados y tienen una buena arquitectura.

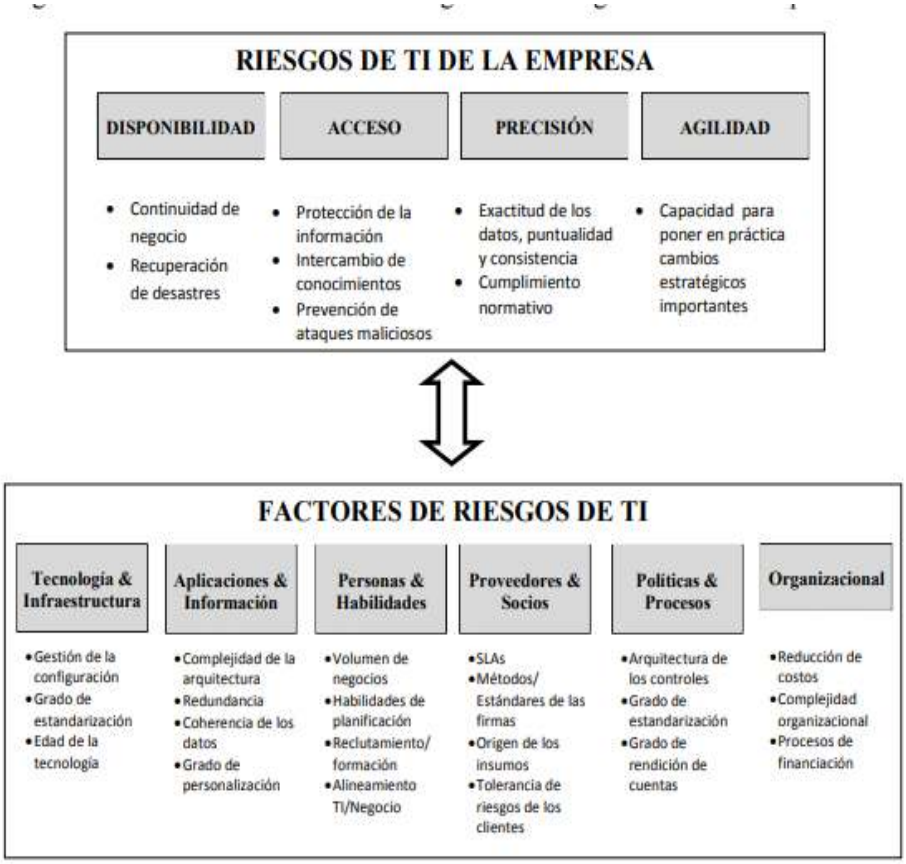


Figura 2: Relación entre apetito, tolerancia y capacidad de riesgo

Fuente: Buenas Prácticas en Gestión de Riesgo. Fábrica del Pensamiento

2.2.4. Gestión de riesgos de tecnologías de información

Concepto

A gestión de riesgos es entonces el término asociado al conjunto de pasos secuenciales, lógicos y sistemáticos que se deben seguir en las organizaciones para identificar, valorar y manejar los riesgos asociados a los procesos de TI de la organización, los cuales ejecutados en forma organizada le permiten encontrar soluciones reales a los riesgos detectados minimizando las pérdidas o maximizando las oportunidades de mejora.

2.2.5. Beneficios de la gestión de riesgos de TI

A nivel organizacional:

- Alcance o logro de los objetivos organizacionales.
- Énfasis en prioridades de negocio: permite a los directivos enfocar sus recursos en los objetivos primarios.
- Tomar acción para prevenir y reducir pérdidas, antes que corregir después de los hechos, es una estrategia efectiva de administración del riesgo.
- Fortalecimiento del proceso de planeación.
- Apoyo en la identificación de oportunidades.
- Fortalecimiento de la cultura de autocontrol.

2.2.6. Metodología de gestión de riesgo de TI

Una metodología de gestión de riesgos consiste en cómo debe llevarse a cabo para cumplir con lo establecido por la Norma ISO 27005. En un contexto general debe estimar el grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización y posteriormente implementar el o los controles adecuados para su tratamiento.

Según ISACA (2009), las etapas mínimas que debe contemplar una metodología de gestión de riesgos de TI son:

- **Estimación de Riesgos**

  La estimación de riesgos describe cómo estudiar los riesgos dentro de la planeación general del entorno informático y se divide en los siguientes pasos:

  - **Identificación de Riesgos**

    En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático. Se puede considerar como los orígenes de la Administración de los Riesgos de TI a los siguientes aspectos:

    - Requerimientos legales, regulatorios, contractuales
    - Acelerados avances tecnológicos
    - Incidentes de seguridad (comunicaciones divulgadas)

- Preocupación de los usuarios
- Pérdidas económicas
- Crecimiento generalizado de procesos de negocio soportados en tecnología de información.

- **Análisis de Riesgos**

  Una vez hayan identificado los riesgos en la planificación, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

  - Exposición a Riesgos: Una actividad útil y necesaria en el análisis de riesgos es determinar su nivel de exposición en cada uno de los procesos en que se hayan identificado.
  - Estimación de la Probabilidad de Pérdida: Las principales formas de estimar la probabilidad de pérdida son las siguientes: Disponer de la persona que está más familiarizada con el entorno informático para que estime la probabilidad de ocurrencia de eventos perjudiciales. Usar técnicas Delphi o de consenso en grupo. El método Delphi consiste en reunir a un grupo de expertos para solucionar determinados problemas. Dicho grupo realiza la categorización individual de las amenazas y de los objetos del riesgo. Utilizar la calibración mediante adjetivos, en la cual las personas involucradas eligen un nivel de riesgo entre (probable, muy probable) y después se convierten a estimaciones cuantitativas.

- **Priorización de Riesgos**

  En este paso de la estimación de riesgos, se estiman su prioridad de forma que se tenga forma de centrar el esfuerzo para desarrollar la gestión de riesgos. Cuando se realiza la priorización (elementos de alto riesgo y pequeños riesgos), estos últimos no deben ser de gran preocupación, pues lo verdaderamente crítico se puede dejar en un segundo plano.

- **Control o tratamiento de Riesgos**

  Una vez que se hayan identificado los riesgos del entorno informático y analizado su probabilidad de ocurrencia, existen bases para controlarlos que son:

  - **Planificación de Riesgos**

Su objetivo, es desarrollar un plan que controle cada uno de los eventos perjudiciales a que se encuentran expuestas las actividades informáticas.

- **Resolución de Riesgos (Incluye Mitigación y transferencia de riesgos)**

  La resolución de los riesgos está conformada por los métodos que controlan el problema de un diseño de controles inadecuado, los principales son:

  - Evitar el Riesgo: No realizar actividades arriesgadas.
  - Conseguir información acerca del riesgo.
  - Planificar el entorno informático de forma que si ocurre un riesgo, las actividades informáticas sean cumplidas.
  - Eliminar el origen del riesgo, si es posible desde su inicio.
  - Asumir y comunicar el riesgo.

- **Monitorización de Riesgos**

  La vida en el mundo informático sería más fácil si los riesgos apareciesen después de que hayamos desarrollado planes para tratarlos. Pero los riesgos aparecen y desaparecen dentro del entorno informático, por lo que se necesita una monitorización para comprobar cómo protegerse el control de un riesgo e identificar como aparecen nuevos eventos perjudiciales en las actividades informáticas.

2.2.7. Metodología MagerIT

MAGERIT es una metodología del grupo "Proceso de Gestión de los Riesgos", por lo que MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información ((Públicas, 2007).

MAGERIT estudia los riesgos que soportan un sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio. Recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados. Para MAGERIT, las tareas de análisis y tratamiento de los riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad. El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel

de riesgo que acepta la Dirección. Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos.

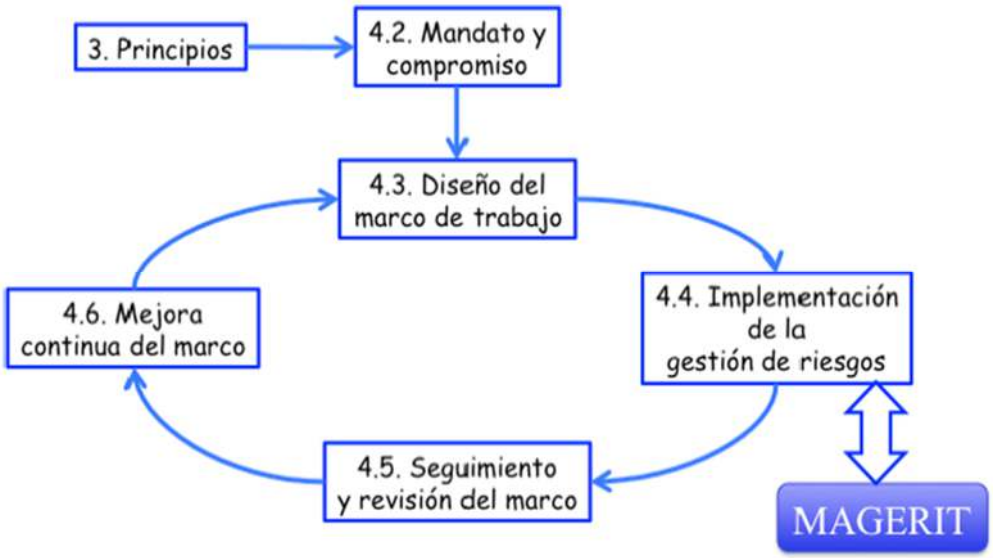


Figura 3: Alcance de MAGERIT para la gestión de riesgos propuesto por la ISO 31000
Fuente: (Gaona Vásquez, 2013)

Para ello, MAGERIT propone un catálogo, abierto a ampliaciones, que marca unas pautas en cuanto a:

- tipos de activos
- dimensiones de valoración de los activos
- criterios de valoración de los activos
- amenazas típicas sobre los sistemas de información
- salvaguardas a considerar para proteger sistemas de información

MAGERIT persigue dos objetivos:

- Por una parte, facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
- Por otra, homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

MAGERIT considera dos grandes tareas a realizar:

- Análisis de riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.
- Tratamiento de los riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la Dirección asume.

Ambas actividades, análisis y tratamiento se combinan en el proceso denominado Gestión de Riesgos.

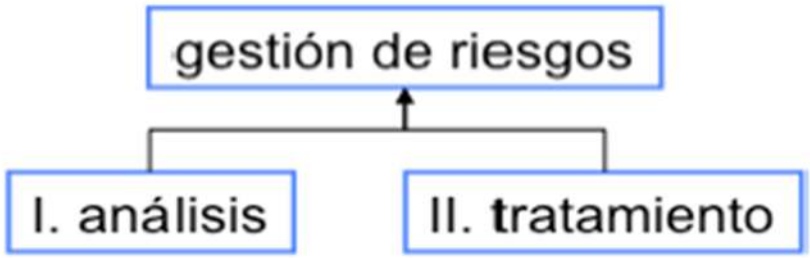


Figura 4: Etapas ara la Gestión de Riesgos según MAGERIT
Fuente: (Gaona Vásquez, 2013)

Para el análisis de riesgos MAGERIT propone los pasos siguientes:

- determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación
- determinar a qué amenazas están expuestos aquellos activos
- determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo
- estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza
- estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza

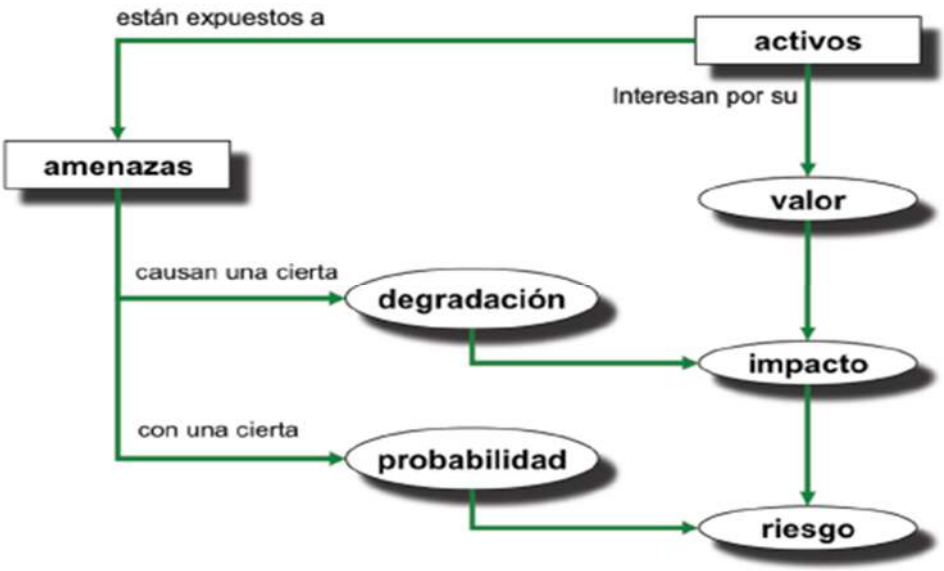


Figura 5: Elementos del análisis de riesgos potenciales según MAGERIT

Fuente: (Gaona Vásquez, 2013)

2.2.8. Tolerancias e indicadores del riesgo

El apetito es el nivel de riesgo que la empresa quiere aceptar, aquél con el que se siente cómoda, su tolerancia será la desviación respecto a este nivel. Por otro lado, la capacidad de asumir riesgos, será el nivel máximo de riesgo que una organización puede soportar en la persecución de sus objetivos. Así, la tolerancia servirá como alerta para evitar que la empresa llegue al nivel establecido por su capacidad, algo que pondría en peligro la continuidad del negocio (Públicas, 2007)

En ese sentido, podemos definir lo siguiente:

- El apetito de riesgo: La cantidad de riesgo que una organización está dispuesta a buscar o aceptar en la búsqueda de sus objetivos a largo plazo.
- Tolerancia al riesgo: Los límites de la asunción de riesgos, fuera de la cual la organización no está dispuesta a aventurarse en la búsqueda de sus objetivos a largo plazo.
- Capacidad de riesgo: la capacidad de llevar los riesgos, y la madurez de gestión de riesgos para su gestión.

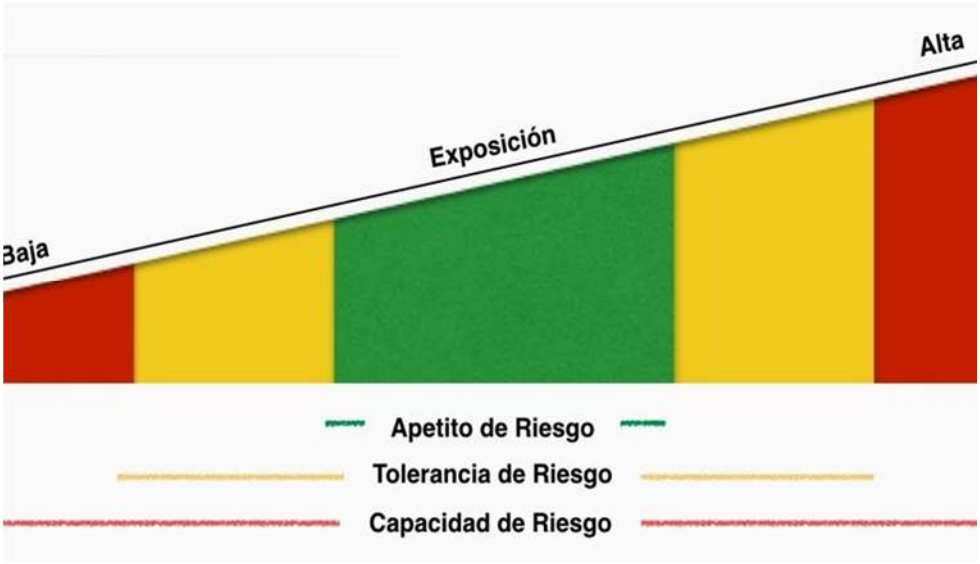


Figura 6: Tolerancia al Riesgo

Fuente: (Sotelo, Torres, & Rivera, 2016)

2.2.9. Metodología de gestión de riesgos operativos

Se considera como referencia las exigencias de la Superintendencia de Banca y Seguros, a través de sus normativas: Resolución SBS 2116-2009 que norma el Sistema de Riesgo Operacional que deben implementar las organizaciones financieras en el Perú y la Circular G-105-2002 que establece los lineamientos para la Gestión de Riesgos de Tecnologías de Información de empresas de este sector.

Para la implementación del Modelo de gestión de riesgos de Tecnologías de Información propuesto se ha diseñado la metodología compuesta por cuatro (04) fases:

Fase 1 - Identificación de los escenarios de riesgos de Tecnologías de Información

a. Identificación y clasificación de los activos de TI
b. Valoración de la criticidad de los activos de TI
c. Identificación de las amenazas de por activo de TI
d. Identificación de vulnerabilidades de cada activo de TI

Fase 2 - Valoración de los escenarios de riesgos de Tecnologías de Información

a. Estimación del impacto de los escenarios de riesgo
b. Estimación de la probabilidad de ocurrencia de los escenarios de riesgo
c. Cálculo de los niveles de exposición a los riesgos
d. Determinación del apetito y tolerancia al riesgo

Fase 3: Tratamiento de los riesgos

a. Definición de las políticas de seguridad

b. Identificación de los controles/salvaguardas de seguridad

c. Definición de la estrategia de implementación de controles/salvaguardas

Fase 4: Seguimiento de la efectividad de los controles

a. Elaboración de planes de acción

b. Cálculo de los niveles de riesgo residual (NRR)

2.3. Definición de términos básicos

- Activos: Son todos aquellos elementos que una organización posee y le genera valor, como por ejemplo la información, el software, el hardware, los recursos humanos, los servicios, entre otros. (Públicas, 2007)
- Amenazas: Es una situación que se puede presentar y puede causarle daño a un activo de la organización. (Públicas, 2007)
- Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos o procesos no autorizados (Públicas, 2007)
- Disponibilidad: consiste en que la información pueda ser accedida por los usuarios autorizados. (Públicas, 2007)
- Información: conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. (Públicas, 2007)
- Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos. (Públicas, 2007)
- Riesgo: Indica lo que le podría llegar a pasar a un activo, en el caso de que una amenaza se materialice, causándole daños y pérdidas a la organización. (Públicas, 2007)
- Vulnerabilidad: Son aquellos puntos débiles que tiene una organización, y que en caso de que se materialice le puede ocasionar pérdidas, en la mayoría de las ocasiones, económicas a la organización. (Públicas, 2007).

2.4. Formulación de la hipótesis

¿Una propuesta de un plan basada en la Metodología MagerIT reducirá los riesgos operativos de tecnologías de la información en la Caja Piura de la ciudad de Chiclayo?

III. Materiales y métodos

3.1. Variables - operacionalización

Variables

Independiente: Propuesta de plan basada en la Metodología MagerIT

Dependiente: Riesgos operativos de tecnologías de la información en la Caja Piura de la ciudad de Chiclayo

Operacionalización

Tabla 1 – *Tabla de operacionalización de la variable independiente*

Variable	Dimensión	Indicador	Técnica
Propuesta de plan basada en la Metodología MagerIT	Identificar los activos	Valorización de Activos	Ficha de observación
	Amenazas	Relación de amenazas	Ficha de observación
	Vulnerabilidades	Activos expuestos	Ficha de observación
	Impacto	Amenazas sobre el activo	Ficha de observación
	Riesgo	Ocurrencia de amenaza	Ficha de observación
	Contingencia	Contrarrestar amenazas	Ficha de observación

Fuente Propia

Tabla 2 – *Tabla de operacionalización de la variable dependiente*

Variable	Dimensión	Indicador	Técnica
Riesgos operativos de tecnologías de la información	Efectividad del diseño del modelo de gestión de riesgos de TI en la estructuración de las actividades de análisis y tratamiento de riesgos	Nivel de definición de las categorías (disponibilidad, integridad y confidencialidad) de los riesgos de TI	Encuesta
		Nivel de integración del modelo a la gestión del riesgo operativo de la entidad	Encuesta
		Nivel de utilización y comprensión del modelo por los empleados relacionados con la gestión del riesgo operativo de TI	Encuesta
	Efectividad del diseño del	Nivel de cumplimiento de los requisitos exigidos por	Encuesta

	modelo de gestión de riesgos de TI en el aseguramiento del gobierno de los riesgos de TI	la SBS para la gestión de riesgos de TI	
		Nivel de coherencia del modelo para evaluar la magnitud de los riesgos de TI	Encuesta
		Nivel de efectividad de los indicadores para el monitoreo de la gestión de riesgos de TI	Encuesta

Fuente Propia

3.2. Tipo de estudio, diseño de investigación o de contrastación de hipótesis

Tipo de Estudio

Descriptivo

Se realiza para describir las características de grupos relevantes, como consumidores, vendedores, organizaciones o áreas de mercado. (Malhotra, 2004)

Propositivo

La investigación es de tipo propositiva por cuanto se fundamenta en una necesidad dentro de la institución, una vez que se tome la información descrita, se realizará una propuesta de estrategia de fidelización de clientes para mejorar el posicionamiento, superar la problemática actual y las deficiencias encontradas. Al identificar los problemas, investigarlos, profundizarlos y dar una solución dentro de un contexto específico.

Diseño de contrastación

La investigación es de diseño no experimental, se desarrolló sin manipular deliberadamente las variables de estudios, por lo que se trató de un estudio que se realiza de manera intencional. (Hernández Sampieri, 2014).

3.3. Población, muestra de estudio y muestreo

Población

Es el conjunto de personas u objetos de los que se desea conocer algo en una investigación. (De Canales, 1994)

La población está conformada por:

- Jefatura de TI
- Jefatura de la Unidad de Riesgos
- Oficialía de Seguridad de TI y de la Información

- Jefatura de la Unidad de Continuidad de negocio
- Auditor interno

Muestra

Es un subconjunto o parte del universo o población en que se llevará a cabo la investigación (De Canales, 1994). La muestra estará conformada por la misma población.

3.4. Métodos, técnicas e instrumentos de recolección de datos

Para la recolección de los datos se hará uso de

Técnicas

- Encuesta: se aplica al personal que participa en la evaluación y tratamiento de los riesgos operativos de tecnología de información en Caja Piura.

Instrumentos

- Cuestionario: Se dice que "Es un sistema de preguntas racionales, ordenadas en forma coherente, tanto desde el punto de vista lógico como psicológico, expresadas en un lenguaje sencillo y comprensible, que generalmente responde por escrito la persona interrogada, sin que sea necesaria la intervención de un encuestador." (De Canales, 1994)

3.5. Plan de procesamiento para análisis de datos

De acuerdo a la naturaleza de la investigación se observa la necesidad de definir, desarrollar y proponer una metodología y una forma estructurada que permita evaluar objetivamente el diseño y la efectividad de la operación de la metodología propuesta para la gestión de riesgos de Tecnologías de Información en la Caja Piura de la ciudad de Chiclayo.

Para atender y solucionar esta necesidad, se aplicó un método no experimental que permita relacionar variables cuantitativas y cualitativas a partir de las valoraciones dadas por las personas que tienen autoridad y desempeñan funciones de gestión de riesgos de Tecnologías de Información en la institución, con el fin de valorar objetivamente la efectividad en el diseño y la efectividad de la operación de la metodología propuesta.

Para la evaluación de la metodología propuesta se utilizó el Método Delphi. A través de éste método se obtuvo la opinión de las personas que cumple funciones relacionadas con la gestión de las tecnologías de la información, la seguridad de la información y la gestión de riesgos operativos en la entidad. Para la aplicación del método se consideraron las siguientes características:

- Anonimato: Durante su aplicación ninguna de las personas conocían que los otros también estaban evaluando la metodología propuesta.

- Iteración y realimentación controlada: La iteración se consiguió al presentar el mismo cuestionario a todos los evaluadores de forma independiente.
- Respuesta del grupo: La información que se presenta a los evaluadores no es sólo el punto de vista de la mayoría, sino que se presentan todas las opiniones indicando el grado de acuerdo obtenido.

El procedimiento realizado consta de cuatro pasos:

- Elaborar un cuestionario tomando como base las preguntas de investigación.
- Conseguir el compromiso de colaboración de las personas seleccionadas; se socializó y explicó de forma individual la metodología propuesta.
- Determinar el contexto y el tiempo de aplicación del cuestionario. En este caso la metodología y modelos propuestos fueron utilizados durante tres (03) meses, entre enero y marzo del 2020.
- Finalmente, se les envío a través de correo electrónico, un archivo con los cuestionarios diseñados en hojas electrónicas, que contienen los niveles, factores y variables definidas a través de preguntas, para que cada uno de ellos comparta sus opiniones sobre la relevancia de la metodología propuesta. La asignación de la relevancia por parte del "experto", se realiza respondiendo "SI" o "NO" a cada factor y variable del cuestionario y la asignación de los pesos, la realiza mediante el análisis y aplicación del criterio profesional y su función dentro de la institución, asignando o distribuyendo un peso porcentual utilizando la escala de (0% al 100%) para cada pregunta, rango, evento y nivel que conforman las variables.

IV. Resultados

4.1. Analizar situación actual de los riesgos operativos de tecnologías de información en la Caja Piura de la ciudad de Chiclayo

4.1.1. Resultados de encuesta

Tabla 3 – *¿Existen políticas de seguridad en la empresa?*

Respuestas	Frecuencia	Porcentaje
Sí	4	80.00
No	1	20.00
Total	5	100.00

Fuente: encuesta

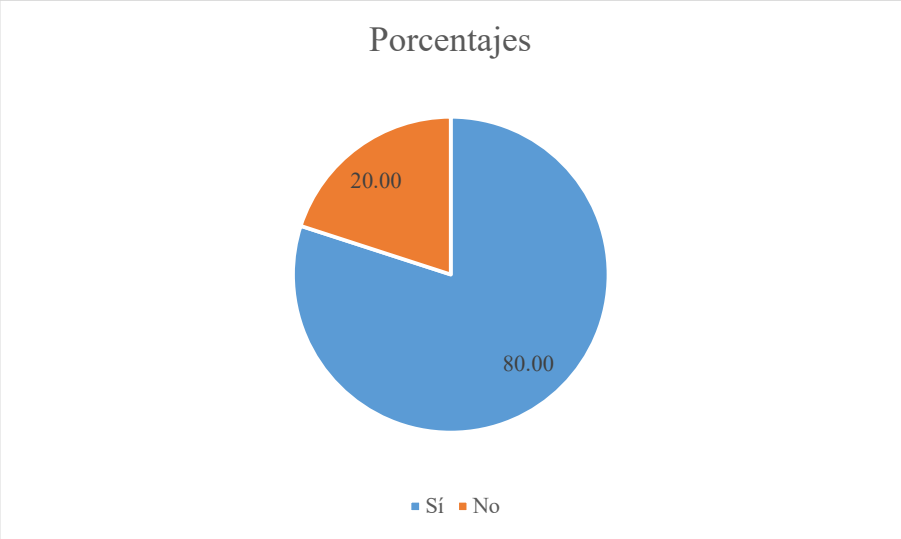


Figura 7: ¿Existen políticas de seguridad en la empresa?
Fuente: encuesta

Según la tabla 3 y figura 7, el 80% de encuestados manifestó que sí existen políticas de seguridad en la empresa y un 20% indicó que no.

Tabla 4 – *¿Tiene conocimiento de medidas de seguridad?*

Respuestas	Frecuencia	Porcentaje
Sí	4	80.00
No	1	20.00
Total	5	100.00

Fuente: encuesta

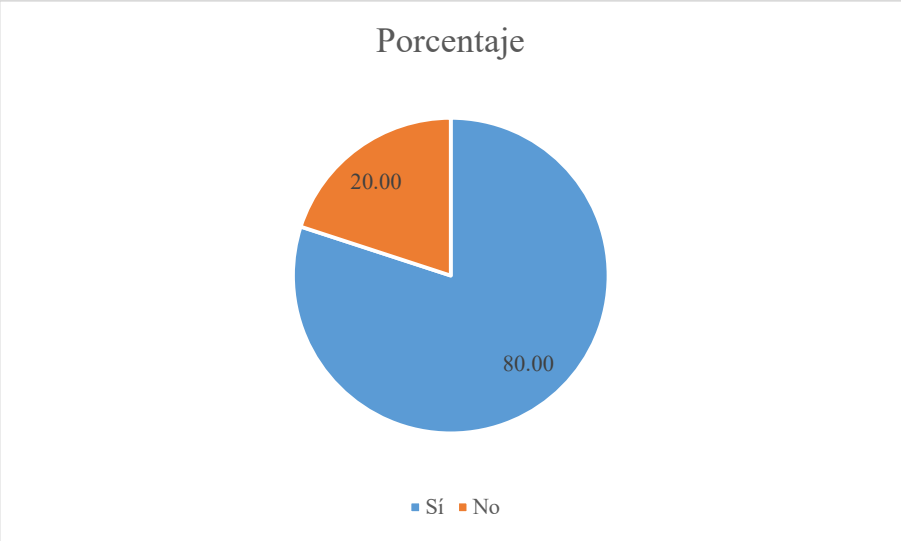


Figura 8: ¿Tiene conocimiento de medidas de seguridad?
Fuente: encuesta

Según la tabla 4 y figura 8, el 80% de encuestados manifestó tener conocimiento de las medidas de seguridad en la empresa y un 20% indicó que no tenía conocimiento de lo consultado.

Tabla 5 – *¿Ha recibido capacitación sobre seguridad de la información de acuerdo a su función Laboral?*

Respuestas	Frecuencia	Porcentaje
Sí	2	40.00
No	3	60.00
Total	5	100.00

Fuente: encuesta

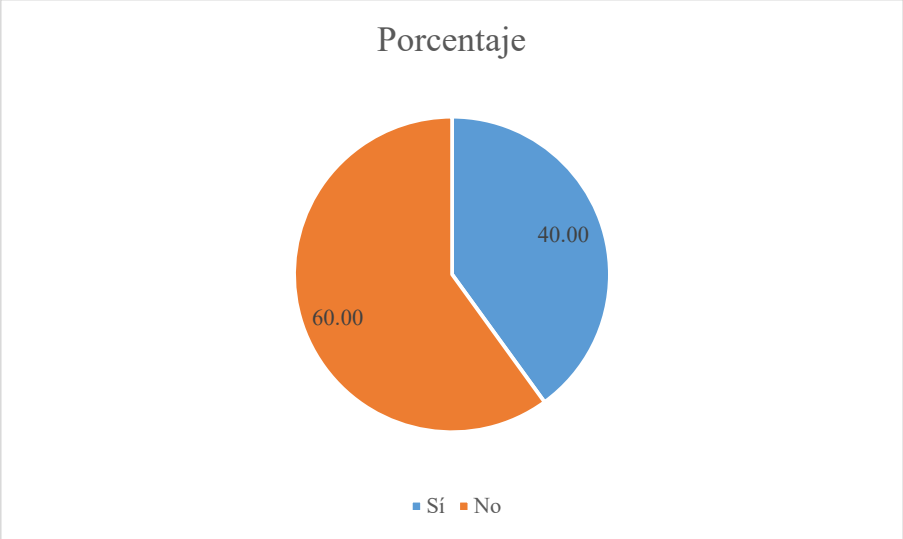


Figura 9: ¿Ha recibido capacitación sobre seguridad de la información de acuerdo a su función Laboral?
Fuente: encuesta

De acuerdo a la tabla 5 y figura 9, sólo el 40% de encuestados indicó que ha recibido capacitación sobre seguridad de la información de acuerdo a su función laboral dentro de la empresa y un 60% dijo que no recibió.

Tabla 6 – *¿Su terminal tiene contraseña para el acceso la información?*

Respuestas	Frecuencia	Porcentaje
Sí	5	100.00
No	0	0.00
Total	5	100.00

Fuente: encuesta

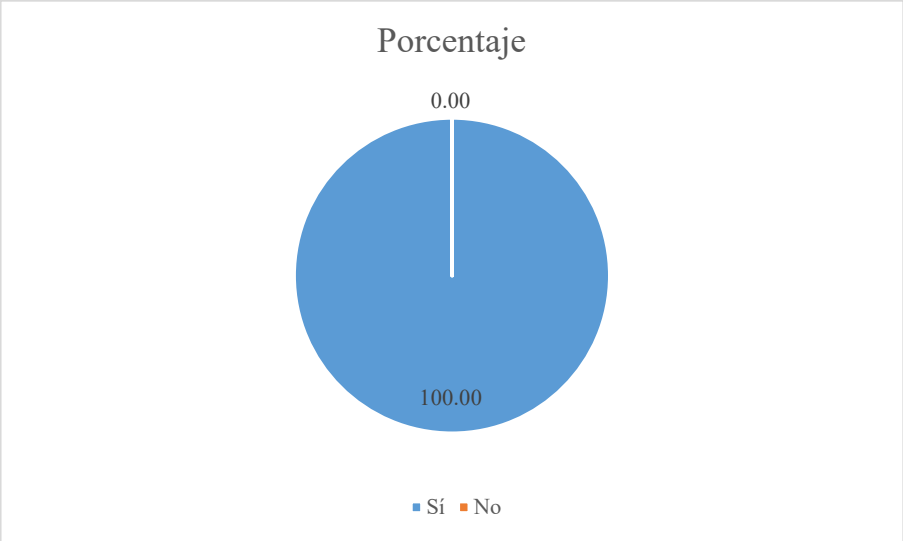


Figura 10: ¿Su terminal tiene contraseña para el acceso la información?
Fuente: encuesta

De acuerdo a la tabla 6 y figura 10, el 100% indicó que su terminal asignado tiene contraseña para el acceso a la información en la empresa.

Tabla 7 – *¿Su área de trabajo cuenta con software antivirus licenciado y actualizado?*

Respuestas	Frecuencia	Porcentaje
Sí	4	80.00
No	1	20.00
Total	5	100.00

Fuente: encuesta

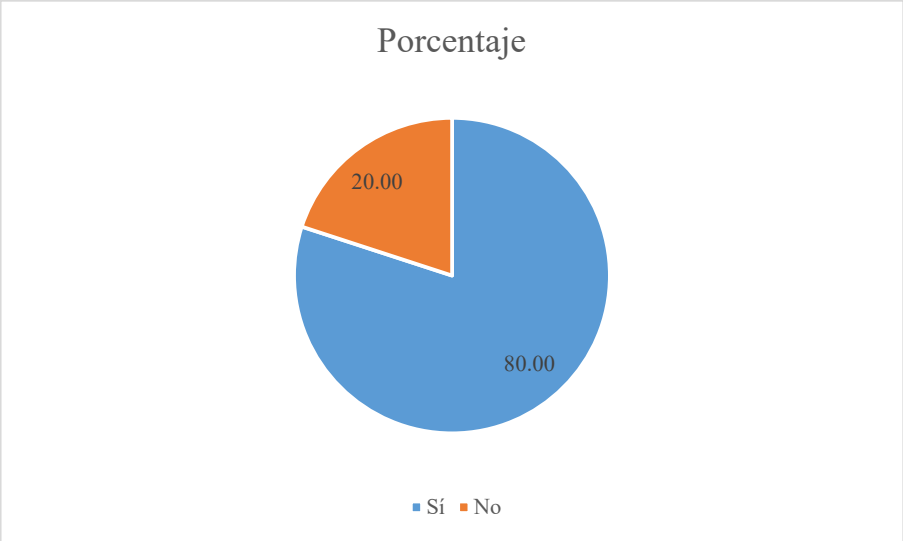


Figura 11: ¿Su área de trabajo cuenta con software antivirus licenciado y actualizado?
Fuente: encuesta

Por otro lado, tal como indica la tabla 7 y figura 11, el 80% de encuestados indicó que su área de trabajo cuenta con software antivirus licenciado y actualizado y solo el 20% dijo que no.

Tabla 8 – *¿Su divulgación no autorizada de información puede afectar el cumplimiento de leyes o normas impartidas por entes de control?*

Respuestas	Frecuencia	Porcentaje
Sí	4	80.00
No	1	20.00
Total	5	100.00

Fuente: encuesta

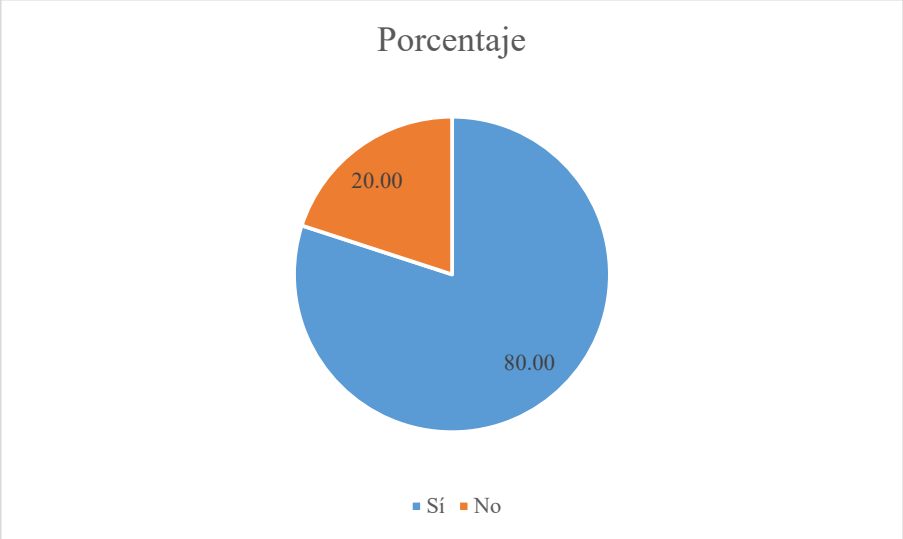


Figura 12: ¿Su divulgación no autorizada de información puede afectar el cumplimiento de leyes o normas impartidas por entes de control?
Fuente: encuesta

Según la tabla 8 y figura 12, el 80% de encuestados, la pregunta ¿Su divulgación no autorizada de información puede afectar el cumplimiento de leyes o normas impartidas por entes de control?, indicó que sí podría afectar mientras que el 20% dijo que no.

Tabla 9 – *¿Si el activo o la información que se gestiona son alterados sin autorización puede afectar la imagen de la entidad?*

Respuestas	Frecuencia	Porcentaje
Sí	5	100.00
No	0	0.00
Total	5	100.00

Fuente: encuesta

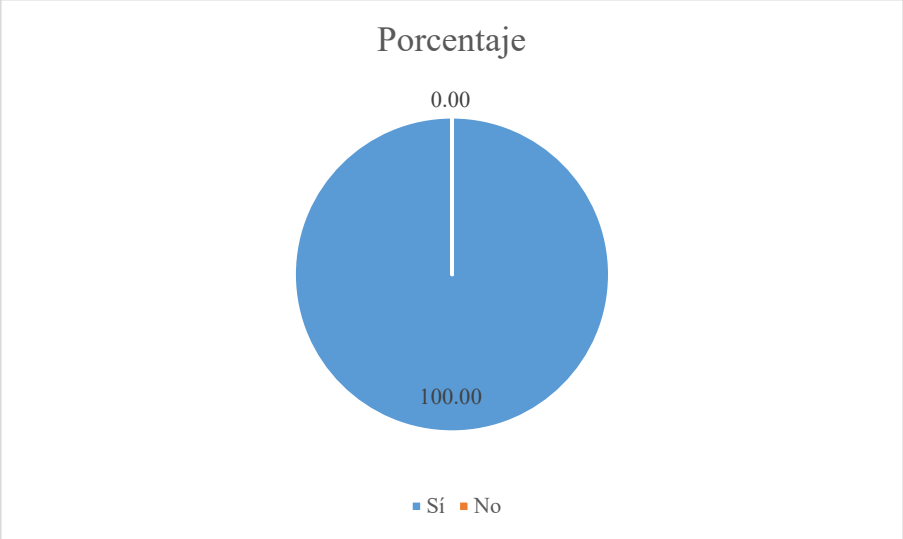


Figura 13: ¿Si el activo o la información que se gestiona son alterados sin autorización puede afectar la imagen de la entidad?
Fuente: encuesta

Según la tabla 9 y figura 13, el 100% de encuestados considera que Si el activo o la información que se gestiona son alterados sin autorización puede afectar la imagen de la entidad.

Tabla 10 – *¿El nivel de seguridad actual cumple con los parámetros establecidos para el ingreso al sistema?*

Respuestas	Frecuencia	Porcentaje
Sí	3	60.00
No	2	40.00
Total	5	100.00

Fuente: encuesta

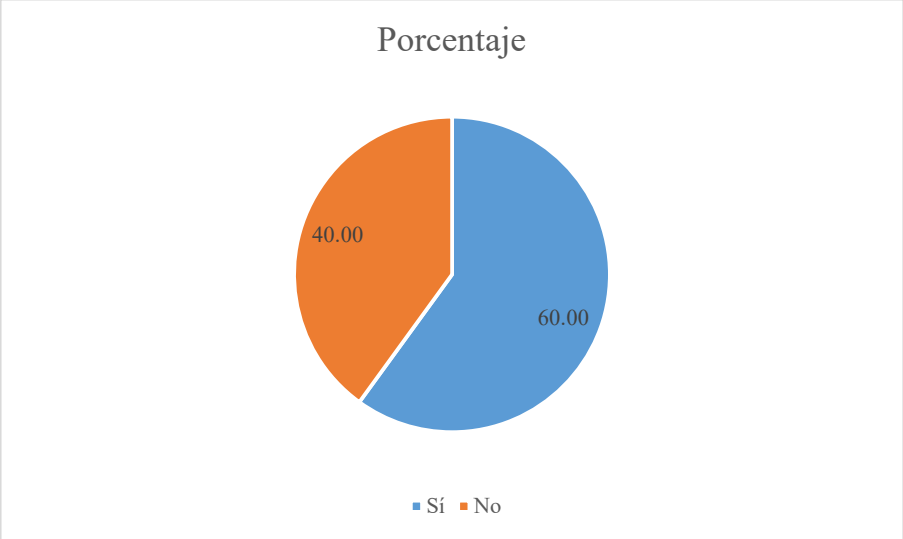


Figura 14: ¿El nivel de seguridad actual cumple con los parámetros establecidos para el ingreso al sistema?
Fuente: encuesta

Según la tabla 10 y figura 14, el 60% de encuestados afirmó que el nivel de seguridad actual sí cumple con los parámetros establecidos para el ingreso al sistema y un 40% dijo que no se cumple.

Tabla 11 – *¿Realiza copias de seguridad para proteger su información?*

Respuestas	Frecuencia	Porcentaje
Sí	2	40.00
No	3	60.00
Total	5	100.00

Fuente: encuesta

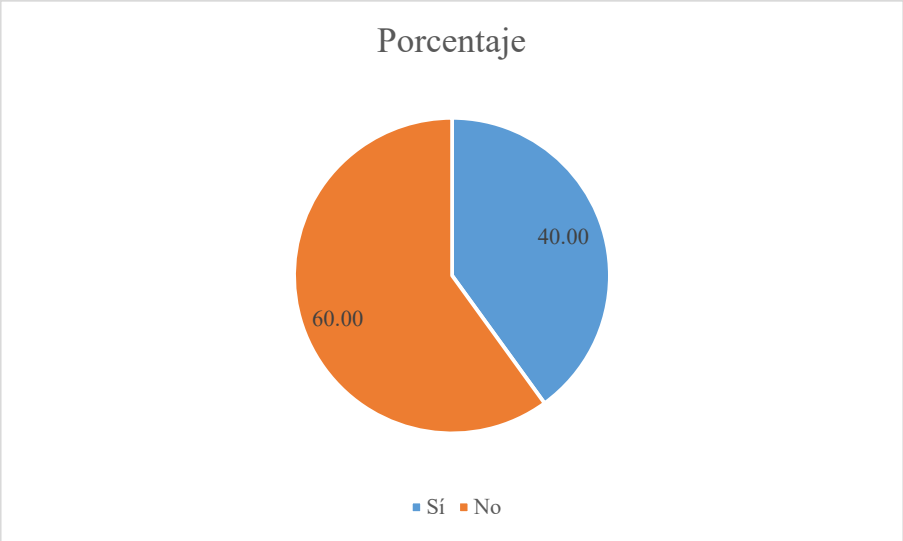


Figura 15: ¿Realiza copias de seguridad para proteger su información?
Fuente: encuesta

Según la tabla 11 y figura 15, sólo el 40% de encuestados realiza copias de seguridad para proteger su información y un mayoritario 60% dijo que no las realiza.

Tabla 12 – *¿Su oficina está protegida frente a ataques cibernéticos?*

Respuestas	Frecuencia	Porcentaje
Sí	0	0.00
No	5	100.00
Total	5	100.00

Fuente: encuesta

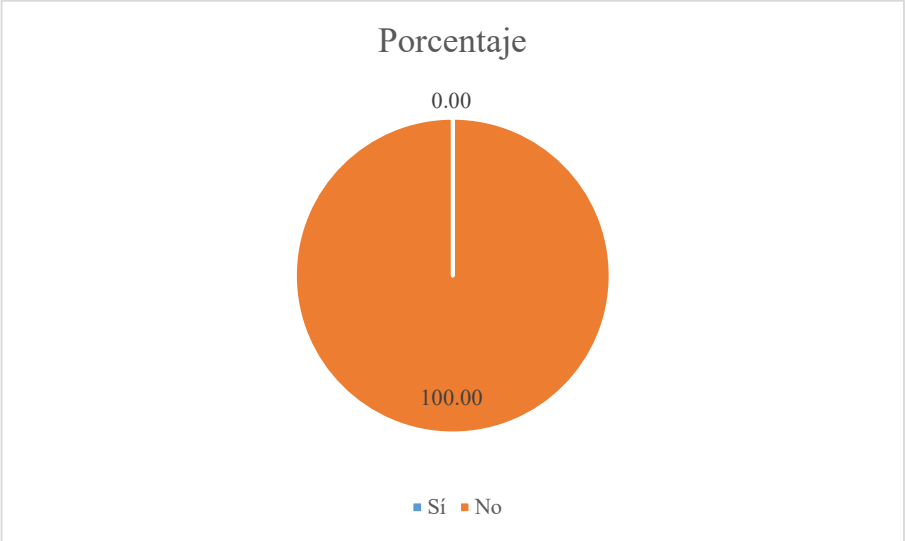


Figura 17: ¿Su oficina está protegida frente a ataques cibernéticos?
Fuente: encuesta

De acuerdo a la tabla 12 y figura 16, el 100% de encuestados afirmó que su oficina está protegida frente a ataques cibernéticos.

4.1.2. Fase 1: Identificación de los escenarios de riesgos de Tecnologías de Información

4.1.2.1. Identificación y clasificación de los activos de TI

Se identifican los activos de Tecnologías de Información que dan soporte a los procesos de negocio considerados dentro del alcance de la investigación, créditos y operaciones; luego de ello se procede a clasificarlos.

Para la clasificación de los activos de TI identificados, se utilizó la clasificación propuesta por la metodología Magerit.

Tabla 13 – *Listado de activos de Caja Piura*

N°	Tipo de activo	Activo
1	Comunicaciones	Red LAN
2	Datos o documentos	Código fuente de las aplicaciones
3	Equipos informáticos	Equipos de cómputo terminales en ventanilla y analista de créditos
4	Información	Bases de Datos
5	Personal	Personal del área de TI
6	Personal	Analistas de sistemas responsables de implementar requerimientos
7	Servicio	Servidor principal de dominio
8	Servicio	Servidor principal de base de datos y aplicaciones
9	Equipamiento auxiliar	Respaldo de base de datos
10	Equipamiento auxiliar	Respaldo de desarrollo y mantenimiento

Fuente Propia

4.1.2.2. Valoración de la criticidad de los activos de TI

Para cada uno de los activos identificados se valora que tanto se afectaría cada una de las dimensiones de seguridad de la información (confidencialidad, integridad y disponibilidad) si es que éstos son afectados por un escenario de riesgo determinado

Las escalas y criterios que se utilizarán para valorar cada una de las dimensiones de seguridad de los activo de TI, fueron referenciadas de la metodología Magerit

Tabla 14 – *Escalas y criterios para valoración de criticidad en los activos de TI*

	Escala	Criterio
Disponibilidad	1	No es relevante
	2	disponible mínimo 10% del tiempo
	3	disponible mínimo 50% del tiempo
	4	disponible mínimo 75% del tiempo
	5	disponible mínimo 95% del tiempo
Integridad	**Escala**	**Criterio**
	1	No es relevante

	2	los errores o la falta de información no afectan el funcionamiento del sistema
	3	La información debe estar correcta y completa al menos en un 50%
	4	La información debe estar correcta y completa al menos en un 70%
	5	La información debe estar correcta y completa al menos en un 95%
	Escala	**Criterio**
Confidencialidad	1	No es relevante
	2	el incidente no repercute en los procesos ni en los sistemas
	3	el incidente repercute en los procesos o en los sistemas dentro del área afectada
	4	el incidente repercute en los procesos o en los sistemas fuera del área afectada
	5	el incidente repercute no solo en los procesos o en los sistemas, sino también en la reputación y la imagen de la institución se verían comprometidas

Fuente Propia

Tabla 15 – *Valoración de criticidad en los activos de TI*

N°	Activo	Dimensión de seguridad			Nivel de criticidad	Descripción de la criticidad
		C	**I**	**D**		
1	Servidor principal de dominio	4	5	5	4	Alto
2	Servidor principal de base de datos y aplicaciones	5	5	5	5	Muy Alto
3	Red LAN	4	1	5	3	Medio
4	Bases de Datos	5	5	5	5	Muy Alto
5	Respaldo de base de datos	5	5	5	5	Muy Alto
6	Personal de área de TI	4	1	5	3	Medio
7	Equipos de cómputo terminales de ventanilla y analistas de créditos:	5	5	5	5	Muy Alto
8	Código fuente de las aplicaciones	4	5	5	4	Alto
9	Analistas de sistemas responsables de implementar requerimientos	4	1	5	3	Medio
10	Respaldo de desarrollo y mantenimiento	4	5	5	4	Alto

Fuente Propia

4.1.2.3.Identificación de las amenazas por activo de TI

Consiste en identificar amenazas potenciales que pueden afectar parcial o totalmente los activos de TI; finalmente, se identifica y relaciona las amenazas con cada activo de TI evaluado. Para ello se tomó en consideración los siguientes criterios:

- El tipo de activo
- La dimensión de seguridad con que está relacionado

- La experiencia de la organización
- Los reportes de incidentes de seguridad

Se consideró como referencia el catálogo propuesto por la metodología Magerit

Tabla 16 – *Listado de amenazas por activo de TI*

N°	Activo	Amenazas
1	Servidor principal de dominio	No se puede acceder a los servicios de red y esto paraliza los procesos del negocio
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible relacionada con datos de los clientes
3	Red LAN	Se detienen los servicios de comunicación
4	Bases de Datos	Pérdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos que generan multas y sanciones.
		Falta de espacio de almacenamiento
5	Respaldo de base de datos	Se detienen los procesos de la empresa, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.
6	Personal del área de TI	Pérdida de información debido a fuga de talentos que genera retraso en actividades o paralización de procesos
		Modificación, divulgación y destrucción de la información
7	Equipos de cómputo terminales en ventanilla y analista de créditos	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio
8	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión del sistema existente en producción.
		Manipulación de código fuente que genera pérdida de información, multas y sanciones.
9	Analistas de sistemas (responsables de la implementación de requerimientos)	Exceso de tiempos comprometidos en cronograma de actividades para desarrollo de requerimientos
		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web
		Pérdida de recursos debido a Implementaciones no acordes a metodología y estándares de desarrollo de software
10	Respaldo de desarrollo y mantenimiento	No es posible revertir las adecuaciones de los sistemas.

Fuente Propia

4.1.2.4.Identificación de vulnerabilidades de cada activo de TI

El resultado de esta actividad permite determinar cuáles son las debilidades que pueden ser aprovechadas por las amenazas para materializarse y atacar a los activos de TI. Por cada relación Activo - Amenaza se han identificado los siguientes riesgos:

Tabla 17 – *Listado de vulnerabilidades por amenazas por activo de TI*

N°	Activo	Amenaza	Riesgos
1	Servidor principal de dominio	No se puede acceder a los servicios de red y esto paraliza los procesos del negocio	Falta de personal especializado, para dar mantenimiento al servidor de dominio
			Falla en los componentes físicos
			Falla en el sistema operativo, falta de actualización de parches
			No se cuenta con un plan de mantenimiento de los servidores
			Ataque de algún virus
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible relacionada con datos de los clientes	El administrador tiene acceso total a la base de datos y realiza modificaciones
			Deficiente normalización en el diseño de base datos
			Los usuarios acceden al servidor de base de datos por canales no autorizados
3	Red LAN	Se detienen los servicios de comunicación	Falla de la línea principal de comunicación
			Falla de la red de comunicaciones con otras agencias
			Falla eléctrica que genera la interrupción de los procesos y servicios
			No cuenta con servidor de firewall a nivel de hardware
4	Bases de Datos	Pérdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos que generan multas y sanciones.	Falta de un procedimiento para la asignación de perfiles para acceso a la BD
			Existencia de contraseñas no adecuados para usuarios locales y de red
			Privilegios para usuarios de acceso a aplicaciones no son revisados frecuentemente
			Acceso a la BD desde otras aplicaciones
			Virus informáticos
			Realización de copias no autorizadas de la Base de Datos.

			Modificación no autorizada de BD
		Falta de espacio de almacenamiento	Incremento de transacciones
			No existe un procedimiento de mantenimiento de la BD.
			Incremento de espacio por virus.
5	Respaldo de base de datos	Se detienen los procesos de la empresa, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.	Falla en los dispositivos de almacenamiento
			Falta de un lugar adecuado para protección de copias de respaldo
			Errores en el proceso de generación de respaldos
			No lleva registro de la generación de respaldos
6	Personal de área de TI	Pérdida de información debido a fuga de talentos que genera retraso en actividades o paralización de procesos	Inadecuada segregación de funciones
			No existe un plan de capacitación adecuado
			Indisponibilidad del personal (enfermedad, accidente, otros actos que impiden al personal realizar sus actividades)
		Modificación, divulgación y destrucción de la información	Abuso de privilegios de accesos
			Falta de control y seguimiento de accesos
			Falta de acuerdos de confidencialidad
			Impulsos mezquinos que hacen que el personal actúe de manera anormal en el desarrollo de sus labores
			Falta de procedimiento de mantenimiento de usuarios
7	Equipos de cómputo terminales en ventanilla y analista de créditos	Pérdida de información sensible debido a fallas de equipos de cómputo que soportan las operaciones del negocio	Personal no capacitado para realizar actividades de mantenimiento de equipos de cómputo
			No se ha determinado la vida útil del equipo
			Incumplimiento del plan de mantenimiento de equipos.
			Fallas en sistema de alimentación eléctrica.
			Errores de configuración de los equipos
			Mal uso del equipo por parte del usuario
			Condición de ambientes inadecuadas

			No se tienen identificados los equipos críticos en caso de evacuación.
			El personal guarda información sensible en sus equipos y no las guarda en el servidor
8	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción.	No se realizan copias de seguridad
			Accesos no autorizados a la PC de Integración de Software
		Manipulación de código fuente que genera pérdida de información, multas y sanciones.	Accesibilidad a todo el código fuente sin restricción por parte del personal de Desarrollo (no se tiene restricción de acceso al personal de desarrollo).
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema
			No complejidad de contraseñas en el respaldo de código fuente
			Manipulación del código fuente que puede alterar el desarrollo normal de un proceso
9	Analistas de sistemas (responsables de la implementación de requerimientos)	Exceso de tiempo comprometido en cronograma de actividades para desarrollo de requerimientos	Personal de desarrollo (nuevo) con poco conocimiento en todos los Procesos de Negocio
			Falta de personal para cumplir con la sobrecarga de requerimientos a desarrollar.
		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web	Falta de monitoreo de envío y recepción de correos
			Acceso total a la Web
		Pérdida de recursos debido a Implementaciones no acordes a metodología y Estándares de desarrollo de Software	Plan de Inducción no adecuado
10	Respaldo de desarrollo y mantenimiento	No es posible revertir las adecuaciones de los sistemas.	No se trasladan copias de respaldo en sitios alternos

Fuente Propia

4.1.3. Fase 2 - Valoración de los escenarios de riesgos de Tecnologías de Información

4.1.3.1.Estimación del impacto de los escenarios de riesgo

Esta actividad permitió estimar el impacto que tendría cada escenario de riesgo identificado sobre el negocio, específicamente sobre los procesos de créditos y operaciones. La estimación de los impactos se realizó utilizando una escala de cinco (05) niveles, la cual se muestra a continuación:

Tabla 18 – *Escala de impacto de los escenarios de riesgo*

Nivel	Impacto	Descripción
1	Insignificante	Tiene un efecto nulo o muy pequeño en las operaciones de créditos y operaciones
2	Menor	Afecta parcialmente las operaciones de créditos y operaciones. Interrumpe servicios pero que no tienen incidencia directa en la relación con los clientes
3	Moderado	Operativamente es sostenible, pero dificulta o retrasa las operaciones de créditos y operaciones. Interrumpe parcialmente algunos servicios importantes que se brindan a los clientes
4	Mayor	Interrumpe la prestación de servicios críticos que se brinda a los clientes, debido a la caída significativa de las operaciones de créditos y operaciones Pérdida potencial de clientes
5	Catastrófico	Paraliza todas las operaciones de créditos y operaciones de la entidad

Fuente Propia

4.1.3.2.Estimación de la probabilidad de ocurrencia de los escenarios de riesgo

Consiste en estimar la probabilidad de que ocurran cada uno de los escenarios de riesgo identificados, en base al historial de incidencias ocurridas en la entidad. La estimación de probabilidades de ocurrencia se realizó utilizando una escala de cinco (05) niveles

Tabla 19 – *Niveles de probabilidad de ocurrencia de una amenaza*

Nivel	Probabilidad	Descripción
1	Raro	No se registra en los últimos 5 años
2	Improbable	Se podría presentar una vez cada 5 años
3	Posible	Se podría presentar una vez al año
4	Probable	Se podría presentar una vez cada mes
5	Casi seguro	Se podría presentar varias veces en el mes

Fuente Propia

4.1.3.3.Cálculo de los niveles de exposición a los riesgos

Para calcular el nivel de exposición al riesgo de cada escenario identificado para cada activo de TI, se utilizó la siguiente relación:

Nivel de Riesgo (NR) = Impacto x Probabilidad de ocurrencia

El producto de esta relación se ubicará en el siguiente mapa de calor:

Tabla 20 – *Mapa de calor de nivel de exposición al riesgo*

Impacto en los procesos	Probabilidad de ocurrencia				
	Raro	**Improbable**	**Posible**	**Probable**	**Casi seguro**
Catastrófico	Bajo	Medio	Alto	Muy alto	Muy alto
Mayor	Bajo	Bajo	Medio	Alto	Muy alto
Moderado	Muy bajo	Bajo	Medio	Medio	Alto
Mínimo	Muy bajo	Bajo	Bajo	Bajo	Medio
Insignificante	Muy bajo	Muy bajo	Muy bajo	Bajo	Bajo

Fuente Propia

- Muy Bajo: Cuando la deficiencia del control actual no ocasiona una degradación importante de los sistemas o no ocasiona una pérdida económica importante o no se impide el logro de los objetivos de seguridad.
- Bajo: Cuando la deficiencia del control actual genera daños menores a la Entidad Financiera, es decir genera pérdidas, pero no significativas.
- Medio: Cuando la deficiencia del control actual podría resultar en una pérdida significativa, pero dentro de rangos aceptables para la entidad.
- Alto: Cuando la deficiencia del control actual podría resultar en una pérdida significativa, del tipo económico, operativo y de seguridad
- Muy Alto: Cuando la deficiencia del control actual expone a la entidad a una pérdida material y/o económica o a una sanción legal no aceptable para la entidad.

Tabla 21 – *Estimación del impacto y probabilidad de ocurrencia de cada amenazas y cálculo de su nivel de exposición al riesgo (NR)*

N°	Activo	Amenaza	Riesgos	Impacto estimado en los procesos		Probabilidad de que la amenaza explote la vulnerabilidad		Nivel de Exposición al Riesgo (NR)		
				Nivel	**Categoría**	**Nivel**	**Categoría**	**Id Riesgo**	**Nivel**	**Categoría**
1	Servidor principal de dominio	No se puede acceder a los servicios de red y esto paraliza los procesos del negocio	Falta de personal especializado, para dar mantenimiento al servidor de dominio	3	Moderado	2	Improbable	R1	2	Bajo
			Falla en los componentes físicos	4	Mayor	3	Posible	R2	3	Medio
			Falla en el sistema operativo, falta de actualización de parches	5	Catastrófico	4	Probable	R3	5	Muy alto
			No se cuenta con un plan de mantenimiento de los servidores	3	Moderado	2	Improbable	R4	2	Bajo
			Ataque de algún virus	2	Menor	2	Improbable	R5	2	Bajo
2	Servidor principal de base de datos y aplicaciones	Pérdida de recursos, multas y sanciones debido a modificación de información sensible relacionada con datos de los clientes	El administrador tiene acceso total a la base de datos y realiza modificaciones	4	Mayor	4	Probable	R6	4	Alto
			Deficiente normalización en el diseño de base datos	2	Menor	3	Posible	R7	2	Bajo
			Los usuarios acceden al servidor de base de datos por canales no autorizados	5	Catastrófico	4	Probable	R8	5	Muy alto
3	Red LAN		Falla de la línea principal de comunicación	5	Catastrófico	3	Posible	R9	4	Alto

		Se detienen los servicios de comunicación	Falla de la red de comunicaciones con otras agencias	4	Mayor	4	Probable	R10	4	Alto
			Falla eléctrica que genera la interrupción de los procesos y servicios	4	Mayor	3	Posible	R11	3	Medio
			No cuenta con servidor de firewall a nivel de hardware	3	Moderado	2	Improbable	R12	2	Bajo
4	Bases de Datos	Pérdida de información sensible de la empresa debido a accesos inadecuados a las bases de datos que generan multas y sanciones.	Falta de un procedimiento para la asignación de perfiles para acceso a la BD	4	Mayor	3	Posible	R13	3	Medio
			Existencia de contraseñas no adecuados para usuarios locales y de red	3	Moderado	2	Improbable	R14	2	Bajo
			Privilegios para usuarios de acceso a aplicaciones no son revisados frecuentemente	3	Moderado	2	Improbable	R15	2	Bajo
			Acceso a la BD desde otras aplicaciones	4	Mayor	3	Posible	R16	3	Medio
			Virus informáticos	3	Moderado	3	Posible	R17	3	Medio
			Realización de copias no autorizadas de la Base de Datos.	4	Mayor	3	Posible	R18	3	Medio
			Modificación no autorizada de BD	5	Catastrófico	4	Probable	R19	5	Muy alto
		Falta de espacio de almacenamiento	Incremento de transacciones	3	Moderado	3	Posible	R20	3	Medio
			No existe un procedimiento de mantenimiento de la BD.	3	Moderado	2	Improbable	R21	2	Bajo
			Incremento de espacio por virus.	3	Moderado	1	Raro	R22	1	Muy bajo
5	Respaldo de	Se detienen los procesos de la	Falla en los dispositivos de almacenamiento	4	Mayor	3	Posible	R23	3	Medio

	base de datos	empresa, debido a pérdida de información sensible por falta de protección en los dispositivos de almacenamiento.	Falta de un lugar adecuado para protección de copias de respaldo	2	Menor	2	Improbable	R24	2	Bajo
			Errores en el proceso de generación de respaldos	5	Catastrófico	4	Probable	R25	5	Muy alto
			No lleva registro de la generación de respaldos	3	Moderado	3	Posible	R26	3	Medio
6	Personal de área de TI	Pérdida de información debido a fuga de talentos que genera retraso en actividades o paralización de procesos	Inadecuada segregación de funciones	3	Moderado	2	Improbable	R27	2	Bajo
			No existe un plan de capacitación adecuado	2	Menor	3	Posible	R28	2	Bajo
			Indisponibilidad del personal (enfermedad, accidente, otros actos que impiden al personal realizar sus actividades)	2	Menor	3	Posible	R29	2	Bajo
		Modificación, divulgación y destrucción de la información	Abuso de privilegios de accesos	4	Mayor	3	Posible	R30	3	Medio
			Falta de control y seguimiento de accesos	5	Catastrófico	3	Posible	R31	4	Alto
			Falta de acuerdos de confidencialidad	4	Mayor	3	Posible	R32	3	Medio
			Impulsos mezquinos que hacen que el personal actúe de manera anormal en el desarrollo de sus labores	3	Moderado	3	Posible	R33	3	Medio
			Falta de procedimiento de mantenimiento de usuarios	3	Moderado	2	Improbable	R34	2	Bajo
7	Equipos de cómputo terminal	Pérdida de información sensible debido a fallas de equipos de cómputo	Personal no capacitado para realizar actividades de mantenimiento de equipos de cómputo	4	Mayor	2	Improbable	R35	2	Bajo

	es en ventanilla y analistas de créditos	que soportan las operaciones del negocio	No se ha determinado la vida útil del equipo	2	Menor	2	Improbable	R36	2	Bajo
			Incumplimiento del plan de mantenimiento de equipos.	2	Menor	3	Posible	R37	2	Bajo
			Fallas en sistema de alimentación eléctrica.	3	Moderado	3	Posible	R38	3	Medio
			Errores de configuración de los equipos	2	Menor	3	Posible	R39	2	Bajo
			Mal uso del equipo por parte del usuario	3	Moderado	4	Probable	R40	3	Medio
			Condición de ambientes inadecuadas	2	Menor	3	Posible	R41	2	Bajo
			No se tienen identificados los equipos críticos en caso de evacuación.	3	Moderado	2	Improbable	R42	2	Bajo
			El personal guarda información sensible en sus equipos y no las guarda en el servidor	4	Mayor	4	Probable	R43	4	Alto
8	Código fuente de las aplicaciones	Pérdida de la correlación del código fuente de la versión existente en producción.	No se realizan copias de seguridad	4	Mayor	2	Improbable	R44	2	Bajo
			Accesos no autorizados a la PC de Integración de Software	4	Mayor	2	Improbable	R45	2	Bajo
		Manipulación de código fuente que genera pérdida de información, multas y sanciones.	Acceso al código fuente sin restricción por parte del personal de desarrollo	4	Mayor	3	Posible	R46	3	Medio
			No se realiza una revisión minuciosa de los controles de cambios entregado por el analista de sistema	4	Mayor	3	Posible	R47	3	Medio

			No complejidad de contraseñas en el respaldo de código fuente	3	Moderado	3	Posible	R48	3	Medio
			Manipulación del código fuente que puede alterar el desarrollo normal de un proceso	5	Catastrófico	4	Probable	R49	5	Muy alto
9	Analistas de sistemas (responsables de la implementación de requerimientos)	Exceso de tiempo comprometido en cronograma de actividades para desarrollo de requerimientos	Personal de desarrollo (nuevo) con poco conocimiento en todos los Procesos de Negocio	2	Menor	4	Probable	R50	2	Bajo
			Falta de personal para cumplir con la sobrecarga de requerimientos a desarrollar.	3	Moderado	3	Posible	R51	3	Medio
		Pérdida de información sensible debido a fuga a través de correos electrónicos y/o páginas web	Falta de monitoreo de envío y recepción de correos	3	Moderado	2	Improbable	R52	2	Bajo
			Acceso total a la Web	4	Mayor	3	Posible	R53	3	Medio
		Pérdida de recursos debido a Implementaciones no acordes a metodología y Estándares de desarrollo de Software	Plan de Inducción no adecuado	2	Menor	2	Improbable	R54	2	Bajo
10	Respaldo de desarrollo y	No es posible revertir las adecuaciones de los sistemas.	No se trasladan copias de respaldo en sitios alternos	5	Catastrófico	3	Posible	R55	4	Alto

manteni miento	

Fuente Propia

4.1.3.4. Determinación del apetito y tolerancia al riesgo

- Los niveles de exposición al riesgo (NR) cuya valoración es “Muy Alta” o “Alta” son los niveles de riesgo que la entidad financiera define como NO ACEPTABLES, por tanto requiere urgente un tratamiento mediante controles y salvaguardas.
- El nivel de exposición al riesgo “Medio” se define como un nivel TOLERABLE, es decir, dependerá de la capacidad instalada que tenga la institución y el costo de implementación del control o salvaguarda requerida para el tratamiento del riesgo.
- Los niveles de exposición al riesgo “Bajo” o “Muy Bajo” se definen como ACEPTABLES.

4.2. Diseñar la propuesta de plan para reducir riesgos operativos de tecnologías de la información

4.2.1. Fase 3: Tratamiento de los riesgos

4.2.1.1. Definición de las políticas de seguridad

Para ISO/IEC 27001, un Sistema de Gestión de la Seguridad de la Información debe estar organizado de acuerdo a Políticas de seguridad, Normas, Procedimientos, Controles e Indicadores. En esta investigación sólo se plantean políticas de seguridad, más no se consideran las normativas y procedimientos.

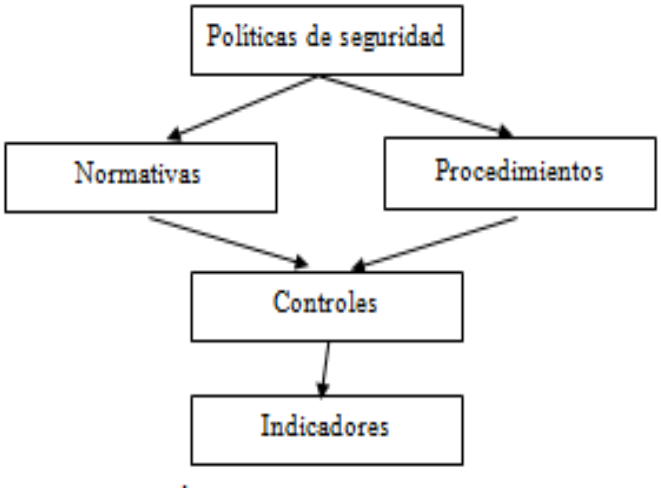


Figura 18: Estructura de un Sistema de Gestión de la Seguridad de la Información

Fuente: Adaptado de la ISO/IEC 27001

La implementación de controles para reducir los niveles de exposición al riesgo NO ACEPTABLES, deben ser gestionados mediante políticas de seguridad, como lo establece la norma ISO/IEC 27001.

4.2.1.2.Identificación de los controles o salvaguardas de seguridad

Para la identificación de los controles o salvaguardas de seguridad necesarias para la mitigación de los riesgos en niveles no aceptables, y de acuerdo a las políticas de seguridad propuestas, se utilizó el catálogo de controles propuesto por la ISO/IEC 27002. Se realizó una declaratoria de aplicabilidad para determinar cuáles de los 114 controles propuesto por la ISO/IEC 27002 son aplicables a la entidad.

Tabla 22 – *Listado de control de seguridad*

Nivel de Riesgo Intrínseco (NRI)			**Controles**	
ID riesgo	**Nivel**	**Categoría**	**ID Control**	**Descripción**
R1	2	Bajo	C1	Mantenimiento correctivo por parte del fabricante
R2	3	Medio	C2	Servicio de mantenimiento por parte del fabricante
			C3	Sala de servidores con controles ambientales
R3	5	Muy alto	C4	Personal capacitado en administración de Windows Server y actualizaciones
R4	2	Bajo	C5	Incluir en presupuesto el plan para mantenimiento a los servidores
R5	2	Bajo	C6	Se cuenta con software antivirus instalado en toda la red y con actualizaciones automáticas
			C7	Se cuenta con copias de seguridad de la BD
			C8	Se cuenta con un servidor de respaldo
			C9	Se tiene implementado un centro de cómputo alterno (CCA), el cual permite generar copias de respaldo en línea
R6	4	Alto	C10	El Oficial de Seguridad de la Información monitorea de manera continua las pistas de auditoría al administrador de la BD
R7	2	Bajo	C11	En el proceso de desarrollo se cuenta con una fase de pruebas y revisión, donde se analizan el diseño de las tablas y de las modificaciones
			C12	La Jefe de Producción, realiza un análisis de los ejecutables y códigos fuentes que pasa a la División de desarrollo
R8	5	Muy alto	C13	Se han establecido restricciones de acceso mediante la asignación de perfiles de usuario (no pueden instalar aplicaciones), se desactivan herramientas adicionales que permiten acceder a la base de datos
			C14	La contraseña de acceso a la base de datos tiene un nivel de complejidad, distinta a las contraseñas que manejan los usuarios locales
			C15	Los perfiles de usuarios que acceden a la base de datos tienen accesos restringidos

R9	4	Alto	C16	Se cuenta con línea de contingencia para comunicaciones
			C17	Reporte inmediato de averías al proveedor
R10	4	Alto	C18	Reporte inmediato de averías al proveedor
R11	4	Alto	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos ante una posible interrupción del corte de energía eléctrica
			C20	Se realizan pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento
			C21	Se cuenta con un plan de mantenimiento al sistema eléctrico
R12	2	Bajo	C22	Se cuenta con firewall a nivel de software
R13	4	Alto	C23	Reglamento de administración de usuarios al SIIF, en el que incluye las opciones para la asignación de perfiles por usuarios
R14	2	Bajo	C24	Se permite la creación de contraseñas con un nivel de seguridad y complejidad, teniendo en cuenta caracteres numéricos y alfanuméricos.
R15	2	Bajo	C25	Incluir en el plan de trabajo de la oficialía de seguridad
R16	4	Alto	C26	Se ha deshabilitado acceso a Ms. Excel en todas las máquinas
			C27	Acceso a la BD protegida por una contraseña que es de conocimiento del jefe de área de producción y soporte
R17	3	Medio	C28	Se realiza la actualización del antivirus en línea
R18	3	Medio	C29	BD está protegida con clave y sólo es de conocimiento de personal autorizado
			C30	No se tiene carpetas compartidas de la BD
R19	5	Muy alto	C31	Se efectúa una revisión general de los script que envía la sección desarrollo para el pase a producción
R20	3	Medio	C32	El Jefe de Producción y Soporte supervisa de manera manual la disponibilidad de la capacidad del disco del servidor, a fin de que exista espacio suficiente para la BD
R21	2	Bajo	C33	Se realiza un mantenimiento de la BD, pero no está documentado
R22	1	Muy bajo	C34	Se cuenta con un antivirus que se actualiza en línea
			C35	Los puertos de control de acceso al servidor se encuentran bloqueados
R23	4	Alto	C36	Se cuenta con políticas y procedimientos de generación de respaldos
			C37	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno
			C38	Se lleva un control trimestral del estado de almacenamiento de los medios de respaldo
			C39	Se realiza un monitoreo del procedimiento de respaldo de las copias de seguridad

			C40	Se cuenta con un centro de cómputo alterno que replica información de la BD de manera automática; asimismo se cuenta con un servidor de base de datos de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario
R24	2	Bajo	C41	Se realiza una verificación de estado de almacenamiento y resguardo de los medios de respaldo.
R25	5	Muy alto	C42	La herramienta que comprime la BD, realiza una verificación automática de los archivos comprimidos
			C43	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación
			C44	Se realiza la verificación periódica de las copias generadas
R26	3	Medio	C45	Se cuenta con un cuaderno de cargos en el cual se consigna el envío de las copias de respaldo por fechas de generación, responsable de envío y recepción
R27	2	Bajo	C46	Se cuenta con manual de organización y funciones en el que se tiene establecido las responsabilidades que debe cumplir el personal en la operativa diaria
R28	2	Bajo	C47	Existe un plan de capacitación presentado por el jefe de TI
R29	2	Bajo	C48	Se tiene personal de reemplazo, pero no está totalmente capacitado en las actividades diarias.
R30	4	Alto	C49	La asignación de privilegios va de acuerdo al manual de funciones
			C50	Se generan pistas de auditoria que son revisadas periódicamente
R31	4	Alto	C51	Se cuenta con un procedimiento para la revisión de usuarios del sistema de manera semestral, lo cual deberá ser verificado por personal de Recursos Humanos
R32	4	Alto	C52	Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos están previamente firmados
R33	3	Medio	C53	Al inicio de la relación laboral, se realizan evaluaciones psicológicos al personal y evaluación de historial
			C54	Se cuenta con políticas de seguridad y se cuenta con reglamentos internos que establecen sanciones
R34	2	Bajo	C55	Se cuenta con reglamento de altas, bajas y modificación de usuarios.
R35	2	Bajo	C56	Se cuenta con un proceso de evaluación del personal nuevo por parte de Recursos Humanos
			C57	Se cuenta con una lista de técnicos que permiten realizar el mantenimiento de los equipos
			C58	La empresa proveedora, brinda servicios de mantenimiento a los equipos arrendados

R36	2	Bajo	C59	Los equipos de cómputo se han arrendado a un proveedor por un periodo de tres años; asimismo se ha firmado un acuerdo un acuerdo de niveles de servicio con el arrendador
R37	2	Bajo	C60	Se realiza un seguimiento al cumplimiento del plan por parte de la persona responsable de Continuidad del Negocio y el seguimiento es reportado en el informe de Continuidad de Negocio de manera bimensual
R38	3	Medio	C61	Existe un plan de mantenimiento del sistema eléctrico, este mantenimiento se realiza de manera semestral
			C62	Se cuenta con una red eléctrica estabilizada
			C63	Las PCs de misión crítica están conectadas a UPS
			C64	Se realizan pruebas periódicas del sistema de respaldo eléctrico (UPS, Grupo electrógeno y motor)
			C65	Se realiza mantenimiento programado a los equipos eléctricos
R39	2	Bajo	C66	Se cuenta con personal capacitado para realizar las configuraciones de los equipos.
R40	3	Medio	C67	En el MOF indica: Es responsabilidad de los usuarios, que el buen uso y conservación de los bienes o activos que la Entidad asigna al trabajador para el cumplimiento de sus funciones.
R41	2	Bajo	C68	Existe un ambiente para la ubicación de los equipos, así mismo estos ambientes cuentan con ambientes de ventilación.
R42	2	Bajo	C69	Se tienen identificados los equipos críticos del área de TI y centro de cómputo Principal
			C70	Se cuenta con políticas para la clasificación de la información
R43	4	Alto	C71	Política de escritorios y pantallas limpias
R44	2	Bajo	C72	Se realizan copias de seguridad de manera semanal, así mismo se lleva un control de los backups del código fuente generado por el personal de desarrollo
			C73	Se mantiene tres copias de respaldo
R45	2	Bajo	C74	Seguridad de acceso local de usuario
			C75	La pc de integración de desarrollo está separada de la red de producción
			C76	Se generar copias de seguridad del código fuentes// existe registro de versiones
R46	4	Alto	C77	El código fuente es clasificada como información restringida y controlada por el Jefe de TI
R47	4	Alto	C78	Se mantiene un documento de control de cambios, donde se detalla todo lo que se modifica a nivel de código fuente , a nivel de base de datos y a nivel de dato
			C79	Se realiza un control de calidad de todos los puntos integrados de los analistas de sistemas
			C80	Control de calidad por parte de la División de producción antes de su implantación

R48	3	Medio	C81	Se ha asignado un complejidad en la contraseñas teniendo en caracteres y números, la contraseña cambia en cada respaldo
R49	5	Muy alto	C82	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario
			C83	El especialista en sistemas de Información puede detectar cambios no programados
			C84	Existe una fase de prueba en desarrollo y certificación antes del pase a producción
R50	2	Bajo	C85	Al ingresar cada analista de sistemas recibe inducción sobre los procesos del negocio y de los procesos automatizados de negocio. Asignación de tareas de manera gradual. Asignación de requerimientos teniendo en cuenta el nivel de experiencia en el desarrollo del proceso del negocio.
R51	3	Medio	C86	Se priorizan los requerimientos de implementación de procesos más importantes
R52	2	Bajo	C87	Existe reglamento específico de acceso a Internet
R53	4	Alto	C88	Existe restricción de acceso a Internet según niveles de acceso de usuarios
R54	3	Medio	C89	Instalación de Antivirus
R55	4	Alto	C90	Se mantiene un inventario de los backups generados, asi mismo se generan tres copias de respaldo que son enviados al sitio alterno

Fuente Propia

4.2.1.3.Definición de la estrategia de implementación de controles/salvaguardas

Define la estrategia de implementación del control según ISO/IEC 27005, se plantea las siguientes estrategias:

- Aceptar el riesgo: cuando los niveles de exposición al riesgo están dentro de los rangos de aceptabilidad
- Elegir controles para mitigar los riesgos: cuando los niveles de exposición al riesgo están en los rangos de tolerancia y/o No aceptabilidad; y además se cuenta con los recursos humanos, tecnológicos y económicos para su implementación
- Transferir el riesgo a terceros: cuando los niveles de exposición al riesgo están en los rangos de tolerancia y/o No aceptabilidad; y además NO se cuenta con los recursos humanos, tecnológicos para su implementación, pero si con la economía necesaria para contratar a un tercero especializado
- Evitar aumento del riesgo: cuando los niveles de exposición al riesgo están en los rangos de tolerancia y/o No aceptabilidad; pero NO se cuenta con los recursos humanos, tecnológicos y económicos para su implementación.

Tabla 23 – *Listado de estrategias de control*

Nivel de Riesgo Intrínseco (NRI)			Control		Estrategia de implementación
ID riesgo	**Nivel**	**Categoría**	**ID Control**	**Descripción**	
R1	2	Bajo	C1	Mantenimiento correctivo por parte del fabricante	Evitar aumento del riesgo
R2	3	Medio	C2	Servicio de mantenimiento por parte del fabricante	Evitar aumento del riesgo
			C3	Sala de servidores con controles ambientales	Evitar aumento del riesgo
R3	5	Muy alto	C4	Personal capacitado en administración de Windows Server y actualizaciones	Transferencia del riesgo a terceros
R4	2	Bajo	C5	Incluir en presupuesto el plan para mantenimiento a los servidores	Evitar aumento del riesgo
R5	2	Bajo	C6	Se cuenta con software antivirus instalado en toda la red y con actualizaciones automáticas	Evitar aumento del riesgo
			C7	Se cuenta con copias de seguridad de la BD	Evitar aumento del riesgo
			C8	Se cuenta con un servidor de respaldo	Evitar aumento del riesgo
			C9	Se tiene implementado un centro de cómputo alterno (CCA), el cual permite generar copias de respaldo en línea	Evitar aumento del riesgo
R6	4	Alto	C10	El Oficial de Seguridad de la Información monitorea de manera continua las pistas de auditoría al administrador de la BD	Elección de controles
R7	2	Bajo	C11	En el proceso de desarrollo se cuenta con una fase de pruebas y revisión, donde se analizan el diseño de las tablas y de las modificaciones	Evitar aumento del riesgo
			C12	La Jefe de Producción, realiza un análisis de los ejecutables y códigos fuentes que pasa a la División de desarrollo	Evitar aumento del riesgo
R8	5	Muy alto	C13	Se han establecido restricciones de acceso mediante la asignación de perfiles de usuario (no pueden instalar aplicaciones), se desactivan herramientas adicionales que permiten acceder a la base de datos	Elección de controles
			C14	La contraseña de acceso a la base de datos tiene un nivel de complejidad, distinta a las contraseñas que manejan los usuarios locales	Elección de controles
			C15	Los perfiles de usuarios que acceden a la base de datos tienen accesos restringidos	Elección de controles
R9	4	Alto	C16	Se cuenta con línea de contingencia para comunicaciones	Transferencia del riesgo a terceros
			C17	Reporte inmediato de averías al proveedor	Transferencia del riesgo a terceros
R10	4	Alto	C18	Reporte inmediato de averías al proveedor	Transferencia del riesgo a terceros
R11	4	Alto	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos ante una posible interrupción del corte de energía eléctrica	Elección de controles

			C20	Se realizan pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento	Elección de controles
			C21	Se cuenta con un plan de mantenimiento al sistema eléctrico	Elección de controles
R12	2	Bajo	C22	Se cuenta con firewall a nivel de software	Evitar aumento del riesgo
R13	4	Alto	C23	Reglamento de administración de usuarios al SIIF, en el que incluye las opciones para la asignación de perfiles por usuarios	Elección de controles
R14	2	Bajo	C24	Se permite la creación de contraseñas con un nivel de seguridad y complejidad, teniendo en cuenta caracteres numéricos y alfanuméricos.	Evitar aumento del riesgo
R15	2	Bajo	C25	Incluir en el plan de trabajo de la oficialía de seguridad	Evitar aumento del riesgo
R16	4	Alto	C26	Se ha deshabilitado acceso a Ms. Excel en todas las máquinas	Elección de controles
			C27	Acceso a la BD protegida por una contraseña que es de conocimiento del jefe de área de producción y soporte	Elección de controles
R17	3	Medio	C28	Se realiza la actualización del antivirus en línea	Evitar aumento del riesgo
R18	3	Medio	C29	BD está protegida con clave y sólo es de conocimiento de personal autorizado	Evitar aumento del riesgo
			C30	No se tiene carpetas compartidas de la BD	Elección de controles
R19	5	Muy alto	C31	Se efectúa una revisión general de los script que envía la sección desarrollo para el pase a producción	Elección de controles
R20	3	Medio	C32	El Jefe de Producción y Soporte supervisa de manera manual la disponibilidad de la capacidad del disco del servidor, a fin de que exista espacio suficiente para la BD	Evitar aumento del riesgo
R21	2	Bajo	C33	Se realiza un mantenimiento de la BD, pero no está documentado	Evitar aumento del riesgo
R22	1	Muy bajo	C34	Se cuenta con un antivirus que se actualiza en línea	Elección de controles
			C35	Los puertos de control de acceso al servidor se encuentran bloqueados	Elección de controles
R23	4	Alto	C36	Se cuenta con políticas y procedimientos de generación de respaldos	Elección de controles
			C37	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno	Elección de controles
			C38	Se lleva un control trimestral del estado de almacenamiento de los medios de respaldo	Elección de controles
			C39	Se realiza un monitoreo del procedimiento de respaldo de las copias de seguridad	Elección de controles
			C40	Se cuenta con un centro de cómputo alterno que replica información de la BD de manera automática; asimismo se cuenta con un servidor de base de datos de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario	Elección de controles
R24	2	Bajo	C41	Se realiza una verificación de estado de almacenamiento y resguardo de los medios de respaldo.	Evitar aumento del riesgo

R25	5	Muy alto	C42	La herramienta que comprime la BD, realiza una verificación automática de los archivos comprimidos	Elección de controles
			C43	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación	Elección de controles
			C44	Se realiza la verificación periódica de las copias generadas	Elección de controles
R26	3	Medio	C45	Se cuenta con un cuaderno de cargos en el cual se consigna el envío de las copias de respaldo por fechas de generación, responsable de envío y recepción	Evitar aumento del riesgo
R27	2	Bajo	C46	Se cuenta con manual de organización y funciones en el que se tiene establecido las responsabilidades que debe cumplir el personal en la operativa diaria	Evitar aumento del riesgo
R28	2	Bajo	C47	Existe un plan de capacitación presentado por el jefe de TI	Evitar aumento del riesgo
R29	2	Bajo	C48	Se tiene personal de reemplazo, pero no está totalmente capacitado en las actividades diarias.	Evitar aumento del riesgo
R30	4	Alto	C49	La asignación de privilegios va de acuerdo al manual de funciones	Elección de controles
			C50	Se generan pistas de auditoria que son revisadas periódicamente	Elección de controles
R31	4	Alto	C51	Se cuenta con un procedimiento para la revisión de usuarios del sistema de manera semestral, lo cual deberá ser verificado por personal de Recursos Humanos	Elección de controles
R32	4	Alto	C52	Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos están previamente firmados	Elección de controles
R33	3	Medio	C53	Al inicio de la relación laboral, se realizan evaluaciones psicológicos al personal y evaluación de historial	Evitar aumento del riesgo
			C54	Se cuenta con políticas de seguridad y se cuenta con reglamentos internos que establecen sanciones	Evitar aumento del riesgo
R34	2	Bajo	C55	Se cuenta con reglamento de altas, bajas y modificación de usuarios.	Evitar aumento del riesgo
R35	2	Bajo	C56	Se cuenta con un proceso de evaluación del personal nuevo por parte de Recursos Humanos	Evitar aumento del riesgo
			C57	Se cuenta con una lista de técnicos que permiten realizar el mantenimiento de los equipos	Evitar aumento del riesgo
			C58	La empresa proveedora, brinda servicios de mantenimiento a los equipos arrendados	Evitar aumento del riesgo
R36	2	Bajo	C59	Los equipos de cómputo se han arrendado a un proveedor por un periodo de tres años; asimismo se ha firmado un acuerdo un acuerdo de niveles de servicio con el arrendador	Evitar aumento del riesgo
R37	2	Bajo	C60	Se realiza un seguimiento al cumplimiento del plan por parte de la persona responsable de Continuidad del Negocio y el seguimiento es reportado en el informe de Continuidad de Negocio de manera bimensual	Evitar aumento del riesgo
R38	3	Medio	C61	Existe un plan de mantenimiento del sistema eléctrico, este mantenimiento se realiza de manera semestral	Evitar aumento del riesgo
			C62	Se cuenta con una red eléctrica estabilizada	Evitar aumento del riesgo

			C63	Las PCs de misión crítica están conectadas a UPS	Evitar aumento del riesgo
			C64	Se realizan pruebas periódicas del sistema de respaldo eléctrico (UPS, Grupo electrógeno y motor)	Evitar aumento del riesgo
			C65	Se realiza mantenimiento programado a los equipos eléctricos	Evitar aumento del riesgo
R39	2	Bajo	C66	Se cuenta con personal capacitado para realizar las configuraciones de los equipos.	Evitar aumento del riesgo
R40	3	Medio	C67	En el MOF indica: Es responsabilidad de los usuarios, que el buen uso y conservación de los bienes o activos que la Entidad asigna al trabajador para el cumplimiento de sus funciones.	Evitar aumento del riesgo
R41	2	Bajo	C68	Existe un ambiente para la ubicación de los equipos, así mismo estos ambientes cuentan con ambientes de ventilación.	Evitar aumento del riesgo
R42	2	Bajo	C69	Se tienen identificados los equipos críticos del área de TI y centro de cómputo Principal	Evitar aumento del riesgo
			C70	Se cuenta con políticas para la clasificación de la información	Evitar aumento del riesgo
R43	4	Alto	C71	Política de escritorios y pantallas limpias	Elección de controles
R44	2	Bajo	C72	Se realizan copias de seguridad de manera semanal, así mismo se lleva un control de los backups del código fuente generado por el personal de desarrollo	Evitar aumento del riesgo
			C73	Se mantiene tres copias de respaldo	Evitar aumento del riesgo
R45	2	Bajo	C74	Seguridad de acceso local de usuario	Evitar aumento del riesgo
			C75	La pc de integración de desarrollo está separada de la red de producción	Evitar aumento del riesgo
			C76	Se generar copias de seguridad del código fuentes// existe registro de versiones	Evitar aumento del riesgo
R46	4	Alto	C77	El código fuente es clasificada como información restringida y controlada por el Jefe de TI	Elección de controles
R47	4	Alto	C78	Se mantiene un documento de control de cambios, donde se detalla todo lo que se modifica a nivel de código fuente , a nivel de base de datos y a nivel de dato	Elección de controles
			C79	Se realiza un control de calidad de todos los puntos integrados de los analistas de sistemas	Elección de controles
			C80	Control de calidad por parte de la División de producción antes de su implantación	Elección de controles
R48	3	Medio	C81	Se ha asignado un complejidad en la contraseñas teniendo en caracteres y números, la contraseña cambia en cada respaldo	Evitar aumento del riesgo
R49	5	Muy alto	C82	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario	Elección de controles
			C83	El especialista en sistemas de Información puede detectar cambios no programados	Elección de controles
			C84	Existe una fase de prueba en desarrollo y certificación antes del pase a producción	Elección de controles
R50	2	Bajo	C85	Al ingresar cada analista de sistemas recibe inducción sobre los procesos del negocio y de los procesos automatizados de negocio. Asignación de tareas de manera gradual. Asignación de requerimientos	Evitar aumento del riesgo

				teniendo en cuenta el nivel de experiencia en el desarrollo del proceso del negocio.	
R51	3	Medio	C86	Se priorizan los requerimientos de implementación de procesos más importantes	Evitar aumento del riesgo
R52	2	Bajo	C87	Existe reglamento específico de acceso a Internet	Evitar aumento del riesgo
R53	4	Alto	C88	Existe restricción de acceso a Internet según niveles de acceso de usuarios	Elección de controles
R54	3	Medio	C89	Instalación de Antivirus	Evitar aumento del riesgo
R55	4	Alto	C90	Se mantiene un inventario de los backups generados, asi mismo se generan tres copias de respaldo que son enviados al sitio alterno	Elección de controles

Fuente Propia

4.2.2. Fase 4: Seguimiento de la efectividad de los controles

4.2.2.1.Elaboración de planes de acción

Definir un plan de acción para asegurar la implementación de los controles que han sido clasificados de acuerdo a los dominios de seguridad de la información de la ISO/IEC 27001.

Tabla 24 – *Políticas de seguridad*

Organización de políticas de seguridad y políticas de aplicación
Objetivos
Desarrollar el plan director de políticas de seguridad y los procedimientos para su aplicación, basados en la normativa ISO.
Descripción
Se elaborará un plan de seguridad, que deberá ser aceptado y debidamente comunicado; donde se indicarán las responsabilidades definiendo un organigrama acorde a la estructura de la organización.
Indicadores
• Verificación de inicio de proyecto con firma de acuerdo con consultor externo. • Firma de aprobación del plan de seguridad al mes de inicio del proyecto. • Documentación de acuerdo de finalización y conformidad, firmado por la dirección y el comité de seguridad a fecha de fin del proyecto.
Amenazas a Mitigar
La definición de las políticas de seguridad, constituye paso fundamental y necesario para poder crear el SGSI en la entidad, al mitigar los riesgos de infringir los niveles de confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad

Fuente Propia

Tabla 25 – *Identificación y manejo de activos*

Identificación y manejo de activos
Objetivos
Asegurar una correcta clasificación de los activos por tipo, departamento y responsables dentro de la organización, tratando de detectar errores o dependencias erróneas para su pronta resolución. Actualizar información de los activos cuando sean modificados, creados o eliminados en el entorno organizativo.

Descripción
Definición de los diferentes activos por tipo, definiendo políticas de creación, modificación y eliminación. Control efectivo de todos los activos para el correcto funcionamiento de los mismos por parte de los usuarios.
Indicadores
• Realizar un registro de incidencias de uso de los activos cada mes. • Registro del estado de los activos y su clasificación cada trimestre, • Verificación de la asignación de responsables de cada activo cada semestral.
Amenazas a Mitigar
[A.11] Acceso no autorizado [A.18] Destrucción de información [A.6] Abuso de privilegios de acceso [E.1] Errores de los usuarios [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.2] Errores del Administrador [E.4] Errores de configuración

Fuente Propia

Tabla 26 – *Clasificación de la Información*

Clasificación de la Información
Objetivos
Asegurar la información clasificándola en base a las fuentes que la generan
Descripción
Proceder a organizar la información en la forma que se genera y utiliza dentro de la organización, atendiendo a su valor económico, requisitos legales y lo crítico de su contenido. Diseñar y asegurar las medidas necesarias de control y seguridad para el aseguramiento de toda la información de la organización.
Indicadores verificación
• Verificar la correcta clasificación de todos los activos de la organización cada año • Verificar las incidencias producidas sobre estos activos cada mes
Riesgos a Mitigar
[A.15] Modificación deliberada de la información [A.22] Manipulación de programas [A.4] Manipulación de la configuración [A.8] Difusión de software dañino [E.15] Alteración accidental de la información [E.18] Destrucción de información [E.19] Fugas de información [E.20] Vulnerabilidades de los programas [E.21] Errores de mantenimiento / actualización de programas [E.7] Deficiencias en la organización [E.8] Difusión de software dañino

Fuente Propia

Tabla 27 – *Formación y concienciación de seguridad*

Formación y concienciación de seguridad.
Objetivos
Definir y documentar un plan de capacitación para los empleados de la organización, adecuado a los distintos roles asignados.
Descripción
Cada empleado, según el puesto asignado, deberá ser instruido en las funciones y responsabilidades que tiene respecto a la seguridad de los activos de la organización.
Indicadores verificación
• Verificar las acciones formativas impartidas, evaluando su funcionalidad cada año
• Revisar la actualización de los planes dotándolo de las mejoras oportunas cada año
Riesgos a Mitigar
[A. 18] Destrucción de información [A. 19] Divulgación de información [A.3] Manipulación de los registros de actividad [A.30] Ingeniería social [A.4] Manipulación de la configuración [E.1] Errores de los usuarios [E.15] Alteración accidental de la información [E.19] Fugas de información [E.2] Errores del Administrador [E.3] Errores de monitorización [I.7] Condiciones inadecuadas de temperatura o humedad

Fuente Propia

Tabla 28 – *Cumplimiento de Requisitos Legales*

Cumplimiento de Requisitos Legales
Objetivos
Asegurar el correcto cumplimiento de los requisitos legales establecidos, adaptándose a la normativa ISO del momento.
Descripción
Adaptar todo el sistema organizativo y de producción a la normativa legal aplicable en materia de seguridad. Correspondiente para superar las auditorias oportunas.
Indicadores verificación
• Realizar la verificación del cumplimiento de los requisitos legales cada semestre. • Realizar una junta de auditoria para un registro de no conformidades/acciones correctivas sobre los requisitos legales establecidos cada año

Fuente Propia

4.2.2.2.Cálculo de los niveles de riesgo residual (NRR)

Finalmente, se determina el Nivel de Riesgo Residual (NRR) y la brecha de seguridad para lograr los niveles de riesgo aceptables por la entidad financiera. De acuerdo al apetito de riesgo definido, sólo se evaluaron los niveles de riesgo que han obtenido valores de “Alto” y “Muy alto”.

Tabla 29 – *Nivel de Riesgo Residual*

Nivel de Riesgo Intrínseco (NRI)		Control Implantado		Valorización del Nivel de riesgo Residual						Brecha de seguridad
ID riesgo	**Categoría**	**ID Control**	**Descripción**	**Nivel**	**Categoría**	**Nivel**	**Categoría**	**Nivel**	**Categoría**	
R3	Muy alto	C4	Personal capacitado en administración de Windows Server y actualizaciones	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R6	Alto	C10	El Oficial de Seguridad de la Información monitorea de manera continua las pistas de auditoría al administrador de la BD	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R8	Muy alto	C13	Se han establecido restricciones de acceso mediante la asignación de perfiles de usuario (no pueden instalar aplicaciones), se desactivan herramientas adicionales que permiten acceder a la base de datos	5	Catastrófico	2	Improbable	3	Medio	Riesgo aceptable
		C14	La contraseña de acceso a la base de datos tiene un nivel de complejidad, distinta a las contraseñas que manejan los usuarios locales							Riesgo aceptable
		C15	Los perfiles de usuarios que acceden a la base de datos tienen accesos restringidos							Riesgo aceptable
R9	Alto	C16	Se cuenta con línea de contingencia para comunicaciones	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
		C17	Reporte inmediato de averías al proveedor							Riesgo aceptable
R10	Alto	C18	Reporte inmediato de averías al proveedor	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R11	Alto	C19	Se cuenta con UPS y grupo electrógeno, el cual permite mantener la operatividad de los equipos ante una posible interrupción del corte de energía eléctrica	4	Mayor	4	Probable	4	Alto	Riesgo NO aceptable
		C20	Se realizan pruebas de operatividad de los equipos eléctricos, con el fin de evaluar su funcionamiento							Riesgo aceptable
		C21	Se cuenta con un plan de mantenimiento al sistema eléctrico							Riesgo aceptable
R13	Alto	C23	Reglamento de administración de usuarios al SIIF, en el que incluye las opciones para la asignación de perfiles por usuarios	4	Mayor	2	Improbable	2	Bajo	Riesgo aceptable
R16	Alto	C26	Se ha deshabilitado acceso a Ms. Excel en todas las máquinas	3	Moderado	3	Posible	3	Medio	Riesgo aceptable

		C27	Acceso a la BD protegida por una contraseña que es de conocimiento del jefe de área de producción y soporte							Riesgo aceptable
R19	Muy alto	C31	Se efectúa una revisión general de los script que envía la sección desarrollo para el pase a producción	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
R23	Alto	C36	Se cuenta con políticas y procedimientos de generación de respaldos	4	Mayor	2	Improbable	2	Bajo	Riesgo aceptable
		C37	Se generan dos copias de respaldo, la cual una de ellas se mantiene en el sitio alterno							Riesgo aceptable
		C38	Se lleva un control trimestral del estado de almacenamiento de los medios de respaldo							Riesgo aceptable
		C39	Se realiza un monitoreo del procedimiento de respaldo de las copias de seguridad							Riesgo aceptable
		C40	Se cuenta con un centro de cómputo alterno que replica información de la BD de manera automática; asimismo se cuenta con un servidor de base de datos de respaldo en el centro de cómputo principal (CCP) en caso de caída del servidor primario							Riesgo aceptable
R25	Muy alto	C42	La herramienta que comprime la BD, realiza una verificación automática de los archivos comprimidos	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
		C43	El programa que graba los archivos comprimidos en los medios, realiza una verificación después de la grabación							Riesgo aceptable
		C44	Se realiza la verificación periódica de las copias generadas							Riesgo aceptable
R30	Alto	C49	La asignación de privilegios va de acuerdo al manual de funciones	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
		C50	Se generan pistas de auditoria que son revisadas periódicamente							Riesgo aceptable
R31	Alto	C51	Se cuenta con un procedimiento para la revisión de usuarios del sistema de manera semestral, lo cual deberá ser verificado por personal de Recursos Humanos	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
R32	Alto	C52	Existen acuerdos de confidencialidad, los cuales han sido entregados al personal al momento de su ingreso a la institución y estos acuerdos están previamente firmados	3	Moderado	3	Posible	3	Medio	Riesgo aceptable
R43	Alto	C71	Política de escritorios y pantallas limpias	4	Mayor	2	Improbable	2	Bajo	Riesgo aceptable
R46	Alto	C77	El código fuente es clasificado como información restringida y controlada por el Jefe de TI	4	Mayor	3	Posible	3	Medio	Riesgo aceptable

R47	Alto	C78	Se mantiene un documento de control de cambios, donde se detalla todo lo que se modifica a nivel de código fuente , a nivel de base de datos y a nivel de dato	4	Mayor	3	Posible	3	Medio	Riesgo aceptable
		C79	Se realiza un control de calidad de todos los puntos integrados de los analistas de sistemas							Riesgo aceptable
		C80	Control de calidad por parte de la División de producción antes de su implantación							Riesgo aceptable
R49	Muy alto	C82	Las modificaciones solo tienen impacto en las aplicaciones, ya que en la integración solo se actualizan los objetos de acuerdo al requerimiento del usuario	4	Mayor	4	Probable	4	Alto	Riesgo NO aceptable
		C83	El especialista en sistemas de Información puede detectar cambios no programados							Riesgo aceptable
		C84	Existe una fase de prueba en desarrollo y certificación antes del pase a producción							Riesgo aceptable
R53	Alto	C88	Existe restricción de acceso a Internet según niveles de acceso de usuarios	3	Moderado	2	Improbable	2	Bajo	Riesgo aceptable
R55	Alto	C90	Se mantiene un inventario de los backups generados, así mismo se generan tres copias de respaldo que son enviados al sitio alterno	3	Moderado	2	Improbable	2	Bajo	Riesgo aceptable

Fuente Propia

4.3. Validar por juicio de expertos la propuesta de plan para reducir riesgos operativos de tecnologías de la información

Prueba de la Efectividad del Diseño: Tiene por objetivo probar la efectividad del diseño del modelo propuesto determinando si los controles de la entidad son operados como se fue prescrito por las personas que poseen la autoridad y competencias necesarias para desempeñar la gestión de la seguridad, el control y la gestión de riesgos y, si satisfacen los objetivos de control exigidos por la SBS para prevenir o detectar riesgos de Tecnologías de Información.

Tabla 30 –*Pesos para calificación de cada uno de los indicadores*

Peso	Significado	Color
1	CLAVE	Verde
2	RELEVANTE	Azul
3	ESTÁNDAR	Amarillo
4	IRRELEVANTE	Rojo

Fuente Propia

- **Clave:** El indicador evaluado del modelo propuesto es importante considerarlo en el Sistema de Gestión de Seguridad de la Información de la entidad, pues cumple con los requisitos exigidos en la normativa la SBS y se adecúa a las funciones de la entidad.
- **Relevante:** El indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Seguridad de la Información de la entidad, porque cumple con los requisitos exigidos en la normativa la SBS.
- **Estándar:** El indicador evaluado del modelo propuesto puede considerarse en el Sistema de Gestión de Seguridad de la Información de la entidad, con algunas modificaciones y mejoras para cumplir con los requisitos exigidos en la normativa de la SBS y para que se adecúe a las funciones de la entidad.
- **Irrelevante:** El **indicador** evaluado del modelo propuesto no cumple con los requisitos exigidos en la normativa la SBS por lo que no podría considerase en el Sistema de Gestión de Seguridad de la Información de la Entidad

Tabla 31 – *Evaluación de los factores y variables para probar la efectividad del diseño del modelo propuesto*

			Jefe de TI		Jefe Unidad Riesgos		Oficialía de Seguridad Información		Jefe Continuidad procesos		Auditor Interno		TOTALES	
Variable	**Factor Relevante (indicador)**		**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**	**SI/NO**	**Peso**
Efectividad del diseño del modelo de gestión de riesgos de TI en la estructuración de las actividades de análisis y tratamiento de riesgos	1	Se ha definición las categorías (disponibilidad, integridad y confidencialidad) de los riesgos de TI en un nivel aceptable	SI	2	SI	2	SI	1	SI	2	SI	2	100%	2
	2	El modelo se integra a la gestión del riesgo operativo de la entidad	SI	2	SI	2	SI	1	SI	2	NO	4	80%	2
	3	La estructura del modelo está diseñada para que los empleados relacionados con la gestión del riesgo operativo de TI puedan utilizarlo y comprenderlo en un nivel aceptable	SI	2	SI	3	SI	2	SI	3	SI	2	100%	2
Efectividad del diseño del modelo de gestión de riesgos de TI en el aseguramiento del gobierno de los riesgos de TI	4	El modelo contempla los requisitos exigidos por la SBS para la gestión de riesgos de TI	SI	2	SI	2	SI	2	SI	2	SI	3	100%	2
	5	Se ha establecido pautas para evaluar la magnitud de los riesgos de TI de modo coherente	SI	2	SI	3	SI	3	SI	2	NO	4	80%	3
	6	El modelo cuenta con indicadores suficientes para monitorizar la gestión de riesgos de TI	SI	3	SI	3	SI	2	SI	2	SI	2	100%	2
TOTAL (%)			100%		100%		100%		100%		67%		93%	2

Fuente. Propia

V. Discusión

Hipótesis

Una propuesta de un plan basada en la Metodología MagerIT reducirá los riesgos operativos de tecnologías de la información en la Caja Piura de la ciudad de Chiclayo.

Variables de Hipótesis

Independiente: Propuesta de un plan basada en la Metodología MagerIT.

Dependiente: Riesgos operativos de tecnologías de la información en la Caja Piura de la ciudad de Chiclayo.

Discusión

Con respecto a la efectividad del diseño del modelo propuesto se concluye que:

- Aceptan en un 93% de los factores considerados para el diseño de la metodología de análisis y tratamiento de riesgos de Tecnologías de Información propuesto, estableciendo que tiene un nivel de madurez de RELEVANTE, es decir, que la metodología de gestión de riesgos propuesta puede considerarse en el Sistema de Gestión de Seguridad de la Información de la Entidad, porque cumple con los requisitos exigidos en la normativa la SBS.
- Aceptan el 100% de los factores considerados para el desarrollo de las actividades iniciales de la gestión de la continuidad de procesos relacionados con Tecnologías de Información, estableciendo que tiene un nivel de madurez de RELEVANTE, es decir, que el modelo propuesto puede considerarse en el Sistema de Gestión de Seguridad de la Información de la Entidad, porque cumple con los requisitos exigidos en la normativa la SBS.

VI. Conclusiones

- Se ha analizado la situación actual de los riesgos operativos de tecnologías de información en la Caja Piura de la ciudad de Chiclayo teniendo como referencia las exigencias de la Superintendencia de Banca y Seguros (SBS), a través de sus normativas Resolución SBS 2116-2009 y la Circular G-105-2002 que establece los lineamientos para la Gestión de Riesgos de Tecnologías de Información de empresas de este sector. Se definieron cincuenta y cinco (55) riesgos operativos de tecnologías de información en la Caja Piura de Chiclayo, agrupados en diez (10) tipos de activo: Comunicaciones, Datos o documentos, Equipos informáticos, Información, Personal, Servicio y Equipamiento auxiliar.
- Se ha implementado un modelo de gestión de riesgos de Tecnologías de Información que incluye todos los elementos necesarios para la gestión de los riesgos de TI: (1) la identificación de los activos de Tecnologías de Información (2) la lista priorizada de activos, (3) la identificación de vulnerabilidades y amenazas, (4) la determinación del impacto si se concreta la amenaza y (5) la determinación de las probabilidades de ocurrencia de cada amenaza. El modelo de gestión de riesgos de Tecnologías de Información propuesto para la Caja Piura de la ciudad de Chiclayo, comprende dos etapas principales de la gestión de riesgos: (1) la identificación y evaluación de los riesgos de TI y (2) el tratamiento de los riesgos de TI que se ubican fuera de los rangos de tolerancia establecidos por la empresa.
- Se validó el modelo propuesto mediante el método Delphi, obteniendo la opinión de los responsables con autoridad en la gestión de los riesgos operacionales de Tecnologías de Información en la Caja Piura, desde la perspectiva de efectividad del diseño del modelo, quienes aceptan en un 93% los factores considerados para el diseño de la metodología de análisis y tratamiento de riesgos de Tecnologías de Información propuesto.

VII. Recomendaciones

- Dado que la evaluación de los riesgos es permanente se recomienda que el modelo de matriz de riesgos que se propone sea implementada en una aplicación informática, que permita actualizaciones más dinámicas, con posibilidades de generar indicadores/resultados gráficos y generación de escenarios.
- Se recomienda cumplir las acciones y directivas que se plantean en el Plan de Acción definido como parte del modelo de gestión de riesgos propuesto.
- Para lograr mejores resultados en la gestión de riesgos de Tecnologías de Información y en la continuidad de procesos, Caja Piura deberá tener en cuenta factores estratégicos como son el apoyo y compromiso de la Alta Dirección, la difusión y sensibilización permanente sobre control y seguridad de la información, la orientación para la formalización de procesos y la constante verificación para garantizar la disponibilidad, integridad y confidencialidad de información.
- Se recomienda designar responsabilidades que permitan, mediante la automatización de la propuesta metodológica, registrar de forma permanentemente la información necesaria para que la gestión del proceso pueda obtener la información del nivel de criticidad de sus procesos, porcentaje de desviación de riesgo de los activos o procesos, capital necesario a invertir en la protección de un activo o proceso, entre otra información relevante.

VIII. Referencias bibliográficas

Celi Arévalo, E. K. (2014). La gestión de riesgos de TI y la efectividad de los sistemas de seguridad de la información: Caso procesos críticos en las pequeñas entidades financieras de Lambayeque, Perú. Chiclayo, Lambayeque, Perú: Universidad Nacional Pedro Ruiz Gallo.

De Canales, F. (1994). *Metodolgía de la investigación. Manual, Organizacion Panamericana de la Salud.* Washington: Organización Panamericana de la Salud.

Galán Santisteban, J. R. (2015). Implementación del marco de trabajo ITIL para apoyar la gestión de los servicios del Centro de Sistemas de Información en la Gerencia Regional de Salud. Chiclayo, Lambayeque, Perú: Universidad Católica Santo Toribio de Mogrovejo.

Gaona Vásquez, K. d. (Octubre de 2013). Aplicación de Metodología MAGERIT para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa pesquera e industrial Bravito SA en la ciudad de Machala. Cuenca, Ecuador: Universidad Politécnica Salesiana.

García Porras, J. C. (2017). Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú. Lima, Perú: Universidad Peruana de Ciencias Aplicadas.

Guevara Chumán, J. G. (2015). Aplicación de la metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo. Lambayeque, Lambayeque, Perú: Universidad Nacional Pedro Ruiz Gallo.

Hernández Sampieri, R. (2014). Metodología de la investigación científica. México: Mc Graw Hill.

INDECOPI. (2007). *EDI. Tecnología de la información. Código de buenas.* Lima: Comisión de Reglamentos Técnicos y Comerciales - INDECOPI.

ISACA. (2009). *Marco de Riesgos de TI.* EEUU: ISACA.

Malhotra, N. K. (2004). *Investigación de mercados: un enfoque aplicado.* México: Prentice Hall.

Paredes, D. A. (17 de Febrero de 2016). Así está el Perú 2016: El uso de tecnología en la educación de nuestro país. (R. Noticias, Entrevistador)

Públicas, M. d. (2007). *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* España: Gobierno de España.

Santos Costas, J. (2012). *Seguridad y Alta Disponibilidad.* España: RAMA.

Sotelo, M., Torres, J., & Rivera, J. (2016). Un Proceso Práctico de Análisis de Riesgos de Activos de Información. *COMTEL 2012 - IV Congreso Internacional de Computación y Telecomunicaciones*, 121 - 127 p.

Valencia Duque, F. J. (2016). *Aseguramiento y auditoría de tecnologías de información orientado a riesgos.* Colombia: Universidad Nacional de Colombia.

Villena Aguilar, M. A. (2015). Planteamiento de un esquema de gestión de seguridad de información que puede ser empleado por una institución financiera en el Perú. Lima, Lima, Perú: Pontificia Universidad Católica del Perú.

Zamalloa Pacheco, W. M. (2018). Aplicación de ITIL V3.0 para mejorar la gestión de servicios en área de soporte en Protransporte. Lima, Lima, Perú: Universidad San Ignacio de Loyola.

IX. Anexos

ANEXO 01 – Modelo de opinión para la Metodología Propuesta

Dimensión	Indicador	SI/ NO	Madurez
Efectividad del diseño del modelo de gestión de riesgos de TI en la estructuración de las actividades de análisis y tratamiento de riesgos	Nivel de definición de las categorías (disponibilidad, integridad y confidencialidad) de los riesgos de TI		
	Nivel de integración del modelo a la gestión del riesgo operativo de la entidad		
	Nivel de utilización y comprensión del modelo por los empleados relacionados con la gestión del riesgo operativo de TI		
Efectividad del diseño del modelo de gestión de riesgos de TI en el aseguramiento del gobierno de los riesgos de TI	Nivel de cumplimiento de los requisitos exigidos por la SBS para la gestión de riesgos de TI		
	Nivel de coherencia del modelo para evaluar la magnitud de los riesgos de TI		
	Nivel de efectividad de los indicadores para el monitoreo de la gestión de riesgos de TI		

ANEXO 02 – Exigencias de la normativa resolución S.B.S. N° 2116 -2009

Exigencia de la norma SBS		ISO/IEC 27001:2007	ISO/IEC 17799:2005	MagerIT
Definiciones básicas (Art. N° 02)	Apetito de riesgo			X
	Evento de pérdida			X
	Tolerancia de riesgo			X
Identificación de riesgo operacional (Art. N° 03 y 4)	Procesos internos			X
	Personal			X
	Tecnologías de la información			X
	Eventos externos			X
Identificación de eventos de pérdida por riesgo operacional (Art. N° 05)	Fraude interno	X		
	Fraude externo	X		
	Relaciones laborales y seguridad en el puesto de trabajo		X	X
	Clientes, productos y prácticas empresariales	X		
	Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales		X	X
	Pérdidas derivadas del incumplimiento involuntario o negligente		X	X
	Daños a activos materiales		X	X
	Interrupción del negocio y fallos en los sistemas		X	X
	Ejecución, entrega y gestión de procesos		X	X
Definición de roles y responsabilidades (Art. N° 06, 07, 08 y 09)	del Directorio	X		
	de la Gerencia	X		
	Comité de Riesgos	X		
Manual de gestión de riesgos operacional (Art. N° 10)				X
Metodología de gestión de riesgos operacional (Art. N° 11)				X
Base de datos de eventos de pérdida (Art. N° 12)			X	
Gestión de la continuidad del negocio y de la seguridad de la información (Art. N° 13)			X	

Requisitos para la Subcontratación de servicios (Art. N° 14)		X	
Informes para la Superintendencia (Art. N° 15)	X	X	X

ANEXO 03 – Catálogo de activos de TI según Magerit

Tipo de activo		Sub clasificación		Descripción de aclaración
[info]	información	[adm]	datos de interés para la administración pública	
		[dv]	datos vitales (registros de la organización)	Información esencial para la supervivencia de la Organización. Su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar: - Aquellos que son imprescindibles para que la Organización supere una situación de emergencia - Aquellos que permiten desempeñar o reconstruir las misiones críticas - Aquellas de naturaleza legal o los derechos financieros de la Organización o sus usuarios.
		[per]	datos de carácter personal	Información concerniente a personas físicas identificadas o identificables. Los datos de carácter personal están regulados por leyes y reglamentos en cuanto afectan a las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente su honor e intimidad personal y familiar.
		[clasificado]	datos clasificados	Información sometida a normativa específica de control de acceso y distribución; es decir

				aquellos cuya confidencialidad es especialmente relevante. La tipificación de qué datos deben ser clasificados y cuáles son las normas para su tratamiento, vienen determinadas por regulaciones gubernamentales, sectoriales, por acuerdos entre organizaciones o por normativa interna.
[dato]	Datos o documentos	[files]	ficheros	
		[backup]	copias de respaldo	
		[conf]	datos de configuración	Los datos de configuración son críticos para mantener la funcionalidad de las partes y del conjunto del sistema de información
		[int]	datos de gestión interna	Incluye la información referente a los niveles de acceso asignados a los distintos tipos de usuario según su función o puesto de trabajo
		[password]	credenciales	Claves de acceso a máquina asignada o a las aplicaciones
		[auth]	datos de validación de credenciales	Códigos de identificación de usuario
		[acl]	datos de control de acceso	
		[log]	registro de actividad	Los registros de actividad sustancian los requisitos de trazabilidad. Bitácoras o log.
		[source]	código fuente	
		[exe]	código ejecutable	
		[test]	datos de prueba	Generados en las pruebas de las aplicaciones o módulos antes de puesta en producción
[keys]	Claves criptográficas	[info]	protección de la información	Claves públicas o privadas de cifrado o descifrado de la información

		[com]	protección de las comunicaciones	Claves de cifrado del canal de comunicación, claves de autenticación
		[disk]	cifrado de soportes de información	Cifrado de soportes de información
[serv]	Servicios	[www]	acceso a Internet	
		[telnet]	acceso remoto a cuenta local	
		[email]	correo electrónico	Servidor de correo electrónico
		[file]	almacenamiento de ficheros	Servidor de datos
		[ftp]	transferencia de ficheros	
		[edi]	intercambio electrónico de datos	
		[dir]	servicio de directorio	Directorio activo. Localización de personas, permitiendo la identificación y facilitando los atributos que caracterizan al elemento determinado
		[idm]	gestión de identidades	Servicios que permiten altas y bajas de usuarios de los sistemas, incluyendo su caracterización y activando los servicios de aprovisionamiento asociados a sus cambios de estado respecto de la organización
		[ipm]	gestión de privilegios	Aplicación para definir niveles de acceso
[sw]	Aplicaciones	[prp]	desarrollo propio (in house)	
		[sub]	desarrollo a medida (subcontratado)	
		[browser]	navegador web	
		[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	
		[office]	ofimática	
		[av]	anti virus	
		[os]	sistema operativo	
		[mv]	gestor de máquinas virtuales	
		[backup]	sistema de backup	
[hw]	Equipos informáticos	[host]	grandes equipos	Se caracterizan por haber pocos, frecuentemente uno sólo, ser económicamente altos y requerir un entorno específico para su operación. Son difícilmente reemplazables en caso de destrucción
		[mid]	equipos medios	Se caracterizan por haber varios, tener un coste económico medio tanto de adquisición como de mantenimiento e imponer requerimientos estándar como entorno de operación. No es difícil reemplazarlos en caso de destrucción
		[pc]	informática personal	Se caracterizan por ser multitud, tener un coste económico relativamente pequeño e imponer solamente unos requerimientos mínimos como entorno de operación. Son fácilmente reemplazables en caso de destrucción
		[mobile]	informática móvil	Se caracterizan por ser equipos afectos a la clasificación como informática personal que, además, son fácilmente transportables de un sitio a

				otro, pudiendo estar tanto dentro del recinto propio de la organización como en cualquier otro lugar
		[pda]	agendas electrónicas	
		[vhost]	equipo virtual	
		[backup]	equipamiento de respaldo	Son aquellos equipos preparados para hacerse cargo inmediato de los equipos en producción.
		[perife]	periféricos	Impresoras y servidores de impresión, escáneres
		[bp]	dispositivo de frontera	Son los equipos que se instalan entre dos zonas de confianza
		[network]	soporte de la red	Dícese de equipamiento necesario para transmitir datos: routers, módems, etc. Modems, conmutadores, routers, bridges, firewalls, wap (punto de acceso inalámbrico)
		[pabx]	centralita telefónica	
		[ipphone]	teléfono IP	
[com]	Comunicaciones	[PSTN]	red telefónica	
		[ISDN]	rdsi (red digital)	
		[X25]	X25 (red de datos)	
		[ADSL]	ADSL	
		[radio]	comunicaciones radio	
		[wifi]	red inalámbrica	
		[mobile]	telefonía móvil	
		[sat]	por satélite	
		[LAN]	red local	
		[MAN]	red metropolitana	
		[Internet]	Internet	
[media]	Soporte de información	[electro]	electrónicos	Dispositivos físicos que permiten almacenar información de forma permanente o, al menos, durante largos periodos de tiempo: discos, DVD, cintas, etc.
		[noelectro]	no electrónicos	Material impreso

[aux]	Equipamiento auxiliar	[power]	fuentes de alimentación	
		[ups]	sistemas de alimentación ininterrumpida	
		[gen]	generadores eléctricos	
		[ac]	equipos de climatización	
		[cabling_wire]	cable eléctrico	
		[cabling_utp]	cable de datos	
		[fiber]	fibra óptica	
		[supply]	suministros esenciales	Toner
		[furniture]	mobiliario: armarios, etc	
		[safe]	cajas fuertes	
[Inmueb]	Intalaciones	[building]	edificio	
		[data]	Cuarto de procesamiento de datos	
		[backup]	instalaciones de respaldo	
[pers]	Personal	[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 04 – Valoración de criticidad de activos de TI según Magerit

[D] disponibilidad
Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren. [UNE 71504:2008]
[I] integridad
Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada. [ISO/IEC 13335-1:2004]
[C] confidencialidad
Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados. [UNE-ISO/IEC 27001:2007]
[T] trazabilidad
Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. [UNE 71504:2008]
[A] autenticidad
Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. [UNE 71504:2008]

[pi] Información de carácter personal	
10	probablemente afecte gravemente a un grupo de individuos y probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
9	probablemente afecte gravemente a un individuo y probablemente quebrante seriamente leyes o regulaciones
7 – 8	probablemente afecte a un grupo de individuos y probablemente quebrante leyes o regulaciones
5 – 6	probablemente afecte a un individuo y probablemente suponga el incumplimiento de una ley o regulación
3 – 4	pudiera causar molestias a un individuo y pudiera quebrantar de forma leve leyes o regulaciones
1 – 2	pudiera causar molestias a un individuo
[lpo] Obligaciones legales	
9 - 10	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7 - 8	probablemente cause un incumplimiento grave de una ley o regulación
5 - 6	probablemente sea causa de incumplimiento de una ley o regulación
3 – 4	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1 – 2	pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad	
9 - 10	probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
7 - 8	probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
5 - 6	probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3 – 4	probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1 – 2	pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales económicos	
9 - 10	de enorme interés para la competencia

	de muy elevado valor comercial causa de pérdidas económicas excepcionalmente elevadas causa de muy significativas ganancias o ventajas para individuos u organizaciones constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7 - 8	de alto interés para la competencia de elevado valor comercial causa de graves pérdidas económicas proporciona ganancias o ventajas desmedidas a individuos u organizaciones constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
5 - 6	de cierto interés para la competencia de cierto valor comercial causa de pérdidas financieras o merma de ingresos facilita ventajas desproporcionadas a individuos u organizaciones constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
3 – 4	de bajo interés para la competencia de bajo valor comercial
1 – 2	de pequeño interés para la competencia de pequeño valor comercial supondría pérdidas económicas mínimas
[da] de interrupción del servicio	
9 - 10	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones Probablemente tenga un serio impacto en otras organizaciones
7 - 8	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones Probablemente tenga un gran impacto en otras organizaciones
5 - 6	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones Probablemente cause un cierto impacto en otras organizaciones
3 – 4	Probablemente cause la interrupción de actividades propias de la Organización
1 – 2	Pudiera causar la interrupción de actividades propias de la Organización
[po] de orden público	
9 - 10	alteración sería del orden público
7 - 8	probablemente cause manifestaciones, o presiones significativas
3 - 6	causa de protestas puntuales
1 – 2	pudiera causar protestas puntuales
[op] operaciones	
10	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7 – 8	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5 – 6	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3 – 4	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)

1 – 2	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] administración y gestión	
9 - 10	probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7 - 8	probablemente impediría la operación efectiva de la Organización
5 - 6	probablemente impediría la operación efectiva de más de una parte de la Organización
3 – 4	probablemente impediría la operación efectiva de una parte de la Organización
1 – 2	pudiera impedir la operación efectiva de una parte de la Organización
[pc] pérdida de confianza (reputación)	
10	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
9	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
8	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
7	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
6	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
5	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
4	Probablemente afecte negativamente a las relaciones internas de la Organización
3	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1 - 2	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[pd] persecución de delitos	
6 - 10	Impida la investigación de delitos graves o facilite su comisión
1 – 5	Dificulte la investigación o facilite la comisión de delitos
[trs] tiempo de recuperación del servicio	
9 –10	RTO < 4 horas
7 – 8	4 horas < RTO < 1 día
4 – 6	1 día < RTO < 5 días
1 – 3	5 días < RTO

ANEXO 05 – Catálogo de amenazas por activo y dimensión de seguridad de la información según Magerit

[N]	**Desastres naturales**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[N.1]	Fuego	Incendios: posibilidad de que el fuego acabe con recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[N.2]	Daños por agua	Inundaciones: posibilidad de que el agua acabe con recursos del sistema	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[N.*]	Desastres naturales	Incidentes que se producen sin intervención humana: rayo, tormenta eléctrica, terremoto, ciclones, avalancha, corrimiento de tierras, etc. Se excluyen desastres específicos tales como incendios Se excluye al personal por cuanto se ha previsto una amenaza específica [E.31] para cubrir la Indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[I]	**De origen industrial**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[I.1]	Fuego	Incendio: posibilidad de que el fuego acabe con los recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[I.2]	Daños por agua	Escapes, fugas, inundaciones: posibilidad de que el agua acabe con los recursos del sistema.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones

[I.*]	Desastres industriales	Desastres debidos a la actividad humana: explosiones, derrumbes, contaminación química, sobrecarga eléctrica, fluctuaciones eléctricas, accidentes de tráfico, etc. Se excluyen amenazas específicas como incendio por cuanto se ha previsto amenazas específicas. Se excluye al personal por cuanto se ha previsto una amenaza específica, [E.31], para cubrir la indisponibilidad involuntaria del personal sin entrar en sus causas.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[I.3]	Contaminación mecánica	Vibraciones, polvo, suciedad, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[I.4]	Contaminación electromagnética	Interferencias de radio, campos magnéticos, luz ultravioleta, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[I.5]	Avería de origen físico o lógico	Fallos en los equipos y/o fallos en los programas. Puede ser debida a un defecto de origen o sobrevenida durante el funcionamiento del sistema. En sistemas de propósito específico, a veces es difícil saber si el origen del fallo es físico o lógico; pero para las consecuencias que se derivan, esta distinción no suele ser relevante.	[D] disponibilidad	- [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[I.6]	Corte del suministro eléctrico	Cese de la alimentación de potencia	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información (electrónicos) - [AUX] equipamiento auxiliar
[I.7]	Condiciones inadecuadas de temperatura y/o humedad	Deficiencias en la aclimatación de los locales, excediendo los márgenes de trabajo de los equipos: excesivo calor, excesivo frío, exceso de humedad, etc.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar

[I.8]	Fallo de servicios de comunicaciones	Cese de la capacidad de transmitir datos de un sitio a otro. Típicamente se debe a la destrucción física de los medios físicos de transporte o a la detención de los centros de conmutación, sea por destrucción, detención o simple incapacidad para atender al tráfico presente.	[D] disponibilidad	- [COM] redes de comunicaciones
[I.9]	Interrupción de otros servicios y suministros esenciales	Interrupción de otros servicios o recursos de los que depende la operación de los equipos; por ejemplo, papel para las impresoras, tóner, refrigerante,	[D] disponibilidad	- [AUX] equipamiento auxiliar
[I.10]	Degradación de los soportes de almacenamiento de la información	Degradación como consecuencia del paso del tiempo	[D] disponibilidad	- Media] soportes de información
[I.11]	Emanaciones electromagnéticas	Hecho de poner vía radio datos internos a disposición de terceros. Es una amenaza donde el emisor es víctima pasiva del ataque. Prácticamente todos los dispositivos electrónicos emiten radiaciones al exterior que pudieran ser interceptadas por otros equipos (receptores de radio) derivándose una fuga de información. No se contempla en esta amenaza la emisión por necesidades del medio de comunicación: redes inalámbricas, enlaces de microondas, etc. que estarán amenazadas de interceptación	[C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] media - [AUX] equipamiento auxiliar - [L] instalaciones
[E]	**Errores y fallos no intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[E.1]	Errores de los usuarios	Equivocaciones de las personas cuando usan los servicios, datos, etc.	[I] integridad [C] confidencialidad [D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [Media] soportes de información
[E.2]	Errores del administrador	Equivocaciones de personas con responsabilidades de instalación y operación.	[D] disponibilidad [I] integridad [C] confidencialidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software)

				- [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones - [Media] soportes de información
[E.3]	Errores de monitorización *(log)*	Inadecuado registro de actividades: falta de registros, registros incompletos, registros incorrectamente fechados, registros incorrectamente atribuidos, etc.	[I] integridad (trazabilidad)	- [D.log] registros de actividad
[E.4]	Errores de configuración	Introducción de datos de configuración erróneos. Prácticamente todos los activos dependen de su configuración y ésta de la diligencia del ad ministrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad	- [D.conf] datos de configuración
[E.7]	Deficiencias en la organización	Cuando no está claro quién tiene que hacer exactamente qué y cuándo, incluyendo tomar medidas sobre los activos o informar a la jerarquía de gestión. Acciones descoordinadas, errores por omisión, etc.	[D] disponibilidad	- [P] personal
[E.8]	Difusión de software dañino	Propagación inocente de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	- SW] aplicaciones (software)
[E.9]	Errores de [re-]encaminamiento	Envío de información a través de un sistema o una red usando, accidentalmente, una ruta incorrecta que lleve la información a donde o por donde no es debido; puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Es particularmente destacable el caso de que el error de encaminamiento suponga un error de entrega, acabando la información en manos de quien no se espera.	[C] confidencialidad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[E.10]	Errores de secuencia	Alteración accidental del orden de los mensajes transmitidos.	[I] integridad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[E.14]	Escapes de información	La información llega accidentalmente al conocimiento de personas que no deberían tener conocimiento de ella, sin que la información en sí misma se vea alterada.	[C] confidencialidad	

[E.15]	Alteración accidental de la información	Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[E.18]	Destrucción de información	Pérdida accidental de información. Esta amenaza sólo se identifica sobre datos en general, pues cuando la información está en algún soporte informático, hay amenazas específicas.	[D] disponibilidad	- D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[E.19]	Fugas de información	Revelación por indiscreción. Incontinencia verbal, medios electrónicos, soporte papel, etc.	[C] confidencialidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones - [P] personal (revelación)
[E.20]	Vulnerabilidades de los programas (software)	Defectos en el código que dan pie a una operación defectuosa sin intención por parte del usuario pero con consecuencias sobre la integridad de los datos o la capacidad misma de operar.	[I] integridad [D] disponibilidad [C] confidencialidad	- [SW] aplicaciones (software)
[E.21]	Errores de mantenimiento / actualización de programas (software)	Defectos en los procedimientos o controles de actualización del código que permiten que sigan utilizándose programas con defectos conocidos y reparados por el fabricante	[I] integridad [D] disponibilidad	- [SW] aplicaciones (software)

[E.23]	Errores de mantenimiento / actualización de equipos (hardware)	Defectos en los procedimientos o controles de actualización de los equipos que permiten que sigan utilizándose más allá del tiempo nominal de uso.	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes electrónicos - [AUX] equipamiento auxiliar
[E.24]	Caída del sistema por agotamiento de recursos	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada.	[D] disponibilidad	- [S] servicios - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[E.25]	Pérdida de equipos	La pérdida de equipos provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. Se puede perder todo tipo de equipamiento, siendo la pérdida de equipos y soportes de información los más habituales. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[E.28]	Indisponibilidad del personal	Ausencia accidental del puesto de trabajo: enfermedad, alteraciones del orden público, guerra bacteriológica, etc.	[D] disponibilidad	- [P] personal interno
[A]	**Ataques intencionados**			
Código	**Nombre**	**Descripción**	**Dimensiones que afecta**	**Tipos de activos que afecta**
[A.3]	Manipulación de los registros de actividad (log)		[I] integridad (trazabilidad)	- [D.log] registros de actividad
[A.4]	Manipulación de la configuración	Afecta la configuración de los activos. Es diligencia del administrador: privilegios de acceso, flujos de actividades, registro de actividad, encaminamiento, etc.	[I] integridad [C] confidencialidad [A] disponibilidad	- [D.log] registros de actividad
[A.5]	Suplantación de la identidad del usuario	Cuando un atacante consigue hacerse pasar por un usuario autorizado, utilizando los privilegios de éste para sus fines propios. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personal contratado temporalmente.	[C] confidencialidad [A] autenticidad [I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[A.6]	Abuso de privilegios de acceso	Cada usuario utiliza un nivel de privilegios para un determinado propósito. Cuando un usuario abusa de su nivel	[C] confidencialidad [I] integridad [D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios

		de privilegios para realizar tareas que no son de su competencia, puede ocasionar problemas.		- [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[A.8]	Difusión de software dañino	Propagación intencionada de virus, espías (spyware), gusanos, troyanos, bombas lógicas, etc.	[D] disponibilidad [I] integridad [C] confidencialidad	- [SW] aplicaciones (software)
[A.9]	[Re-]encaminamiento de mensajes	Envío de información a un destino incorrecto a través de un sistema o una red, que llevan la información a donde o por donde no es debido. Puede tratarse de mensajes entre personas, entre procesos o entre unos y otros. Un atacante puede forzar un mensaje para circular a través de un nodo determinado de la red donde puede ser interceptado. Un ataque de encaminamiento lleve a una entrega fraudulenta, acabando la información en manos de quien no debe.	[C] confidencialidad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[A.10]	Alteración de secuencia	Alteración del orden de los mensajes transmitidos. Con ánimo de que el nuevo orden altere el significado del conjunto de mensajes, perjudicando a la integridad de los datos afectados.	[I] integridad	- [S] servicios - [SW] aplicaciones (software) - [COM] redes de comunicaciones
[A.11]	Acceso no autorizado	El atacante consigue acceder a los recursos del sistema sin tener autorización para ello, típicamente aprovechando un fallo del sistema de identificación y autorización.	[C] confidencialidad [I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios - [SW] aplicaciones (software) - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[A.12]	Análisis de tráfico	El atacante, sin necesidad de entrar a analizar el contenido de las comunicaciones, es capaz de extraer conclusiones a partir del análisis del origen, destino, volumen y frecuencia de los intercambios.	[C] confidencialidad	- [COM] redes de comunicaciones

		A veces se denomina “monitorización de tráfico”.		
[A.13]	Repudio	Negación a posteriori de actuaciones o compromisos adquiridos en el pasado. Repudio de origen: negación de ser el remitente u origen de un mensaje o comunicación. Repudio de recepción: negación de haber recibido un mensaje o comunicación. Repudio de entrega: negación de haber recibido un mensaje para su entrega a otro.	[I] integridad (trazabilidad)	- S] servicios - [D.log] registros de actividad
[A.14]	Interceptación de información (escucha)	El atacante llega a tener acceso a información que no le corresponde, sin que la información en sí misma se vea alterada.	[C] confidencialidad	- [COM] redes de comunicaciones
[A.15]	Modificación deliberada de la información	Alteración intencional de la información, con ánimo de obtener un beneficio o causar un perjuicio.	[I] integridad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información - [L] instalaciones
[A.18]	Destrucción de información	Eliminación intencional de información, con ánimo de obtener un beneficio o causar un perjuicio.	[D] disponibilidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW) - [Media] soportes de información - [L] instalaciones
[A.19]	Revelación de información	Revelación de información (divulgación, copia ilegal de software)	[C] confidencialidad	- [D] datos / información - [keys] claves criptográficas - [S] servicios (acceso) - [SW] aplicaciones (SW) - [COM] comunicaciones (tránsito) - [Media] soportes de información

				- [L] instalaciones
[A.22]	Manipulación de programas	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (alteración de programas)	[C] confidencialidad [I] integridad [D] disponibilidad	- [SW] aplicaciones (software)
[A.22]	Manipulación de los equipos	Alteración intencionada del funcionamiento de los programas, persiguiendo un beneficio indirecto cuando una persona autorizada lo utiliza (sabotaje de hardware)	[C] confidencialidad [D] disponibilidad	- [HW] equipos - [Media] soportes de información - [AUX] equipamiento auxiliar
[A.24]	Denegación de servicio	La carencia de recursos suficientes provoca la caída del sistema cuando la carga de trabajo es desmesurada (saturación del equipo informático)	[D] disponibilidad	- [S] servicios - [HW] equipos informáticos (hardware) - [COM] redes de comunicaciones
[A.25]	Robo	La sustracción de equipamiento provoca directamente la carencia de un medio para prestar los servicios, es decir una indisponibilidad. El robo puede afectar a todo tipo de equipamiento, siendo el robo de equipos y el robo de soportes de información los más habituales. El robo puede realizarlo personal interno, personas ajenas a la Organización o personas con tratadas de forma temporal, lo que establece diferentes grados de facilidad para acceder al objeto sustraído y diferentes consecuencias. En el caso de equipos que hospedan datos, además se puede sufrir una fuga de información.	[D] disponibilidad [C] confidencialidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar
[A.26]	Ataque destructivo	Vandalismo, terrorismo, acción militar, etc. Esta amenaza puede ser perpetrada por personal interno, por personas ajenas a la Organización o por personas contratadas de forma temporal. (destrucción de hardware o de soportes)	[D] disponibilidad	- [HW] equipos informáticos (hardware) - [Media] soportes de información - [AUX] equipamiento auxiliar - [L] instalaciones
[A.27]	Ocupación enemiga	Cuando los locales han sido invadidos y se carece de control sobre los propios medios de trabajo.	[D] disponibilidad [C] confidencialidad	- [L] instalaciones

[A.28]	Indisponibilidad del personal	Ausencia deliberada del puesto de trabajo: como huelgas, absentismo laboral, bajas no justificadas, bloqueo de los accesos, etc. (daños a la disponibilidad del personal)	[D] disponibilidad	- [P] personal interno
[A.29]	Extorsión	Presión que, mediante amenazas, se ejerce sobre alguien para obligarle a obrar en determinado sentido.	[C] confidencialidad [I] integridad [D] disponibilidad	- [P] personal interno
[A.30]	Ingeniería social	Abuso de la buena fe de las personas para que realicen actividades que interesan a un tercero.	[C] confidencialidad [I] integridad [D] disponibilidad	- [P] personal interno

ANEXO 06 – Catálogo de vulnerabilidades potenciales usado en el modelo de gestión de riesgos según Magerit

N°	Vulnerabilidad
1	Ausencia de personal
2	Acceso físico no autorizado
3	Acceso no autorizado a la documentación del sistema
4	Acceso no autorizado a la información
5	Acceso no autorizado a la información, redes y sistemas
6	Acceso no autorizado a las infraestructuras informáticas
7	Acceso no autorizado a las librerías fuente de los programas
8	Acceso no autorizado a los ordenadores
9	Acceso no autorizado a redes y sus servicios
10	Acceso no autorizado al equipamiento informático
11	Acceso no autorizado, inadecuado o corrupción del soporte en el tránsito
12	Activos no protegidos
13	Atribución incorrecta de privilegios de acceso
14	Código malicioso
15	Complicated user interface
16	Confianza de las organizaciones clave hacia la compañía.
17	Conformidad con estándares
18	Conformidad con la política de seguridad
19	Control mal implantado
20	Coordinación de actividades de seguridad
21	Cumplimiento de las obligaciones y deberes del outsourcing
22	Derecho a auditar en contratos de terceras partes
23	Derechos de propiedad intelectual
24	Disponibilidad de las infraestructuras de procesamiento de la información
25	Disposición o reutilización de los medios de almacenaje sin una apropiada verificación
26	Externalización y uso de terceras partes contratadas
27	Clima extremo
28	Fallo del sistema
29	Falta de un acuerdo de intercambio de software e información
30	Falta de coordinación y organización de la seguridad
31	Falta de planes y procedimientos de continuidad de negocio
32	Falta de política de seguridad
33	Falta de responsabilidades, pruebas y formación en la continuidad de negocio
34	Falta de seguridad en el equipamiento informático
35	Falta de seguridad en los soportes informáticos
36	Falta de sensibilización
37	Falta de una gestión apropiada de las claves criptográficas
38	Falta de una política determinada en el uso de controles criptográficos
39	Gestión de contraseñas que es demasiado simple
40	Manejo inadecuado de la red
41	Uso inadecuado o descuidado del control de acceso físico al edificio
42	Procedimientos inadecuados de reclutamiento
43	Respuesta inadecuada del servicio de mantenimiento
44	Uso Incorrecto del hardware y software
45	Incorrecta clasificación, etiquetado o manejo de la información.
46	Incumplimiento de la legislación

47 Insuficiente mantenimiento / mala instalación de los medios de almacenaje.
48 Entrenamiento insuficiente de seguridad
49 Insuficiente seguridad construida dentro del sistema
50 falta de seguimiento
51 Falta de copias back-up
52 Falta de cuidado en la disposición
53 Falta de documentación
54 Falta del control del cambio eficaz
55 Falta de control eficiente del cambio de configuración
56 Falta de mecanismos de identificación y de autentificación tales como autentificación de usuario
57 Falta de identificación y autentificación del remitente y del receptor
58 Falta de mecanismos de supervisión
59 Falta de esquemas de reemplazo periódicos
60 Falta de protección física del edificio, puertas y ventanas;
61 Falta de políticas para el uso correcto de los medios de telecomunicación y mensajería
62 Falta de pruebas de envío y recibimiento del mensaje
63 Falta del conocimiento sobre seguridad
64 Localización en un área susceptible a la inundación
65 Nivel inapropiado de protección criptográfica
66 Dejar en sesión el sistema al salir del Workstation.
67 Prueba insuficiente del software
68 Pobre cableado
69 Administración pobre de contraseñas
70 Prevención del uso no autorizado de las infraestructuras de procesamiento
71 Procesamiento de negocio correcto
72 Protección de datos y privacidad de la información personal
73 Protección de la información de la organización
74 Recolección de evidencias
75 Regulación de los controles criptográficos
76 Responsabilidades no claramente definidas
77 Riesgos de comercio electrónico
78 Riesgos de los sistemas ofimáticos compartidos entre las organizaciones
79 Riesgos de los sistemas públicamente disponibles
80 Riesgos desde terceras partes
81 Riesgos provenientes de la informática móvil
82 Riesgos provenientes del teletrabajo
83 Riesgos relacionados con el outsourcing
84 Seguridad de Internet
85 Seguridad de la Intranet
86 Seguridad del comercio electrónico
87 Seguridad del teletrabajo
88 Seguridad en los negocios móviles
89 Sensibilidad a la radiación electromagnética
90 Únicos puntos de falla
91 Susceptibilidad a la humedad, al polvo
92 Susceptibilidad a las variaciones de la temperatura
93 Susceptibilidad a las variaciones del voltaje
94 Transferencia de passwords claramente
95 Especificaciones confusas o incompletas para los desarrolladores

96 Copiado incontrolado
97 Descarga y uso incontrolado de software
98 Líneas de comunicación desprotegidas
99 Password desprotegidos
100 Conexiones de red pública desprotegidas
101 Unprotected sensitive traffic
102 Almacenaje desprotegido
103 Unsupervised work by outside or cleaning staff
104 Saber bien los defectos en el software
105 Wrong allocation of access right

ANEXO 07: Técnica - Encuesta

INSTRUCCIONES: Marque con un aspa (X), la alternativa correcta.

1. ¿Existe políticas de seguridad en la empresa?
   a) Si b) No

2. ¿Tiene conocimiento de medidas de seguridad?
   a) Si b) No

3. ¿Ha recibido capacitación sobre seguridad de la información de acuerdo a su función Laboral?
   a) Si b) No

4. ¿Su terminal tiene contraseña para el acceso la información?
   a) Si b) No

5. ¿Su área de trabajo cuenta con software antivirus licenciado y actualizado?
   a) Si b) No

6. ¿Su divulgación no autorizada de información puede afectar el cumplimiento de leyes o normas impartidas por entes de control?
   a) Si b) No

7. ¿Si el activo o la información que se gestiona son alterados sin autorización puede afectar la imagen de la entidad?
   a) Si b) No

8. El nivel de seguridad actual cumple con los parámetros establecidos para el ingreso al sistema.
   a) Si b) No

9. ¿Realiza copias de seguridad para proteger su información?
   a) Si b) No

10. ¿Su oficina está protegida frente a ataques cibernéticos?
    a) Si b) No

ANEXO 08: Validación de encuesta

ANEXO 09: Validación de cuestionario a juicio de expertos

PLAN PARA REDUCIR LOS RIESGOS OPERATIVOS DE TECNOLOGÍAS DE LA INFORMACIÓN BASADA EN METODOLOGIA MAGERIT EN LA CAJA PIURA DE LA CIUDAD DE CHICLAYO

Responsable: Wilber Santa María Huamán

Indicación: Señor (a) especializado (a) solicito su colaboración para que luego de un riguroso análisis de los ítems del cuestionario de la encuesta que le mostramos, marque con una (x) en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional demostrando si cuenta o no cuenta con los requisitos mínimos de formulación para su posterior aplicación.

NOTA: Para cada pregunta se considera la escala de Likert:

1. EXCELENTE (E)	2. BUENO (B)	3. REGULAR (R)	4. MALO (M)	5. PESIMO (P)

N°	ITEMS	Medición				
		E	B	R	M	P
1	Se ha definición las categorías (disponibilidad, integridad y confidencialidad) de los riesgos de TI en un nivel aceptable		X			
2	El modelo se integra a la gestión del riesgo operativo de la entidad	X				
3	La estructura del modelo está diseñada para que los empleados relacionados con la gestión del riesgo operativo de TI puedan utilizarlo y comprenderlo en un nivel aceptable		X			
4	El modelo contempla los requisitos exigidos por la SBS para la gestión de riesgos de TI		X			
5	Se ha establecido pautas para evaluar la magnitud de los riesgos de TI de modo coherente		X			
6	El modelo cuenta con indicadores suficientes para monitorizar la gestión de riesgos de TI		X			

Nombre Completo	Eddie Jhon Gonzáles Cotrina	
Grado académico	Ingeniero de Sistemas	

PLAN PARA REDUCIR LOS RIESGOS OPERATIVOS DE TECNOLOGÍAS DE LA INFORMACIÓN BASADA EN METODOLOGIA MAGERIT EN LA CAJA PIURA DE LA CIUDAD DE CHICLAYO

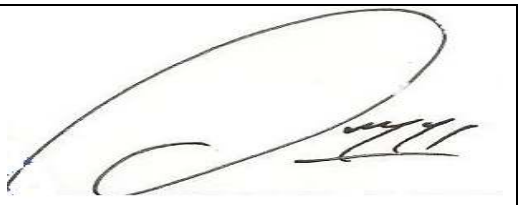
Responsable: Wilber Santa María Huamán

Indicación: Señor (a) especializado (a) solicito su colaboración para que luego de un riguroso análisis de los ítems del cuestionario de la encuesta que le mostramos, marque con una (x) en el casillero que cree conveniente de acuerdo a su criterio y experiencia profesional demostrando si cuenta o no cuenta con los requisitos mínimos de formulación para su posterior aplicación.

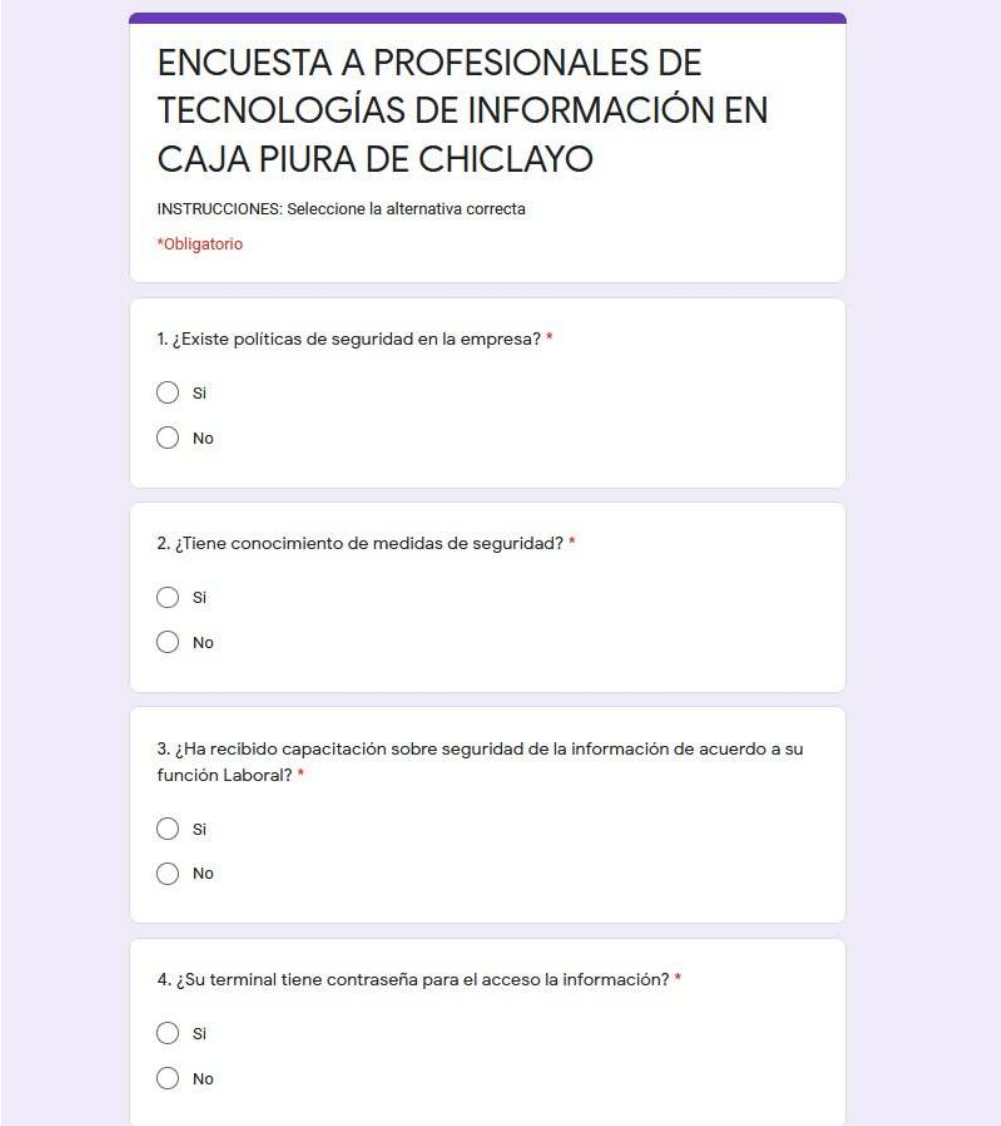
NOTA: Para cada pregunta se considera la escala de Likert:

1. EXCELENTE (E)	2. BUENO (B)	3. REGULAR (R)	4. MALO (M)	5. PESIMO (P)

N°	ITEMS	Medición				
		E	B	R	M	P
1	Se ha definición las categorías (disponibilidad, integridad y confidencialidad) de los riesgos de TI en un nivel aceptable	X				
2	El modelo se integra a la gestión del riesgo operativo de la entidad	X				
3	La estructura del modelo está diseñada para que los empleados relacionados con la gestión del riesgo operativo de TI puedan utilizarlo y comprenderlo en un nivel aceptable	X				
4	El modelo contempla los requisitos exigidos por la SBS para la gestión de riesgos de TI		X			
5	Se ha establecido pautas para evaluar la magnitud de los riesgos de TI de modo coherente		X			
6	El modelo cuenta con indicadores suficientes para monitorizar la gestión de riesgos de TI		X			

Nombre Completo	Gilberto Martín Ampuero Pasco	
Grado académico	Ingeniero de Sistemas Maestro en Ciencias con Mención en Ingeniería de Sistemas e Informática	

ANEXO 10: Formulario virtual



ENCUESTA A PROFESIONALES DE TECNOLOGÍAS DE INFORMACIÓN EN CAJA PIURA DE CHICLAYO

INSTRUCCIONES: Seleccione la alternativa correcta

*Obligatorio

1. ¿Existe politicas de seguridad en la empresa? *

- Si
- No

2. ¿Tiene conocimiento de medidas de seguridad? *

- Si
- No

3. ¿Ha recibido capacitación sobre seguridad de la información de acuerdo a su función Laboral? *

- Si
- No

4. ¿Su terminal tiene contraseña para el acceso la información? *

- Si
- No

4. ¿Su terminal tiene contraseña para el acceso la información? *

- ◯ Si
- ◯ No

5. ¿Su área de trabajo cuenta con software antivirus licenciado y actualizado? *

- ◯ Si
- ◯ No

6. ¿Su divulgación no autorizada de información puede afectar el cumplimiento de leyes o normas impartidas por entes de control? *

- ◯ Si
- ◯ No

7. ¿Si el activo o la información que se gestiona son alterados sin autorización puede afectar la imagen de la entidad? *

- ◯ Si
- ◯ No

8. El nivel de seguridad actual cumple con los parámetros establecidos para el ingreso al sistema. *

- ◯ Si
- ◯ No

9. ¿Realiza copias de seguridad para proteger su información? *

- ◯ Si
- ◯ No

10. ¿Su oficina está protegida frente a ataques cibernéticos? *

- ◯ Si
- ◯ No