UNIVERSIDAD NACIONAL TECNOLÓGICA DE LIMA SUR

FACULTAD DE INGENIERÍA Y GESTIÓN

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

"DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA ISO 27001 PARA LA REDUCCIÓN DE RIESGOS DE LOS ACTIVOS EN LA EMPRESA LOYALTY PERÚ SAC"

TRABAJO DE SUFICIENCIA PROFESIONAL

Para optar el Título Profesional de

INGENIERO DE SISTEMAS

PRESENTADO POR EL BACHILLER

CIPRIAN DURAN, FRANKLIN

Villa El Salvador

2019

DEDICATORIA

El presente proyecto está dedicado a mis queridos padres Gregorio y Martha, como reconocimiento a su apoyo incondicional, durante todo el proceso de mi formación profesional.

AGRADECIMIENTO

En el desarrollo de este trabajo, se realizaron varias reuniones, muchas sugerencias de compañeros de trabajo y amigos que contribuyeron de manera positiva, por eso, quiero expresar mi agradecimiento a aquellas personas que de manera directa o indirectamente me apoyaron en el desarrollo del proyecto.

A la Universidad Nacional Tecnológica de Lima Sur (UNTELS), autoridades y personal que hacen la Unidad Educativa, en particular a la comisión del II programa de titulación por trabajo de suficiencia profesional por la aprobación y facilidades concedidas.

A la Empresa Loyalty Perú SAC, directivos y personales de trabajo un fuerte agradecimiento por la disponibilidad y la forma solidaria y comprometida con que colaboraron. A todo el equipo de trabajo del área de Sistemas que me acogieron con simpatía y afecto y, siempre estuvieron disponibles, aportando una contribución relevante. A todos y, sin excepción.

Al Dr. Ing. Frank Escobedo, mi asesor, un agradecimiento especial por el apoyo, orientación, colaboración, experiencia, conocimiento, motivación y amistad que me brindo para concretar este proyecto de investigación, y no debe olvidarse a todos los Profesores de la UNTELS que me han inculcado sus conocimientos y hoy puedo sentirme dichoso y contento.

A mi querida familia por la paciencia y por el apoyo motivacional que me dio durante la realización de este proyecto, y a todos los demás que, no están mencionados aquí, que de alguna forma formaron parte de la realización de este proyecto. La pregunta central del proyecto es ¿De qué manera el diseño de un plan de seguridad de información basado en la Norma ISO 27001 ayuda a reducir los riesgos de los activos de la empresa Loyalty Perú SAC?

ÍNDICE

CAPÍTULO III: DISEÑO DEL PLAN DE SEGURIDAD DE INFORMACIÓN

LISTADO DE FIGURAS

LISTADO DE TABLAS

INTRODUCCIÓN

El actual trabajo se focaliza en temas de seguridad de información, riesgos y activos de la información. Se entiende por seguridad de información como la protección de los activos de la organización ya sea de la utilización, propagación o destrozo no autorizada. El riesgo es la probabilidad de que una amenaza o algo malo o desagradable se concreten sobre los activos de información causando deterioro y destrucción. Y los activos son representados por las páginas web, base de datos, contratos, imágenes, correos, documentos, etc. Estos activos son fundamentales para el logro de propósitos de una empresa.

El motivo por el cual se aborda los temas mencionados previamente, por un lado, es por la necesidad que lo requiere la empresa Loyalty Perú SAC de no contar con un proyecto de invulnerabilidad de información y por el otro lado, es por los requerimientos legales y contractuales de los socios de la empresa, clientes y proveedores. Finalmente, el motivo personal de profundizar, indagar y conocer el correcto diseño de un proyecto de sistema de administración de la seguridad de la información fundamentado la norma ISO/IEC 27001.

Uno de muchos problemas que afronta la empresa es no contar las medidas de seguridad adecuadas para la custodia de los bienes de información de la empresa, carece de identificación y tratamiento estructurado de riesgos de información, también no posee políticas definidas y objetivos marcados en base a la seguridad de información. La interrogante central del proyecto es ¿Cómo ayuda el diseño del plan de seguridad de información basado en la Norma ISO 27001 a reducir los riesgos de los activos de la empresa Loyalty Perú SAC? El objetivo central del trabajo consiste en diseñar un plan de seguridad de la información basado en la ISO 27001 para la reducción de los riesgos de los activos en la empresa Loyalty Perú SAC.

Para llevar acabo del plan trazado, el proyecto se ha ordenado en tres capítulos.

En el capítulo I, planteamiento del problema donde se describe de la realidad problemática de la organización; se justifica el proyecto; se delimita el plan

trazado en tres dimensiones teórica, temporal, espacial; también se realiza la formulación del problema, y finalmente se proponen las metas del proyecto.

En el capítulo II, se expone el marco teórico, se efectúan la búsqueda de los antecedentes del proyecto, se realiza las revisiones bibliográficas de la norma ISO 27001 y del procedimiento de gestión de riesgos MAGERIT, y por último se definen algunos términos básicos que ayudaran a entender el trabajo planificado.

En el capítulo III, se realiza la identificación de los activos de información, se estiman los riesgos de los activos de información, se proponen los controles de seguridad de información, se realiza plan de invulnerabilidad de información aplicando la estructura de la norma, se analiza los peligros de seguridad de información bajo el procedimiento de MAGERIT V3, se plantean la medida de seguridad de información, para culminar se desarrolla un plan de seguridad de información.

CAPÍTULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción de la realidad problemática

En la coyuntura actual, la tecnología se ha transformado en la pieza importante en el ámbito personal y empresarial; en los últimos años las organizaciones a nivel mundial adquieren nuevas tecnologías para sacar ventajas competitivas. Sin embargo, la seguridad no se aborda adecuadamente, lo que permite que los ataques de los adversarios inteligentes sean más frecuentes y cada vez más sofisticados. Esta distracción puede resultar en pérdidas de negocios y fracasos en la visión general de las organizaciones.

En el caso de Perú, de acuerdo con los datos de la revista Fortinet Perú, la mayoría de las organizaciones invierten poco o nada en temas de seguridad de los activos de la empresa, a pesar que, en los últimos años más de 150 millones de ataques únicamente en Latinoamérica, sitúa a Perú en el puesto N° 5 de los países atacados. A pesar de todo esto, las inversiones en cuestión de seguridad información no son aún una prioridad en las empresas peruanas.

Loyalty Perú SAC, es una sociedad peruana establecido en el año 1998, se dedica a la creación de programas de fidelización, que emite tarjetas de beneficio y descuento, tiene como principales socios centros comerciales Wong, Metro, Paris, los grifos Primax y las tiendas de conveniencia Listo; y todos los restaurantes de Delosi (KFC, Pizza Hut, Chili’s, Burger King, Pink Berry, Madam Tusan y Olive Garden), entre otros(Ruperto, 2016).

Esta empresa no es ajena a esta problemática, ya que no cuenta con las prevenciones de seguridad convenientes para salvaguardar los activos de información, no cuenta con un plan de gestión de riesgos. Tal es el caso donde se puede contemplar muchas deficiencias en las instalaciones de conexión de red, carencia de verificación de acceso autorizado a los datos de la organización, falta de gestión de mantenimiento y actualización de los equipos hardware y software, no cuenta con de políticas definidas para la gestión de copias de seguridad, escasos documentos de manuales de procedimientos, etc.

Por lo ya mencionado anteriormente, el presente proyecto de titulación tiene como propósito diseñar un plan de seguridad de información que permita salvaguardar los bienes de información de la empresa, utilizando controles, políticas de seguridad, programas de tratamiento de riesgos, entre otros.

1.2. Justificación del problema

Ante el avance científico de la actualidad y la poca inversión en cuestiones protección de información en la mayoría de las organizaciones peruanas, surge el interés de conocer la situación actual que afronta la empresa Loyalty Perú SAC, en asuntos de seguridad de información.

Observando, la gran cantidad de bienes que posee la empresa y percibiendo la escasa protección sus activos, el actual proyecto intenta ser una guía para mejorar la confidencialidad, integridad y la disponibilidad de los datos de la empresa de Loyalty Perú SAC, de la misma manera el proyecto aspira ser la referencia para poder detectar y prevenir los riesgos que pueden sufrir los bienes y servicios de la empresa y en un futuro optar por la certificación de la norma ISO 27001, ya que hoy en día la cantidad ataques informáticos están en aumento, de manera que, este proyecto ayudaría a preservar y mejorar la confidencialidad de su información, para ser organización competitiva, segura que crea un ambiente de trabajo satisfactorio para obtener un resultado óptimo y diferenciador .

Este proyecto también busca proporcionar un modelo de un plan que será útil para otras empresas que pretendan mejorar el control sus activos de información, las amenazas que pueden sufrir cada uno de sus activos, y las formas de prevenir los riesgos de sus recursos de información, ya que, hoy en día la inseguridad está en aumento esencialmente por el uso abundante y global del Internet y sus tecnologías. La norma ISO 27001 se aplica para cualquier modelo de empresa micro o macro de cualquier tipo de actividad

Por otra parte, el proyecto contribuye ampliar conocimiento e incentivar la aplicación de la norma ISO 27001 para otros proyectos similares que pretendan aplicar la norma en empresas, organizaciones, instituciones que desean invertir

en la protección de sus activos y de esa manera demostrar su compromiso y conformidad con los mejores estándares y prácticas en asuntos de seguridad de la información.

1.3. Delimitación del proyecto

1.3.1. Teórica

El desarrollo del plan está centrado en la norma ISO 27001 versión 2013 que contribuirá a la empresa Loyalty Perú a mantener sus recursos bajo los fundamentos de confidencialidad, integridad y disponibilidad. En tal sentido este proyecto aborda temas relacionado con:

Seguridad de información. Tiene como finalidad salvaguardar la información ante cualquier ingreso no autorizado, empleo no permitido, expansión de la información, la detención o eliminación no autorizada, etc. La seguridad se entiende también como una condición de un sistema o un modelo de información que debe estar libre de cualquier amenaza, daño o riesgo. Se define el daño como aquello que puede causar el mal funcionamiento de los activos resultados.

Activos de la información. Son los recursos necesarios con los que cuenta una empresa o una organización para conseguir los objetivos propuesto dirigidos por la alta dirección. Cada uno de los activos tiene su propia particularidad que se diferencian en su condición, en tema de seguridad, en sus fundamentos de, confidencialidad, integridad y disponibilidad. Los activos también se pueden clasifican por tipos pueden ser hardware, software, datos, personal, servicios, instalaciones, etc.

Riesgos de seguridad. Es la posibilidad de que una organización pueda sufrir daños o pérdidas ya sea económicas, o también de clientes, o de reputación, etc. La amenaza pertenece a un riesgo, y pueden ser de procedencia natural, industrial o causados por el hombre, también pueden ser los defectos de aplicaciones, originadas por las personas de forma accidental. El proyecto utilizará el procedimiento de análisis de

gestión de riesgos MAGERIT V3, esta metodología ayudará a la empresa a saber a qué riesgos se enfrenta.

1.3.2. Temporal

El desarrollo del proyecto propuesto fue llevado a cabo durante los meses comprendidos entre 7 enero hasta abril 7 del año 2019.

1.3.3. Espacial

En cuanto al ámbito espacial el proyecto propuesto se realizó en la empresa Loyalty Perú SAC, ubicado en la dirección Jr. Señor de Sipán Nro. 297 Urb. Las Poncianas Ref. Esquina Jr. Tambo Real en Santiago de Surco – Lima – Perú.

1.4. Formulación del problema

1.4.1. Problema general

¿De qué manera el diseño de un plan de seguridad de información basado en la Norma ISO 27001 ayuda a reducir los riesgos de los activos de la empresa Loyalty Perú SAC?

1.4.2. Problemas específicos

- ¿Cómo identificar los activos de información para valorar según sus tres dimensiones de confidencialidad, disponibilidad e integridad basadas en la norma ISO 27001?
- ¿Cómo reconocer las posibles amenazas de los activos de información para estimar el nivel de riesgo según el impacto y probabilidad de ocurrencia, aplicando la metodología de gestión de riesgos MAGERIT V3?
- ¿Cómo descubrir las vulnerabilidades de los activos de información para proponer son los controles de seguridad de información según la norma ISO 27001?

1.5. Objetivos

1.5.1. Objetivo general

Diseñar un plan de seguridad de la información basado en la ISO 27001 para la reducción de los riesgos de los activos en la empresa Loyalty Perú SAC.

1.5.2. Objetivos específicos

- Identificar los activos de información para valorar según sus tres dimensiones de confidencialidad, disponibilidad e integridad basadas en la norma ISO 27001.
- Reconocer las posibles amenazas de los activos de información para estimar el nivel de riesgo según el impacto y probabilidad de ocurrencia, aplicando la metodología de gestión de riesgos MAGERIT V3.
- Descubrir las vulnerabilidades de los activos de información para proponer los controles de seguridad de información según la norma ISO 27001.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes

2.1.1. Antecedentes internacionales

- El trabajo de Manuel Muñoz, titulado *"Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001"* Cataluña - España, se realiza un plan de referencia para implantar un SGSI en una empresa denominada TREVAL, dedicada a prestar servicios TI a micro empresas o pymes; en dicha investigación se apoya de la metodología del Ciclo de Deming para desarrollar las dos primeras fases del proyecto, en la primera fase define el plan de seguridad y el alcance del proyecto alto nivel, en la segunda fase realiza un análisis de requerimientos de la norma para ayudar a establecer en SGSI en la organización.

  Seguidamente el proyecto mencionado analiza y gestiona los riesgos de seguridad de información con ayuda de la metodología MAGERIT, con la finalidad de reducir los riesgos que se presentan en la organización, luego en el proyecto se realiza un recuento de los activos e identificar las amenazas y oportunidades, el trabajo también se define el documento de aplicabilidad con el objetivo de realizar los controles que fueron necesarios para su implementación, seguidamente crea el plan de trabajo de implantación, donde logra ver los resultados tales como: mejora de instalaciones de red, mejora de los procedimientos de seguridad de información, mejora de sus actividades, creación de proceso nuevos. Finalmente el proyecto concluye sugerencia que la aplicar la norma ISO 27001 y seguir el desarrollo de las fases del Ciclo de Deming que son efectivas para definir los controles de seguridad de información.

  El trabajo se relaciona con el proyecto, ya que propone un material de enseñanza e información, a través la efectiva de análisis de riesgos bajo la metodología de MAGERIT, además el proyecto tiene una estructura definida donde aborda la mayoría de los documentos de la norma española UNE-ISO 27001. (Manuel Muñoz, 2015).

- Proyecto de Juan Pablo Berrío López, denominado *"Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001"*, Medellín - Colombia, se trata de un proyecto de desarrollo de una metodología para evaluar del desempeño de SGSI basado en la norma ISO 27001, para lo cual propone un modelo de evaluación de los controles de seguridad conocido como método DELPHI. Este método, consiste en preguntar a dos expertos llamados especialistas y afectados para lograr un consenso entre las partes involucradas, de esa manera, identificar los activos de una organización y proponer controles claves que se deben implementarse para proteger dichos activos identificados.

  Este trabajo demuestra que la metodología DELPHI sirve para identificar los activos de información y para el estudio de la verificación de seguridad apoyado en las reglas de la ISO 27001, simultáneamente la propuesta de Berrío (2016) es muy interesante, en cuanto al logro de resultados aplicados en las reglas de ISO 27001, en seguida mejora la seguridad de información en las organizaciones y que puede ser adaptado en los requerimientos de la organización.

  El proyecto de Berrío López se relaciona con la investigación, ya que demuestra que al preguntar a los especialistas y afectados se puede lograr identificar los activos de una organización, también dicha metodología le permite estimar y posteriormente elegir los chequeos de seguridad teniendo como base el criterio de los expertos (Berrío López, 2016).
- Proyecto de Luz Moyano y Jazmín Suarez, que lleva por título *"Plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y Soluciones",* se trata de un proyecto especial, aplicado una empresa desarrolladora de software, el objetivo del proyecto fue establecer un SGSI basado en la reglas de la ISO: 27001: 2013 para los técnicas del área tecnológica de la sociedad, para ello, identifica las necesidades y requerimientos de la organización como también las

vulnerabilidades, amenazas, riesgos, de la empresa y define las políticas y controles para mitigar los riesgos.

Durante el progreso del proyecto se aprecia labores de análisis y tratamientos de riesgos empleando etapas de la técnica Ciclo de Deming en coordinación con las metas, estrategias y políticas de la empresa. Especifica cinco capítulos en primer lugar plantea los objetivos del proyecto, en segundo lugar, analiza la situación de la empresa donde detalla la estructura organizacional de la empresa, el tercer lugar gestiona los riesgos de seguridad siguiendo la estructura de la norma, en cuarto lugar, selecciona las estrategias y técnicas controles y políticas de SGSI y por último evalúa el cumplimiento y la madures de la puesta en marcha de la norma ISO 27001.

Este trabajo es pertinente con el proyecto planteado, ya que aborda el desarrollo de la estructura de los 14 dominios de la norma ISO 27001, incluyendo contenidos estadísticos las cuales son adecuadas para analizar los requerimientos de la empresa, asimismo el trabajo fija las bases mínimas para la correcta implementación del SGSI en una empra tecnología. (Moyano & Suárez, 2017)

2.1.2. Antecedentes nacionales

- En el proyecto de Rodrigo Talavera, que presenta a la Faculta de ciencias e ingeniería de la Pontificia Universidad Católica del Perú una tesis titulada *“Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de la Salud de acuerdo a La ISO/IEC 27001-2013”,* como requisito para preferir título Ingeniero de informático.

  El trabajo se centra en el desarrollo, de la distinción y planteamiento de un Sistema de Gestión de Seguridad de la Información para organismo público del departamento de Salud, en el Instituto Nacional Materno Perinatal, Lima, donde desarrolla el plantea de técnica de estudio de gestión de riesgos y el estándar ISO/ FDIS 31000:2000, dicho estándar también es utilizado para valorar los bienes de información de organismo,

seguidamente se apoya de la metodología BPM (Business Process Management) para mapear los procesos del alcance del proyecto, finalmente deduce que existe una brecha significante con la seguridad de información y la responsabilidad de la dirección de involucrarse en la implantación de la norma ISO 27001, y también de la importancia de definir una delegación de seguridad de información, quien es el ente que debe velar por la implantación de la norma.

El trabajo realizado por Talavera, aporta al presente proyecto, la comprensión del desarrollo de la ISO 27001, también cabe recalcar la importancia de la creación de un comisión de seguridad de información que el cuál debe ser el encargado de la implantación de la norma ISO 27001, y de la seguridad de información, el presente proyecto se plantea crear un una comisión de seguridad de información que será el responsable del desarrollo de la seguridad de información, la elaboración del proyecto de seguridad de información, orienta la utilización de indicadores para medir la eficacia de la ISO 27001 en una institución del sector público. (Tavalera, 2015).

- El trabajo de Jaime Vázquez, que presenta a la Facultad de Ingeniería Industrial de la Universidad Nacional Mayor de San Marcos para preferir Título Profesional de Ingeniero Industrial, el tesis que lleva de nombre *"Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI"*, Lima Perú.

  Este trabajo establece los lineamientos básicos para una correcta implementación de SGSI bajo las reglas de la ISO 27001:2013 en los procesos de tecnología de información de la empresa GMD®, la organización administra plataformas tecnológicas y mesa de ayuda de sus clientes ONP (La Oficina de Normalización Previsional). El proyecto de investigación tiene como objetivo de proteger la información en sus tres perspectivas: confidencialidad, integridad y disponibilidad mediante la implementación de una metodología de riesgos, para ello se basa en un trabajo es descriptivo y aplicativo y de diseño experimental, toma muestras

a una población de 56 personas utilizando las técnicas de encuestas, análisis documentario y auditorías, así mismo, realiza un análisis de brechas conocido como GAP para establecer la comparación de los procesos de negocio con los lineamientos o requisitos internacionales.

Seguidamente concluye destacando que el modelo de gestión de invulnerabilidad de la información ISO 27001:2013 permite salvaguardar la información de diversas amenazas mediante el logro de las metas de seguridad, menciona que si la metodología de gestión se aplica de manera correcta, permite establecer los bienes o activos de información más significantes para el negocio, de la misma manera concluye que el personal es un factor importante por ellos es necesario concientizar con la seguridad de información.

Esta investigación aporta al proyecto ya que se destaca por utilización de técnicas y métodos por el ejemplo el método GAP que sirve para determinar las brechas entre los procesos y los lineamientos o requisitos internacionales, conduce y orienta a profundizar en otros aspectos de la de la Norma ISO 27001 (Vázquez, 2018).

- El trabajo de Juan Guzmán, en su proyecto titulado *"Elaboración de un marco de referencia para la implementación de la norma ISO/IEC 27001:2013 y ley de protección de datos personales en la dirección de admisión de la Universidad Nacional del Santa"*, se refiere a un trabajo que tiene como objetivo establecer una marco teórico al grado de procesos, tecnológicos y legales para la puesta de funcionamiento de las reglas de la ISO/IEC 27001, bajo la ley de protección de datos personales para lo cual se basa en la metodología BPMN 2.0 (Notación de procesos de negocio) que consiste en graficar los métodos de negocio en un modo de trabajo, lo cual permite tramitar de forma conveniente las funciones, recursos y servicios.

  De la misma manera se apoya del modelo de evaluación de la madurez CMMI y la tendencia propuesta por la Ley de Protección de Datos Personales. Llegando a la conclusión de obtener un inventario de procesos

que permite a la dirección a gestionar sus funciones y recursos de manera oportuna.

Este trabajo también se relación con la investigación ya que aborda temas de protección de Datos Personales aplicando métodos de análisis con diagrama de procesos, el cual permite gestionar los procesos de manera oportuna llegando a obtener un inventario de procesos. El proyecto que se desarrolla tomará en cuenta la de protección de datos de los usuarios de la organización bajo el reglamento de las leyes actuales, en ese sentido el trabajo de (Guzman, 2015) servirá de apoyo para el presente proyecto.

- Trabajo final César Augusto, Berríos Mesía y Martín Augusto Rocha Cam, que presentan a la Faculta de ingeniería de la Universidad Peruana de Ciencias Aplicada para optar Título de Ingeniero de Sistemas, el proyecto se titula *"Propuesta de un modelo de Sistema de Gestión de la Seguridad de la Información en una pyme basado en la norma ISO/IEC 27001",* el propósito del proyecto consistió en realizar un ofrecimiento de un modelo de Gestión de Seguridad para una empresa IT Expert, que se encargada de brindar servicios de TI, basado en la norma ISO/IEC 27001.

  En el desarrollo del trabajo se apoyan del método GAP para definir y aclarar la situación actual de la empresa, seguidamente desarrolla la propuesta SMESEC que está estructurado en tres partes las cuales son: gobierno, operación y la inspección, cada una de las sesiones dividen la estructura de la norma ISO 27001 con el firme propósito de desarrollar cada una de las partes de la norma. Seguidamente para analizar los riesgos de invulnerabilidad de información se basa en tres técnicas las cuales son: diversa propuesta de ideas, estudio de posibles factores críticos de éxito, juicio de experto, estos métodos permitieron ubicar y tratar los riesgos de seguridad de información.

  El proyecto llega a la conclusión que el desarrollo del modelo SMESEC soluciona la carencia de un SGSI en las microempresas del Perú, seguidamente que la correcta aplicación del modelo anteriormente

mencionado permite gestionar de manera correcta un plan de SGSI en una micro empresa, también, permite aminorar los costos y medios, dado que se brindan guías, modelos para la adecuada protección de los activos de información.

El proyecto desarrollado por los autores mencionados en al inicio del cuarto antecedente, también se tomará en cuenta en el desarrollo del presente proyecto, sobre todo en la parte del análisis de la situación actual de una organización conocido como análisis GAP. (Berríos Mesía & Rocha Cam, 2018)

2.2. Bases teóricas.

2.2.1. Sistema de Gestión Integral de la Seguridad de Información

SGSI son siglas utilizadas para referirse a un Sistema de Gestión de la Seguridad de la Información, en inglés: Information Security Management System, ISMS. Según la definición de la Organización Internacional de Normalización ISO (2018).

a) Conceptos de seguridad de información

Un SGSI es una perspectiva sistemática para administrar información reservada de una compañía, con el propósito de que permanezca seguro. Incluye individuos, técnicas y sistemas de TI por medio de la utilización de un modo de gestión de riesgos. Puede contribuir a pequeñas, medianas y grandes empresas de cualquier dedicación, a mantener seguros sus bienes de información. Menciona (BSI, 2013).

Se podría definir que el SGSI es un método de gestión que sirve para entender, gestionar y aminorar los riesgos que pueden vulnerar la seguridad de la información en las empresas (López Neira, Agustín; Ruiz Spohr, 2012).

La seguridad de la información, según ISO 27001, se refiere a la protección de la confidencialidad, integridad y disponibilidad, de los activos de información en los sistemas contenidos en su procedimiento, en una empresa u organización.

b) Beneficios del SGSI

Según ISOTools Excellence Chile (2016), un Sistema de gestión de Seguridad de la Información aporta a la empresa los siguientes beneficios.

- Aminora los riesgos que producen perdidas, robos, corrupción o manipulación de la información en las organizaciones.
- Otorga a la organización una garantía frente a clientes y socios, ya que, muestra a los mismos como un organismo que se encarga por la confidencialidad e invulnerabilidad de la información que es depositan.

- Consiente a la empresa realizar su producción con tranquilidad en caso de que ocurra problemas significantes.
- Favorece la reducción de los costos y un mejor funcionamiento de los procesos.
- Favorece a la organización frente a la competencia, pues al tener planificado un sistema de gestión de seguridad de información aumentar su imagen a nivel nacional o internacional de una empresa.
- seguridad y principios claros para el equipo de trabajadores de la organización.
- Concordancia con la normativa vigente sobre datos personales, propiedad intelectual y otras.
- Instauración de una metodología de gestión de la seguridad bien definida.
- Posibilidad de unirse con otros sistemas de gestión (ISO 9001, ISO 14001)

c) Amenazas de la información

Se puede definir como algo que es capaz explotar una vulnerabilidad para obtener, modificar o impedir el acceso a un activo o comprometerlo (Carpentier, 2016), las amenazas surgen cuando existen las fragilidades, es decir un amenaza puede encontrarse solo cuando hay una vulnerabilidad que puede ser utilizada. También pueden existir varias amenazas para cada vulnerabilidad.

Según Carpentier (2016), las amenazas se pueden clasificar según el origen o fuente, tipo, motivación o acción. En la figura N° 1 se muestra la clasificación de las amenazas según el autor anteriormente mencionado.

Figura N° 1. Clasificación de las amenazas

Fuente: Carpentier (2016), La seguridad informática en la PYME

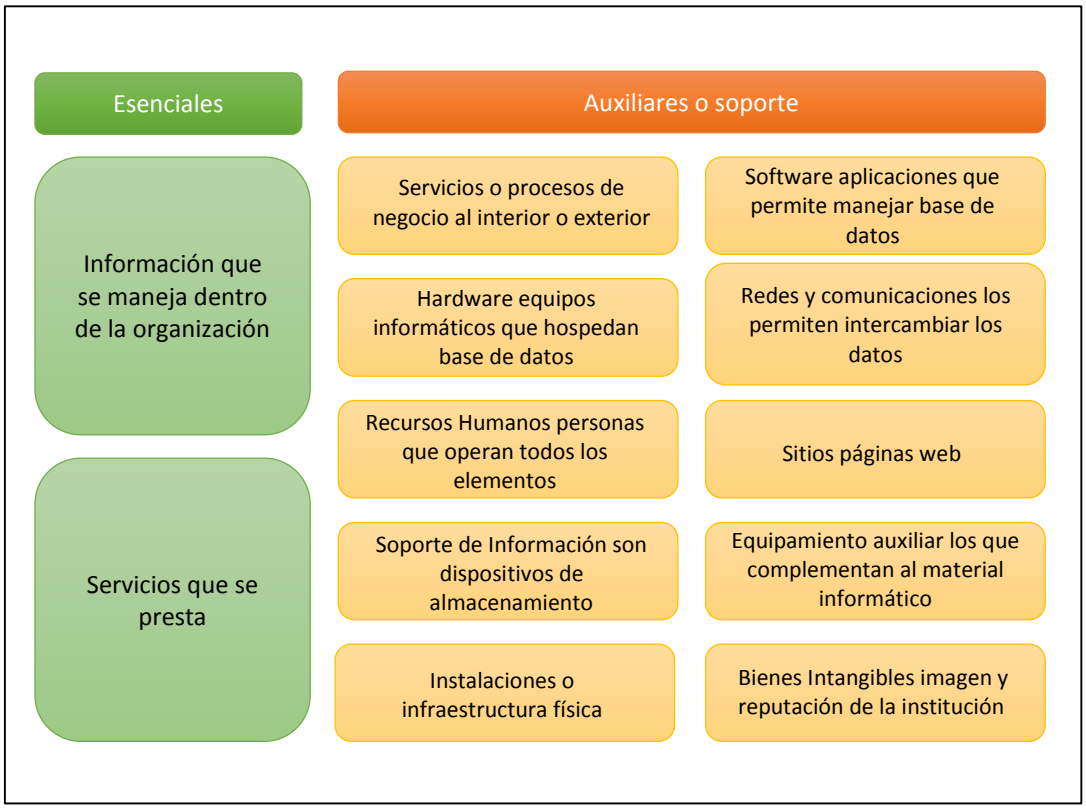
d) Activos de información

De acuerdo a la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT V3, un activo se define como:

"Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos" (Electrónica Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración, 2012, pp. 22-23).

En la figura N° 2 se muestra a manera de resumen los activos de información según la Metodología MAGERIT, donde clasifica de la siguiente manera: activos esenciales y activos relevantes o de soporte.

Figura N° 2. Clasifican de activos de información



Fuente: Elaboración propia

e) Riesgos de la información

Según el comité de Electrónica Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración (2012), un riesgo es la estimación del nivel de exhibición a que una amenaza se concrete sobre uno o más activos ocasionando daños o perdidas a la empresa.

Los riesgos se pueden clasificar según sus orígenes pueden ser externos e internos, a continuación se muestra la clasificación de riesgos según (Carpentier, 2016).

- **Riesgos externos**

  Los ataques dirigidos. Puede ser la infección de virus o ataques globales a la red (denegación de servicio).

  Ataques no dirigidos. Los riesgos físicos (robo o destrucción material) o lógicos accesos de intrusos.

- **Riesgos internos**

  Son más fáciles de entender ya que pertenecen a los recursos internos de la organización.

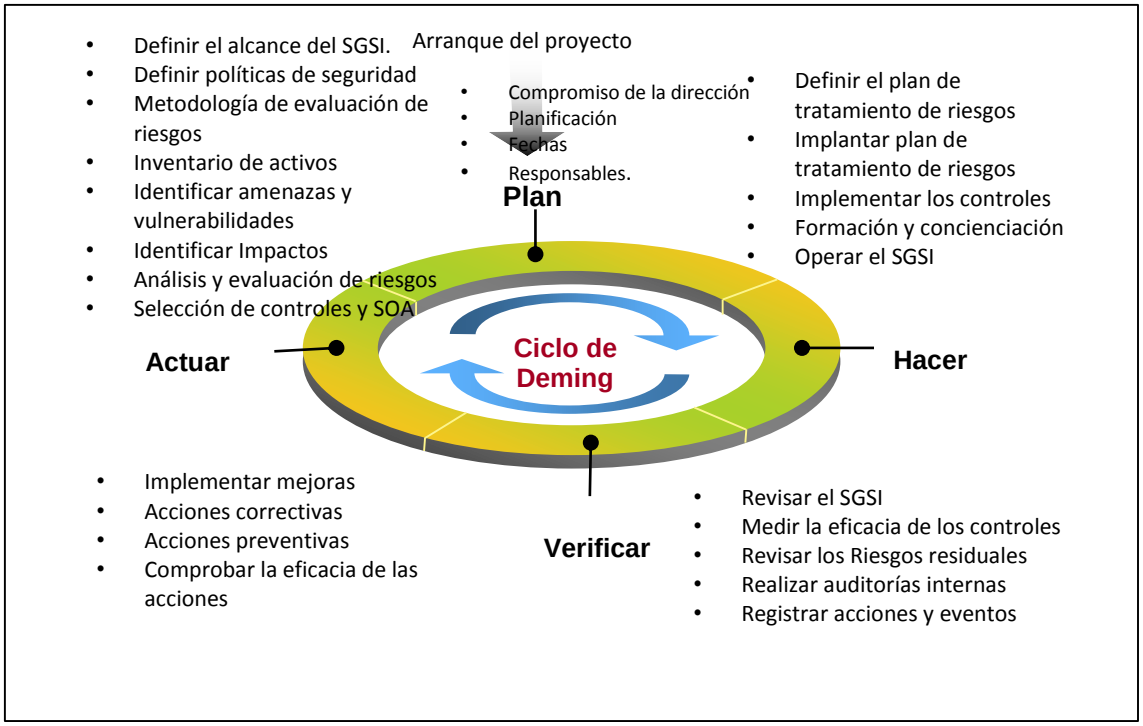
2.2.2. Ciclo de Deming métodos de gestión

Anteriormente la norma ISO 27001 exigía el uso del modelo de Ciclo de Deming, más reconocido como PDCA (del inglés plan, do, check, act, en español es planificar, hacer, verificar, actuar), para crear un SGSI, después de la actualización del año 2013, la Norma ofrece mayor flexibilidad en cuanto a la elección de metodologías tales como todos de administración ITIL o COBIT 5. Según Vinod et al., (2015), considera las siguientes tareas en cada una de las etapas PDCA:

- Plan (instaurar el SGSI): establecer el alcance, la política de seguridad, los objetivos, las metas y los procesos relevantes y examinar el riesgo para llevar a cabo una valuación de riesgos para mejorar la seguridad de la información de modo que ofrezca resultados de acuerdo a las políticas y objetivos generales de la organización.
- Hacer (llevar a cabo y ejecutar el SGSI): llevar a cabo y ejecutar la política de seguridad, y los controles que se eligieron como conclusión del proceso de evaluación de riesgos, así como las técnicas y procedimientos del SGSI, también la asignación de funciones y responsabilidades, asignación de fondos y presupuestos, documentación, gestionar equipos.
- Verificar (monitorear y revisar el SGSI): evaluar y supervisar todas las metas y el proyecto de gestión de servicios, cuando corresponda, determinar la realización del proceso en contraposición con la política de seguridad, los objetivos y la experiencia práctica, y reportar los efectos a la administración para su revisión. Esto incluirá medir la efectividad del sistema de gestión y los controles que implementación.
- Actuar (mantener y mejorar el SGSI): elegir operaciones correctivas y preventivas, con base a los efectos de la revisión de la administración, para la mejora continua.

En la Figura N° 3, se puede visualizar el ciclo de Deming que sirve para gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001:2013.

Figura N° 3. Ciclo de Deming



Fuente: ISO27000. Gestión de Seguridad de la Información, (www.iso27000.es)

2.2.3. Principios de la seguridad de información

Un programa de seguridad puede tener diversos objetivos, grandes o pequeños, pero los principios más importantes en todos los programas de estabilidad son la confidencialidad (exclusividad), la integridad y disponibilidad. Según Hintzbergen, Hintzbergen, Smulders, & Baars, (2015), estos principios que se mencionan se conoce como el triángulo CIA. El nivel de seguridad requerido para explicar estos principios es diferente para cada empresa, pues cada una estas empresas tienen sus propios objetivos, requisitos de negocio y de seguridad. En la figura N° 4, se ilustra el triángulo CIA.

Figura N°4. Triangulo de CIA

Fuente: Elaboración Propia

Definimos cada uno de las de los fundamentos de seguridad de información según el autores Hintzbergen et al., (2015).

- Confidencialidad. La confidencialidad también llamado exclusividad asegura en mantener en secreto cada elemento de procesamiento de datos e impide la divulgación no autorizada. Por ejemplo, los ejecutivos pueden estar preocupados por la protección de sus planes estratégicos de su empresa en relación con sus competidores, por otro lado, las personas pueden estar preocupados por el acceso no autorizado de sus registros financieros. La confidencialidad puede ser fortalecida a través de la criptografía de datos que a medida son amenazados y transmitidos aprovechando el tráfico de redes, también se puede aprovechar el control de acceso a personas autorizadas, etc.
- Integridad. La integridad se refiere a la no alteración del estado de los datos. Cualquier modificación no autorizada de datos, ya sea deliberada o accidentalmente, es una violación de la no alteración de los datos. Por ejemplo, se espera que los datos almacenados en el disco no sean alterados aleatoriamente por problemas con los controladores de disco, de

forma similar se espera que los programas de las aplicaciones graven información correcta y no introduzcan datos diferentes a los deseados. Algunos ejemplos de medidas de integridad. Cada usuario debe ser registrado en la base de datos, de esa manera puede ser determinado quien modificó los datos.

- Disponibilidad. Se considera que la información tiene que estar al alcance cuando sea necesario, las características de disponibilidad son: la oportunidad (consiste que la información esté utilizable o libre cuando se requiera), continuidad (consiste que el equipo puede seguir trabajando en caso de alguna falla), robusto (se refiere que existe capacidad suficiente para permitir que todo el equipo trabaje en el sistema). Ejemplo tanto una falla en el disco como un acceso denegado al servicio causan violación de disponibilidad. Cualquier atraso que se exceda a nivel de servicio esperado para un sistema puede ser considerado como una violación de disponibilidad, la disponibilidad también puede ser afectado por falla de un dispositivo o software, para eso los dispositivos de backup deben ser utilizados para sustituir rápidamente al sistema crítico.

2.2.4. ISO 27001

a) Historia

El punto de arranque para la gestión de seguridad estandarizada en el procesamiento de la información se encuentra, sin duda, en el continente europeo. En el año 1901, aparece la primera institución de estandarización a nivel mundial, BSI (British Standards Institution, la organización británica), que es el encargado de la difusión de las normas esenciales.

El Estándar Británico BS 7799 de BSI, que se emitió en el año 1995, constaba de dos divisiones; la primera división (BS 7799-1), constituye un Código de buenas aprendizajes o prácticas, que contiene una pequeña cantidad de información, medidas y mejores ejemplos para la seguridad de la información que se publicó en el mismo año. La segunda parte (BS 7799-

2) se publica por primera vez en el año 1998, se titula Especificación de SGSI, describe en forma de especificaciones un modelo de un SGSI.

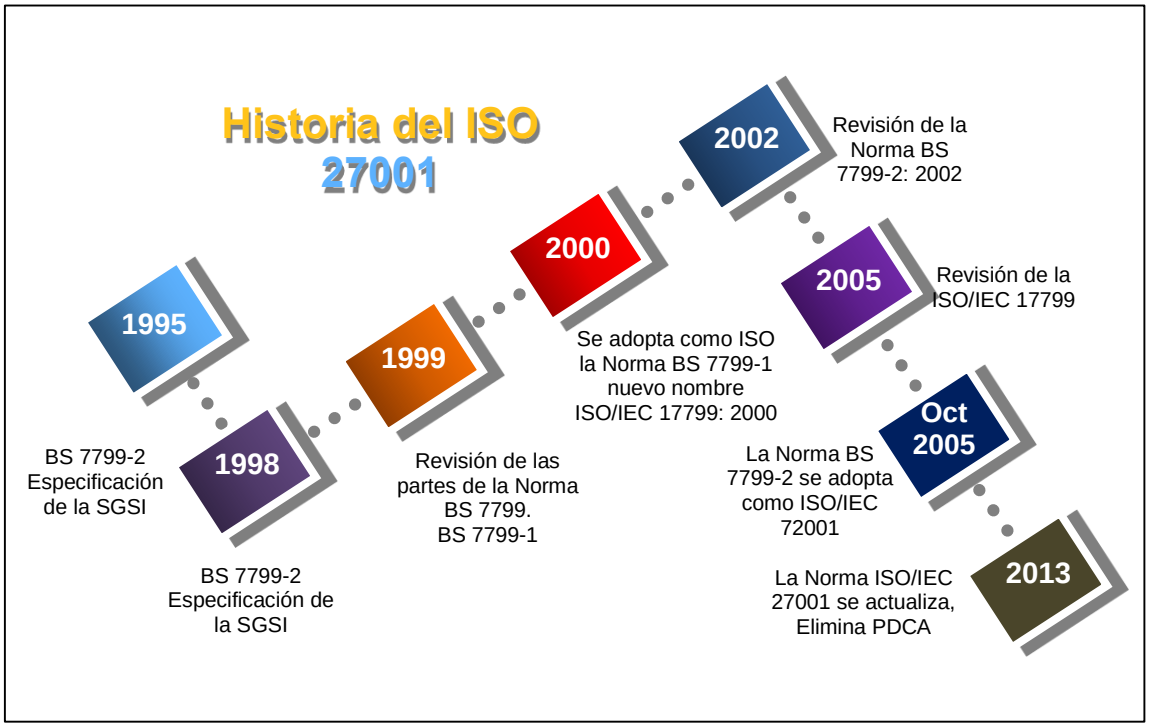
Como paso intermedio, las dos divisiones de la norma BS 7799 se examinaron en el año 1999 y la Norma BS 7799-1 se incorporó en el ISO 17799 en el año 2000. Posteriormente en el año 2002, se actualizo la Norma BS 7799-2 para acomodarse a las normas ISO de sistemas de gestión, donde se incorpora el Ciclo Deming PDCA (del inglés plan, do, check, act).

En el año 2005, con más de 1700 organizaciones autentificadas en BS 7799-2, se publica por la ISO, con algunas modificaciones, como la norma ISO 27001. Al mismo tiempo se renueva ISO 17799. Este último estándar se cambia de nombre como ISO 27002:2005 el 1 de Julio de 2007.

En el año 2013, se publica el actual norma ISO/IEC 27001:2013, donde no se encuentra la sección “Enfoque a procesos”, que definía la metodología de trabajo según el Ciclo Deming de mejora continua, también cambia la estructura conforme al Anexo SL que es común para otras normas ISO, permitiendo que la integración de sistemas sea un trabajo más sencillo, entre otros.

En la figura N° 5, se muestra un breve resumen de la historia de ISO 27001 e ISO 17799 al año 2013. El año 2013 se ha propagado la actual versión de la ISO 27001 donde hubo muchas modificaciones significativos en su forma o estructura, evaluación y tratamiento de los riesgos, estos cambios se tratarán más a detalle posteriormente.

Figura N° 5. Historia y evolución del ISO 27001



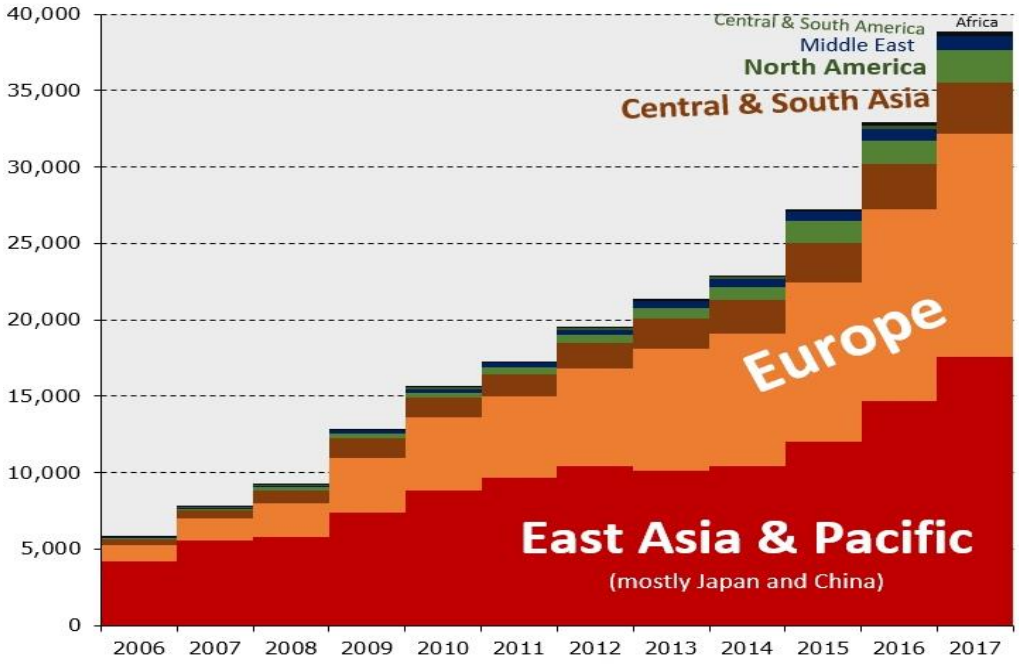
Fuente: Elaboración propia

b) Certificaciones ISO 27001

La organización internacional de normalización (ISO) cada año elabora un informe denominado El ISO Survey, (Encuesta ISO), donde muestra la evolución de las certificaciones de sistema de gestión en el mundo.

En la Figura N° 6 se visualiza los certificados emitidos por la ISO 27001 en todo el mundo hasta el año 2017, donde la norma ISO/IEC 27001 se reafirma a nivel mundial como un alusivo de calidad, muchas organizaciones están preocupadas por la seguridad de su bienes de información y la seguridad en todas las cadenas de suministro o red. Según la encuesta ISO para 2017, hay alrededor de 40,000 certificados ISO / IEC 27001 en todo el mundo, que aumentan en un 20% anual. Noticebored, (2018).

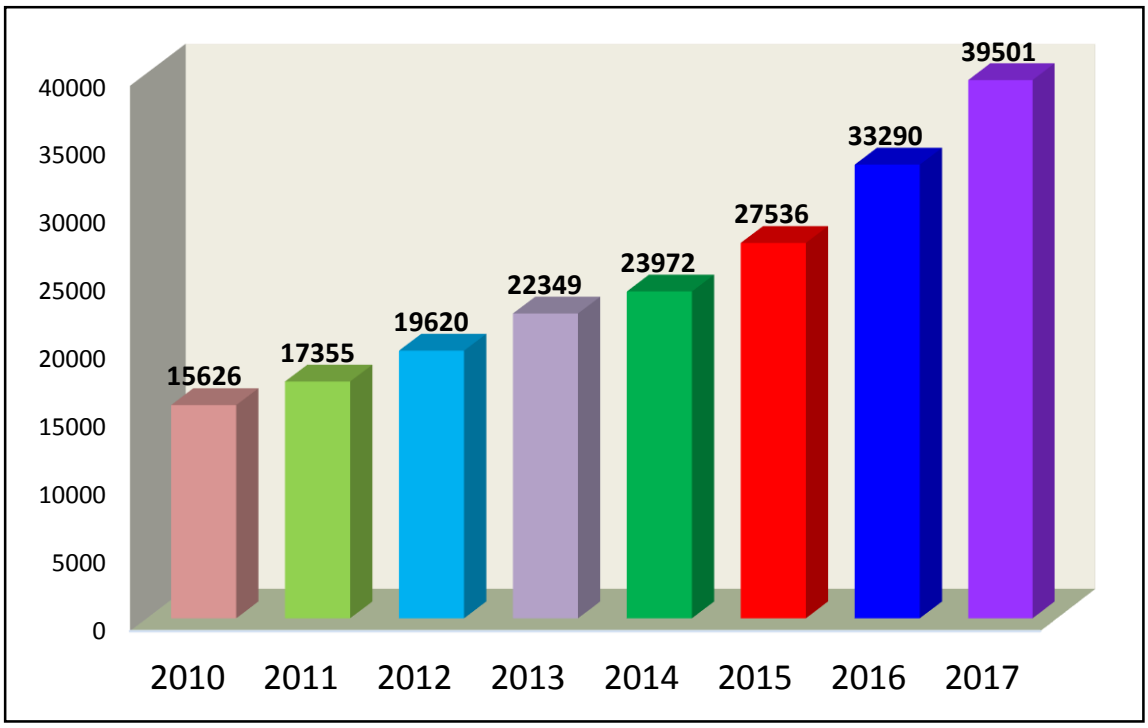
Figura N° 6. Certificados ISO 27001 en todo el mundo



Fuente: Noticebored (2019) ISO/IEC 27001 Certification standard, (www.iso27001security.com)

De acuerdo a los datos de Asociación Española de Normalización, (2016), en la figura N° 7, se muestra el crecimiento de certificación de la norma ISO 27001 durante el periodo 2010 hasta el año 2017 realizado en todo el mundo en más de 200 países de todos continentes, donde se evidencia el aumento de número de empresas que apuestan por la certificación de la norma, ya que, la certificación ayuda a proteger y reforzar los sistemas de información de las organizaciones.

Figura N° 7. Evolución de la ISO 27001 periodo 2010-2017 en el mundo



Fuente: Elaboración propia

Según la publicación de GTDI Tecnología de información y consultoria, (2018), menciona, para el caso de Perú, la cantidad de empresas con certificación válida de la ISO/IEC 27001 en el año 2017 se reporta en una aproximación oficial un total de 43 certificados válidos, en los 5 últimos años el incremento de empresas con certificados ISO 27001 va en aumento.

En Perú poco a poco, más empresas adquieren la certificación nacional o internacional, que los ayuda a posicionarse en los mercados competitivos globales. En el Perú existen muchas empresas certificadoras podemos mencionar algunas de las empresas certificadoras, por ejemplo: ABS Quality Evaluations, AENOR Perú, BV Bureau Veritas, CERPER Certificaciones del Perú S.A, TÜV Rheinland en Perú, SGS Société Générale de Surveillance, INCOTEC.

En la figura N° 8 podemos observar el aumento de empresas con certificación ISO 27001 desde el año 2010 hasta el año 2017

Figura N° 8. Certificados ISO 27001 válido periodo 2010-2017 en el Perú

Fuente: Encuesta ISO - 2017 *(http://www.iso.org)*

2.2.5. Estructura del ISO 27001

La norma ISO 27001 desde su adopción, ha sufrido modificaciones la última revisión fue en el año 2013, que actualmente sigue como la vigente y certificable. A continuación, en la tabla N° 1, se visualiza a modo resumido la conformación de la Norma ISO 27001 versión 2013 según la (Organización Internacional de Normalización ISO, 2013).

Tabla N° 1 Estructura de la norma ISO 27001: 2013

ESTRUCTURA	EXPLICACIÓN
0. Introducción	La norma empieza recomendar sobre el uso, adopción e implementación del SGSI es por la necesidad y los objetivos de la organización, también expone la importancia de la adopción de la norma para que sea parte del diseño de procesos, sistema de información y controles.
1. Alcance	Menciona que las referencias normativas en su totalidad se encuentran en la ISO 27001 y que son indispensables para su aplicación, en ese sentido ya no se tomará como referencia el

	ISO 27002.
2. Referencias normativas	Menciona que las referencias normativas en su totalidad se encuentran en la ISO 27001 y que son indispensables para su aplicación, en ese sentido ya no se tomará como referencia el ISO 27002.
3. Términos y definiciones	Expone que los vocablos y significados que se encuentran en la ISO 27001 figuran en ISO / IEC 27000.
4. Contexto de la organización	**4.1 Comprender la organización y su contexto.** Menciona que se debe establecer los asuntos externos e internos que son importantes para logro de metas y que alteran su capacidad de lograr los objetivos planificados en su gestión de seguridad de información.
	4.2 Comprender las necesidades y expectativas de las partes interesadas. La empresa debe establecer las partes más importantes para la gestión de seguridad de información y las condiciones de estas partes más importantes.
	4.3 Determinar el alcance de SGSI. La empresa determina los límites y la aplicabilidad del SGSI para considerar el alcance, aspectos internos y externos, los vínculos de las actividades realizadas por la organización, el alcance debe estar disponible como información documentada.
5. Liderazgo	**5.1 Liderazgo y compromiso.** Los directivos deben demostrar ejercicio de liderazgo y obligación con respecto al SGSI. Como, Asegurando que las estrategias de seguridad y los objetivos de seguridad de información sean compatibles, asegurando los sistemas de seguridad de información en los procesos, comunicando la importancia de una gestión de seguridad.
	5.2 Política. Los directivos deben establecer políticas de seguridad de información apropiadas, que incluyan objetivos, que satisfaga las exigencias aplicables con concordancia a la seguridad de información, que forma parte compromiso y mejora continua, que sea disponible y documentada.
	5.3 roles responsabilidades y autoridades

	organizacionales. Los directivos deben asignar la responsabilidad y autoridad a la persona encargada para asegurar que el SGSI esté conforme, y reportar el desempeño del SGSI
6. Planificación	**6.1 Acciones para generar riesgos y las oportunidades.** La planificación del SGSI, se toma en cuenta la situación actual de la empresa, el alcance, y las faltas de carencias de las partes interesadas para tratar de asegurar los resultados esperados, prevenir y reducir los efectos indeseados. También se planifica para tomar acciones a los riesgos.
	6.2 Objetivos de seguridad de información y planificación. La empresa debe implantar objetivos de seguridad de información que sean medibles, consistentes, apropiados. También debe planificar como va lograr ese objetivo los recursos que va utilizar, quien será el responsable, y como terminará.
7. Soporte	**7.1 Recursos.** La organización establece los recursos importantes para el establecimiento e implementación del SGSI.
	7.2 Competencia. La sociedad u organización determina quién es la persona encarga para realizar el SGSI y también debe asegura que esta persona sea competente y con experiencia, debe retener información adecuada como certeza de competencia.
	7.3 Concientización. El equipo de trabajo que laboran en la empresa debe conocer la política de seguridad de información, y contribuir con la efectividad del SGSI.
	7.4 Comunicación. La organización debe establecer las carencias de comunicación interna y externa importantes para la SGSI debe saber que comunicar, cuando, a quien y quienes deben comunicar.
	7.5 Información documentada. El SGSI debe incluir información importante y que sea documentada por la organización sobre la efectividad del SGSI, tamaño de la

	organización, complejidad de procesos y otros.
8. Operación	**8.1 Planificación y control operacional.** La asociación u organización debe planificar e implementar y controlar los procesos importantes y necesarios para lograr los requisitos de la organización, para eso debe mantener la información documentada, y controlar los cambios planificados, también debe revisar los efectos de estos cambios, del mismo modo debe mantener que los procesos tercerizados son determinados y controlados.
	8.2 Evaluación de riesgos de seguridad de la información. La organización debe realizar evaluaciones de los riesgos en tiempos definidos tomando criterios establecidos, y debe retener información documentada de estos riesgos de seguridad de información.
	8.3 Tratamiento de riesgos de seguridad de información. La empresa debe establecer un plan de tratamiento de riesgos y también retener información documentada del tratamiento de riesgos.
9. Evaluación de desempeño	**9.1 monitoreo, medición, análisis y evaluación.** La empresa debe estimar el desempeño de la seguridad de información a través de monitoreo, medición de los procesos y controles de seguridad de información, aplicando métodos análisis de evaluación.
	9.2 Auditoria Interna. La empresa u organización debe realizar auditorías internas cada intervalo de tiempos definidos para verificar la conformidad. La organización también debe planificar, implementar auditorias, definir criterios y alcance de auditorías.
	9.3 Revisión de gerencia. La dirección debe revisar el SGSI para asegurar su conveniencia y adecuación y continuar incluyendo cambios en asuntos externos e internos, retroalimentación sobre el desempeño.
10. mejora	**10.1 No conformidad y acción correctiva.** Cuando ocurre la

	no conformidad se debe tomar acciones para controlar y corregir, también se revisa la eficiencia de cualquier acción correctiva, al realizar cambios en la SGSI.
	10.2 Mejora continua. La empresa debe seguir con la mejora continua con la convivencia y la efectividad del SGSI.

Fuente: Elaboración propia

2.2.6. Cambios de la norma ISO/IEC 27001

La norma ISO 27001 ha sido revisada y publicada en octubre de 2013, los cambios de la norma se reflejan en la nueva estructura. Según BSI Group México (2013), muestra en la Tabla N° 2, los principales cambios de la norma en la columna de la izquierda se enlista los títulos de la norma ISO/IEC 27001:2013. Y para contrastar o diferenciar, en la columna derecha expone los títulos de la norma ISO/IEC 27001:2005.

Tabla N°2, Mapeo de las cláusulas ISO 27001:2013 a ISO 27001:2005

ISO 27001:2013	ISO 27001:2005
0. Introducción	**0.** Introducción
1. Alcance	**1.** Alcance
2. Referencias normativas	**2.** Referencias normativas
3. Términos o definiciones	**3.** Términos o definiciones
4. Contexto de la Organización	
4.1 Comprender la organización y su contexto	**8.3** Acciones preventivas
4.2 Comprender las necesidades y expectativas de las partes interesadas	**5.2.1 c)** Identificar y conducir los requerimientos legales y regulatorios y las obligaciones contractuales de seguridad
4.3 Determinar el alcance del sistema de gestión de seguridad de la información	**4.2.1 a)** Define el alcance y los limites **4.2.3 f)** Asegurar que el alcance sea adecuado
4.4 Sistema de gestión de seguridad de la información	**4.1** Requerimientos generales
5. Liderazgo	
5.1 Liderazgo y compromiso	**4.1** Compromiso de la dirección
5.2 Políticas	**4.2.1 b)** Definir una política de SGSI

5.3 Roles organizacionales, responsabilidades y autoridades	**5.1 c)** Establecer roles y responsabilidades para la seguridad de información
6. Planificación	
6.1 Acciones para tratar Riesgos y oportunidades	
6.1.1 Generalidades	**8.3** Acciones preventivas
6.1.2 Evaluación de riesgos de seguridad de la información	**4.2.1 c)** Defina el enfoque de la evaluación de riesgos **4.2.1 d)** Identificar los riesgos **4.2.1 e)** Analizar y evaluar los riesgos
6.1.3 Tratamiento de riesgos de seguridad de la información	**4.2.1 f)** Identifique y evalúe opciones para el tratamiento de riesgos **4.2.1 g)** Seleccionar objetivos de control y controles para el tratamiento de riesgos **4.2.1 h)** Obtener aprobación de la dirección sobre los riesgos residuales propuestos **4.2.1 i)** Preparar un enunciado de aplicabilidad **4.2.1 j)** Preparar un enunciado de aplicabilidad **4.2.2 a)** Formular un plan de tratamiento de riesgos
6.2 Objetivos de seguridad de la información y planeación de los mismos	**5.2 b)** Asegurar los objetivos del SGSI y establecer los planes
7. Soporte	
7.1 Recursos	**4.2.2 g)** Gestión de recursos para el SGSI **5.2.1** Provisión de recursos
7.2 Competencia	**5.2.2** Capacitación, conocimiento y competencia
7.3 Conocimiento	**4.2.2** e) Implementar capacitación y programas de conocimiento **5.2.2** Capacitación, conocimiento y competencia
7.4 Comunicación	**4.2.4** Comunicar las acciones y mejoras **5.1 d)** Comunicar a la organización
7.5 Información documentada	**4.3** Requerimientos de documentación

8. Operación	
8.1 Planeación operacional y control	**4.2.2 f)** Gestionar operaciones es del SGSI
8.2 Evaluación de riesgos de seguridad de la información	**4.2.3 d)** Revisar evaluaciones de riesgos en intervalos planeados
8.3 Tratamiento de riesgos de seguridad de la información	**4.2.2 b)** Implementar el plan de tratamiento de riesgos **4.2.2 c)** Implementar controles
9. Evaluación del desempeño	
9.1 Monitoreo, medición, análisis y evaluación	**4.2.2 d)** Definir cómo medir la efectividad **4.2.3 b)** Tomar revisiones regulares de la efectividad del SGSI **4.2.3 c)** Medir la efectividad de los controles
9.2 Auditoría interna	**4.2.3 e)** Conducir auditorías internas al SGSI **6** Auditorías internas del SGSI
9.3 Revisión de la gestión	**4.2.3 f)** Tomar una revisión de la gestión del SGSI **7** Revisión de la gestión del SGSI
10. Mejora	
10.1 No conformidades y acciones correctivas	**4.2.4** Mantener y mejorar el SGSI **8.2** Acciones correctivas
10.2 Mejora continua de la información	**4.2.4** Mantener y mejorar el SGSI **8.1** Mejora continua

Fuente: BSI Group México (2013)

2.2.7. Documentos y registros requeridos en la ISO 27001:2013

A continuación, se presenta las peticiones para la seguridad de información, documentada que están distribuidos en la Norma ISO/IEC 27001. Según BSI Group México (2013), en esta de verificación se visualiza los documentos y la lista de registros que se necesitan en el estructura principal de la Norma y son obligatorios para la ISO 27002:2013. Se puede establecer varias formas de documentación. Pero, no se necesitan a todos. En tabla N° 3, se mencionan los documentos obligatorios según la norma ISO 27001.

Tabla N° 3 Información documentada de la ISO/2013 27001

DOCUMENTOS	**CAPITULO ISO 27001:2013**
Alcance del SGSI	4.3
Políticas y objetivos de seguridad de la información	5.2 - 6.2
Metodología de evaluación y tratamiento de riesgos	6.1.2
Declaración de aplicabilidad	6.1.3.d
Plan de tratamiento del riesgo	6.1.3.e - 6.2
Informe sobre evaluación y tratamiento de riesgos	8.2 - 8.3
Definición de funciones y responsabilidades de seguridad	A.7.1.2 - A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos operativos para gestión de TI	A.12.1.1
Principios de ingeniería para sistema seguro	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5
Procedimientos de la continuidad del negocio	A.17.1.2
Requisitos legales, normativos y contractuales	A.18.1.1

Fuente: BSI Group México (2013)

2.2.8. NTP ISO/IEC 27001: 2014

En el Perú la ISO 27001 se conoce como la Norma Técnica Peruana NTP ISO/IEC 27001:2014 Tecnología de la Información. Esta norma técnica de seguridad de la Información. Presenta requisitos en su 2ª Edición. La norma es emitida bajo la resolución ministerial Nº 004-2016-PCM publicado por el diario peruano el 8 de enero del año 2016, donde se resuelve el uso obligatorio de las reglas de la norma en todas las instituciones integran al Sistema Nacional de Informática con un plazo de 2 años para su adopción de la norma, también se resuelve que las entidades que desean certificarse bajo lo establecido en la Norma Técnica Peruana, para realizar la certificación es de manera opcional y con su propio economía (Comité Técnico de Normalización de Codificación Norma Técnica Peruana, 2014).

La Norma Técnica Peruana reemplaza a la NTP ISO/IEC 27001: 2008 (examinado el año 2013) y es una norma adoptada de ISO/IEC 27001:2013.

La norma técnica peruana también presentó cambios en su estructura fundamentalmente en la terminología que se emplea por el propio del idioma español y ha sido dividida en concordancia a las Guías Peruanas GP 001:1995 y GP 002: 1995.

En la figura N° 9, se presenta la estructura de la Norma Técnica Peruana ISO/IEC 27001:2014

Figura N° 9. Estructura de la NTP ISO/IEC 27001:2014

Fuente: Comité Técnico de Normalización de Codificación Norma Técnica

2.2.9. Normas Generales

Las normas generales son una guía para gestionar la seguridad de información en una organización, se ha creado un conjunto de estándares

bajo el nombre de ISO/IEC 27000. A continuación se mencionan una lista de serie de normas de referencia que van desde van de 27000 hasta 27019, según Carpentier(2016), estas ayudan a gestionar los riesgos de seguridad de información.

- ISO/IEC 27000: 2014, esta norma proporciona los términos y definiciones que se emplean en toda la serie 27000 y aporta las bases de por qué es importante la implantación de un SGSI.
- ISO/IEC 27001: 2013, es la norma principal de la serie que proporciona los requisitos del sistema de gestión de seguridad de la información, esta norma corresponde al principio de certificación de las organizaciones. En el Anexo A, de esta norma se enumera en forma de resumen los objetivos de control que desarrolla la ISO 27002:2005.
- ISO/IEC 27002: 2013, es una guía de descripción de las mejores prácticas que describe los objetivos de control y controles recomendables en cuanto a la seguridad de información. No es certificable.
- ISO/IEC 27003: 2017, es una guía que se centra en el diseño e implementación detallada de un SGSI de acuerdo ISO/IEC 27001. Describe el proceso de especificación y diseño desde la concepción hasta la puesta en marcha de planes de implementación, así como el proceso de aprobación de la dirección para implementar un SGSI. No certificable.
- ISO/IEC 27004: 2016, contiene la norma que establece el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI. No certificable.
- ISO/IEC 27005: 2018, establece las directrices para la gestión del riesgo de seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001 e incluye los consejos sobre la aplicación satisfactoria de seguridad de la información basada en un enfoque de gestión de riesgos. No certificable.
- ISO/IEC 27006: 2015, guía que describe los requisitos para realizar la acreditación de entidades de auditoría y certificación de sistemas de gestión

de seguridad de la información que han obtenido la certificación ISO/IEC 27001. No es una norma de acreditación por sí misma.

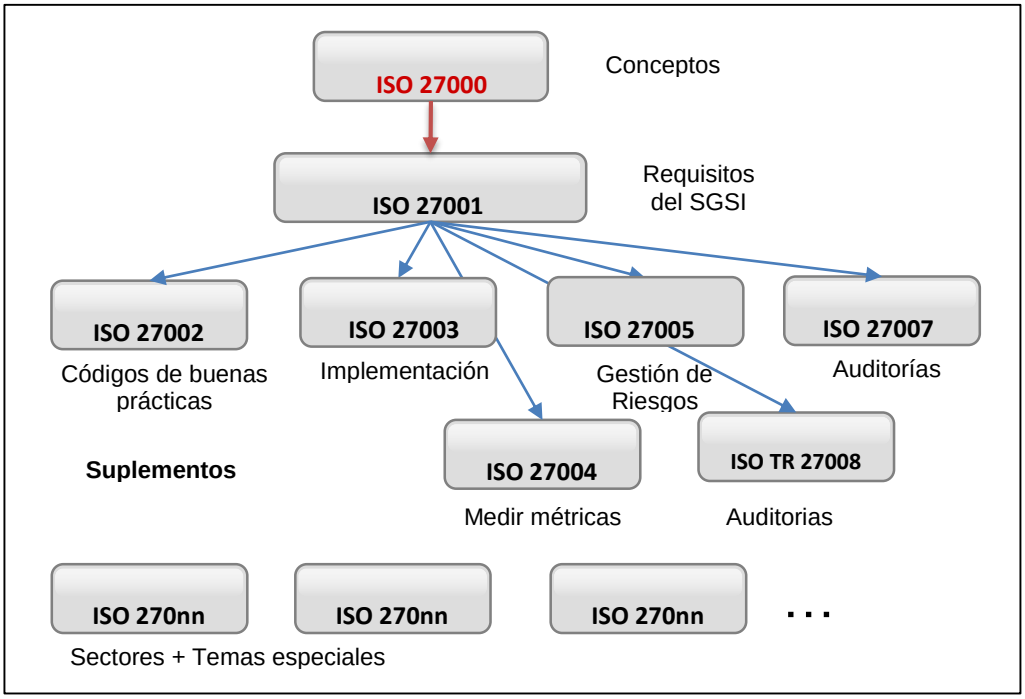
- ISO/IEC 27007: 2017, Es una guía de auditoría de sistemas de gestión de seguridad de información (SGSI), es una herramienta destinada a las auditorias de un SGSI interno o externo para ayudar en la comprensión y ejecución de la auditoria que se va realizar. No es certificable.
- ISO/IEC TR 27008: 2011, es una guía de auditoría de controles de seguridad, se centra en la forma en que se implementan las comprobaciones de un SGSI. No es certificable.
- ISO/IEC 27009: 2016, define los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector específico. Explica cómo incluir requisitos adicionales a los de ISO / IEC 27001, cómo refinar cualquiera de los requisitos de ISO / IEC 27001 y cómo incluir controles o conjuntos de control además de ISO / IEC 27001. No es certificable.
- ISO/IEC 27010: 2012 es la guía que proporciona la gestión de la seguridad de información para las comunicaciones entre las empresas del mismo sector industrial, en diferentes sectores de la industria y con los gobiernos, ya sea en tiempos de crisis o para proteger la infraestructura crítica o para cumplir con las normativas legales.
- ISO/IEC 27011: 2016, guía de interpretación de la implementación y gestión de la seguridad de la información, en el sector de telecomunicaciones basadas en ISO/IEC 27002. (también como norma ITU- 1051)
- ISO/IEC 27013: 2013, guía para la integración de la implementación, la alineación y coordinación entre ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
- ISO/IEC 27014: 2013, Consiste en una guía de gobierno corporativo de la seguridad de la información, mediante la cual las organizaciones pueden evaluar, dirigir, monitorear y comunicar las actividades relacionadas con la seguridad de la información.
- ISO/IEC TR 27015: 2012, guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.

- ISO/IEC TR 27016: 2014, una guía de valoración de los aspectos financieros de la seguridad de la información.
- ISO/IEC 27017: 2015, guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.
- ISO/IEC 27018: 2014, es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.
- ISO/IEC TR 27019: 2017, guía con referencia a ISO/IEC 27002:2005 para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía.
- ISO/IEC 27032: 2012, proporciona orientación para la mejora del estado de seguridad cibernética.
- ISO/IEC 27033: 2010, Norma dedicada a la seguridad en redes.
- ISO/IEC 27035: 2011, guía sobre la gestión de incidentes de seguridad en la información. Consta de tres partes principios en la gestión de incidentes, guías para la elaboración de un plan de respuesta a incidentes, guía de operaciones en la respuesta a incidentes.
- ISO/IEC 27039: 2015, es una guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión (IDS/IPS).
- ISO/IEC 27038: 2014, es una guía de especificación para seguridad en la redacción digital.
- ISO/IEC 27040: 2015, es una guía para la seguridad en medios de almacenamiento.
- ISO/IEC 27041: 2015, es una guía para la garantizar la idoneidad y adecuación de los métodos de investigación.
- ISO 27799: 2016. Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002.

En la siguiente figura N° 10, se puede observar la multiplicidad de estas normas, que nos ayuda a obtener una buena información sobre el estado actual de todas las normas. según Kersten, Reuter, & Schröder (2013),

podemos visualizar que la norma 27000 de términos básicos se utiliza en la mayoría de las normas.

Figura N°10. Resumen de la serie de normas 27000



Fuente. Kerten, Reuter, & Schröder, (2013), IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz

La ISO 27001 ha continuado, y continúa, emitiendo otras normas dentro de la serie 27000 que sirvan de apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie. La Norma ISO/IEC 27000 publicado el 1 de mayo de 2009, es un conjunto de estándares desarrollados por la ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional), que proporciona una visión general y vocabulario sobre sistemas de gestión de seguridad de la información.

2.2.10.Metodologías de gestión de riesgos

Existen muchas metodologías de análisis de gestión de riesgos A continuación, se presenta un resumen de algunas metodologías para la gestión de riesgo según artículos científicos de López & Ruiz, (2012).

a) ***OCTAVE***. (Operationally Critical Threat, Asset, and Vulnerability Evaluation) es una metodología de evaluación de riesgos desarrollada por el Software Engineering Institute (SEI) de la Carnegie Mellon University. Los beneficios de esta metodología son:

- Identificar los riesgos de seguridad de la información que pueden
- impedir el logro de objetos de la organización
- Enseña a evaluar los riesgos de seguridad de información.
- Crea estrategias de protección con el din de reducir los riesgos
- Ayuda a la organización cumplir las regulaciones de la seguridad de información.

b) ***ISO 27005*** es el estándar ISO de la serie 27000 dedicado a la gestión de riesgos de seguridad de la información. La norma provee las directrices para la gestión de riesgos de seguridad de la información en una organización, apoyado en el sistema de gestión de seguridad de la información definidos en ISO 27001.

c) ***ISO 31000*** es un Estándar ISO internacional que ofrece las directrices y principios para gestionar el riesgo de las empresas, y tiene como objetivo que todas las organizaciones de todo tipo sin importar el tamaño puedan gestionar los riesgos de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente, tiene como actividades: alcance, términos y definiciones, principios, framework y procesos.

d) ***COSO ERM*** es una metodología que proporciona un marco de gestión de riesgos, generalmente este método implica identificar los eventos o circunstancias, la evaluación es en términos de magnitud de impacto y probabilidad que determinan la estrategia de respuesta.

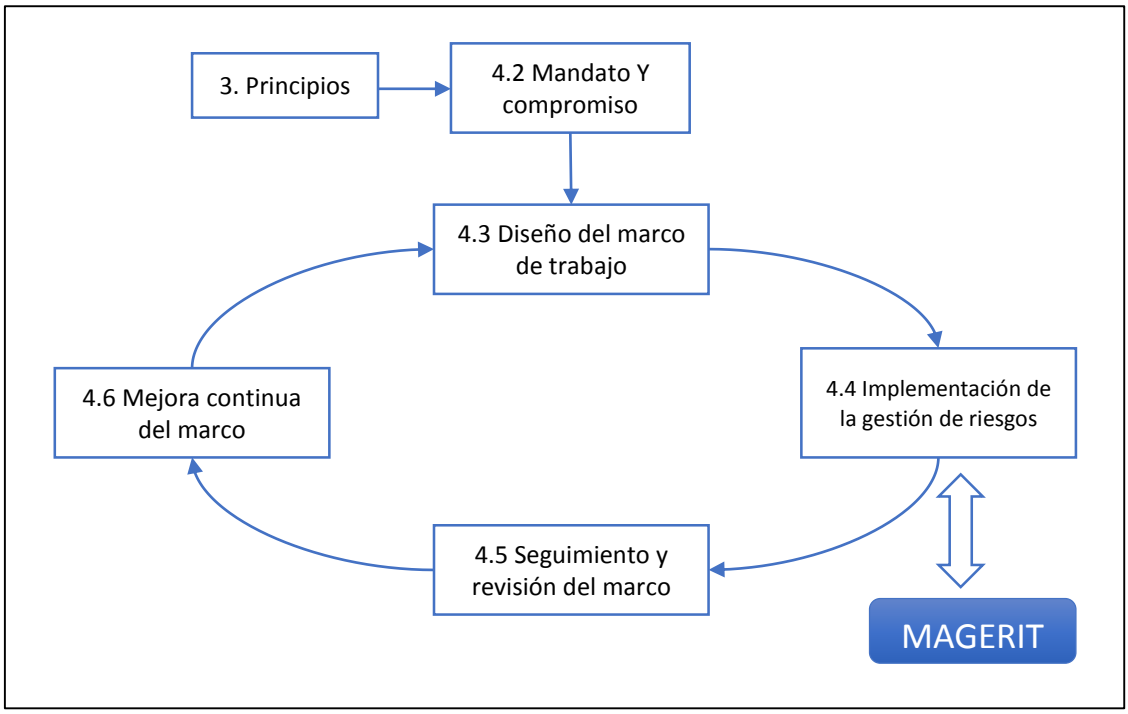
Podemos encontrar muchas otras metodologías para el análisis y gestión de riesgos en el proyecto propuesto se utilizará la metodología de análisis de riesgos conocido como MAGERIT, que a continuación se detalla más profundamente.

2.2.11.Metodología MAGERIT

Metodología MAGERIT de Análisis y Gestión de Riesgos de los Sistemas de Información, es fomentada por el Ministerio de Administraciones Públicas de España. Esta metodología, responde a lo que se denomina “Proceso de Gestión de los Riesgos” siguiendo al término de la ISO 31000. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno que tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Electrónica Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración, (2012)

En el presente proyecto si utilizara la metodología MAGERIT para poder analizar y gestionar los riesgos de la seguridad de información, en la figura N° 11, se ilustra el marco de trabajo para la gestión de riesgos según la metodología mencionado anteriormente.

Figura N° 11. Marco de Trabajo para gestionar los riesgos



Fuente: ISO 31000 Marco de trabajo de gestión de riesgos

Según la metodología MAGERIT, persigue los siguientes objetivos según Portal de Administración Electrónica España (2013), menciona lo siguiente líneas abajo.

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos.
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

2.2.12.Estructura de la Metodología MAGERIT.

La metodología MAGERIT versión 3 se ha estructurado en tres libros: Método, Catálogo de Elementos y Guía de Técnicas. (Portal de Administración Electrónica España, 2013). A continuación, se detalla cada uno de ellas.

a) Métodos

Según Portal de Administración Electrónica España (2013), se muestra la estructura del libro de métodos consta de los siguientes capítulos.

- El capítulo 2 presenta los conceptos básicos de la gestión de riesgos. En particular se presentas las actividades de análisis y tratamiento dentro de un proceso integral de gestión de riesgos.
- El capítulo 3 se menciona los pasos y las actividades de análisis de gestión de riesgos.
- El Capítulo 4 se describe las opciones y los criterios para el tratamiento de los riesgos, seguidamente se formalizan las actividades de gestión de riesgos.
- El capítulo 5 se realiza proyectos de análisis de gestión de riesgos, para realizar análisis de gestión de riesgos.

- El capítulo 6 se formaliza las actividades para los planes de seguridad o planes estratégicos.
- El capítulo 7 se centra en el desarrollo de sistemas de información y análisis de riesgos sirve para gestionar la seguridad del producto final desde su inicio hasta poner en marcha o producción.
- El capítulo 8 se anticipan a los problemas que aparecen recurrentemente cuando se realizan los análisis de riesgos.

Los apéndices recogen material de consulta.

- Glosarios
- Referencias bibliográficas
- Referencias al marco legal de las tareas de análisis y gestión de administración pública española.
- Marco normativo de evaluación de certificación

b) Catálogo de elementos

Según el Portal de Administración Electrónica España (2013), la metodología MAGERIT en un libro aparte se proponen un catálogo para marcar las 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

Se persiguen dos objetivos

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

c) Guía de técnicas

En un libro aparte se adiciona la orientación de algunas técnicas que se emplean habitualmente para llevar a cabo proyectos de análisis y gestión de riesgos.

- Técnicas específicas para el análisis de riesgos
- Análisis mediante tablas
- Análisis algorítmico
- Árboles de ataque
- Técnicas generales
- Técnicas gráficas
- Sesiones de trabajo: entrevistas, reuniones y presentaciones

Valoración Delphi Se trata de una guía de consulta. Según el lector avance por la tarea del proyecto, se le recomendará el uso de ciertas técnicas específicas.

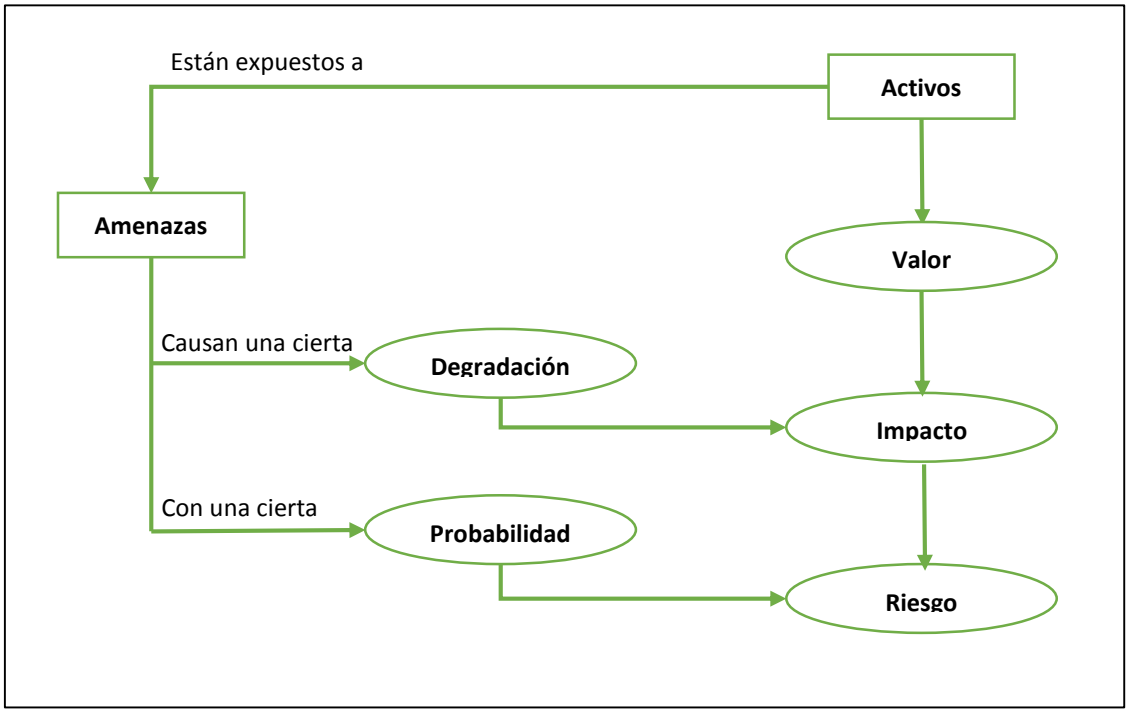
2.2.13.Método de análisis de riesgos MAGERIT

Según la Metodología MAGERIT el análisis de riesgos es una aproximación metódica para determinar el riesgo siguiendo ciertos pasos:

- El primer paso es determinar los activos de importantes de la Organización, su interrelación y valor, en el sentido de qué perjuicio o cuánto costaría su degradación.
- El segundo paso es determinar a qué amenazas están expuestos aquellos activos.
- Tercer paso es determinar qué medidas hay disponibles y cuales son eficaces para frenar los riesgos de la organización.
- Cuarto paso es estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- Quinto paso es estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

La siguiente figura N° 12, recoge los pasos a seguir en la metodología de MAGERIT

Figura N° 12. Elementos del análisis de riesgos potenciales



Fuente: Metodología MAGERIT V3

a) Tipos de activos

Según la metodología de MAGERIT los activos se clasifican en esenciales, datos, servicios, Software, hardware, redes de comunicaciones, soporte de información, equipamiento auxiliar, instalaciones y personal. En la tabla N° 4, se detalla cada una de los activos anteriormente mencionados.

Tabla N° 4. Tipos de activos

Tipo de Activo	Explicación
[Esenciales] Activos Esenciales	Los activos esenciales marcan los requisitos de seguridad para todos los demás componentes del sistema.
[D] Datos	Los datos es el corazón de la organización ya que permite prestar sus servicios. Es un activo abstracto que será almacenado en equipos o soportes de información

[S] Servicios	Son activos que satisfacen una necesidad de los usuarios (el servicio). Esta sección contempla servicios prestados por el sistema
[SW] Aplicaciones Informáticas (Software)	Son denominados (programas, aplicativos, desarrollos, etc.). Sirven para automatizar, gestionar, analizar datos
[HW] Equipamiento Informático (Hardware)	Son medios materiales, físicos, destinados a soportar directa o indirectamente los servicios que presta la organización
[COM] Redes de Comunicaciones	Son instalaciones dedicadas como servicios de comunicaciones contratados a terceros
[Media] Soporte de Información	Son dispositivos físicos que permiten almacenar información de forma permanente
[AUX] Equipamiento Auxiliar	Son equipos que sirven de soporte a los sistemas de información, sin estar directamente relacionados con datos
[I] Instalaciones	Son lugares donde se hospedan los sistemas de información y comunicaciones
[P] Personal	Son las personas relacionadas con los sistemas de información

Fuente: Metodología MAGERIT V3

b) Dimensiones de valoración de un activo

Las dimensiones de la seguridad de información En la tabla N° 5, se detalla las dimensiones de la valoración de un activo:

- **La confidencialidad:** responde a la pregunta ¿Qué daños puede causar que lo conociera quien no debe? Esta valoración es típica de datos.
- **La integridad:** responde a la pregunta ¿Qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración también es típica de los datos, que pueden estar manipulados, total o parcialmente.
- **La disponibilidad:** responde a la pregunta ¿Qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios

Tabla N° 5. Dimensiones de los activos

Código	Confidencialidad	Descripción
R	Restringido	Sólo personas autorizadas de la organización
I	Uso Interno	Personal de la organización o terceros autorizados

P	Uso Público	Dispuesto para el público en general
Código	**Integridad**	**Descripción**
S	Sensible	Activo que requiere controles estrictos para su protección
N	Normal	Activo que requiere controles habituales para su protección
B	Baja	Activo que requiere controles mínimos para su protección
Código	**Disponibilidad**	**Descripción**
MA	Muy Alta	Tiempo tolerable de interrupción menor a 2 h
A	Alta	Tiempo tolerable de interrupción mayor a 2 h y menor a 4 h
M	Media	Tiempo tolerable de interrupción mayor a 4 h y menor a 1 día
MB	Media Baja	Tiempo tolerable de interrupción mayor a 1 día y menor a 2 días
B	Baja	Tiempo tolerable de interrupción mayor a 2 días y menor a 5 días

Fuente: Metodología MAGERIT V3

c) Valor cualitativo de un activo

Según la metodología MAGERIT las escalas cualitativas permiten avanzar con rapidez, y posicionar el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como “órdenes de magnitud” y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

En la Tabla N° 6, se observa a valoración cualitativa de los activos de información según la metodología

Tabla N° 6. Valoración cualitativa de los activos

Código	Valor de activo	Descripción
MA	Muy Alto	Nivel Confidencialidad: Restringido
		Nivel Integridad: Sensible
		Nivel Disponibilidad: Muy Alta
A	Alto	Nivel Confidencialidad: Restringido
		Nivel Integridad: Sensible
		Nivel Disponibilidad: Alta
M	Medio	Nivel Confidencialidad: Uso Interno
		Nivel Integridad: Normal

		Nivel Disponibilidad: Media
B	Bajo	Nivel Confidencialidad: Uso Público
		Nivel Integridad: Baja
		Nivel Disponibilidad: Media Baja
MB	Muy Bajo	Nivel Confidencialidad: Uso Público
		Nivel Integridad: Baja
		Nivel Disponibilidad: Baja

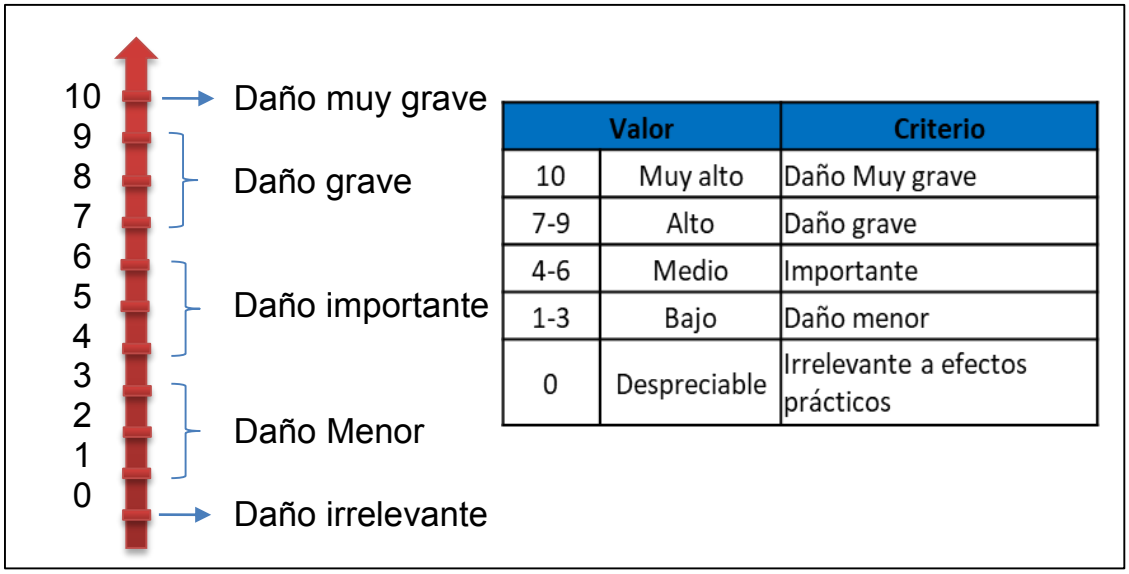
Fuente: Metodología MAGERIT V3

d) Valoración de activos

Para valorar los activos de información según la metodología MAGERIT en su libro II de catálogo de elementos, expone para efectos prácticos una escala común para todas las dimensiones, permitiendo comparar riesgos con criterio homogéneo que permitirá comparar análisis realizados por separado.

En la figura N° 13, se muestra los valores de los riesgos de información,

Figura N° 13. Valoración dimensión de la seguridad



Valor		Criterio
10	Muy alto	Daño Muy grave
7-9	Alto	Daño grave
4-6	Medio	Importante
1-3	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente: Metodología MAGERIT V3

el valor 0 sería un valor despreciable (a efectos de riesgo).

e) Amenazas

La amenaza consiste en la causa potencial de un incidente que puede causar daños a un sistema de información o a una organización.

En la Tabla N° 7, se visualiza la clasificación de amenazas de los activos según la metodología MAGERIT.

Tabla N° 7. Tipo de Amenazas

Tipo de Amenazas	Descripción
[N] Naturales	Son sucesos que pueden ocurrir sin intervención de los seres humanos, pueden ser terremotos, inundaciones, fuegos, sismos, etc.
[IN] Origen Industrial	Son sucesos que pueden ocurrir de forma accidental, o por la actividad humana de tipo industrial, pueden ser de origen accidental o deliberado
[E] Errores y fallos no intencionados	Son fallos no intencionales causados por las personas. Pueden ocurrir de manera accidental.
[A] Ataques intencionados	Fallos deliberados causados por las personas. Son ataques deliberados con alguna intención

Fuente: Metodología MAGERIT V3

f) Valoración de las amenazas

Según la metodología MAGERIT cuando un activo es atacado por una amenaza, no afecta a todas sus dimensiones, ni en la misma cantidad. Una vez que se ha determinado una amenaza que puede dañar un activo, se tiene que valorar su influencia en el valor de los activos en dos sentidos de degradación y probabilidad.

En la Tabla N° 8, se visualiza la degradación de valor de los activos según la escala cualitativa.

Tabla N° 8. Degradación del valor

MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

Fuente: Metodología MAGERIT V3

2.3. Definición de términos básicos.

- **Activo.** Es todo aquello que tenga valor para la organización.
- **Análisis de riesgos**. Proceso que consiste en comprender la naturaleza del riesgo y estimar su magnitud (Anticona Tupia, 2013).
- **Activo de información.** Es el activo que constituye información importante para los procesos de la empresa, tales como registros, procesamientos, almacenamientos o transmisión de esta información (Anticona Tupia, 2013).
- **Autenticidad.** Es la propiedad que permite que los usuarios o responsables de manipular la información deban demostrar su identidad es decir quién es el autor.
- **Amenazas.** que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
- **Batch.** Archivo magnético que tiene almacenado una secuencia de comandos que al ejecutarse reemplaza la operación de digitar los comandos en secuencia cada vez que se requiere efectuar una operación. Se utiliza para almacenar operaciones repetitivas.
- **Confidencialidad**. Es el atributo que nos permite que la información se divulgue y sea manejada o difundida por personas que tengan derechos o autorización sobre ellas, esta característica hace referencia de ocultar o mantener en secreto la información. (Anticona Tupia, 2013).
- **Control.** Son las políticas, los procedimientos, y las estructuras organizativas utilizadas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. (López Neira, Agustín; Ruiz Spohr, 2012).
- **Control correctivo.** Es el control que corrige un riesgo, cometido por error, omisión o deliberadamente antes de que produzca pérdidas importantes. (López Neira, Agustín; Ruiz Spohr, 2012).
- **Control preventivo.** Es el control que evita que se produzca un riesgo, error u omisión. Impide que una amenaza llegue siquiera a materializarse.(López Neira, Agustín; Ruiz Spohr, 2012)
- **Disponibilidad.** Cualidad de la información que consiste que la información sea accesible para su uso cuando se la requieran por personas autorizadas en

todo momento. El objetivo de esta característica es prevenir interrupciones no autorizadas de los recursos informáticos.

- **Declaración de aplicabilidad.** Es el documento se enumera los controles aplicados por el SGSI en una organización tras el resultado de los procesos de evaluación y tratamiento de riesgo. (López Neira, Agustín; Ruiz Spohr, 2012).
- **Degradación.** Consiste cuán perjudicado resultaría el valor de un activo.
- **Evento de seguridad de la información.** La ocurrencia detectada en un estado de un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.
- **Evaluación de riesgos.** Consiste en dar un paso más allá del análisis técnico y traduce las consecuencias a términos de negocio. Aquí se trata de factores de percepción, de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no. (Electrónica Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración, 2012).
- **Firewall.** Dispositivo tecnológico que tiene como función proteger la red interna de una organización de accesos no autorizados del exterior vía Internet.
- **Inventario de activos**. Conformado por los activos de información que tiene valor para la empresa y que están dentro del alcance del Sistema de Gestión de Seguridad de la Información existente. (ISOTools Excellence, 2014)
- **Integridad.** propiedad de proteger la exactitud y la integridad de los activos. El concepto de integridad asegura que se prevean modificaciones al software y al hardware que no se efectúen modificaciones no autorizadas a los datos, por personal autorizado o no autorizado y/o proceso, y que el dato sea internamente y externamente consistente. (Hintzbergen et al., 2015).
- **Identificación de riesgos**. Proceso de encontrar, reconocer y caracterizar los elementos de riesgo.
- **Impacto.** Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

- **Mapa de riesgos**. Es la relación de las amenazas que pueden afectar a los activos. Según MAGERIT.
- **No repudio.** Es la propiedad que garantiza el intercambio y transferencia de la información entre distinta ubicación geográfica usando la tecnología, se diferencia dos tipos de no repudio. El no repudio de origen y no repudio de destino, el primero garantiza que la persona que envía el mensaje no puede negar que es el emisor, ya que el receptor tendrá pruebas de envió y el segundo del mismo modo. El recepto por no podrá negar que recibió el mensaje, porque el emisor tiene pruebas. (Anticona Tupia, 2013).
- **No conformidad.** Es el no cumplimiento de un requisito.
- **Parte interesada**. Es la persona o empresa que puede afectar, o puede ser afectada por o percibirse a sí misma como afectada por una decisión o actividad. (López Neira, Agustín; Ruiz Spohr, 2012).
- **Plan de tratamiento de riesgos.** Es un documento donde se definen que decisiones se va tomar para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (López Neira, Agustín; Ruiz Spohr, 2012).
- **Plan de seguridad.** Es un conjunto de proyectos de seguridad que van a culminar con decisiones de tratamiento de riesgos. MAGERIT V3.
- **Propietario del activo.** Persona u organización que, con la aprobación gerencial respectiva, tiene la bajo su responsabilidad el control de un activo, su desarrollo, su mantenimiento, y seguridad de los activos.
- **Probabilidad.** Consiste en que tan probable o improbable puede suceder una amenaza.
- **Riesgo.** Es la posibilidad de sufrir daños o pérdidas en una empresa. La amenaza es un componente del riesgo y se puede considerar como: un agente de amenazas, ya sea humano o no humano en la empresa.
- **Red privada virtual – VPN.** Es un medio de conexión por Internet que utilizan los usuarios para conectarse a la red corporativa empleando conexiones públicas, a través de medios seguros de comunicación.

- **Salvaguardar.** Son acciones de protección que debe extenderse para frenar aquellas amenazas para que no causen mas daño.
- **Seguridad de información.** Preservación de la confidencialidad, integridad y disponibilidad de la información. (López Neira, Agustín; Ruiz Spohr, 2012).
- **Tratamiento de riesgos.** Son proceso de toma de decisiones frente a los riesgos con el propósito de modificar los riesgos.
- **Vulnerabilidad.** Tiene que ver con la debilidad que puede afectar una amenaza a un activo.

CAPÍTULO III: DISEÑO DEL PLAN DE SEGURIDAD DE INFORMACIÓN

3.1. Desarrollo del trabajo propuesto.

En el presente capítulo se realiza el trabajo de diseño un plan de seguridad de información según las reglas de la Norma ISO/IEC 27001: 2013, el modelo a seguir como se ha indicado en el apartado anterior, será Ciclo de Deming de gestión del sistema invulnerabilidad de información. Las dos primeras partes de del trabajo de suficiencia corresponden a las fases del Ciclo vida de Deming.

La modelo para analizar los riesgos de seguridad de información estará bajo la metodología de MAGERIT que permitirá determinar los puntos críticos y vitales de la organización, de esta manera se logrará el cumplimiento de los objetivos de la empresa, que es crear relaciones duraderas con los clientes, tanto internos como externos.

3.1.1. Situación actual de la empresa

Loyalty, se creó por iniciativa de Shell, el cual tenía en varios países donde operaba un área de fidelización para sus clientes, en Perú convoco a las empresas y marcas para hacer un programa de fidelización para sus clientes, en este caso convocaron a Wong, Delosi (KFC, PH). En principio se crearon varios nombres y al final quedo Bonus. Bonus es el nombre comercial de Loyalty Perú S.A.C, Bonus inicio sus operaciones un 15 de febrero de 1998 y gracias a los socios ha quedado posicionado en los clientes, hasta la actualidad ya lleva 21 años en el mercado.

La empresa inició su actividad en un pequeño local situado en San Borja, después de un plan más ambicioso se mudó a un edificio situado en Monterrico, en donde se ubica hasta el día de hoy. El año 2004 la tarjeta Bonus ya estaba posicionada en el mercado, cada vez que se consumía gasolina en los Grifos Shell y cuando se realizaba las compras en Wong. En ese año sólo existía una tarjeta que competía con Bonus conocida como tarjeta Más Más de Santa Isabel, pero al no estar aliada a otras marcas perdió fuerza, hasta desaparecer.

En el año 2007 se acepta por acuerdo de Directorio manejar programas de Fidelización e Incentivos para otros negocios que no sean competidores de las marcas Asociadas a Bonus, para evitar conflictos de Intereses, es donde se comienza a manejar marcas que continúan hasta la actualidad como Alicorp, Nestlé, Cosapi, Tasa, San Fernando, Molitalia, etc.

En la actualidad la empresa se encuentra como líder en su rubro teniendo como competencia a Promotick y a otras agencias que ofrecen el servicio de Fidelización, pero no tienen la logística necesaria para cubrir todo lo que el rubro requiere. Loyalty tiene productos potentes, la cual es una ventaja como carta de presentación.

Loyalty, como lo mencionado anteriormente, es una empresa dedicada a la creación de programas de fidelización e incentivos para sus cliente B2B, Distribuidores, Mayoristas, Minoristas, Fuerza de ventas y también B2E para colaboradores internos, desarrolla y administra dichos programas de lealtad para cada necesidad, a continuación se explica en que consiste dicho programas.

- programa B2B (Business to Business), negocios entre empresas, tiene como objetivo lograr mayor inserción de las marcas en el mercado, está dirigido a empresas mayoristas, minoristas y fuerzas de ventas.
- programa B2C (Business to Consumer) negocios donde el consumidor final es el cliente, su objetivo es cambiar a través de marketing los hábitos de compra sus clientes y está dirigido a consumidor final de Bonus y Claro.
- programa B2E (Business to Employee) negocios entre empresa con sus empleados, su objetivo retener el talento humano a través de premios y reconocimientos dirigidos a fuerzas de ventas y empleados.

En la actualidad la empresa tiene como accionistas a las siguientes empresas: Cencosud 42.5%, Primax parte del grupo Romero 42.5% y el grupo Delosi que maneja franquicias como (KFC, Pizza Hut, Chili’s, Burger King, Pink Berry, Madam Tusan y Olive Garden) 15% (Ruperto, 2016).

La empresa se desempeña en el sector económico de asesoramiento empresarial consultoría, brinda servicios como outsourcing donde planifica e

implementa los programas de fidelización, soporte tecnológico a través del cual opera centros de cómputo para procesar los datos, infraestructura y logística cuenta con más de 60 puntos de canje en el ámbito nacional, economía de escala entrega anualmente gran cantidad de premios productos importados de distintos países, cuenta con 311 trabajadores activos.

En la figura N° 14, se muestra los principales socios de Loyalty Perú SAC que también se les denomina socios, la empresa es conocida más por su nombre comercial Puntos Bonus.

Figura N°14. Principales socios de Loyalty Perú SAC

Fuente. Elaboracion propía

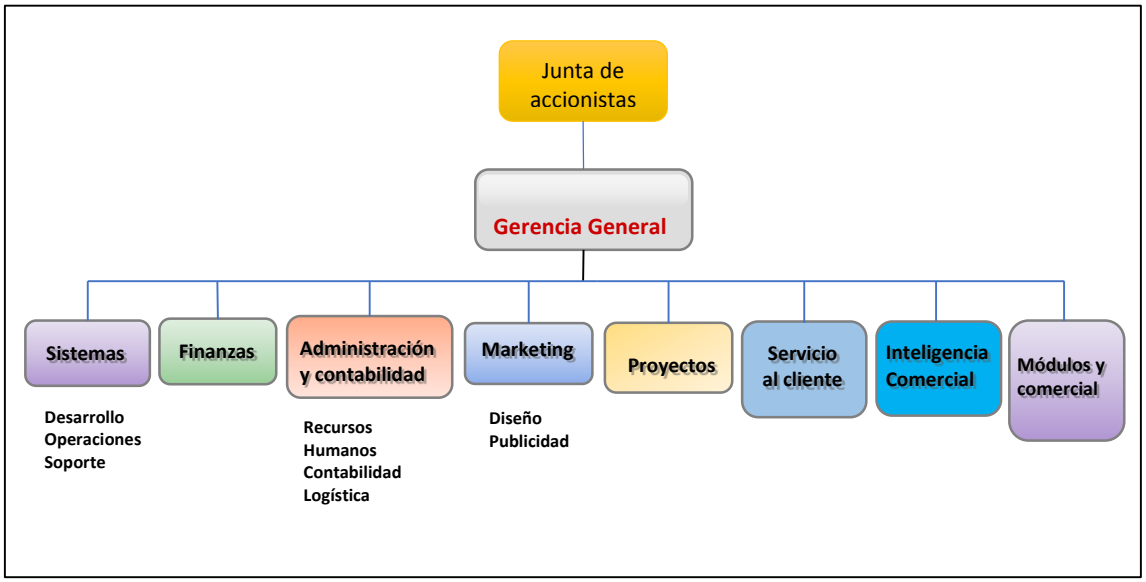
Loyalty actualmente cuenta 5 millones de clientes activos y desarrolla una plataforma de trabajo que consiste en identificar los problemas y oportunidades luego planifica diseña procesos finalmente lo implementa soluciones de plataforma tecnológica.

3.1.2. Estructura organizacional

Loyalty dispone varios de centros de canje que también se denominan módulos de canje que se encuentra ubicados en las mayorías de los supermercados de Wong, Metro, Paris y centros comerciales. En las tiendas Wong ubicados en diferentes departamentos del Perú, cuenta con 16 módulos de canje, mientras tanto en las tiendas de Metro en las diferentes ciudades del Perú cuenta con 35 módulos de canje, en las tiendas de París cuenta con 2 módulos de canje y en los centros comerciales cuenta con 3 módulos de canje en total cuenta 60 módulos, todos estos módulos son administrados desde la oficina principal, este último se encuentra divididos por áreas.

En la figura N°15, se visualiza la estructura organizacional de la empresa Loyalty que se compone 9 áreas.

Figura N° 15. Estructura organizacional de la empresa Loyalty



Fuente. Elaboracion propía

La oficina principal está conformada por 9 áreas que a continuación se detalla cada una de las estas áreas.

a) ***Junta de accionistas.*** Está compuesta por los socios de la empresa tales como Cencosud, Primax y Delosi donde se toman las decisiones más importantes para el funcionamiento de la organización.

b) ***Gerencia General.*** Compuesta por el gerente general que es el responsable de todas las áreas de la organización.

c) ***Sistemas.*** Esta área tiene un responsable que es el gerente de Tecnología de información que se encarga de gestionar la plataforma tecnológica para mejorar los procesos y servicios de la empresa, que a su vez se subdivide en tres sub áreas: el sub área de desarrollo lo componen 5 desarrolladores, encargados del diseño e implementación de productos software, sub área de soporte lo componen 3 empleados encargados de la asistencia tecnológica de todo los usuarios de la oficina, sub área de operaciones lo componen 4 empleados que se encarga de control y ejecución de los programas de sistema.

d) ***Finanzas.*** Responsable de medir las estrategias estableciendo tiempos definidos para lograr alcanzar los objetivos, controla los resultados cuando la acumulación de puntos esta debajo de lo planificado, procura que los recursos estén disponibles para el desarrollo de tareas.

e) ***Administración y contabilidad.*** Esta área tiene un responsable que es el gerente administrativo, que se encarga asegurar que las actividades administrativas funcionen de manera eficiente tiene a su cargo los siguientes sub áreas. El sub área de recursos humanos que se encarga de reclutar talentos humanos, el sub área de contabilidad que se encarga de operar y lleva a cabo la captación y registro de las operaciones financieras.

f) ***Marketing***. Esta área tiene un responsable que es el gerente de marketing encargado de manejar y operar las estrategias de ventas que a su vez tiene a su cargo dos sub áreas: el sub área de diseño y publicidad.

g) ***Proyectos***. Esta área tiene un responsable que se denomina el jefe de proyectos encargado de los procesos, generalmente relacionados con terceros, tales como el programa de Alicorp, COSAPI entre otros.

h) ***Servicio al cliente***. Esta área tiene dos responsables denominados jefes de servicio de atención al cliente, tiene a su cargo personal o empleado que permite mantener permanentemente en contacto directo con los clientes para atender todas sus consultas, dudas y reclamos.

i) ***Inteligencia comercial.*** Encargado de un responsable de área que es el gerente de inteligencia comercial, tiene a su cargo varios personales que se encargan de procesar la información para la toma de decisiones ya sea para el área de marketing o para el área de gerencia general.

j) ***Módulos y comercial.*** En esta área se encuentra un gerente de comercial que tiene a su cargo 4 supervisores de los módulos o centros de canje que a su vez controlan a todos los operadores de tienda en los distintos puntos de canje en Lima y provincias

.

3.1.3. Misión, Visión y valores

El éxito de Loyalty se debe generalmente al apoyo constante de los Socios y al esfuerzo multidisciplinario y multitareas del equipo humano por el cual está conformado, a continuación se expone la misión, visión, valores de la empresa.

Visión:

"Ser reconocidos como la mejor empresa en operar sistemas de fidelización e incentivos en los mercados nacional"

Misión:

"Servir a los establecimientos/empresas en su esfuerzo de premiación, retención y adquisición de los clientes internos y externos"

Valores:

- Vocación de servicio
- Trabajo en equipo
- Mejora continua e innovación

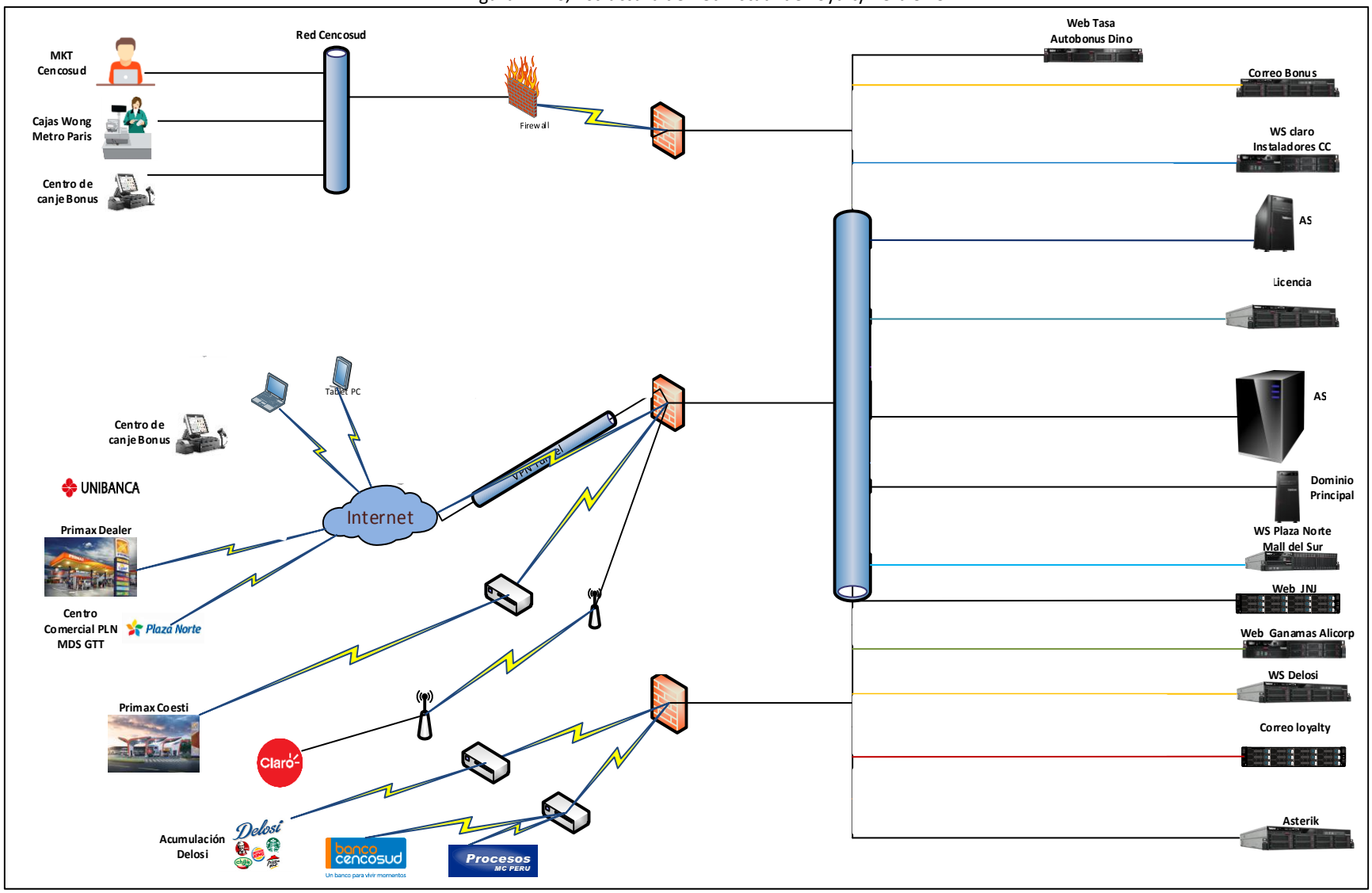
3.1.4. Diagrama de red

En la siguiente sección se muestra la estructura de diseño red de la empresa Loyalty Perú SAC, a alto nivel. En la figura N° 16, se puede observar las interconexiones de la oficina principal con los Puntos de Ventas y los socios de la organización.

La red está compuesta por 3 Check Point que sirven como cortafuegos para controlar el acceso de las computadoras a la red, posee 30 servidores que se detalla en la Tabla N° 9, que describen las características y los servicios que incluye cada servidor. La red tiene conexión con otras redes como: red de Cencosud, Red de Americatel, Red de Primax Coesti, Red de Delosi, entre otros.

Se utiliza una red privada virtual para conectarse de manera segura de una red de área local sobre una red pública o no controlada como el Internet, para comunicarse entre las redes que están fuera del área local.

Figura N° 16, Estructura de Red Actual de Loyalty Perú SAC



Fuente: Elaboración Propia

3.1.5. Alcance de SGSI

Para formalizar el alcance del proyecto debemos identificar los puntos críticos de la organización, ya que nos permitirá conocer e identificar qué información será privilegiada para la protección de los riesgos de información, y también se debe abarcar lo más necesario de acuerdo a los objetivos planteados mostrado en los apartados anteriores. En tal sentido, el SGSI para el presente proyecto abarca el área de sistemas ya que es el área funcional que da la ayuda y el servicio a toda la empresa abarca los demás áreas de la asociación.

El área de sistemas se encarga de gestionar la plataforma tecnológica para revisar los procesos y servicios de la empresa, es el área donde se realizan los procesos más importantes de la organización ya que se encarga de la comunicación, de los proyectos y seguridad de Loyalty.

Esta área funcional comprende:

- ***Área de desarrollo.*** Es el área encargado de desarrollar software para el consumidor final de las demás áreas tales como: sistema para la Administración General del Sistema, sistema para los Módulos de Canje, sistema para los Supervisores de Módulos de Canje, sistema para el área Comercial, sistema para el área de Contabilidad, sistema para el área de Marketing, sistemas para Recursos Humanos, sistemas para el área de Logística, sistema para el área Servicio al Cliente, sistema para las operaciones y sistema para el área de Gerencia, también se desarrolla aplicaciones para los socios y asociados a Loyalty, tales como. Primax. Cencosud, Delosi, Plaza Lima Norte, Mall del Sur, Claro, Pacifico Seguros entre otros.
- ***Área de soporte****:* Es el área encardo de la solución de problemas técnicos de hardware y software en las computadoras a las diferentes áreas de la empresa, el soporte técnico se convierte en indispensable para restablecer la normalidad de las actividades de la organización, esta área también da

ayuda remota a los usuarios que se encuentran en los diferentes módulos de canje de Loyalty, entre otras actividades.

- ***Área de operaciones:*** Es el área encargado de realizar copias de respaldo es un proceso automático mediante el cual se salvaguardan las tablas, configuraciones y valores de todo el sistema que se ejecuta en la plataforma i5, también es el área encargo de las validaciones de las plataformas web, atenciones a usuarios terceros, entre otros.

Las conexiones de red entre equipos, la infraestructura de la empresa, los servicios a terceros, los sistemas de detección de intrusos, también están incluidos en el presente proyecto.

3.1.6. Política de seguridad de información

En esta sección se define algunas medidas, reglas para garantizar la confidencialidad, disponibilidad, e integridad de los bienes y servicios de la información, de la empresa Loyalty Perú SAC, para lo cual se define una política de seguridad a alto nivel, esta política será como una guía para posteriormente plantear otras medidas de acuerdo al tratamiento de riesgos.

Política de seguridad de información de Loyalty

La política de seguridad de Loyalty Perú SAC emerge como una herramienta para capacitar a todos los trabajadores acerca de la importancia y gran valor de la información y todos los servicios importantes, de la mejora de los errores, fallas y de las debilidades, de manera que permita a la empresa cumplir con sus objetivos y su misión.

a) Objetivos.

Para mejorar la calidad de información y la ayuda continua de los servicios supervisando las actividades diarias y aprendiendo, reaccionando con habilidades para frenar los incidentes. La política de seguridad de Loyalty Perú SAC persigue los siguientes objetivos.

- Asegurar la información con la que cuenta Loyalty mediante medidas que sean necesarias para afrontar los riesgos, y así evaluar el impacto

ante un eventual ataque. Si la organización sufre un ataque, se debe reducir los ataques a través de un plan efectivo y planificado

- Establecer controles de seguridad apropiados para cuidar las instalaciones, los equipamientos, el trabajador, el software y tablas de datos ante una posibilidad de una destrucción o perjuicio, ya sea de manera accidental o deliberada. Y de esa manera mantener la totalidad de las operaciones y de los servidores.
- Implementar reglas y procedimientos para afrontar los riesgos identificados para evitar incidentes similares en el futuro.
- Asegurar que los procesos sean planificados previamente, para ser controlados y autorizados por la persona responsable para su respectiva utilización de datos que requieran los usuarios.

b) Alcance.

En base a los lineamientos de la norma ISO 27001, el presente política se aplicará a todos los sistemas de información que sostienen los servicios de:

- Albergue físico de la base de datos, llamado también servidores locales de gestión de información de la empresa y de terceros
- Almacenamiento y mantenimiento de todos los servidores dedicados
- Gestión de copias de seguridad de información.
- Red de comunicaciones.
- Recursos Humanos.
- Gestión de los activos.

Para mejorar el cumplimiento de la política, todo el personal de Loyalty Perú SAC. (Funcionarios, colaboradores, locadores de servicios y otros) están incluidos en el cumplimiento de la política.

c) Comités: funciones y responsabilidades.

Loyalty Perú S.A.C. asigna responsabilidades a un Comité de seguridad integrado por el Gerente General, el Gerente de Tecnologías de la Información, el Gerente de Finanzas y el Gerente de Administración y

Contabilidad que pueden ser complementados por consultores internos o externos cuando se estime conveniente.

El Comité de seguridad reporta al Directorio de la empresa.

Funciones:

- El Comité de Seguridad de la Información se encarga de realizar los mecanismos y canales necesarios para crear el Plan de Seguridad de la Información, debe conocer los reportes de casos y errores, fallas de los sistemas. Asimismo, el Comité, debe estar informado, de cómo se realiza el seguimiento de la investigación, debe evaluar la evolución e impulsará la solución ante cualquier incidente a la seguridad de información.
- Cada integrante del Comité de Gestión de Seguridad de la información, debe asignar a un representante de su área para que tome decisiones como un miembro que reemplaza al titular solamente cuando el titular se encuentre ausente temporalmente y debe ser acreditado, tiene que asistir a las reuniones del Comité, con las mismas responsabilidades, obligaciones del miembro Titular.
- El Comité debe programar una reunión una vez cada 2 meses y debe ser una reunión de mucha importancia, cuando el presidente decida o cuando se presente nuevas necesidades o problemas de seguridad de la información.
- Después de cada sesión se deberá redactar el acta de la reunión las cuales deberán ser firmadas por los participantes y archivadas.

Funciones inherente al cargo:

- Coordinar y aprobar las acciones en materia de seguridad de la información.
- Impulsar el conocimiento en seguridad de la información basándose primordialmente en estándares internacionales ISO.
- Resolver discrepancias y asuntos que suelen suceder en la gestión de la seguridad.

- Proponer y revisar nuevas políticas reglas y estándares para la mejora del sistema de seguridad de la información.
- Establecer los proyectos de cambio en materias de seguridad de la información en aplicaciones o sistemas.

d) Control de Acceso.

- Todos los personales, colaboradores y terceros que trabajan para Loyalty Perú SAC deben tener acceso sólo a la información necesitan para realizar su trabajo.
- Para las personas que no trabajan en la organización, el Oficial de Seguridad o quien lo reemplace en su ausencia debe autorizar para que tenga acceso solo a información necesaria para el cual fue contratado, previa justificación.
- Para que un personal, colaborador o tercero desea tener acceso a los servicios e información con la que cuenta la empresa Loyalty Perú SAC., se debe pedir autorización del jefe inmediato o gerente solicite al Área de Sistemas mediante un papel escrito, para dar acceso a dichos servicios con las que desea trabajar y poner restricciones pertinentes.
- El beneficio de acceso a la información debe estar controlado mediante las reglas y procedimientos ya establecidos para ese fin.
- Todos los beneficios para la utilización de los sistemas de información de la empresa debe culminar inmediatamente cuando termine el trabajador su servicio de prestar a la organización.
- Los proveedores o personas, exclusivamente deben tener beneficios de acceso durante el tiempo que lo solicita para llevar a cabo sus trabajos y previo aprobación del responsable.
- El control de acceso a todos los sistemas de computación de Loyalty Perú SAC debe realizarse mediante una identificación y contraseñas únicas para cada personal, todo este control debe administrar el Directorio o un software similar con la tarea de controlar el acceso.
- El acceso remoto seguro debe controlarse estrictamente con claves cifrados, es decir, (Red Privada Virtual VPN).

- Loyalty Perú SAC. deberá contar con un instrumento de control de acceso por ejemplo contar con unos sistemas de control y alarmas en las diferentes áreas que son muy importantes.

e) Seguridad de recursos humanos.

- Todos los trabajadores de Loyalty Perú SAC. tienen la obligación de conocer la Política de Seguridad de la Información, que es de cumplimiento obligatorio dentro de la empresa.
- Todos los empleados de Loyalty Perú SAC que tengan acceso a información importante de la organización, se debe firmar un acuerdo de no difundir antes de acceder a la información.
- Se debe determinar un plan de capacitación continua para atender a todos las conexiones de la empresa, en particular se debe capacitar al personal nuevo.
- En situación de incumplimiento o violaciones a la política de seguridad de información se debe aplicar sanciones conforme a la mala conducta y procede a un proceso disciplinario.
- Culminado el contrato laboral de un trabajador de Loyalty Perú SAC, es necesario la devolución de los documentos corporativos, manuales y equipos. Seguidamente se debe quitar los derechos de acceso a los bienes de información.

f) Gestión de activos.

- Los activos de la empresa Loyalty Perú SAC deben ser identificadas, clasificadas según su valor, importancia, responsabilidad y ubicación para su respectiva protección ante cualquier situación de riesgo. Seguidamente deben ser registradas, en caso de realizar algún cambio o actualización mencionar en el registro la hora, fecha, y responsable del cambio.
- Los integrantes de la alta gerencia son los responsables de gestionar los activos, tales como la calidad y la seguridad y también son los

encargados dar acceso a los recursos necesarios para el logro de las metas.

- Todo los activos que se utiliza en la Loyalty Perú SAC, se debe asignar a un personal designado por el comité de seguridad, para asegurar que sean correctamente clasificados, y bajo restricciones de acceso, teniendo en cuenta las políticas de acceso.

g) Seguridad física y del entorno.

- El Área de Sistemas, el Centro de Datos y Comunicaciones y las áreas que la empresa considere importantes, no deben acceder cualquier persona, el que desea ingresar previamente deben registrase e informar el motivo de su ingreso y debe estar acompañado por un personal que trabaje diariamente en el lugar.
- Las persona que trabajan en dentro de la empresa deben portar su tarjeta de identificación y debe ser visible.
- Todas las laptops, módems y celulares se deben registrar al ingresar a la empresa y al salir de la empresa, no se debe abandonar en la empresa, a menos que sea autorizado, por su jefe inmediato, y supervisado por el vigilantes de turno.
- Los equipos tales como: PCs, servidores, equipos de comunicaciones, y otros. No se debe trasladar de su ubicación a menos que sea previamente aprobado.
- En el Área de Sistemas, la Data Center de Datos y Comunicaciones de la empresa, y las áreas más importantes deben tener equipos de control de incendio, inundación y alarmas.
- La Data Center y las redes de cableado deben ser considerados como zonas de alto riesgo, y control de acceso.
- Los empleados, colaboradores y terceros se deben comprometer a no utilizar a la energía eléctrica para conectar equipos electrónicos a excepción de su equipo de cómputo.

- La información de almacenados en los equipos que ya no serán el uso para Loyalty Perú SAC, debe ser eliminado por completa, ya que la información puede verse comprometida por reutilización inapropiada.

h) Acceso a Internet.

- El acceso a Internet por parte del personal a ciertas paginas tales como: redes sociales, páginas música, entre otros, que no tienen con las necesidades del negocio resulta en el mal uso de los recursos. Estas actividades afectan a la productividad debido al tiempo empleado en navegar por Internet.
- Todo acceso a Internet se debe utilizar únicamente para fines comerciales. Las capacidades para los servicios algunos servicios se encuentran libres distribuidos tales como: correo, navegación, protocolos de transferencia de archivos.

i) Medios extraíbles.

- El personal de Loyalty Perú SAC, solo puede usar los medios extraíbles de la empresa en su computadora personal. Los medios extraíbles de Loyalty Perú SAC, no se pueden conectar ni usar en otras computadoras que no son de su propiedad.
- La información confidencial debe almacenarse en medios extraíbles. Solo cuando sea requerido para desempeñar sus tareas asignadas o cuando proporcione información por otras agencias o empresas. Cuando la información confidencial se almacena en medios extraíbles, esta debe estar encriptada.

j) Administración de hardware y software.

- En caso de realizar un cambio hardware o software que causen problemas a los recursos informáticos, previamente deben autorizar los usuarios que son dueños de la información y del proceso y todo este cambio debe ser aprobado por los funcionarios del Área de Sistemas (Oficial de Seguridad y Jefe de Producción), y el visto bueno del jefe inmediato.

- El Responsable del control de los accesos o quien lo supla en ausencia, en el Área de Sistemas, tendrá la facultad de verificar la solicitud y aceptar o rechazar dicha solicitud.
- En ningún caso el reemplazo de hardware o software puede realizarse, por el personal del área, sin previa autorización de área de sistemas.
- Para la administración el reemplazo de hardware o software se debe efectuar bajo los procedimientos y reglas de la empresa LOYALTY PERU S.A.C, de acuerdo con el tipo de cambio solicitado en los recursos tecnológicos.
- Cualquier tipo de cambio en el recurso tecnológico debe quedar formalmente documentado desde su solicitud hasta su implantación. Este mecanismo proveerá herramientas para efectuar seguimiento y garantizar el cumplimiento de los procedimientos definidos en nuestro sistema de Calidad.
- Toda alteración de los bienes informáticos relacionado con el cambio de accesos, reparación de software o variación de parámetros debe realizar siempre y cuando no se ponga en riesgo la seguridad actual de los bienes.

k) Software utilizado.

- Todos los programas que utilizan en Loyalty Perú SAC, deben ser legales con respetando las leyes vigentes y siguiendo los métodos específicos de la empresa o los reglamentos internos.
- El software de motor de base de datos que utilice en Loyalty Perú SAC. y en sus sistemas, deben ser las más avanzadas de tecnología para garantizar la integridad de los datos.
- En Loyalty Perú SAC, se debe realizar una capacitación tecnología para que el personal tenga conocimientos, y los funcionarios, empleados y contratistas tiene que el instalar software legal en las computadoras de la empresa.

l) Email

- El correo electrónico debe ser claro y consistente con las políticas y procedimientos de Loyalty Perú SAC y de conducta ética, seguridad, cumplimiento de las leyes aplicables y prácticas comerciales adecuadas.
- La cuenta de correo electrónico de Loyalty debe utilizarse principalmente para fines relacionados con el negocio de la empresa; la comunicación personal está permitida, pero de forma limitada.
- Los datos de Loyalty Perú SAC contenidos en los mensajes de correos electrónicos o archivos adjuntos deben ser asegurados según el estándar de protección de datos.
- Los empleados de Loyalty Perú SAC no deben tener ninguna expectativa de privacidad en nada de lo que almacena, envía o recibe en el correo electrónico de la organización.

m) Establecimiento, uso y protección de claves de acceso.

- Las contraseñas deberían cambiarse periódicamente el tiempo de duración es de 30 días calendario. Pasados estos 30 días, el usuario cuando intente ingresar al dominio, el sistema le informara que su contraseña ha vencido y deberá cambiarla, si no lo hace no podrá ingresar. La excepción a esta política se dio para los usuarios de módulo ya que el usuario está relacionado al centro de canje y son muchas personas que emplean el mismo usuario para entrar al sistema.
- Longitud mínima y máxima de las contraseñas se ha considerado como mínimo es de 6 caracteres y como máximo el sistema permite 14 caracteres. No se está considerado como contraseña espacio en blanco.
- Las contraseñas no deben repetirse, el sistema verifica que no se repita ninguna de las 4 contraseñas anteriores, esto da mayor seguridad.
- Bloqueo de usuarios Si un usuario se equivoca tres veces consecutivas su contraseña, ésta quedará bloqueada hasta que el administrador vuelva a habilitarla.

n) Relaciones con los proveedores.

- Los responsables de los recursos informáticos y tecnológicos que no sean propiedad de Loyalty Perú SAC. Deben ser ubicados y administrados por la empresa, para garantizar la legalidad del recursos y para su funcionamiento,
- Los proveedores o terceros deben tener acceso a los Servicios y Recursos Informáticos, siempre y cuando se debe utilizar los servicios estrictamente necesarios para el realizar la función de su trabajo, dichos servicios deben ser aprobados por el responsable de los activos. En todo caso deben firmar una solicitud de activación y acceso a servicios tecnológicos y aceptaran a dar un buen uso a los recursos y servicios.
- La interconexión entre los sistemas internos de empresa con otros de proveedores o terceros, previamente se debe aprobar y debe ser certificadas por el Jefe de Producción con la finalidad de no interrumpir la seguridad interna de la empresa.

3.1.7. Metodología de evaluación de riesgos

La metodología para analizar los riesgos en el proyecto se seguirá las reglas del método MAGERIT, que permitirán analizar y tratar de los riesgos de los bienes o activos de información que también encajan en la actividad continua de gestión de la seguridad de la norma ISO 27001.

La examinación de riesgos permitirá establecer ¿Cómo son los riesgos?, ¿Cuánto es el valor? y ¿Cómo está protegido sistema? Todas estas preguntas están en coordinación con las metas, planes y políticas de la empresa, de la misma manera se realizara el tratamiento de los riesgos permitirán establecer un plan de seguridad de información que, será tomado en cuenta para proponer controles de seguridad en la organización para lograr los objetivos propuestos.

El análisis de riesgos proporcionará permite controlar los activos, amenazas, que es muy importante para las actividades en la organización. A continuación se una lista de inventarios de la organización que nos servirá para el análisis de los riesgos.

3.1.8. Inventario de Activos

Los bienes de la empresa Loyalty se han clasificado según la Metodología de MAGERIT que comprende Hardware, software, redes, recursos humanos, servicios o procesos de negocio, páginas web, entre otros.

Hardware:

Loyalty cuenta con los principales activos de hardware que a continuación se detalla los activos de hardware, tales como, los servidores, impresoras,

a) ***Servidores:*** Los servidores son los equipos que hospedan la base datos de Loyalty, en la tabla N° 9, se muestra los principales servidores y características de cada uno de ellos, el uso, su ubicación y el nombre de cada uno de ellos.

Tabla N° 9, Servidores de Loyalty Perú SAC

Sistema Operativo	Ubicación Física	Uso
OS400	Área sistemas	Producción
Windows Server 2016	Área sistemas	Contabilidad, páginas de terceros, consultas web, facturación electrónica
Windows Server 2008	Área sistemas	Web Servicie usuarios Primax
CentOS	Área sistemas	Servidores de correos
Windows Server 2012	Área sistemas	Servidores de Páginas web Bonus, Cencosud
Windows Server 2012 R2 - 64 bits	Área sistemas	Servidor de páginas Web Delosi
Windows Server 2016	Área sistemas	Servidores DNS Principal
Windows 20012	Área sistemas	Servidor de Control de Asistencia

Fuente: Elaboración propia

b) ***Impresoras:*** son activos de empresa que son utilizados para la actividad y el trabajo de los personales de empresa están bajo la responsabilidad are, en la tabla N° 10, se visualiza los equipos de impresoras con sus respectivas características.

Tabla N° 10, Equipo de impresoras

Tipo	Tipo impresión	Marca	Modelo
Impresoras	Matricial	EPSON	FX-500
Impresoras	Laser	XEROX	PHASER 5550V_DNP
Impresoras	Laser	HP	LaserJet M402dn
Impresoras	Laser	HP	LaserJet M400dn
Impresoras	Laser	HP	Enterprise M606dn
Impresoras	Laser	HP	T6B82A
Impresoras	Laser	HP	Universal Printing PCL6

Fuente: Elaboración propia

c) ***Equipos de escritorio:*** los activos de computadora personal están distribuidas por las diferentes áreas de la empresa, bajo la responsabilidad del área de sistemas. En la tabla N° 11, se muestra la distribución de las computadoras personales o laptop por cada área funcional.

Tabla N° 11, Equipos Computadora Personal

Ubicación Física	Tipo de PC	Responsable
Área Sistemas	PC Escritorio	Área de Sistemas
	Laptop	Área de Sistemas
Sub Área de Recursos Humanos	PC Escritorio	Área de Sistemas
	Laptop	Área de Sistemas
Sub Área Logística	PC Escritorio	Área de Sistemas
Sub Área Contabilidad	PC Escritorio	Área de Sistemas
Área de Finanzas	Laptop	Área de Sistemas
Área de Proyectos	PC Escritorio	Área de Sistemas
	Laptop	Área de Sistemas
Área de Servicio al Cliente	PC Escritorio	Área de Sistemas
	Laptop	Área de Sistemas
Área de Inteligencia Comercial	PC Escritorio	Área de Sistemas
	Laptop	Área de Sistemas
Área de Módulos	Laptop	Área de Sistemas
Área de Gerencia	Laptop	Área de Sistemas

Fuente: Elaboración propia

d) ***Dispositivos de red:*** Comprende los activos de conexiones de red**,** en la tabla N° 12, se muestra los diferentes dispositivos de red clasificados según el tipo de dispositivo.

Tabla N° 12, Dispositivos de Red

Tipo dispositivo de red	Modelo	Responsable
Router	Cisco	Área Sistemas Loyalty
Analog VoIP Gateway	Dinstar	Área Sistemas Loyalty
Switch	D-Link	Área Sistemas Loyalty
Firewall	Check Point	Área Sistemas Loyalty
Mifi	Claro	Área Sistemas Loyalty
Hub USB	Distintas marcas	Área Sistemas Loyalty
Wifi Corporativo	OLO	Área Sistemas Loyalty
Teléfonos IP	CP-3870	Área Sistemas Loyalty
Celulares	Samsung, Motorola	Área Sistemas Loyalty
Gabinetes servidores	Racks	Área Sistemas Loyalty
Escritorios	Distintas marcas	Área Sistemas Loyalty
NAS	-	Área Sistemas Loyalty
Tablet	Samsung	Área Sistemas Loyalty
Cartuchos de datos Backup	LTO Ultrium	Área Sistemas Loyalty
Telefonía corporativa en la nube	YX Wireless	Área Sistemas Loyalty
Reloj Biométrico	ZKTeco	Área Sistemas Loyalty

Fuente: Elaboración propia

e) ***Páginas web:*** Son los activos de la empresa desarrollados por el personal de la empresa**,** comprende las páginas web y los Web Service. En la tabla N° 13, se muestra los diferentes servicios, alojados en los servidores web de la empresa.

Tabla N° 13, Páginas web, Web Service

Servicios Uso	Dirección web	Responsable
Web Service acumulación puntos Bonus	(http://Webservicedeacumulacion/)	Área Sistemas Loyalty
Página Web Bonus	(http://www.bonus.pe/)	Área Sistemas Loyalty
Web Service Ganamás	(http://webserviceganamas/)	Área Sistemas Loyalty
Página Web Punto Cash	(http://www.puntocash.pe/)	Área Sistemas Loyalty

Web Service Facturación Electrónica	(http://webservicedefacturacion/)	Área Sistemas Loyalty
Web Service Módulos de Canje	(http://consultadepuntosbonus/modulos/)	Área Sistemas Loyalty
Página Web Xtends	(http://www.xtends.com.pe/)	Área Sistemas Loyalty
Web Service de Acumulación EESS COESTI	(http://webserviceprimaxcoesti/)	Área Sistemas Loyalty
Web Service de Acumulación de Puntos Grupo DELOSI	(http://delosipuntosbonus/delosi/servlet/	Área Sistemas Loyalty
Página Web de plataformas ALICORP	(www.plataformasalicorp.com.pe)	Área Sistemas Loyalty
Web Service de Afiliación de Clientes Banco CENCOSUD	(http://afiliaciondebonus/modulos/servlet/)	Área Sistemas Loyalty
Web de Preafiliación Bonus	(http://www.loyaltyperu.com/afiliacion/)	Área Sistemas Loyalty
Web Service de Módulos de Canjes	(http://modulosdecanje/modulos/servlet/)	Área Sistemas Loyalty
Página Web Programa Auto Bonus	(http://autobonus/servlet/com.kbautobonuswebv07.sure.wpa_login)	Área Sistemas Loyalty

Fuente: Elaboración propia

f) ***Documentos y archivos.*** Los documentos es la parte importante de la organización. Es un activo que no es material que está guardado en equipos o soportes de información estos activos son trasladados en medios de almacenamiento. En la tabla N° 14, se muestra los activos de empresa, tales como los datos o documentos con los cuales cuenta.

Tabla N° 14, Documentos y archivos

Tipo de Activo	Nombre de activo	Responsable
Manuales	Manual Administrador General del sistema	Sistemas
	Manual de programas de terceros	Sistemas
	Manual Carga Emailing Bonus	Sistemas
	Manual Instalación puntos Canjes Primax	Sistemas
	Manual Puntos de Programas de Terceros	Sistemas
	Manual Datamart	Sistemas
	Manual Respaldo Web	Sistemas

	Manual Solicitudes de Requerimientos	Sistemas
	Manual Proceso de Puntos Pacifico	Sistemas
Datos	Clientes Bonus	Sistemas
	Clientes Terceros Bonus	Sistemas
	Clientes Banco Cencosud	Sistemas
Documentos	Lista Proveedores	Sistemas
	Lista Socios de la empresa	Sistemas
	Facturas	Sistemas
	Boletas	Sistemas
	Guías de remisión	Sistemas
	Guías de recepción	Sistemas
	Guías de devolución	Sistemas
	Plan de invulnerabilidad de base de datos	Sistemas
	Actas de mantenimiento Correctivos	Sistemas
	Hoja de contactos de Proveedores	Sistemas
Contratos Terceros	Proveedores de software externo	Sistemas
	Proveedores de software Firmas Digitales	Sistemas
	Proveedores de software VoIP	Sistemas

Fuente: Elaboración propia

g) ***Servicios terceros.*** Comprende los servicios de usuarios terceros para complementar los tareas. En la tabla N° 15, se muestra los servicios que la empresa Loyalty adquiere.

Tabla N° 15, Servicios Terceros

Nombre servicios	Numero de servicios terceros	Responsable
Conectividad a internet	1	Sistemas
Mantenimiento de hardware local	1	Sistemas
Soporte de hardware local	1	Sistemas
Mantenimiento de software local	1	Sistemas
Soporte de software local	1	Sistemas
Soporte de software en Outsourcing	2	Sistemas
Correo Corporativo	1	Sistemas
Actualizaciones en software en Outsourcing	1	Sistemas

Fuente: Elaboración propia

h) ***Software y licencias.*** Comprende las licencias más importantes de la empresa Loyalty en la tabla N° 16, se visualiza el número de licencia de cada uno del software.

Tabla N° 16, Software y licencias

Software	**Número de Licencias**	**Responsable**
Antivirus EndPoint Corporativo	80	Área de sistemas
Microsoft Office 2010	1	Área de sistemas
Windows 7	4	Área de sistemas
Windows 10	4	Área de sistemas
Windows XP	3	Área de sistemas
Windows Server 2012	2	Área de sistemas
Windows Server 2008	2	Área de sistemas
Windows Server 2003	1	Área de sistemas
Linux Centos	Libre	Área de sistemas
SQL Server 2012	1	Área de sistemas
SQL Server 2003	1	Área de sistemas
SQL Server 2008	1	Área de sistemas
IBM AS	1	Área de sistemas
QlickView	1	Área de sistemas
Bizagi	libre	Área de sistemas
NET	1	Área de sistemas
Project	1	Área de sistemas
Reloj biométrico	5	Área de sistemas
Rapider Mineria	1	Área de sistemas
QlickSense	1	Área de sistemas
CCS6	1	Área de sistemas
Genexus	1	Área de sistemas

Fuente: Elaboración propia

i) ***Instalación de red eléctrica.*** Son aquellos activos que transmiten energía eléctrica a todos los equipos, servidores, y otros aparatos eléctricos. En la tabla N° 17, se muestra los dispositivos eléctricos.

Tabla N° 17, Dispositivos Eléctricos

Dispositivos de conexiones eléctricas	**Tipo de dispositivo**	**Responsable**
Medidor de Luz	Luz del Sur	Sistemas
Tablero de Transferencia	-	Sistemas
Grupo Electrógeno	-	Sistemas
Llave térmica	-	Sistemas

Transformador de aislamiento	-	Sistemas
UPS	3KBA	Sistemas
UPS	6KBA	Sistemas

Fuente: Elaboración propia

j) ***Personal.*** Son aquellas personas que conforman el equipo de trabajadores del área de sistemas de la organización.

- Desarrolladores**:** Conformados por los equipo de desarrolladores de los programas de software de la empresa Loyalty los cuales son: 3 desarrolladores en Genexus, 2 desarrolladores en C# .NET
- Soporte técnico: conformad por 3 personas, jefe de soporte y 2 soporte de segundo nivel.
- Operadores: conformado por 4 personas un jefe de operaciones y tres operadores.
- Controlador de base de datos: conformado por el gerente de área de sistemas.

3.1.9. Análisis de riesgos

Para analizar los riesgos que probablemente afecten a activos de la información se agrupará los bienes de la organización según la clasificación de la metodología MAGERIT. En la tabla N° 18, se expone la clasificación de los activos de información para su posterior análisis y tratamiento.

Tabla N° 18, Clasificación de los activos

Tipo de Activo	Nombre del Activo
[Esenciales] Activos Esenciales	Registro de acumulación de Puntos Bonus
	Registro de Puntos de Venta
	Registro de Estaciones de Servicio
	Registro de Facturación de Puntos Bonus
	Registro de Factura Y Boletas
	Plan de acceso de datos
[D] Datos	Manual Actualización Nuevos Programas Terceros
	Manual Administrador General sistema
	Manual Carga y Reproceso Datamart
	Manual Configuración Conexión Nuevo Sistema

	Manual Instalación Canjes Primax
	Manual Marca masiva de direcciones erradas
	Manual de Reserva de Pts de Prog de Terceros
	Manual Datamart
	Manual Respaldo Web
	Manual Solicitudes de Requerimientos
	Base de datos de control de acceso
	Reporte de credenciales Password
	Reporte de bajas de Hardware y Software
	Código fuente de los programas
[S] Servicios	Página Web Bonus
	Web Service Ganamás
	Web Service Facturación Electrónica
	Web Service Consul de Pts Bonus para Módulos
	Página Web Xtends
	Web Service de Afil de Clientes Banco Cencosud
[SW] Aplicaciones Informáticas (Software)	Software Propio Software Asignación de Puntos
	Software Propio Sistema de Modulos de Canje
	Navegador Chrome
	Antivirus EndPoint Corporativo
	Microsoft Office 2010
	Windows 7
	Windows 10
	Windows XP
	Windows Server 2012
	Linux Centos
	SQL Server 2012
	IBM AS/400
	QlickView
	Bizagi
	NET
	Project
	BioTime
	RapidMiner
	QlickSense
	CCS6
	Genexus
	Apache Tomcap
	Correo Electrónica Microsoft
[HW] Equipamiento Informático (Hardware)	Servidor Producción
	Servidor Correo Bonus
	Servidor Facturación Electrónica

	Servidor de Correo Loyalty Xtends
	Servidor de DNS
	Impresoras matricial, Laser
	Computadora Personal
	Laptop
	Escáneres
	Análogo VOIP
	IP-10 Ceragon
	Tablet
	Reloj Biométrico
	Firewall
	Router
	Teléfono IP
	Modem
	Switch
	Celulares
[COM] Redes de Comunicaciones	Red de telefónica IP
	Red de datos de Celulares
	Internet Claro
	Red Local
	WIFI Corporativo OLO
	MIFI
	Telefónica Corporativa en la Nube
	El Protocolo de transferencia de archivos (FTP)
	Red de datos
[Media] Soporte de Información	Disco Externo Toshiba storage
	Almacenamiento conectado en red (NAS)
	Medios Extraíbles USB
	DVD
	Cartuchos de datos Backup
	Discos Virtuales
	Materiales impresos de manuales
	Tarjetas de Memorias
	CD-ROM
[AUX] Equipamiento Auxiliar	Sistema de Alimentación Ininterrumpida (UPS)
	Generador Eléctrico
	Llave Térmica
	Cableado Eléctrico
	Cableado de Red
	Fuentes de alimentación
	Transformador de aislamiento

	Escritorios y armarios
	Cajas fuertes
	Sistema de detección de incendios
	Sistema de aire acondicionado (Data Center)
	Extintores
	Gabinetes para servidores
[I] Instalaciones	Data Center
	Oficina de Desarrolladores
	Oficina de Soporte Técnico
[P] Personal	Soporte Técnico
	Administrador de Base de Datos
	Programadores
	Operadores
	Proveedores
	Usuarios internos
	Usuarios externos

Fuente: Elaboración propia

3.1.10.Valoración de activos

En el presente apartado se calculan los valores de los activos de información según mencionado en la metodología MAGERIT explicados en la Figura N° 9, donde muestra la valoración de una escala de 0 a 10, tomando en cuenta también el documento de Valoración de bienes según las reglas de la ISO 27001. La estimación de los activos según los fundamentos de confidencialidad, integridad y disponibilidad se muestra en la tabla N° 19, que quedaría de la siguiente manera:

Leyenda:

- Confidencialidad [C]
- Integridad [I]
- Disponibilidad [D]

Tabla N° 19, Valoración de activos de información Loyalty

Tipo de Activo	Nombre de activos	[C]	[I]	[D]	Total
[Esenciales] Activos Esenciales	Registro Acum de Puntos Bonus	10	10	10	30
	Registro Tabla de BD	10	10	10	30
	Registro Puntos de Venta	9	9	9	27
	Registro Proveedores	8	9	9	26
	Registro Estaciones de Servicio	8	9	9	26

	Registro Facturación de Pts Bonus	9	8	9	26
	Registro Fact Y Boletas	8	8	9	25
	Registro Clientes Bonus	9	9	9	27
	Facturas	6	5	5	16
	Boletas	6	5	5	16
	Guías de remisión	6	5	5	16
	Guías de recepción	6	5	5	16
	Guías de devolución	6	5	5	16
	Plan de seguridad DB	7	6	5	18
	Plan de acceso de datos	9	8	6	23
	Manual Administrador General	5	6	6	17
	Manual Canjes Primax	5	6	7	18
	Manual Carg Email Masivo Bon	5	5	5	15
	Manual Carg y Repro Datamart	5	6	7	18
	Manual Reserva Pts Prog de Terc	6	6	5	17
	Manual Datamart	7	5	5	17
	Manual Respaldo Web	7	6	5	18
	Copias de respaldo	9	9	9	27
	Datos de control de acceso	8	7	6	21
	Report Credenciales Password	9	7	9	25
	Report bajas de HD y SW	6	5	6	17
	Código fuente de los programas	9	8	9	26
[S] Servicios	Página Web Bonus	9	9	9	27
	WS Ganamás	8	7	8	23
	PW Cosapi en Acción	7	6	7	20
	WS Facturación Electrónica	8	8	8	24
	WS Cst Pto Bon M de Canj	8	7	8	23
	PW Xtends	7	6	7	20
	PW Plataformas Alicorp	7	7	8	22
	PW Programa Auto Bonus	7	6	8	21
	WS de Acum módulo en MDS	7	6	8	21
[SW] Aplicaciones Informáticas (Software)	SW Propio Asig de Puntos	7	8	8	23
	SW Propio Esquemas Terceros	7	8	8	23
	SW Propio Modulos de Canje	7	8	8	23
	SW Propio Supervisores	7	8	8	23
	Navegador Chrome	3	5	5	13
	Antivirus EndPoint Corporativo	7	7	8	22
	Microsoft Office 2010	6	8	8	22
	Windows 7	6	6	7	19

	Windows 10	6	6	7	19
	Windows XP	6	6	7	19
	Windows Server 2012	6	6	7	19
	Windows Server 2008	6	6	7	19
	Windows Server 2003	6	6	7	19
	Linux Centos	8	8	9	25
	SQL Server 2012	8	9	9	26
	SQL Server 2003	8	9	9	26
	SQL Server 2008	8	9	9	26
	IBM AS/400	9	10	10	29
	QlickView	5	6	6	17
	Bizagi	4	5	7	16
	NET	4	5	7	16
	Project	4	5	7	16
	Rapid Mineria	4	6	6	16
	QlickSense	5	7	7	19
	CCS6	5	6	7	18
	Apache Tomcap	5	7	8	20
	Correo Electrónica Microsoft	8	8	8	24
[HW] Equipamiento Informático (Hardware)	Servidor Producción	10	10	10	30
	Servidor Correo Bonus	9	8	9	26
	Servidor WS Cencosud	9	8	9	26
	Servidor Facturación Electrónica	10	9	9	28
	Servidor Web Service Primax	9	8	9	26
	Servidor de DNS	9	9	9	27
	Impresoras matricial, Laser	5	6	7	18
	PC Área Sistemas	7	7	8	22
	Laptop Área Sistemas	6	7	6	19
	Escáneres	3	3	3	9
	Análogo VOIP	6	8	9	23
	IP-10 Ceragon	4	4	4	12
	Tablet	3	4	4	11
	Reloj Biométrico	3	6	5	14
	Firewall	7	6	9	22
	Router	5	7	8	20
	Teléfono IP	4	3	4	11
	Modem	3	2	3	8
	Switch	4	6	7	17
	Celulares	3	4	5	12

[COM] Redes de Comunicaciones	Red de telefónica IP	5	6	7	18
	Red de datos de Celulares	5	5	6	16
	Internet Claro	7	7	8	22
	Red Local	8	8	8	24
	WIFI Corporativo OLO	4	3	3	10
	MIFI	4	3	3	10
	Telefónica Corp de la Nube	6	6	6	18
	Protocolo transferencia de arch	7	6	8	21
	Red de datos	7	8	9	24
[Media] Soporte de Información	Disco Externo	3	3	5	11
	NAS	9	7	8	24
	Medios Extraíbles USB	3	3	3	9
	DVD	3	3	3	9
	Datos de Backup	6	6	6	18
	Discos Virtuales	6	6	6	18
	Materiales impresos manuales	6	2	3	11
	Tarjetas de Memorias	3	2	3	8
	CD-ROM	3	2	3	8
[AUX] Equipamiento Auxiliar	UPS	6	7	10	23
	Generador Eléctrico	5	7	8	20
	Llave Térmica	3	5	6	14
	Cableado Eléctrico	9	10	9	28
	Cableado de Red	9	9	9	27
	Fuentes de alimentación	5	6	7	18
	Escritorios y armarios	4	6	6	16
	Cajas fuertes	7	7	6	20
	Transformador de aislamiento	4	6	6	16
	Detección de incendios	5	6	6	17
	Aire acondicionado	5	7	8	20
	Extintores	4	6	7	17
	Gabinetes para servidores	4	5	6	15
[I] Instalaciones	Data Center	10	10	10	30
	Oficina de Gerente de sistemas	10	9	8	27
	Oficina de Desarrolladores	9	8	9	26
	Oficina de Soporte Técnico	5	6	7	18
[P] Personal	Soporte Técnico	9	8	7	24
	Gerente BD	10	10	10	30
	Programadores	7	7	9	23
	Operadores	4	6	5	15

	Proveedores	5	4	4	13
	Usuarios internos	6	6	7	19
	Usuarios externos	3	4	3	10

Fuente: Elaboración propia

El grafico anterior se obtiene la suma de las dimensiones mostradas en la Tabla N°19, (Valor de los activos en números de confidencialidad, integridad y disponibilidad), se seleccionarán aquellos activos cuya dimensión son mayores, esta valoración de activos permitirá proseguir con la gestión de riesgos de seguridad de información.

3.1.11.Identificación de Amenazas

En la presente sección se identificaran las amenazas que pueden dañar a los bienes de la empresa Loyalty Perú SAC.

La situación o evento que impide que se pueda realizar normalmente las actividades de una empresa pueden ser de diferentes tipos. El siguiente la Tabla N° 20, se muestra las amenazas según la clasificación de metodología MAGERIT.

Tabla N° 20, Amenazas de los activos

Tipo de activo	Nombre activo	Amenazas
Auxiliar	Aire acondicionado	Posibilidad de sufrir incendio accidental
		Posibilidad de que se contamine polvos suciedad
		Posibilidad de sufrir desastre natural fenómeno sísmico
		Posibilidad de sufrir fugas por escape de agua
		Posibilidad de ocurrir fallas en el equipo
		Cese de alimentación eléctrica
	Cableado de Red	Posibilidad de ocurrir un incendio y dañar el red cableado
		Posibilidad de que las fugas de agua inunden el red de cableado
		Posibilidad de equivocaciones en la instalación
		Ataque destructivo vandalismo
	Cableado Eléctrico	Posibilidad de un corte eléctrico
		Posibilidad de fugas de agua accidental o deliberada
		Posibilidad de que el fuego acabe con el cable
	Cajas fuertes	Posibilidad de acceso no autorizado
	Escritorios y	Posibilidad de que el fuego acabe el escritorio

	armarios	Degradación por consecuencia del tiempo
		Posibilidad de vandalismo
	Fuentes de alimentación	Posibilidad de que el fuego acabo con la fuente
		Cese de alimentación eléctrica
		Fuga de escape de agua
Comunicación	Internet Claro	Acceso no permitido de internet
		Abuso de beneficios de acceso
		Caída de los servicios de internet
	Protocolo transferencia de archivos	Interceptación del protocolo
		Monitorización del trafico
		Suplantación de identidad
		Acceso no autorizado de transferencia de datos
		Caída de los servicios de transferencia
		Alteración de transmisión archivos de datos
	Red Local	Interceptación de red
		Monitorización del trafico
		Acceso no permitido a la red local
		Caída de red de comunicaciones
Datos	Código Fuente programas	Eliminación del código fuente
		Alteraciones del código fuente
		Fuga de información por indiscreción verbal o medios electrónicos
		Error en el desarrollo del código fuente
	Copias de respaldo	Eliminación de las copias de respaldo
		Equivocación al realizar copias de seguridad
		Modificación deliberada de las copias de seguridad
		Fugas de información por medios electrónicos
	Datos de control acceso	Divulgación de los acceso de control
		Eliminación intencional de datos de control de acceso
		Modificación de los accesos de control
		Manipulación de registro de actividad
		Acceso no autorizado a los datos de control
	Manuales	Equivocación al momento de crear de los manuales
		Fuga de información revelación de los manuales
		Manipulación de los datos de los manuales
		Eliminación de los manuales
		Alteraciones de los registro de manuales
	Reportes de control	Manipulación de los registros
		Equivocación al realizar el reporte de control
		Eliminación de reportes de control
		Fugas de información por medios electrónicos
Esenciales	Documentos	Eliminación de documentos

		Fugas de información por medios electrónicos
		Manipulación de documentos
		Alteración de documentos
	Registro de base de datos	Eliminación de los registros de datos por error o deliberadamente
		Fugas de información por medios electrónicos
		Registros incompletos
		Alteración intencional de registros
		Acceso no autorizado a los registros
		Alteración accidental de los registros
		Introducción de datos erróneos
Hardware	Gateways analógicos	Posibilidad de que el fuego acabe
		Acceso no autorizado personal interno
		Desconexión del equipo
		Corte de suministro eléctrico
	Computadoras	Posibilidad de que el fuego acabe
		Desgaste debido a su uso
		Avería del hardware
		Uso ilícito de la computadora
		Desconexión de la PC
		Errores en el mantenimiento actualización del equipo
		Contaminación mecánica polvo
		Corte de suministro eléctrico
	Firewall	Posibilidad de que el fuego acabe
		Acceso no autorizado
		Radiación electromagnética
		Corte de suministro eléctrico
		Error de mantenimiento actualización del equipo
	Impresoras	Desgaste debido a su uso
		Avería del hardware
		Desconexión del equipo
		Errores en el mantenimiento actualización del equipo
		Corte de suministro eléctrico
		Posibilidad de que el fuego acabe
	IP-10 Ceragon	Corte de suministro eléctrico
		Errores en el mantenimiento actualización del equipo
		Radiación electromagnética
	Laptop	Desgaste debido a su uso
		Avería del hardware
		Uso ilícito del laptop
		Robo de laptop
		Corte de suministro eléctrico

	Reloj Biométrico	Desgaste debido a su uso
		Avería del hardware
		Radiación electromagnética
		Corte de suministro eléctrico
	Router	Contaminación mecánica polvo
		Desconexión del equipo
		Corte de suministro eléctrico
		Errores en el mantenimiento actualización del equipo
	Servidores	Posibilidad de que el fuego acabe
		Posibilidad de un suceso sísmico
		Contaminación mecánica polvo
		Avería del hardware
		Perjuicio en el mantenimiento del servidor
		Desconexión del equipo
	Switch	Posibilidad de que el fuego acabe
		Contaminación mecánica polvo
		Perjuicio en el mantenimiento del switch
		Desconexión del equipo
	UPS	Posibilidad de que el fuego acabe
		Contaminación mecánica polvo
		Perjuicio en el mantenimiento del equipo
		Desconexión del equipo
Instalación	Data Center	Divulgación de la geolocalización
		Modificación deliberadas por perjuicio
		Posibilidad de que el fuego acabe de origen accidental o deliberada
		Posibilidad de ocurrir desastre natural sismo
		Acceso no autorizado aprovechando fallo del sistema
		Posibilidad de inundación accidental o deliberada
		Fuga de información revelación por discreción
	Oficinas	Acceso no autorizado a las oficinas
		Posibilidad de ocurrir sismo o terremoto
		Posibilidad de ocurrir inundación de origen deliberada o accidental
		Posibilidad de que las llamas de fuego acaben con la oficina
Media	Cartuchos de datos Backup	Falla de funcionamiento del cartucho
		Contaminación mecánica por polvo suciedad
		Degradación por consecuencia del tiempo
		Alteración accidental del etiquetado de cartuchos
		Uso indebido del equipo
		Posibilidad de que se inunde de agua
		Posibilidad de que las llamas del fuego acabe con los

		cartuchos
	Disco Externo Toshiba storage	Avería del hardware
		Contaminación mecánica por polvo suciedad
		Robo de Disco
		Destrucción deliberada del disco
		Degradación por consecuencia del tiempo
	NAS	Falla de funcionamiento del NAS
		Posibilidad de que las llamas del fuego acabe el NAS
		Degradación por consecuencia del tiempo
		Error en la actualización del equipo
Personal	Trabajadores	Indisponibilidad por ausencia deliberada
		Extorsión por obligar a obrar en mal sentido
		Ingeniería social aprovechamiento de buena fe
Servicio	Páginas web	Saturación de página web
		Revelación de código fuente de la pagina
		Modificación intencional de código fuente
		Error accidental en el desarrollo de la pagina
		Repudio o negación a posteriori de cambios realizados en el código fuente
		Fuga de información por indiscreción
		Alteración accidental del código fuente
	Web service	Saturación de la web Service
		Modificación deliberadas del código fuente
		Divulgación de la información de la web Service
		Repudio Negación a posteriori de cambios realizados en el código fuente
		Alteración del código fuente de la Web Service
		Error accidental en el desarrollo de la Web Service
Software	Apache Tomcat	Difusión de software dañino virus
		Falla del funcionamiento del software
		Divulgación de información
		Saturación de operación del software
		Alteración intencional del programa
	Correo Electrónico Microsoft	Equivocación por uso de servicio
		Expansión de software contaminado de virus
		Uso no permitido
		Negación de haber recibió un mensaje
	Genexus	Difusión de software dañino virus
		Falla del funcionamiento del software
		Abuso de beneficios de acceso Genexus
		Modificación intencional del programa
	IBM AS/400	Difusión de software dañino virus

		Falla del funcionamiento del software
		Saturación de la operación del software
		Alteración intencional del programa
		Hacking/ Cracking
	Linux	Equivocación por uso de servicio
		Propagación de software dañado
		Uso no permitido de Linux
		Saturación de operación del software
	.NET	Uso no previsto
		Falla del funcionamiento del software
		Hacking/ Cracking
	Office	Uso no previsto
		Propagación de software contaminado virus
		Abuso de Beneficios de acceso
		Alteración intencional del programa
	QlickView	Difusión de software dañino virus
		Instalación de software no licenciado
		Alteración del funcionamiento del software
		Uso no Previsto
		Alteración intencional del programa
	Software Propio	Difusión de software dañino virus
		Uso no Previsto
		Alteración intencional del programa
	SQL Server 2012	Difusión de software dañino virus
		Instalación de software no licenciado
		Abuso de benéficos de acceso
		Uso no permitido de SQL server
		Alteración del funcionamiento del software
		Falla del funcionamiento del software
	Windows	Equivocación por uso de servicio
		Difusión de software dañino virus
		Instalación de Windows no licenciado
		Instalaciones de programas de origen sospechoso
		Falla del funcionamiento del software
		Abuso de beneficios de acceso
		Uso no permitido de software
		Alteración intencional del programa

Fuente: Elaboración propia

3.1.12.Estimación del riesgo.

El nivel de riesgo se modelará mediante escalas cuantitativas, para ello se calcula el valor del impacto y la posibilidad de que cada activo, susceptible a ser perjudicado por una o varias amenazas. Llamase impacto a al grado del agravio sobre el activo, después de que se origine una amenaza. En la tabla N° 21, se muestra la estimación del impacto, el valor de la probabilidad y el riesgo.

Tabla N° 21, Estimación de probabilidad e impacto

Escalas			
Impacto		Probabilidad	
Valor	Tasación	Valor	Tasación
5	MA: Muy alto	5	MA: Prácticamente seguro
4	A: Alto	4	A: Probable
3	M: Medio	3	M: Posible
2	B: Bajo	2	B: Poco probable
1	MB: Muy bajo	1	MB: Muy Raro

Fuente: Elaboración propia

La estimación del riesgo se obtiene por la posterior ecuación matemática *Riesgo=Probabilidad*impacto*, de esta observación se origina un mapa de riesgos en la tabla N° 22, se muestra las escalas de estimación de riesgos.

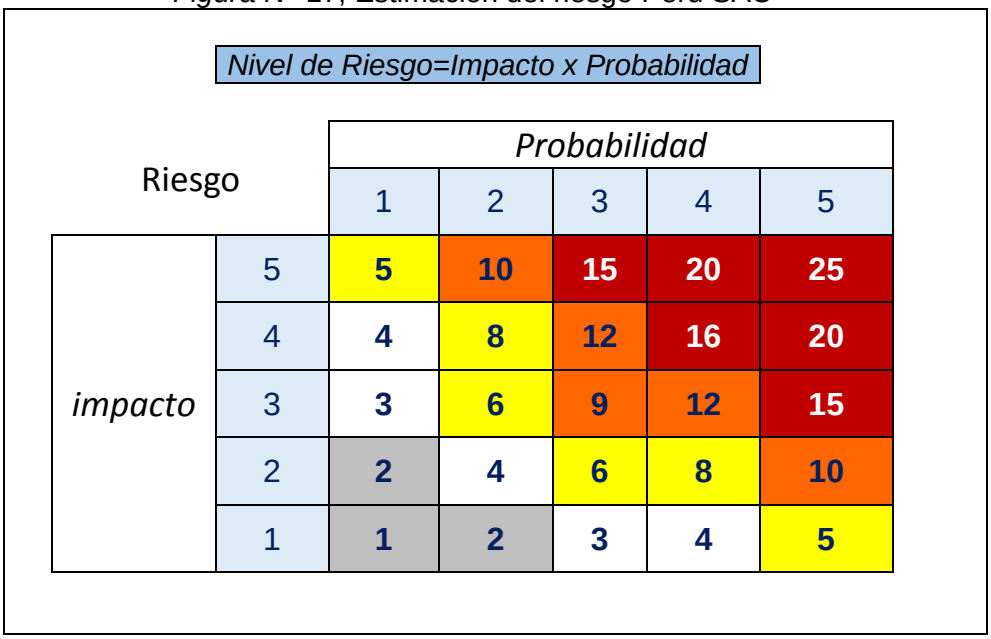
Tabla N° 22, Escalas del riesgo

Riesgo	
Escala	Tasación
15-25	MA: Crítico
9-14	A: Importante
5-8	M: Apreciable
3-4	B: Bajo
1-2	MB: Despreciable

Fuente: Elaboración propia

Seguidamente en la figura N° 17, se visualiza el mapa de riesgos conocido también como mapa del calor.

Figura N° 17, Estimación del riesgo Perú SAC



Fuente: Elaboración Propia

A continuación la tabla N° 23, se expone la estimación del riesgo por cada amenaza y activo de información de la empresa Loyalty Perú SAC, para aquellos activos que reciban una calificación de escala crítica se debe dar mayor atención inmediata.

Leyenda.

- Impacto [Im]
- Probabilidad [Prob]
- Riesgo [R]

Tabla N° 23, Estimación del riesgo

Tipo de activo	Nombre activo	Amenazas	[Im]	[P]	[R]
Auxiliar	Aire acondicionado	Posibilidad de sufrir incendio accidental	3	2	6
		Posibilidad de que se contamine polvos suciedad	2	2	4
		Posibilidad de sufrir desastre natural fenómeno sísmico	4	3	12
		Posibilidad de sufrir fugas por escape de agua	3	4	12
		Posibilidad de ocurrir fallas en el equipo	3	5	15

		Cese de alimentación eléctrica	3	3	9
	Cableado de Red	Posibilidad de ocurrir un incendio accidental o deliberado	3	3	9
		Posibilidad de fugas de agua accidental o deliberada	2	3	6
		Posibilidad de equivocaciones en la instalación	3	4	12
		Ataque destructivo vandalismo	1	2	2
	Cableado Eléctrico	Posibilidad de un corte eléctrico	3	5	**15**
		Posibilidad de fugas de agua accidental o deliberada	3	2	6
		Posibilidad de que el fuego acabe con el cable	3	2	6
	Cajas fuertes	Posibilidad de acceso no autorizado	3	2	6
	Escritorios y armarios	Posibilidad de que el fuego acabe el escritorio	3	2	6
		Degradación por consecuencia del tiempo	2	4	8
		Posibilidad de vandalismo	1	2	2
	Fuentes de alimentación	Posibilidad de que el fuego acabo con la fuente	2	2	4
		Cese de alimentación eléctrica	3	3	9
		Fuga de escape de agua	2	2	4
Comunicación	Internet Claro	Acceso no permitido a internet	3	4	12
		Abuso de beneficios de acceso	3	5	**15**
		Caída de los servicios de internet	3	3	9
	Protocolo transferencia de archivos	Interceptación del protocolo	4	3	12
		Monitorización del tráfico por usuarios externos	3	3	9
		Suplantación de identidad	3	2	6
		Acceso no autorizado de transferencia de datos	4	3	12
		Caída de los servicios de transferencia	4	5	**20**
		Alteración de transmisión de datos	4	3	12
	Red Local	Interceptación de red	3	2	6
		Monitorización del trafico	3	3	9
		Acceso no autorizado a la red local	3	3	9
		Caída de red de comunicaciones	4	4	**16**
Datos	Código Fuente programas	Eliminación del código fuente	3	2	6
		Alteraciones del código fuente	4	3	12
		Fuga de información por indiscreción verbal o medios electrónicos	4	3	12
		Error en el desarrollo del código fuente	5	4	**20**
	Copias de respaldo	Eliminación de las copias de respaldo	4	3	12
		Equivocación al realizar copias de respaldo	4	4	**16**
		Modificación deliberada de las copias de seguridad de datos	4	3	12
		Fugas de información por medios electrónicos	3	3	9

	Datos de control acceso	Divulgación de los acceso de control	3	2	6
		Eliminación intencional de los datos de control	3	2	6
		Modificación de los datos de control	3	3	9
		Manipulación de registro de actividad	3	2	6
		Acceso no permitido a los datos de control acceso	2	2	4
	Manuales	Equivocación al momento de crear de los manuales	3	3	9
		Fuga de información revelación de los manuales	3	4	12
		Manipulación de los datos de los manuales	3	2	6
		Eliminación de los manuales	4	4	**16**
		Alteraciones de los registro de manuales	3	3	9
	Reportes de control	Manipulación de los registros	3	2	6
		Equivocación al realizar el reporte de control	3	3	9
		Eliminación de reportes de control	3	2	6
		Fugas de información por medios electrónicos	4	2	8
Esenciales	Documentos	Eliminación de documentos	4	3	12
		Fugas de información por medios electrónicos	3	2	6
		Manipulación de documentos	3	3	9
		Alteración de documentos	4	3	12
	Registro de base de datos	Eliminación de registros de la base de datos por error o casualmente	5	4	**20**
		Fugas de información por medios electrónicos	5	3	**15**
		Registros incompletos	4	4	**16**
		Alteración intencional de registros	4	4	**16**
		Acceso no autorizado a los registros	4	4	**16**
		Alteración accidental de los registros	4	5	**20**
		Introducción de datos erróneos	4	5	**20**
Hardware	Gateways analógicos	Posibilidad de que el fuego acabe	3	2	6
		Acceso no autorizado personal interno	2	2	4
		Desconexión del equipo	3	3	9
		Corte casual de suministro eléctrico	3	3	9
	Computadoras	Posibilidad de que el fuego acabe	4	3	12
		Desgaste debido a su uso	3	4	12
		Avería del hardware	3	5	**15**
		Uso ilícito de la computadora	4	4	**16**
		Desconexión de la PC	3	4	12
		Errores en el mantenimiento actualización del equipo	3	4	12
		Contaminación mecánica polvo	4	5	**20**
		Corte de suministro eléctrico	3	3	9
	Firewall	Posibilidad de que el fuego acabe	3	2	6
		Acceso no autorizado	3	2	6

	Radiación electromagnética	2	1	2
	Corte de suministro eléctrico	2	3	6
	Error de mantenimiento actualización del equipo	3	2	6
Impresoras	Desgaste debido a su uso	4	5	**20**
	Avería del hardware	3	4	12
	Desconexión del equipo	2	4	8
	Errores en el mantenimiento actualización del equipo	3	2	6
	Corte casual de suministro eléctrico	3	3	9
	Posibilidad de que el fuego acabe	2	2	4
IP-10 Ceragon	Corte de suministro eléctrico	3	2	6
	Errores en el mantenimiento actualización del equipo	2	2	4
	Radiación electromagnética	2	1	2
Laptop	Desgaste debido a su uso	4	4	**16**
	Avería del hardware	3	4	12
	Uso ilícito del laptop	4	5	**20**
	Robo de laptop	2	3	6
	Corte casual de suministro eléctrico	3	1	3
Reloj Biométrico	Desgaste debido a su uso	4	4	**16**
	Avería del hardware	3	3	9
	Radiación electromagnética	2	1	2
	Corte de suministro eléctrico	3	3	9
Router	Contaminación mecánica polvo	2	3	6
	Desconexión del equipo	4	2	8
	Corte de suministro eléctrico	2	2	4
	Errores en el mantenimiento actualización del equipo	2	3	6
Servidores	Posibilidad de que el fuego acabe	3	3	9
	Posibilidad de un suceso sísmico	3	3	9
	Contaminación mecánica polvo	3	5	**15**
	Avería del hardware	4	4	**16**
	Perjuicio en el mantenimiento del servidor	5	3	**15**
	Desconexión del equipo	3	3	9
Switch	Posibilidad de que el fuego acabe	3	2	6
	Contaminación mecánica polvo	4	2	8
	Perjuicio en el mantenimiento del switch	3	3	9
	Desconexión del equipo	3	2	6
UPS	Posibilidad de que el fuego acabe	3	2	6
	Contaminación mecánica polvo	3	2	6
	Perjuicio en el mantenimiento del equipo	2	2	4
	Desconexión del equipo	3	3	9

Instalación	Data Center	Divulgación de la geolocalización	4	4	16
		Modificación deliberadas por perjuicio	3	3	9
		Posibilidad de que el fuego acabe de origen accidental o deliberada	3	3	9
		Posibilidad de ocurrir desastre natural sismo	3	3	9
		Acceso no autorizado aprovechando fallo del sistema	3	3	9
		Posibilidad de inundación accidental o deliberada	4	3	12
		Fuga de información revelación por discreción	4	3	12
	Oficinas	Acceso no autorizado a las oficinas	3	3	9
		Posibilidad de ocurrir sismo o terremoto	3	3	9
		Posibilidad de ocurrir inundación de origen deliberada o accidental	3	2	6
		Posibilidad de que el fuego acabe con las oficinas	2	2	4
Media	Cartuchos de datos Backup	Falla de funcionamiento del cartucho	3	4	12
		Contaminación mecánica por polvo suciedad	3	3	9
		Degradación por consecuencia del tiempo	1	3	3
		Alteración accidental del etiquetado de cartuchos	2	3	6
		Uso indebido del equipo	3	2	6
		Posibilidad de que las llamas del fuego acaben con los archivos	2	3	6
	Disco Externo Toshiba storage	Avería del hardware	4	4	16
		Contaminación mecánica por polvo suciedad	2	3	6
		Robo de Disco	3	3	9
		Destrucción deliberada del disco	2	2	4
		Degradación por consecuencia del tiempo	3	4	12
	NAS	Falla de funcionamiento del NAS	3	3	9
		Posibilidad de que el fuego acabe	2	3	6
		Degradación por consecuencia del tiempo	2	3	6
		Error en la actualización del equipo	2	3	6
Personal	Trabajadores	Indisponibilidad por ausencia deliberada	3	4	12
		Extorsión por obligar a obrar en mal sentido	3	3	9
		Ingeniería social aprovechamiento de buena fe	4	3	12
Servicio	Páginas web	Saturación de página web	4	4	16
		Revelación de código fuente de la pagina	3	3	9
		Modificación intencional de código fuente	3	3	9
		Error accidental en el desarrollo de la pagina	3	3	9
		Repudio o negación a posteriori de cambios realizados en el código fuente	2	4	8
		Fuga de información	3	4	12
		Alteración accidental del código fuente	4	4	16
	Web service	Saturación de la web Service	5	5	25

		Modificación deliberadas del código fuente	3	4	12
		Divulgación de la información de la web Service	3	4	12
		Repudio Negación a posteriori de cambios realizados en el código fuente	3	4	12
		Alteración del código fuente de la Web Service	3	4	12
		Error accidental en el desarrollo de la Web Service	4	4	**16**
Software	Apache Tomcap	Difusión de software dañino virus	3	3	9
		Falla del funcionamiento del software	4	3	12
		Divulgación de información	2	2	4
		Saturación de operación del software	4	4	**16**
		Alteración intencional del programa	3	2	6
	Correo Electrónico Microsoft	Equivocación por uso de servicio	3	3	9
		Difusión de software dañino virus	3	3	9
		Uso indebido del software	4	3	12
		Negación de haber recibió un mensaje	4	4	**16**
	Genexus	Difusión de software dañino virus	3	3	9
		Falla del funcionamiento del software	3	4	12
		Abuso de privilegios de acceso	5	3	**15**
		Alteración intencional del programa	3	3	9
	IBM AS/400	Difusión de software dañino virus	3	4	12
		Falla del funcionamiento del software	4	4	**16**
		Saturación de la operación del software	5	5	**25**
		Alteración intencional del programa	3	3	9
		Hacking/ Cracking	4	4	**16**
	Linux	Equivocación por uso de servicio	4	2	8
		Difusión de software dañino virus	1	1	1
		Uso no indebido del software	3	3	9
		Saturación de operación del software	4	4	**16**
	.NET	Uso no previsto	3	4	12
		Falla del funcionamiento del software	2	4	8
		Hacking/ Cracking	2	3	6
	Office	Propagación de software contaminado virus	4	3	12
		Abuso de beneficios de acceso	3	3	9
		Alteración intencional del programa	4	3	12
		Uso no Previsto	3	4	12
	QlickView	Difusión de software dañino virus	3	3	9
		Instalación de software no licenciado	2	1	2
		Alteración del funcionamiento del software	3	2	6
		Uso no Previsto	3	2	6
		Alteración intencional del programa	3	3	9

	Software Propio	Difusión de software dañino virus	3	3	9
		Uso no Previsto	3	3	9
		Alteración intencional del programa	3	3	9
	SQL Server 2012	Difusión de software dañino virus	3	3	9
		Instalación de software no licenciado	2	1	2
		Abuso de beneficios de acceso	3	4	12
		Uso no permitido de SQL	2	3	6
		Alteración del funcionamiento del software	4	3	12
		Falla del funcionamiento del software	4	2	8
	Windows	Equivocación por uso de servicio	1	3	3
		Difusión de software dañino virus	5	5	25
		Instalación de Windows no licenciado	2	1	2
		Instalaciones de programas de origen sospechoso	4	5	20
		Falla del funcionamiento del software	5	4	20
		Abuso de beneficios de acceso	4	3	12
		Uso no permitido de Windows	3	3	9
		Alteración intencional del Windows	3	2	6

Fuente: Elaboración propia

3.1.13.Tratamiento de riesgos

Una vez analizado los riesgos, se procederá a decidir qué medidas o actividades o acciones se deberá elegir para que los activos no sean afectados por los riesgos, para ellos se aplicaran estrategias que se muestra en la tabla N° 24.

Tabla N° 24, Medidas frente al riesgo

Formas de mitigar	Explicación
Aceptar	Consiste en aceptar la posibilidad que pueda ocurrir un riesgo sin tomar acción alguna
Reducir	Aplicar controles de seguridad implementando de medidas de seguridad
Eliminar	Consiste en eliminar una actividad o un procedimiento que pueda causar alguna amenaza
Compartir o transferir	Contratar a una empresa para que asuma el compromiso de velar por la integridad del activo

*Fuente: (ISOTools Excel*lence, 2014)

Para aplicar las medidas o las actividades que se va tomar para frenar a los riesgos, se seleccionará aquellos riesgos con nivel significativo que

necesitan un tratamiento inmediato por ser los activos de mayor nivel de riesgos. En la tabla N° 25, se muestra las acciones o medidas que se tomará para mitigar después de seleccionar los riesgos de mayor nivel.

Tabla N° 25, Medidas frente al riesgo

Tipo de activo	Nombre activo	Amenazas	[R]	Formas de mitigar
Auxiliar	Aire acondicionado	Posibilidad de sufrir incendio accidental	6	Reducir
		Posibilidad de que se contamine polvos suciedad	4	Aceptar
		Posibilidad de sufrir desastre natural fenómeno sísmico	12	Aceptar
		Posibilidad de sufrir fugas por escape de agua	12	Reducir
		Posibilidad de ocurrir fallas en el equipo	15	Transferir
		Cese de alimentación eléctrica	9	Reducir
	Cableado de Red	Posibilidad de ocurrir un incendio accidental o deliberado	9	Reducir
		Posibilidad de fugas de agua accidental o deliberada	6	Aceptar
		Posibilidad de equivocaciones en la instalación	12	Reducir
		Ataque destructivo vandalismo	2	Aceptar
	Cableado Eléctrico	Posibilidad de un corte eléctrico	15	Transferir
		Posibilidad de fugas de agua de manera accidental o deliberada	6	Aceptar
		Sobrecarga Eléctrica	9	Reducir
		Posibilidad de que el fuego acabe con el cable	6	Reducir
	Cajas fuertes	Posibilidad de acceso no autorizado	6	Eliminar
	Escritorios y armarios	Posibilidad de que el fuego acabe el escritorio	6	Reducir
		Degradación por consecuencia del tiempo	8	Aceptar
		Posibilidad de vandalismo	2	Aceptar
	Fuentes de alimentación	Probabilidad de que las llamas del fuego acaben con la fuente	4	Reducir
		Cese de alimentación eléctrica	9	Reducir
		Fuga de escape de agua	4	Aceptar
Comunicación	Internet Claro	Acceso no permitido internet	12	Reducir
		Abuso de beneficios de acceso	15	Reducir
		Caída de los servicios de internet	9	Transferir
	Protocolo	Interceptación del protocolo	12	Reducir

	transferencia de archivos	Monitorización del tráfico por usuarios externos	9	Reducir
		Suplantación de identidad	6	Reducir
		Acceso no autorizado de transferencia de datos	12	Reducir
		Caída de los servicios de transferencia	20	Reducir
		Alteración de transmisión de datos	12	Reducir
	Red Local	Interceptación de red	6	Reducir
		Monitorización del trafico	9	Reducir
		Acceso no permitido a la red local	9	Reducir
		Caída de red de comunicaciones	16	Transferir
Datos	Código Fuente programas	Eliminación del código fuente	6	Reducir
		Alteraciones del código fuente	12	Reducir
		Fuga de información por indiscreción verbal o medios electrónicos	12	Reducir
		Error en el desarrollo del código fuente	20	Reducir
	Copias de respaldo	Eliminación de las copias de respaldo	12	Reducir
		Equivocación al realizar copias de respaldo	16	Reducir
		Modificación deliberada de las copias de seguridad	12	Eliminar
		Fugas de información por medios electrónicos	9	Reducir
	Datos de control acceso	Divulgación de los acceso de control	6	Reducir
		Eliminación intencional de la base de datos de control de acceso	6	Reducir
		Modificación de los la información de control acceso	9	Eliminar
		Manipulación de registro de actividad	6	Reducir
		Acceso no autorizado a los datos de control	4	Eliminar
	Manuales	Equivocación al momento de crear de los manuales	9	Reducir
		Fuga de información revelación de los manuales	12	Reducir
		Manipulación de los datos de los manuales	6	Eliminar
		Eliminación de los manuales	16	Reducir
		Alteraciones de los registro de manuales	9	Reducir
	Reportes de control	Manipulación de los registros	6	Eliminar
		Equivocación al realizar el reporte de control	9	Reducir
		Eliminación de reportes de control	6	Reducir
		Fugas de información por medios electrónicos	8	Reducir
Esenciales	Documentos	Eliminación de documentos	12	Reducir

		Fugas de información por medios electrónicos	6	Reducir
		Manipulación de documentos	9	Eliminar
		Alteración de documentos	12	Eliminar
	Registro de base de datos	Eliminación de la base de datos por error o deliberadamente	**20**	Eliminar
		Fugas de información por medios electrónicos	**15**	Reducir
		Registros incompletos	**16**	Reducir
		Alteración intencional de registros	**16**	Reducir
		Acceso no autorizado a los registros	**16**	Reducir
		Alteración accidental de los registros	**20**	Reducir
		Introducción de datos erróneos	**20**	Reducir
Hardware	Gateways analógicos	Posibilidad de que el fuego acabe	6	Reducir
		Acceso no autorizado personal interno	4	Reducir
		Desconexión del equipo	9	Reducir
		Corte de suministro eléctrico	9	Reducir
	Computadoras	Posibilidad de que el fuego acabe	12	Reducir
		Desgaste debido a su uso	12	Reducir
		Avería del hardware	**15**	Reducir
		Uso ilícito de la computadora	**16**	Reducir
		Desconexión de la PC	12	Reducir
		Errores en el mantenimiento actualización del equipo	12	Reducir
		Contaminación mecánica polvo	**20**	Reducir
		Corte de suministro eléctrico	9	Reducir
	Firewall	Posibilidad de que el fuego acabe	6	Reducir
		Acceso no autorizado	6	Reducir
		Radiación electromagnética	2	Aceptar
		Corte de suministro eléctrico	6	Transferir
		Error de mantenimiento actualización del equipo	6	Transferir
	Impresoras	Desgaste debido a su uso	**20**	Reducir
		Avería del hardware	12	Transferir
		Desconexión del equipo	8	Reducir
		Errores en el mantenimiento actualización del equipo	6	Transferir
		Corte de suministro eléctrico	9	Reducir
		Posibilidad de que el fuego acabe	4	Reducir
	IP-10 Ceragon	Corte de suministro eléctrico	6	Reducir

		Errores en el mantenimiento actualización del equipo	4	Eliminar
		Radiación electromagnética	2	Aceptar
	Laptop	Desgaste debido a su uso	16	Reducir
		Avería del hardware	12	Reducir
		Uso ilícito del laptop	20	Reducir
		Robo de laptop	6	Reducir
		Corte de suministro eléctrico	3	Aceptar
	Reloj Biométrico	Desgaste debido a su uso	16	Reducir
		Avería del hardware	9	Transferir
		Radiación electromagnética	2	Aceptar
		Corte de suministro eléctrico	9	Transferir
	Router	Contaminación mecánica polvo	6	Reducir
		Desconexión del equipo	8	Reducir
		Corte de suministro eléctrico	4	Aceptar
		Errores en el mantenimiento actualización del equipo	6	Transferir
	Servidores	Posibilidad de que el fuego acabe	9	Reducir
		Posibilidad de un suceso sísmico	9	Aceptar
		Contaminación mecánica polvo	15	Reducir
		Avería del hardware	16	Reducir
		Perjuicio en el mantenimiento del servidor	15	Transferir
		Desconexión del equipo	9	Reducir
	Switch	Posibilidad de que el fuego acabe	6	Reducir
		Contaminación mecánica polvo	8	Reducir
		Perjuicio en el mantenimiento del switch	9	Transferir
		Desconexión del equipo	6	Reducir
	UPS	Posibilidad de que el fuego acabe	6	Reducir
		Contaminación mecánica polvo	6	Reducir
		Perjuicio en el mantenimiento del equipo	4	Transferir
		Desconexión del equipo	9	Reducir
Instalación	Data Center	Divulgación de la geolocalización	16	Reducir
		Modificación deliberadas por perjuicio	9	Eliminar
		Posibilidad de que el fuego acabe de origen accidental o deliberada	9	Reducir
		Posibilidad de ocurrir desastre natural sismo	9	Aceptar
		Acceso no autorizado aprovechando fallo del sistema	9	Reducir

		Posibilidad de inundación accidental o deliberada	12	Transferir
		Fuga de información revelación por discreción	12	Reducir
	Oficinas	Acceso no autorizado a las oficinas	9	Reducir
		Posibilidad de ocurrir sismo o terremoto	9	Aceptar
		Posibilidad de ocurrir inundación de origen deliberada o accidental	6	Reducir
		Probabilidad de que las llamas acaben con las oficinas	4	Reducir
Media	Cartuchos de datos Backup	Falla de funcionamiento del cartucho	12	Reducir
		Contaminación mecánica por polvo suciedad	9	Reducir
		Degradación por consecuencia del tiempo	3	Aceptar
		Alteración accidental del etiquetado de cartuchos	6	Reducir
		Uso indebido del equipo	6	Reducir
		Perdida del cartucho	6	Reducir
		Destrucción deliberada de los cartuchos	12	Reducir
		Posibilidad de que el fuego acabe con los cartuchos	6	Reducir
	Disco Externo Toshiba storage	Avería del hardware	16	Reducir
		Contaminación mecánica por polvo suciedad	6	Reducir
		Robo de Disco	9	Reducir
		Destrucción deliberada del disco	4	Aceptar
		Degradación por consecuencia del tiempo	12	Aceptar
	NAS	Falla de funcionamiento del NAS	9	Transferir
		Probabilidad de que el fuego acabe	6	Reducir
		Degradación por consecuencia del tiempo	6	Aceptar
		Error en la actualización del equipo	6	Transferir
Personal	Trabajadores	Indisponibilidad por ausencia deliberada	12	Aceptar
		Extorsión por obligar a obrar en diferentes sentido	9	Reducir
		Ingeniería social exceso de buena fe	12	Reducir
Servicio	Páginas web	Saturación de página web	16	Reducir
		Revelación de código fuente de la pagina	9	Reducir
		Modificación intencional de código fuente	9	Reducir
		Error accidental en el desarrollo de la pagina	9	Reducir
		Repudio o negación a posteriori de cambios realizados en el código fuente	8	Reducir
		Fuga de información	12	Reducir

		Alteración accidental del código fuente	16	Reducir
	Web service	Saturación de la web Service	25	Reducir
		Modificación deliberadas del código fuente	12	Reducir
		Divulgación de la información de la web Service	12	Reducir
		Repudio Negación a posteriori de cambios realizados en el código fuente	12	Reducir
		Alteración del código fuente de la Web Service	12	Reducir
		Error accidental en el desarrollo de la Web Service	16	Reducir
Software	Apache Tomcat	Difusión de software dañino virus	9	Reducir
		Falla del funcionamiento del software	12	Aceptar
		Divulgación de información	4	Aceptar
		Saturación de operación del software	16	Reducir
		Alteración intencional del programa	6	Reducir
	Correo Electrónico Microsoft	Equivocación por uso de servicio	9	Reducir
		Difusión de software dañino virus	9	Reducir
		Uso indebido del software	12	Reducir
		Negación de haber recibió un mensaje	16	Reducir
	Genexus	Difusión de software dañino virus	9	Reducir
		Falla del funcionamiento del software	12	Reducir
		Abuso de privilegios de acceso	15	Reducir
		Alteración intencional del programa	9	Reducir
	IBM AS/400	Difusión de software dañino virus	12	Transferir
		Falla del funcionamiento del software	16	Transferir
		Saturación de la operación del software	25	Reducir
		Alteración intencional del programa	9	Reducir
		Hacking/ Cracking	16	Reducir
	Linux	Equivocación por uso de servicio	8	Aceptar
		Difusión de software dañino virus	1	Aceptar
		Uso no indebido del software	9	Reducir
		Saturación de operación del software	16	Transferir
	.NET	Uso no previsto de software	12	Reducir
		Falla del funcionamiento del software	8	Transferir
		Hacking/ Cracking	6	Reducir
	Office	Propagación de software contaminado virus	12	Reducir
		Abuso de beneficios de acceso	9	Reducir

		Alteración intencional del programa	12	Reducir
		Uso no Previsto	12	Reducir
	QlickView	Difusión de software dañino virus	9	Reducir
		Instalación de software no licenciado	2	Aceptar
		Alteración del funcionamiento del software	6	Reducir
		Uso no Previsto	6	Aceptar
		Alteración intencional del programa	9	Eliminar
	Software Propio	Difusión de software dañino virus	9	Reducir
		Uso no Previsto	9	Reducir
		Alteración intencional del programa	9	Reducir
	SQL Server 2012	Difusión de software dañino virus	9	Reducir
		Instalación de software no licenciado	2	Aceptar
		Abuso de beneficios de acceso	12	Reducir
		Uso no adecuado de SQL	6	Aceptar
		Alteración del funcionamiento del software	12	Reducir
		Falla del funcionamiento del software	8	Aceptar
	Windows	Equivocación por uso de servicio	3	Aceptar
		Difusión de software dañino virus	25	Reducir
		Instalación de Windows no licenciado	2	Aceptar
		Instalaciones de programas de origen sospechoso	20	Reducir
		Falla del funcionamiento del software	20	Reducir
		Abuso de privilegios de acceso	12	Reducir
		Uso no adecuado de Windows	9	Reducir
		Modificación intencional del Windows	6	Reducir

Fuente: Elaboración propia

3.1.14.Controles de seguridad de información

En la siguiente tabla N° 26, se detallan las los controles de seguridad que se tomaran en cuenta para disminuir los riesgos que afecta a las seguridad de los activos de información, también las vulnerabilidades que presentan dichos activos, del mismo modo las amenazas que deterioran a los bienes de información. A Cada riesgo se le asignó controles de seguridad de acuerdo a las reglas de la norma ISO 27001. El objetivo de los controles es considerar para evitar el posible riesgo.

Tabla N° 26, Controles de seguridad de información

Tipo de activo	Nombre activo	Amenazas	[R]	Medidas frente al riesgo	Vulnerabilidades	Controles según la ISO 27001
Auxiliar	Aire acondicionado	Posibilidad de sufrir incendio accidental	6	Reducir	Ubicación de aire acondicionado en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Posibilidad de que se contamine polvos suciedad	4	Reducir	Susceptibilidad del equipamiento a contaminación mecánica	A.11.2.1 Ubicación y protección del equipo
		Posibilidad de sufrir desastre natural fenómeno sísmico	12	Aceptar	Condiciones de los equipos donde los activos son fácilmente afectado por desastres	A.11.1.1 Perímetro de seguridad física
		Posibilidad de sufrir fugas por escape de agua	12	Reducir	El aire acondicionado falta de protección física adecuada ante la posibilidad de fuga de agua	A.11.1.4 Protección contra amenazas externas y ambientales
		Posibilidad de ocurrir fallas en el equipo	15	Transferir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Cese de alimentación eléctrica	9	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
	Cableado de Red	Posibilidad de ocurrir un incendio accidental o deliberado	9	Reducir	Ubicación de aire acondicionado en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Posibilidad de fugas de agua accidental o deliberada	6	Reducir	El cableado de red falta de protección física adecuada ante la posibilidad de fuga de agua	A.11.1.4 Protección contra amenazas externas y ambientales
		Posibilidad de equivocaciones en la instalación	12	Reducir	Insuficiente entrenamiento de personal	A.13.1.2 Seguridad de los servicios de red
	Cableado Eléctrico	Posibilidad de un corte eléctrico	15	Transferir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Posibilidad de fugas de agua accidental o deliberada	6	Reducir	El Cableado eléctrico falta de protección física adecuada ante la posibilidad de fuga de agua	A.11.1.4 Protección contra amenazas externas y ambientales
		Posibilidad de que el fuego acabe con el cable	6	Reducir	Ubicación de cableados eléctricos en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales

	Caja fuerte	Posibilidad de acceso no autorizado	6	Eliminar	Falta de protección de datos e información	A.9.2.6 Eliminación o ajuste de derechos de acceso
	Escritorios y armarios	Posibilidad de que el fuego acabe el escritorio	6	Reducir	Ubicación de Escritorios y armarios en lugares falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Degradación por consecuencia del tiempo	8	Aceptar	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
	Fuentes de alimentación	Posibilidad de que el fuego acabo con la fuente	4	Reducir	Ubicación de Fuentes de alimentación en lugares falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Cese de alimentación eléctrica	9	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Fuga de escape de agua	4	Reducir	La fuente de alimentación falta de protección física adecuada ante la posibilidad de fuga de agua	A.11.1.4 Protección contra amenazas externas y ambientales
		Posibilidad de sobrecarga eléctrica	9	Transferir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
Comunicación	Internet Claro	Acceso no autorizado internet	12	Transferir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información
		Abuso de privilegios de acceso	**15**	Reducir	Falta de protección de datos e información	A.9.2.5 Revisión de los derechos de acceso del usuario
		Caída de los servicios de internet	9	Transferir	Capacidad insuficiente de datos	A.12.1.1 Procedimientos documentados de operación
	Protocolo transferencia de archivos	Interceptación del protocolo	12	Reducir	Falta de protección de seguridad de red	A.13.1.2 Seguridad de los servicios de red
		Monitorización del tráfico por usuarios internos	9	Reducir	Falta de protección de trafico de seguridad de trafico de red	A.13.1.2 Seguridad de los servicios de red
		Suplantación de identidad	6	Reducir	Falta de protección de datos de información	A.9.1.1 Política de control de acceso
		Acceso no autorizado de transferencia de datos	12	Reducir	Falta de protección de datos e información	A.9.2.5 Revisión de los derechos de acceso del usuario
		Caída de los servicios de transferencia	**20**	Reducir	Capacidad insuficiente de recursos	A.12.1.1 Procedimientos documentados de operación

		Alteración de transmisión de datos	12	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso
	Red Local	Interceptación de red	6	Reducir	Falta de protección de datos e información	A.13.1.2 Seguridad de los servicios de red
		Monitorización del trafico	9	Reducir	Falta de protección de datos e información	A.9.1.2 Acceso a redes y a servicios de red
		Acceso no autorizado a la red local	9	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información
		Caída de red de comunicaciones	**16**	Transferir	Inadecuado protección de red de comunicaciones	A.13.1.2 Seguridad de los servicios de red
Datos	Código Fuente programas	Eliminación del código fuente	6	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado Reglas para control de acceso no definidos con claridad	A.9.1.1 Política de control de acceso A.9.4.5 Control de acceso al código fuente del programa
		Alteraciones del código fuente	12	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso
		Fuga de información por indiscreción verbal o medios electrónicos	12	Reducir	Información no protegida	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información
		Error en el desarrollo del código fuente	**20**	Reducir	Única copia, sólo una copia de la información	A.12.1.4 Separación de ambientes de desarrollo, prueba y operacionales
	Copias de respaldo	Eliminación de las copias de respaldo	12	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Equivocación al realizar copias de respaldo	**16**	Reducir	Única copia, sólo una copia de la información	A.12.3.1 Copia de seguridad de la información
		Modificación deliberada de las copias de respaldo	12	Eliminar	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso

		Fugas de información por medios electrónicos	9	Reducir	Información no protegida	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información
	Datos de control acceso	Divulgación de los acceso de control	6	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información
		Eliminación intencional de los datos de control	6	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Modificación de los datos de control	9	Eliminar	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Manipulación de registro de actividad	6	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Acceso no autorizado a los datos de control	4	Eliminar	Falta de protección de datos e información	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
	Manuales	Equivocación al momento de crear de los manuales	9	Reducir	Falta de supervisión de trabajos	A.18.2.3 Revisión de cumplimiento técnico
		Fuga de información revelación de los manuales	12	Reducir	Información no protegida	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información
		Manipulación de los datos de los manuales	6	Eliminar	Falta de protección de datos e información	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Eliminación de los manuales	**16**	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Alteraciones de los registro de manuales	9	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso

	Reportes de control	Manipulación de los registros	6	Eliminar	Falta de protección de datos e información	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Equivocación al realizar el reporte de control	9	Reducir	Falta de control de acceso	A.12.1.1 Procedimientos documentados de operación
		Eliminación de reportes de control	6	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Fugas de información por medios electrónicos	8	Reducir	Información no protegida	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información
Esenciales	Documentos	Eliminación de documentos	12	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Fugas de información por medios electrónicos	6	Reducir	Información no protegida	A.6.2.1 Política sobre dispositivos móviles A.5.1.1 Políticas para seguridad de la información
		Manipulación de documentos	9	Eliminar	Falta de protección de datos e información	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Alteración de documentos	12	Eliminar	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
	Registro de base de datos	Eliminación de la base de datos por error o deliberadamente	**20**	Eliminar	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Fugas de información por medios electrónicos	**15**	Reducir	Información no protegida	A.5.1.1 Políticas para seguridad de la información
		Registros incompletos	**16**	Reducir	Falta de supervisión de trabajos	A.18.2.3 Revisión de cumplimiento técnico
		Alteración intencional de registros	**16**	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso

		Acceso no autorizado a los registros	16	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información
		Alteración accidental de los registros	20	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso A.9.4.5 Control de acceso al código fuente del programa
		Introducción de datos erróneos	20	Reducir	Falta de supervisión de trabajos	A.18.2.3 Revisión de cumplimiento técnico
Hardware	Gateways analógicos	Posibilidad de que el fuego acabe	6	Reducir	Ubicación de Gateway analógicos en lugares falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Acceso no autorizado personal interno	4	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información
		Desconexión del equipo	9	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Corte de suministro eléctrico	9	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
	Computadoras	Posibilidad de que el fuego acabe	12	Reducir	Ubicación de computadoras en lugares falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Desgaste debido a su uso	12	Reducir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Avería del hardware	15	Reducir	Falta de revisión del equipo	A.15.1.2 Tratamiento de la seguridad en contratos con proveedores
		Uso ilícito de la computadora	16	Reducir	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Desconexión de la PC	12	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Errores en el mantenimiento actualización del equipo	12	Reducir	Única copia, sólo una copia de la información	A.12.3.1 Copia de seguridad de la información
		Contaminación mecánica polvo	20	Reducir	Susceptibilidad del equipamiento a contaminación mecánica	A.11.2.1 Ubicación y protección del equipo A.11.2.9 Política de pantalla y

						escritorio limpio
		Corte de suministro eléctrico	9	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
	Firewall	Posibilidad de que el fuego acabe	6	Reducir	Ubicación equipo de hardware Firewall en lugares falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Acceso no autorizado	6	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información
		Corte de suministro eléctrico	6	Transferir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Error de mantenimiento actualización del equipo	6	Transferir	Única copia, sólo una copia de la información	A.12.3.1 Copia de seguridad de la información
	Impresoras	Desgaste debido a su uso	**20**	Reducir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Avería del hardware	12	Transferir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Desconexión del equipo	8	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Errores en el mantenimiento actualización del equipo	6	Transferir	Falta de mantenimiento	A.12.3.1 Copia de seguridad de la información
		Corte de suministro eléctrico	9	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Posibilidad de que el fuego acabe	4	Reducir	Ubicación de Impresoras en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
	IP-10 Ceragon	Corte de suministro eléctrico	6	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Errores en el mantenimiento actualización del equipo	4	Eliminar	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.4.1 Restricción al acceso a la información
	Laptop	Desgaste debido a su	**16**	Reducir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo

		uso				
		Avería del hardware	12	Reducir	Falta de control de mantenimiento	A.12.1.1 Procedimientos documentados de operación
		Uso ilícito del laptop	**20**	Reducir	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Robo de laptop	6	Reducir	Falta de control de acceso de personas externas	A.9.1.1 Política de control de acceso
		Corte de suministro eléctrico	3	Aceptar	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
	Reloj Biométrico	Desgaste debido a su uso	**16**	Reducir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Avería del hardware	9	Transferir	Falta de control de mantenimiento de hardware	A.12.1.1 Procedimientos documentados de operación
		Corte de suministro eléctrico	9	Transferir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
	Router	Contaminación mecánica polvo	6	Reducir	Susceptibilidad del equipamiento a contaminación mecánica	A.11.2.1 Ubicación y protección del equipo
		Desconexión del equipo	8	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Corte de suministro eléctrico	4	Aceptar	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
		Errores en el mantenimiento actualización del equipo	6	Transferir	Única copia, sólo una copia de la información	A.12.3.1 Copia de seguridad de la información
	Servidores	Posibilidad de que el fuego acabe	9	Reducir	Ubicación de Servidores en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Posibilidad de un suceso sísmico	9	Aceptar	Condiciones de los equipos donde los activos son fácilmente afectado por desastres	A.11.1.1 Perímetro de seguridad física
		Contaminación mecánica polvo	**15**	Reducir	Susceptibilidad del equipamiento a contaminación mecánica	A.11.2.1 Ubicación y protección del equipo

		Avería del hardware	16	Reducir	Falta de control de mantenimiento de hardware	A.12.1.1 Procedimientos documentados de operación
		Perjuicio en el mantenimiento del servidor	15	Transferir	Inadecuado mantenimiento de equipos de hardware	A.12.3.1 Copia de seguridad de la información
		Desconexión del equipo	9	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
	Switch	Posibilidad de que el fuego acabe	6	Reducir	Ubicación de Switch en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Contaminación mecánica polvo	8	Reducir	Susceptibilidad del equipamiento a contaminación mecánica	A.11.2.1 Ubicación y protección del equipo
		Perjuicio en el mantenimiento del switch	9	Transferir	Inadecuado mantenimiento de equipos de hardware	A.12.3.1 Copia de seguridad de la información
		Desconexión del equipo	6	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
	UPS	Posibilidad de que el fuego acabe	6	Reducir	Ubicación de UPS en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Contaminación mecánica polvo	6	Reducir	Susceptibilidad del equipamiento a contaminación mecánica	A.11.2.1 Ubicación y protección del equipo
		Perjuicio en el mantenimiento del equipo	4	Transferir	Inadecuado mantenimiento de equipos de hardware	A.12.3.1 Copia de seguridad de la información
		Desconexión del equipo	9	Reducir	Funcionamiento no fiable de la UPS	A.11.2.4 Mantenimiento de equipo A.11.2.2 Servicios públicos
Instalación	Data Center	Divulgación de la geolocalización	16	Reducir	Información no protegida	A.9.4.1 Restricción al acceso a la información
		Modificación deliberadas por perjuicio	9	Eliminar	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Posibilidad de que el fuego acabe de origen accidental o deliberada	9	Reducir	Ubicación de Data Center en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales

		Posibilidad de ocurrir desastre natural sismo	9	Aceptar	Condiciones de los equipos donde los activos son fácilmente afectado por desastres	A.11.1.1 Perímetro de seguridad física
		Acceso no autorizado aprovechando fallo del sistema	9	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información A.9.2.5 Revisión de los derechos de acceso del usuario
		Posibilidad de inundación accidental o deliberada	12	Transferir	Ubicación física inadecuada ante la posibilidad de fuga de agua	A.11.1.4 Protección contra amenazas externas y ambientales
		Fuga de información revelación por discreción	12	Reducir	Información no protegida	A.5.1.1 Políticas para seguridad de la información
	Oficinas	Acceso no autorizado a las oficinas	9	Reducir	Acceso no autorizado a instalaciones	A.9.4.1 Restricción al acceso a la información
		Posibilidad de ocurrir sismo o terremoto	9	Aceptar	Condiciones de los equipos donde los activos son fácilmente afectado por desastres	A.11.1.1 Perímetro de seguridad física
		Posibilidad de ocurrir inundación de origen deliberada o accidental	6	Reducir	Ubicación física inadecuada ante la posibilidad de fuga de agua	A.11.1.4 Protección contra amenazas externas y ambientales
		Posibilidad de que el fuego acabe con las oficinas	4	Reducir	Oficinas con falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
Media	Cartuchos de datos Backup	Falla de funcionamiento del cartucho	12	Reducir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Contaminación mecánica por polvo suciedad	9	Reducir	Susceptibilidad del equipamiento a contaminación mecánica	A.11.2.1 Ubicación y protección del equipo
		Degradación por consecuencia del tiempo	3	Aceptar	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Alteración accidental del etiquetado de cartuchos	6	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso
		Uso no indebido del equipo	6	Reducir	Falta de control de acceso Inadecuada supervisión del	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de

					trabajo de los empleados	empleo
		Posibilidad de que el fuego acabe con los cartuchos	6	Reducir	Ubicación de cartuchos en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
	Disco Externo Toshiba storage	Avería del hardware	16	Reducir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Contaminación mecánica por polvo suciedad	6	Reducir	Susceptibilidad del equipamiento a contaminación mecánica	A.11.2.1 Ubicación y protección del equipo
		Eliminación intencional del Disco externo	6	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso A.9.2.6 Eliminación o ajuste de derechos de acceso
		Robo de Disco	9	Reducir	Falta de control de acceso de personas externas	A.9.1.1 Política de control de acceso
		Degradación por consecuencia del tiempo	12	Aceptar	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
	NAS	Falla de funcionamiento del NAS	9	Transferir	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Posibilidad de que el fuego acabe	6	Reducir	Ubicación de NAS en lugares de falta de protección contra fuegos	A.11.1.4 Protección contra amenazas externas y ambientales
		Degradación por consecuencia del tiempo	6	Aceptar	Falta de mantenimiento	A.11.2.4 Mantenimiento de equipo
		Error en la actualización del equipo	6	Transferir	Única copia, sólo una copia de la información	A.12.3.1 Copia de seguridad de la información
Personal	Trabajadores	Indisponibilidad por ausencia deliberada	12	Aceptar	Empleados desmotivados o disconformes Inadecuada supervisión del trabajo de los empleados	A.7.3.1 Terminación o cambio de condiciones del empleo
		Extorsión por obligar a obrar en determinado sentido	9	Reducir	Inadecuada separación de tareas	A.7.1.2 Términos y condiciones de empleo
		Ingeniería social abuso de buena fe	12	Reducir	Inadecuados derechos de usuario	A.7.1.2 Términos y condiciones de empleo

Servicio	Páginas web	Saturación de página web	16	Reducir	Capacidad insuficiente de recursos	A.13.1.1 Controles de red A.12.1.1 Procedimientos documentados de operación
		Revelación de código fuente de la pagina	9	Reducir	Información no protegida	A.9.4.1 Restricción al acceso a la información
		Modificación intencional de código fuente	9	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso
		Error accidental en el desarrollo de la pagina	9	Reducir	Única copia, sólo una copia de la información	A.12.1.4 Separación de ambientes de desarrollo, prueba y operacionales
		Repudio o negación a posteriori de cambios realizados en el código fuente	8	Reducir	Falta de registro de cambios de código fuente.	A.12.4.1 Registro de eventos
		Fuga de información	12	Reducir	Información no protegida	A.5.1.1 Políticas para seguridad de la información
		Alteración accidental del código fuente	16	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado Reglas para control de acceso no definidos con claridad	A.9.1.1 Política de control de acceso A.9.4.5 Control de acceso al código fuente del programa
	Web service	Saturación de la web Service	25	Reducir	Capacidad insuficiente de recursos	A.13.1.1 Controles de red A.12.1.1 Procedimientos documentados de operación
		Modificación deliberadas del código fuente	12	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso
		Divulgación de la información de la web Service	12	Reducir	Información no protegida	A.9.4.1 Restricción al acceso a la información
		Repudio Negación a posteriori de cambios realizados en el código fuente	12	Reducir	Falta de evidencia en envío o recepción de mensajes	A.12.4.1 Registro de eventos
		Alteración del código fuente de la Web Service	12	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso

		Error accidental en el desarrollo de la Web Service	**16**	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.12.1.4 Separación de ambientes de desarrollo, prueba y operacionales
Software	Apache Tomcap	Difusión de software dañino virus	9	Reducir	Falta de protección actualizada	A.12.2.1 Controles contra software malicioso
		Falla del funcionamiento del software	12	Aceptar	Mantenimiento inadecuado	A.14.2.8 Prueba de seguridad del sistema A.14.2.9 Prueba de aceptación del sistema
		Divulgación de información	4	Aceptar	Información no protegida	A.9.1.1 Política de control de acceso
		Saturación de operación del software	**16**	Reducir	Capacidad insuficiente de recursos	A.13.1.1 Controles de red A.12.1.1 Procedimientos documentados de operación
		Alteración intencional del programa	6	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso
	Correo Electrónico Microsoft	Equivocación por uso de servicio	9	Reducir	Falta de capacitación del empleado	A.12.4.1 Registro de eventos
		Difusión de software dañino virus	9	Reducir	Falta de protección actualizada	A.12.2.1 Controles contra software malicioso
		Uso no indebido del software	12	Reducir	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Negación de haber recibió un mensaje	**16**	Reducir	Falta de evidencia en envío o recepción de mensajes	A.12.4.1 Registro de eventos
	Genexus	Difusión de software dañino virus	9	Reducir	Falta de protección actualizada	A.12.2.1 Controles contra software malicioso
		Falla del funcionamiento del software	12	Reducir	Mantenimiento inadecuado	A.14.2.8 Prueba de seguridad del sistema A.14.2.9 Prueba de aceptación del sistema
		Abuso de privilegios de acceso	**15**	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información
		Alteración intencional del programa	9	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso

	IBM AS/400	Difusión de software dañino virus	12	Transferir	Falta de protección actualizada Bases de datos con protección desactualizada contra códigos maliciosos	A.12.2.1 Controles contra software malicioso
		Falla del funcionamiento del software	**16**	Transferir	Mantenimiento inadecuado	A.14.2.8 Prueba de seguridad del sistema A.14.2.9 Prueba de aceptación del sistema
		Saturación de la operación del software	**25**	Reducir	Capacidad insuficiente de recursos	A.13.1.1 Controles de red A.12.1.1 Procedimientos documentados de operación
		Alteración intencional del programa	9	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso
		Hacking/ Cracking	**16**	Reducir	Falta de protección actualizada	A.12.2.1 Controles contra software malicioso
	Linux	Equivocación por uso de servicio	8	Aceptar	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Uso no indebido del software	9	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso
		Saturación de operación del software	**16**	Transferir	Capacidad insuficiente de recursos	A.13.1.1 Controles de red A.12.1.1 Procedimientos documentados de operación
	.NET	Uso no indebido del software	12	Reducir	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Falla del funcionamiento del software	8	Transferir	Mantenimiento inadecuado	A.14.2.8 Prueba de seguridad del sistema A.14.2.9 Prueba de aceptación del sistema
		Hacking/ Cracking	6	Reducir	Falta de protección actualizada Bases de datos con protección desactualizada contra códigos maliciosos	A.12.2.1 Controles contra software malicioso
	Office	Difusión de software dañino virus	12	Reducir	Falta de protección actualizada	A.12.2.1 Controles contra software malicioso
		Abuso de privilegios de	9	Reducir	Falta de protección de datos e	A.9.4.1 Restricción al acceso a la

		acceso			información	información
		Alteración intencional del programa	12	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso
		Uso no indebido del software	12	Reducir	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
	QlickView	Difusión de software dañino virus	9	Reducir	Falta de protección actualizada Bases de datos con protección desactualizada contra códigos maliciosos	A.12.2.1 Controles contra software malicioso
		Alteración del funcionamiento del software	6	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso
		Uso no indebido del software	6	Aceptar	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Alteración intencional del programa	9	Eliminar	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso A.9.4.5 Control de acceso al código fuente del programa
	Software Propio	Difusión de software dañino virus	9	Reducir	Falta de protección actualizada	A.12.2.1 Controles contra software malicioso
		Uso no indebido del software	9	Reducir	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Alteración intencional del programa	9	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado Requisitos para desarrollo de software no definidos con claridad	A.9.1.1 Política de control de acceso A.9.4.5 Control de acceso al código fuente del programa A.14.2.1 Política de desarrollo seguro
	SQL Server 2012	Difusión de software dañino virus	9	Reducir	Falta de protección actualizada Bases de datos con protección desactualizada contra códigos maliciosos	A.12.2.1 Controles contra software malicioso
		Abuso de privilegios de acceso	12	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información A.9.2.5 Revisión de los derechos de

						acceso del usuario
		Uso no indebido del software	6	Aceptar	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Alteración del funcionamiento del software	12	Reducir	Inadecuado control de cambios Sistemas desprotegidos ante acceso no autorizado	A.9.1.1 Política de control de acceso
		Falla del funcionamiento del software	8	Aceptar	Mantenimiento inadecuado	A.14.2.8 Prueba de seguridad del sistema A.14.2.9 Prueba de aceptación del sistema
	Windows	Equivocación por uso de servicio	3	Aceptar	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo
		Difusión de software dañino virus	**25**	Reducir	Falta de protección actualizada	A.12.2.1 Controles contra software malicioso
		Instalaciones de programas de origen sospechoso	**20**	Reducir	Falta de control de acceso	A.9.1.1 Política de control de acceso
		Falla del funcionamiento del software	**20**	Reducir	Mantenimiento inadecuado	A.14.2.8 Prueba de seguridad del sistema A.14.2.9 Prueba de aceptación del sistema
		Abuso de privilegios de acceso	12	Reducir	Falta de protección de datos e información	A.9.4.1 Restricción al acceso a la información
		Uso no Previsto de Windows	9	Reducir	Falta de control de acceso Inadecuada supervisión del trabajo de los empleados	A.9.1.1 Política de control de acceso A.7.1.2 Términos y condiciones de empleo

Fuente: Elaboración propia

3.2. Modelo Propuesto

3.2.1. Plan de gestión de riesgos

En esta fase se realizará los planes de seguridad de información, ya mencionado anteriormente el riesgo, como un suceso que puede afectar desfavorablemente a los activos de información, para elaborar el plan gestión de riesgos se realizara una serie acciones para identificar los riesgos.

Objetivos.

- Controlar los riesgos que pueden ocasionar daños y perjuicios a la empresa.
- Trazar un marco de referencia para conocer qué acciones tomar y cómo hacerlo.
- Cuantificar los riesgos para conocer las consecuencias y la probabilidad de ocurrencia.

Establecimiento del plan de gestión de riesgos.

Para identificar los riesgos se debe seguir los pasos de la Metodología de MAGERIT en cual nos permite realizar un análisis de cada uno de las posibles amenazas que pueden afectar a los activos de información.

- Identificamos los procesos de la empresa, activos importantes, sus relaciones y el costo de su valor en desgaste.
- Se determinará a que amenazas están expuestos todos aquellos activos, listar y clasificar cada uno de ellos.
- Proponer que acciones tomar frente a cada de las amenazas que afectan a los activos de información.
- Se estima el impacto, el daño que puede causar a cada uno de los activos.
- Valorar el riesgo definitivo como un riesgo ponderado.
- Unir los resultados y proceder a tomar acciones preventivas, y correcciones de tal manera que lo alimente, y sea revisado por los auditores internos del sistema.
- Periodo de identificación de riesgos se debe realizar con una frecuencia no mayor a 6 meses.

- Se debe realizar una actualización periódica de los posibles riesgos de información.

Resultado

- Para obtener el resultado el nivel de riesgo por cada amenaza y tipo de activo de información

Costo

El costo de plan de gestion de riesgos por horas de trabajo de del personal asignado 200 soles aproximado.

Equipo responsable.

- German Chiock Cargo: Programador AS 400
- Rodolfo Rodriguez: Jefe de Operaciones
- Franklin Ciprian Cargo: Operador de sistema

3.2.2. Plan de política de seguridad de información

El establecimiento de un documento de seguridad de información para la empresa Loyalty Perú SAC es importante y crucial, ya que en este documento establecerán las medidas y procedimientos la proteger los activos de información de la empresa, y el cumplimiento será obligatorio para todos los trabajadores, contratistas, proveedores, socios entre otros.

Objetivos

- Establecer un documento donde se describan las reglas de seguridad de información.
- Diseñar una política acorde con las actuales legislaciones vigentes.
- Alinear la política de seguridad de información con las metas y objetivos de la empresa Loyalty Perú SAC.
- Adoptar la Norma ISO 27001 para poder diseñar la política de seguridad de información de la empresa Loyalty Perú SAC

Tiempo estimado

El plan de seguridad de información se debe realizar o actualizar en un periodo no mayor a 1 año y en un tiempo más próximo de tres meses.

Costo

El costo por horas de trabajo de plan de politica de informacion por el personal asignado 400 soles aproximado.

Contenido de plan política de seguridad de información

- Organizar un comité de seguridad de información que debe estar conformado por el gerente general, el gerente de sistemas, el gerente de finanzas, y gerente de administración de Loyalty Perú S.A.C. y pueden también complementados por algunos trabajadores internos y externos.
- El Comité de seguridad de información debe coordinar y aprobar las los cambios, las acciones, la actualización de la política de información.
- El comité debe concientizar a los trabajadores de empresa a al conocimiento de seguridad de la información basado en las normas internacionales.
- El comité debe realizar acciones de mejoramiento de plan de seguridad de información periódicamente, ya que surgen nuevos cambios en la organización.
- Los integrantes del comité deben estar presentes en la clasificación de los sistemas y el análisis de riesgos de los activos de información.
- Se debe aprobar los cambios e incrementar la seguridad de la información, de acuerdo a las nuevas competencias y responsabilidades asignadas a cada área.

Equipo responsable

- Juan Aspillaga Cargo: Gerente General de Loyalty Perú SAC
- José Suarez Cargo: Jefe de Soporte Técnico
- Franklin Ciprian Cargo: Operador de sistema

3.2.3. Plan de gestión de activos

El plan de gestión de activos será útil para aumentar la capacidad de servicio, y la mejor adquisición de infraestructura para las áreas de en la empresa Loyalty Perú SAC.

Objetivos:

- Aminorar el costo de duración de un activo aprovechando la utilización y mantenimiento
- Establecer un costo y utilidad, acompañado con el estándar de servicio establecido.

Tiempo estimado

El tiempo periódico para realizar la gestión de activos no debe sobrepasar de un año, y el tiempo necesario para realizar es un aproximado de tres meses.

Costo

El costo por horas de trabajo de implementación del plan de gestión de activos por el personal asignado 300 soles aproximado.

Contenido de plan de gestión de activo

- El equipo responsable debe establecer un documento, para considerar una política de actualización de los activos de la organización y controlar su cumplimiento.
- El equipo responsable debe realizar la clasificación de los activos de información según la metodología MAGERIT.
- Una vez realizado la clasificación se procede a realizar la dependencia entre activos, vale decir un activo superior se vería más dañado que otro inferior.
- El equipo responsable debe establecer la valoración de los activos, es decir a mayor valor de activo mayor protección. La valoración puede ser cuantitativa o cualitativa.
- Los responsables del gestión de activo deben dimensionar los activos, para lo cual se debe utilizar las tres dimensiones, es decir confidencialidad, integridad y disponibilidad.

- Finalmente al analizar las tres dimensiones de los activos se debe obtener: acciones de mejoramiento de política de seguridad de información.

Equipo responsable:

- David Samaniego Cargo: Jefe de Sistemas
- José Suarez Cargo: Jefe de Soporte Técnico
- William Enríquez: Gerencia de Inteligencia comercial

3.2.4. Plan de seguridad de recursos humanos

El plan de seguridad de recursos humanos corresponde al octavo apartado de la norma ISO 27001, nos permitirá evaluar el desempeño de los trabajadores de la empresa Loyalty Perú SAC.

Objetivos

- Desarrollar y promover la concientización de los trabajadores, previniendo y controlando las actividades realizados; para disminuir los riesgos seguridad.
- Establecer de reglas disciplinarias para controlar y medir el cumplimiento de los controles de seguridad.
- Formar o capacitar al personal para lograr las metas y objetivos planificados por la empresa.

Tiempo estimado

El tiempo estimado para realizar la seguridad de recursos humanos no mayor a 6 meses, y un aproximado a 3 meses.

Costo

El costo por horas de trabajo de implementación del plan de seguridad de recursos humanos por el personal asignado 200 soles aproximado.

Contenidos del plan de seguridad de recursos humanos

- Los jefes de cada departamento o área de la empresa decidirán de la formación y capacitación del personal en materia de seguridad de información.
- Los gerentes de cada área establecerán las reglas disciplinarias en caso de que los trabajadores ocasionen algún fraude o que no respeten las reglas de la seguridad de la empresa.

- El equipo responsable debe establecer políticas sobre los accesos conexiones a los clientes, a los proveedores, para utilizar los servicios de la empresa.

Equipo responsable

- German Chiock Cargo: Programador AS 400
- Franklin Ciprian: Operador de sistemas

3.2.5. Plan seguridad física de entorno

El plan de seguridad física se refiere a la protección del acceso a los Servidores y Computadoras de agentes externos, y también valida el acceso a Internet, evitar la sobrecarga de correos publicitarios y prevenir la infección archivos infectaros de virus en los equipos entre otros.

Objetivos

- Prevenir el acceso a lugares físicos de la empresa Loyalty Perú SAC.
- Verificar las entradas de los usuarios a los lugares físicos de la empresa.
- Protección de los computadores, servidores y otros equipos.
- Establecer mecanismos de seguridad en la eliminación de los equipos y su reutilización.
- El perímetro de la empresa Loyalty Perú SAC debe ser bien definida

Contenido del plan de seguridad física

- Establecer mecanismos de seguridad para el control de acceso al área más importante de la empresa que viene ser la DATA CENTER donde se encuentran los servidores y equipos de alto valor.
- El ingreso a las oficinas serán limitadas y controlados mediando un equipo electrónico que controle los accesos a las oficinas.
- El área de soporte se debe responsabilizar de administrar los equipos, generar las reglas, instalar el software en los equipos. Propone la renovación del licenciamiento o el cambio de producto de acuerdo a las nuevas tecnologías.
- El área de soporte debe crear y documentar las reglas de desuso de los equipos, verificando que no haya fuga de información de la empresa.

- La oficina de Loyalty Peru SAC debe estar señalizada en caso de ocurrir algún fenómeno natural.

Tiempo estimado

El tiempo estimado para realizar el plan de seguridad de entorno físico no debe exceder a 6 meses, y un aproximado a 3 meses.

Costo

El costo por horas de trabajo de implementación del plan de seguridad física de entorno realizado por el personal asignado 200 soles aproximado.

Equipo responsable

- German Chiock Cargo: Programador AS 400
- Franklin Ciprian Cargo: Operador de sistema
- William Davalos Cargo: Soporte Técnico

3.2.6. Plan de control de accesos

En el presente apartado se considerará los mecanismos control de acceso ya sea a los redes, a la base de datos, a las zonas restringidas, entre otros. El control de acceso debe ser automatizado.

Objetivos

- Registrar a todos los usuarios que tiene acceso a los servicios de la empresa.
- Proveer permisos para que los usuarios realicen sus actividades.
- Generar contraseñas personalizadas para los usuarios.
- Crear políticas de trabajo.

Contenido del plan de control de acceso

- Los responsables debe crear o diseñar de las reglas de control de acceso de los usuarios a los servicios de la empresa, cada usuario debe registrarse al momento de ingresar a los servicios, aplicaciones de la empresa.
- Los responsables debe diseñar las políticas de periodo cambios de contraseña, y los cambios deben ser documentadas y accesibles para el personal autorizado.

- Se debe crear políticas de puestos de trabajo y debe ser controlados a través de un servidor de administración, que también debe controlar el bloqueo de usuarios.
- Se debe diseñar registros de cambios ya sea para el área de programación y base de datos, los puestos de USB debe ser bloqueados.
- El equipo responsable debe comunicar al comité de seguridad de los cambios realizado.

Tiempo estimado

El tiempo estimado de periodicidad para implementar el control de accesos no debe exceder a 6 meses, y no debe ser menor a 3 meses.

Costo

El costo por horas de trabajo de implementación del plan de control de accesos realizado por el personal asignado 300 soles aproximado.

Equipo responsable

- José Suarez Cargo: Jefe de Soporte Técnico
- German Chiock Cargo: Programador AS 400
- David Samaniego Cargo: Gerente de Sistemas

3.2.7. Plan de contingencia

Según los estándares el plan de contingencia, para ser aplicados en la empresa Loyalty Perú SAC, debe estar orientado para garantizar la continuidad del Servicio de Producción proporcionado por la empresa.

Objetivos:

- Disminuir suficientemente la detención de las operaciones habituales.
- Fijar la magnitud de los daños.
- Disminuir las consecuencias económicas de la detención de las operaciones.
- Fijar los medios de ejecución alternativos ante la posible detención de las operaciones.
- Capacitar al personal para que puedan seguir los procedimientos de emergencia.

- Facilitar una guía rápida de restauración de la mayoría de los servicio.

Se entiende como Servicio de Producción, a todos los equipos que brinda el Área de Sistemas a los demás áreas para realizar sus operaciones, utilizando hardware, software y elementos complementarios o datos críticos.

Después de examinar la infraestructura de hardware, software y comunicaciones, se concluye que se debe centrar más atención en el servidor AS/400 i5, que es el que brinda los servicios de Producción a la empresa.

Costo

El costo por horas de trabajo de implementación del plan de contigencia realizado por el personal asignado 400 soles aproximado.

Equipo responsable:

- David Samaniego Cargo: Jefe de Sistemas
- José Suarez Cargo: Soporte Técnico

Plan de respaldo

El plan de respaldo está basado en un documento de procedimiento (sistemas) copias de respaldo de la plataforma AS/400 i5.

Establecimiento de procedimientos manuales.

El restablecimiento de sistema de contingencia durará 24 horas, los usuarios de Servicio al Cliente tiene que atender las consultas de los clientes utilizando los siguientes medios:

Sistema de consulta de puntos

En el servidor de correo, se actualiza diariamente los saldos de los clientes BONUS, este servidor puede ser consultado a través de un aplicativo desarrollado en Visual Basic la Consulta Puntos. Los datos a consultar son:

- Cuenta BONUS.
- Nombre del Cliente.
- Dirección del Cliente.
- Documento de identidad.
- Saldo de puntos.
- Fecha de proceso.

Procedimiento de recuperación

1. Iniciación del plan
   - Notificar a la Gerencia.
   - Ponerse en contacto con el equipo de recuperación del siniestro y ponerlo a punto.
   - Determinar el grado del siniestro.
   - Implementar el plan adecuado de recuperación de aplicaciones según el alcance del Siniestro.
   - Supervisar el progreso.
   - Ponerse en contacto con los proveedores, tanto de hardware como de software.
   - Notificar a los usuarios la interrupción del servicio.
2. Lista de comprobación de seguimiento
   - Lista todo el personal y sus números de teléfono.
   - Establecer suministros de oficina de emergencia.
   - Preparar el equipamiento.
   - Determinar las aplicaciones que se ejecutarán y en qué orden.
   - Buscar cartuchos adicionales, si es necesario.
   - Llevar copias de la documentación del sistema, de funcionamiento y los manuales de procedimientos.
   - Asegurarse de que todo el personal involucrado conoce sus tareas.
   - Notificar a las compañías de seguros.

3.2.8. Plan de recuperación

El servicio de recuperación, después de solucionar el inconveniente técnico en el servidor de producción, para que el sistema quede como estaba antes del siniestro, utilice los procedimientos según las características del siniestro.

Antes de empezar: Busque los siguientes cartuchos, equipo e información en la sala de máquinas donde se resguardaban los cartuchos en el local o en la ubicación de almacenamiento fuera del local.

- Se instala a partir del dispositivo de instalación alternativo, necesitará el soporte de cartuchos y el CD-ROM que contiene el código interno bajo licencia.
- Todos los cartuchos de la operación de salvar completa más reciente
- Los cartuchos más recientes de salvar datos de seguridad (SAVSECDTA o SAVSYS)
- Los cartuchos más recientes de salvar la configuración, si es necesario
- Todos los cartuchos que contienen diarios y receptores de diario salvados desde la operación de salvar diaria más reciente
- Todos los cartuchos de la operación de salvar diaria más reciente
- Lista de los PTF (almacenada con los cartuchos de la operación de salvar completa o los cartuchos de la operación de salvar semanal más recientes o ambos conjuntos de cartuchos)
- Lista de cartuchos de la operación de salvar completa más reciente
- Lista de cartuchos de la operación de salvar semanal más reciente
- Lista de cartuchos de las operaciones de salvar diarias
- Anotaciones históricas de la operación de salvar completa más reciente
- Anotaciones históricas de la operación de salvar semanal más reciente
- Anotaciones históricas de las operaciones de salvar diarias
- El manual Software Installation
- El manual Backup and Recovery
- Manual del módem
- Kit de herramientas

3.3. Plan de elaboración de proyecto

El plan de elaboración de proyecto tiene una duración de tres meses en la tabla N° 18, se muestra las actividades que se desarrollaron para el planificar el proyecto.

Figura N° 18, Cronograma de actividades de la elaboración del proyecto

ACTIVIDADES / Meses*	Enero				Febrero				Marzo				Abril				Mayo				Junio
Semanas	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21
Elección del Tema																					
Clases metodológicas																					
Desarrollo del anteproyecto de investigación																					
Aprobacion del anteproyecto de investigación																					
Revisión Bibliográfica																					
Desarrollo del marco teórico																					
Identificacion de los activos de informacion																					
Desarrollo de la Metodología de análisis de gestión de riesgos																					
Selección de controles de seguridad de información																					
Desarrollo del plan de seguridad de información																					
Análisis y conclusiones																					
Primer presentación del proyecto																					
Primer revisión e informe del proyecto de investigación (jurado)																					
Levantamiento de observaciones																					
Segunda revisión e informe del proyecto de investigación (jurado)																					
Desarrollo final de proyecto de investigación																					
Presentación final del proyecto de investigación																					
Sustentación del proyecto de investigación																					

Fuente: Elaboración propia

Presupuesto

El proyecto de diseño un plan de seguridad de información podría ascender a un monto aproximado 4694 soles detallado líneas debajo se detalla el presupuesto según el tipo de recurso utilizado.

Gastos en los equipos utilizados.

- Licencia Microsoft Office Estándar S/183.31
- Computadora HP ProDesk 400 G4 SFF, Intel Core i7-7700 3.60GHz, 4GB DDR4, 1TB S/2,811.48
- Cámaras fotográficas S/200.00
- Internet S/200.00
- Licencia de ESET Endpoint antivirus S/100.00

Gastos en los materiales

- Papel Bond S/300.00

- Utilitarios (Lapiceros, Cuadernos) S/50.00
- Libros, revistas, etc. S/500.00

Gastos de mano de obra

- Cursos de capacitación S/200.00

3.4. Resultados

En la siguiente sección se muestran los resultados a las preguntas suscitadas de la realidad problemática de la empresa Loyalty Perú SAC. Estos resultados fueron obtenidos después del desarrollo de cada una de las etapas de la metodología del proyecto.

En respuesta a la pregunta de **¿Cómo identificar los activos de información para valorar según sus tres dimensiones de confidencialidad, disponibilidad e integridad basadas en la norma ISO 27001?**

Para identificar el inventario de los activos tangibles e intangibles de la empresa Loyalty Perú SAC, se recurrió a la captura directa y la entrevista al personal responsable del área, es decir al gerente de área de sistemas, al jefe de soporte técnico y operaciones, y jefe de desarrollo.

La captura directa consistió en tener acceso a la ubicación física o lugar de operación de cada uno de los activos y registrar las principales características y responsables. La entrevista a los responsables del área de sistemas, se muestra en el Anexo A proyecto.

En la tabla N° 27, se puede visualizar la suma de las dimensiones por tipo de activos, de manera esta clasificación de activos nos muestra quien tiene la mayor suma de dimensiones.

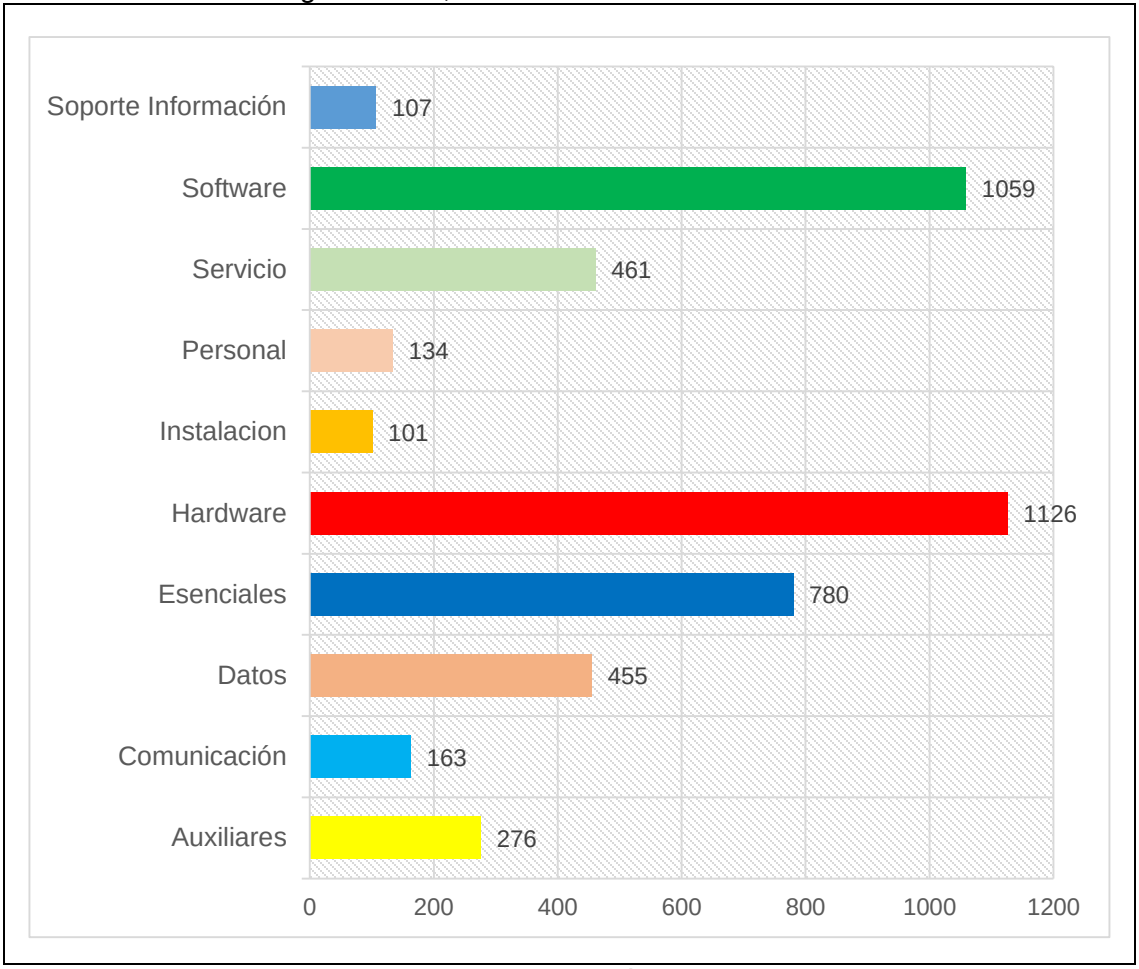
Tabla N° 27, Dimensiones de seguridad de información

Tipos de activos	**Suma de Dimensiones**
Auxiliares	80
Comunicación	48
Datos	78
Esenciales	520
Hardware	676
Instalación	83
Personal	54
Servicio	75
Software	277
Total general	1891

Fuente: Elaboración propia

En la figura N° 19, se muestra un gráfico donde se visualiza la mayor dimensión de los activos, de los cuales se evidencia que los activos que tienen mayores sumas de dimensiones se encuentran en los activos de hardware software y los activos esenciales.

Figura N° 19, Suma de dimensión de activos



Fuente: Elaboración Propia

De manera que, esta mayor suma de dimensiones de los activos que se evidencian en la figura N° 18, vienen a ser los activos más importantes de la empresa Loyalty Perú SAC y que merecen ser protegidos ante cualquier riesgo que se presente en la organización, para lo cual se tiene que realizar el análisis de las amenazas y el despliegue de las vulnerabilidades para su respectivo tratamiento de los riesgos.

Para poder responder a la pregunta **- ¿Cómo reconocer las posibles amenazas de los activos de información para estimar el nivel de riesgo según el impacto y probabilidad de ocurrencia, aplicando la metodología de gestión de riesgos MAGERIT V3?**

En la tabla N° 23, se muestra el impacto, la probabilidad y el riesgo por cada activo y cada amenaza, a continuación analizaremos el resultado de los riesgos obtenidos por cada tipo de activo bajo el Diagrama de Pareto, es una gráfica utilizada para separar los aspectos más significativos de un problema para dirigir los esfuerzos a reducir el problema más importantes o que necesitan intervención inmediata para solucionar, la barra más larga de la Gráfica de Pareto servirá para una mejora general. La minoría vital aparece a la izquierda de la gráfica y la mayoría normal a la derecha.

Como resultado del análisis de riesgos, se dispone de las siguientes tablas que se muestra por cada servicio tipo de activo.

- Activos auxiliares

Después de estimar el riesgo en los activos auxiliares se obtuvo una Tabla N° 28, donde la segunda columna indica la suma de los valores de los riesgos por cada activo, la tercera columna es el porcentaje de la suma de riesgos de cada activo auxiliar.

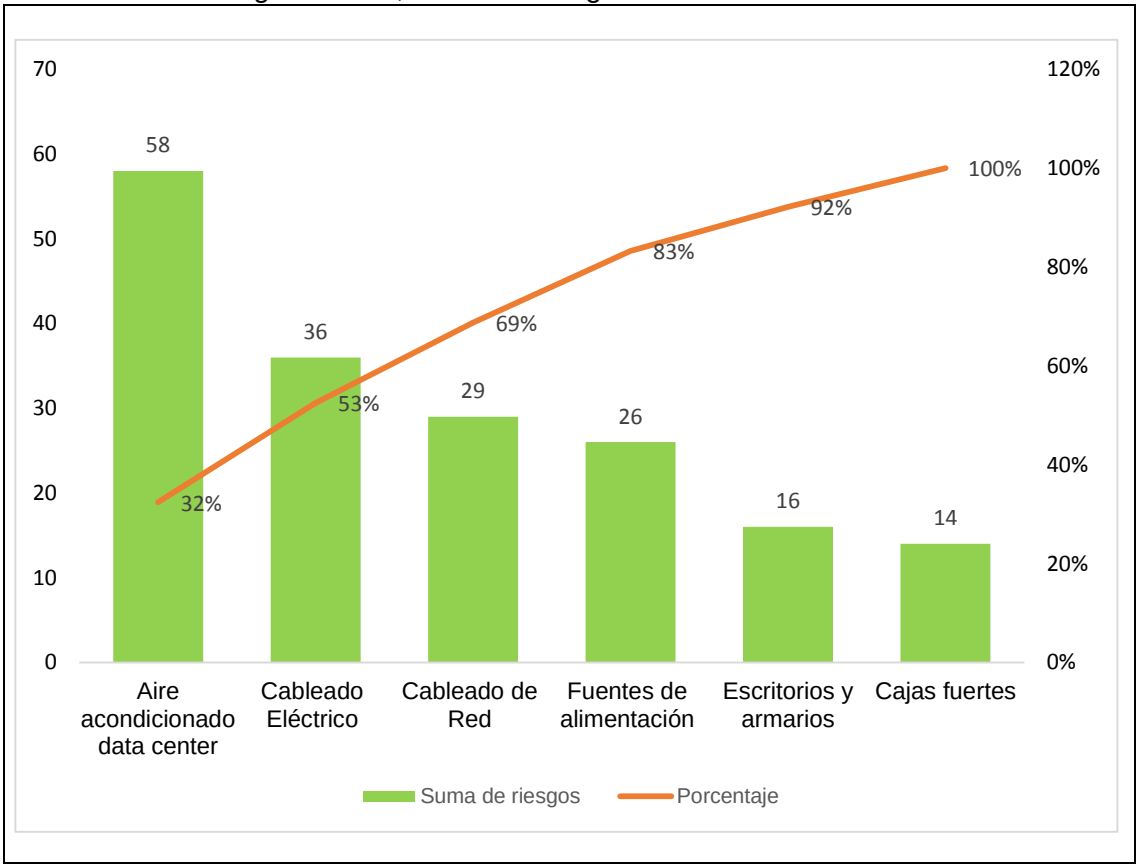
Tabla N° 28, Porcentaje de riesgos de activos auxiliares

Activos auxiliares	Suma de riesgos por cada activo	Porcentaje	Agregado
Aire acondicionado data center	58	32%	58
Cableado Eléctrico	36	53%	94
Cableado de Red	29	69%	123
Fuentes de alimentación	26	83%	149
Escritorios y armarios	16	92%	165
Cajas fuertes	14	100%	179

Fuente: Elaboración propia

En la figura N° 20, vemos cuales son los tipos de activos auxiliares con la mayor alta suma de riesgos. Podemos observar que los tres primeros activos auxiliares aire acondicionado de la Data Center, Cableado eléctrico y Cableado de red acumulan el mayor porcentaje de la suma de riesgos.

Figura N° 20, Suma de riesgos de activos auxiliares



Fuente: Elaboración Propia

Por el Principio de Pareto, concluimos que: La mayor parte de la suma de riesgos encontrados en la tabla N° 28, pertenece sólo a 3 tipos de activos auxiliares, de manera que si se realiza el tratamiento de los riesgos se reduciría los riesgos de los activos auxiliares.

- Hardware

De manera similar después de estimar el riesgo en los activos de hardware se obtuvo una Tabla N° 29, donde la segunda columna indica la suma de los valores de los riesgos por cada activo, la tercera columna es el porcentaje de la suma de riesgos de cada activo auxiliar.

Tabla N° 29, Porcentaje de riesgos de activos hardware

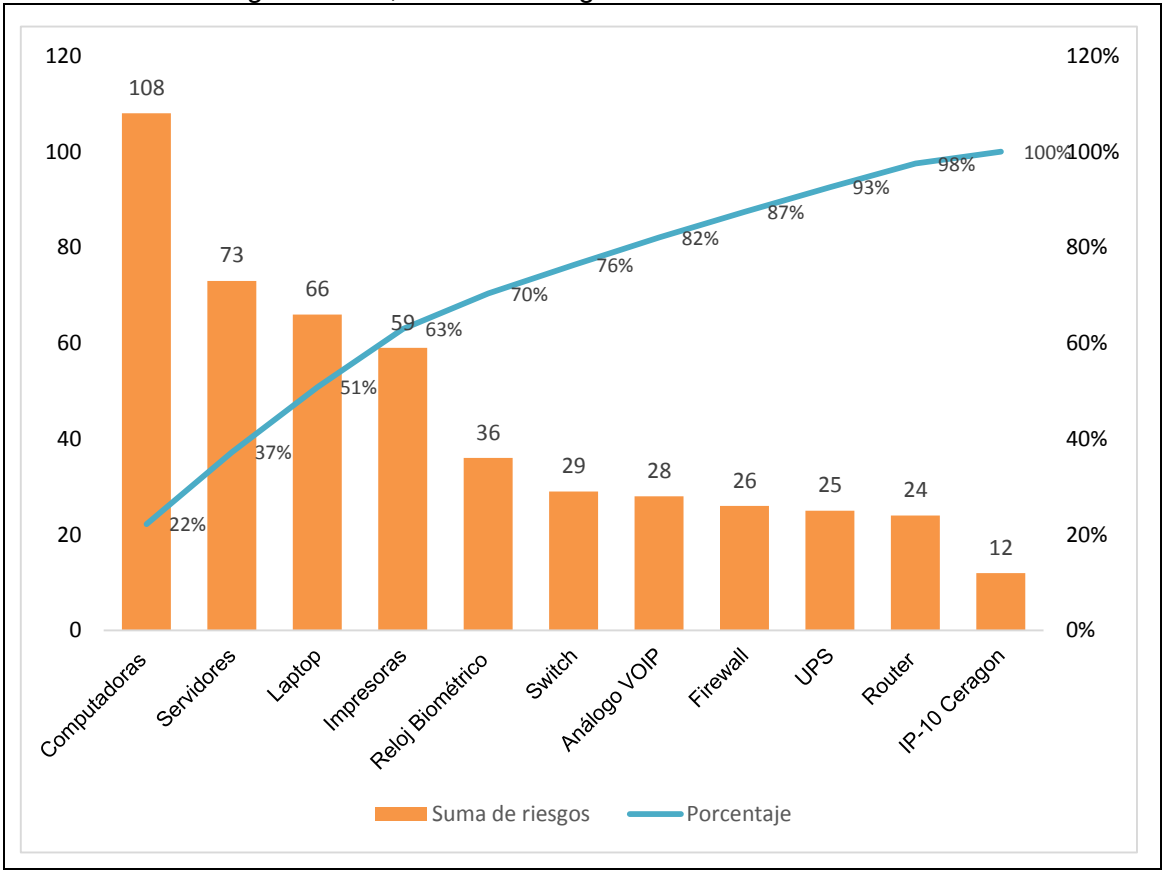
Activos hardware	Suma de riesgos	Porcentaje	Agregado
Computadoras	108	22%	108
Servidores	73	15%	181

Laptop	66	14%	247
Impresoras	59	12%	306
Reloj Biométrico	36	7%	342
Switch	29	6%	371
Análogo VOIP	28	6%	399
Firewall	26	5%	425
UPS	25	5%	450
Router	24	5%	474
IP-10 Ceragon	12	2%	486

Fuente: Elaboración propia

En la figura N° 21, vemos cuales son los tipos de activos de hardware con la mayor alta suma de riesgos. Podemos observar que los 4 primeros tipos de activos tienen el 63% de porcentaje de la suma de riesgos.

Figura N° 21, Suma de riesgos de activos de hardware



Fuente: Elaboración Propia

Por el Principio de Pareto, concluimos que: La mayor parte de la suma de riesgos encontrados en la tabla N° 29, pertenece sólo a 4 tipos de activos de hardware, de manera que si se realiza el tratamiento de los riesgos se reduciría los riesgos de los activos.

- Software

Seguidamente se estima el riesgo en los activos de tipo software obteniendo una Tabla N° 30, donde la segunda columna indica la suma de los valores de los riesgos por cada activo, la tercera columna es el porcentaje de la suma de riesgos de cada activo auxiliar.

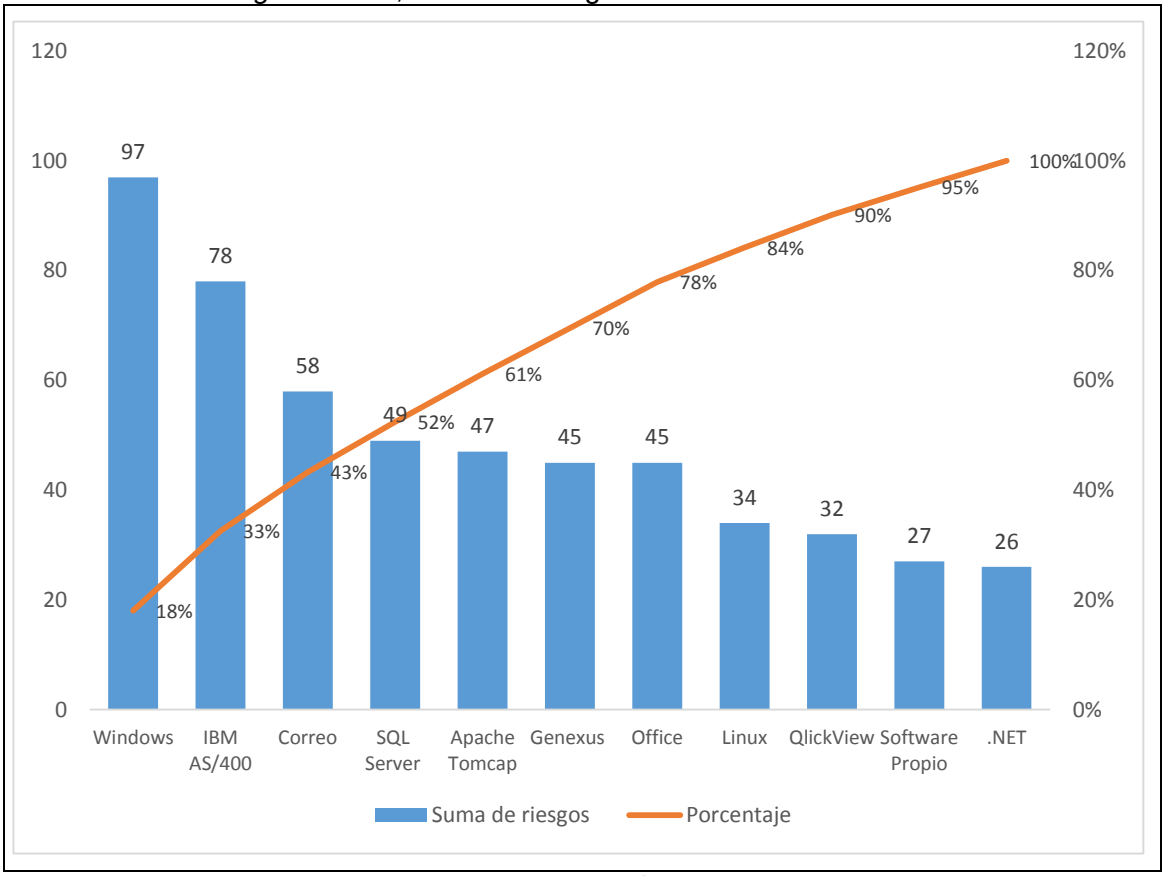
Tabla N° 30, Porcentaje de riesgos de activos software

Activos Software	Suma de riesgos	Porcentaje	Agregado
Windows	97	18%	97
IBM AS/400	78	33%	175
Correo Electrónico Microsoft	58	43%	233
SQL Server	49	52%	282
Apache Tomcap	47	61%	329
Genexus	45	70%	374
Office	45	78%	419
Linux	34	84%	453
QlickView	32	90%	485
Software Propio	27	95%	512
.NET	26	100%	538

Fuente: Elaboración propia

En la siguiente figura N° 22, vemos cuales son los tipos de activos de software con la mayor alta suma de riesgos. Podemos observar que los 6 primeros tipos de activos tienen el mayor porcentaje de la suma de riesgos.

Figura N° 22, Suma de riesgos de activos de software



Fuente: Elaboración Propia

Por el Principio de Pareto, concluimos que: La mayor parte de la suma de riesgos encontrados en la tabla N° 30, pertenece sólo a 4 tipos de activos de software, de manera que si se realiza el tratamiento de los riesgos se reduciría los riesgos de los activos.

- Datos

Seguidamente se estima el riesgo en los activos de tipo datos obteniendo una Tabla N° 31, donde la segunda columna indica la suma de los valores de los riesgos por cada activo, la tercera columna es el porcentaje de la suma de riesgos de cada activo auxiliar.

Tabla N° 31, Porcentaje de riesgos de activos de datos

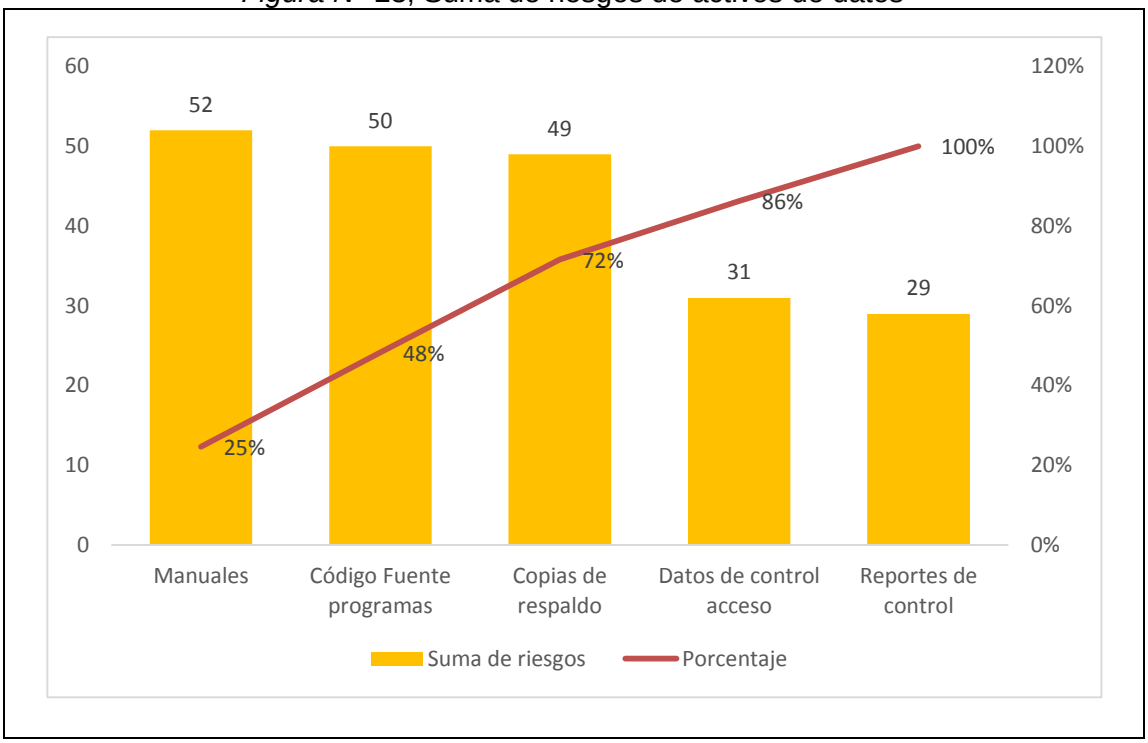
Activos auxiliares	**Suma de riesgos**	**Porcentaje**	**Agregado**
Manuales	52	25%	52
Código Fuente programas	50	48%	102
Copias de respaldo	49	72%	151

Datos de control acceso	31	86%	182
Reportes de control	29	100%	211

Fuente: Elaboración propia

En la siguiente figura N° 23, vemos cuales son los tipos de activos de datos con la mayor alta suma de riesgos. Podemos observar que los 6 primeros tipos de activos tienen el mayor porcentaje de la suma de riesgos.

Figura N° 23, Suma de riesgos de activos de datos



Fuente: Elaboración Propia

Por el Principio de Pareto, concluimos que: La mayor parte de la suma de riesgos encontrados en la tabla N° 31, pertenece sólo a 3 tipos de activos de datos, de manera que si se realiza el tratamiento de los riesgos se reduciría los riesgos de los activos.

- Media

En el siguiente apartado se estima el riesgo en los activos de tipo Medios obteniendo una Tabla N° 32, donde la segunda columna indica la suma de los valores de los riesgos por cada activo, la tercera columna es el porcentaje de la suma de riesgos de cada activo auxiliar.

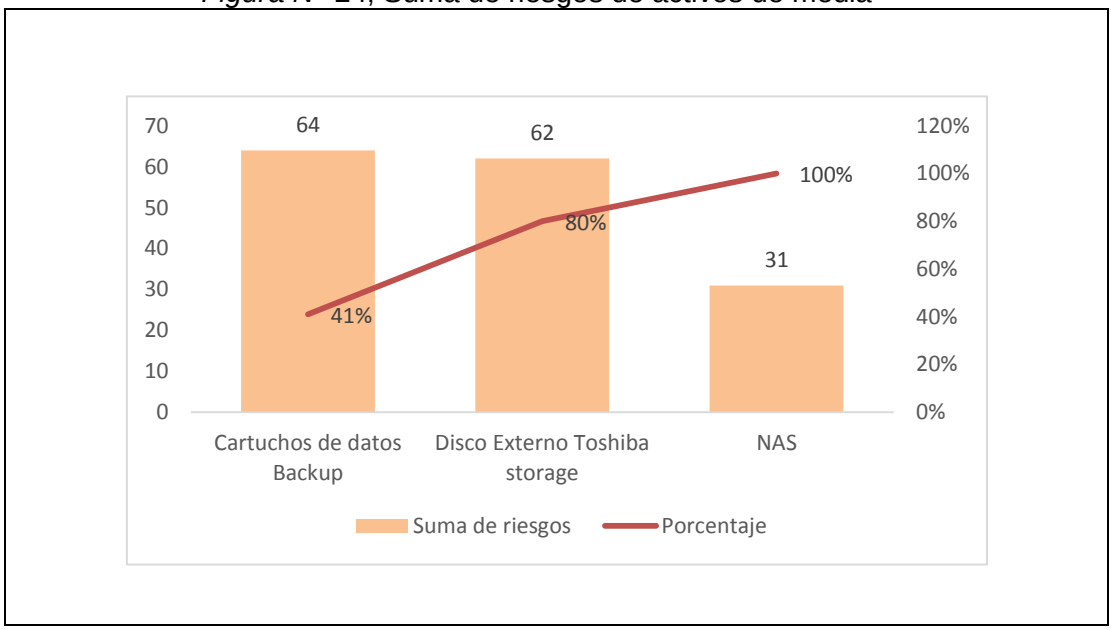
Tabla N° 32, Porcentaje de riesgos de activos de media

Activos auxiliares	Suma de riesgos	Porcentaje	Agregado
Cartuchos de datos Backup	64	41%	64
Disco Externo Toshiba storage	62	80%	126
NAS	31	100%	157

Fuente: Elaboración propia

En la siguiente figura N° 24, vemos cuales son los tipos de activos de media con la mayor alta suma de riesgos. Podemos observar que los dos primeros tipos de activos tienen el mayor porcentaje de la suma de riesgos.

Figura N° 24, Suma de riesgos de activos de media



Fuente: Elaboración Propia

Por el Principio de Pareto, concluimos que: La mayor parte de la suma de riesgos encontrados en la tabla N° 32, pertenece sólo a 2 tipos de activos de media, de manera que si se realiza el tratamiento de los riesgos se reduciría los riesgos de los activos.

Para poder responder a la pregunta **¿Cómo descubrir las vulnerabilidades de los activos de información para proponer son los controles de seguridad de información según la norma ISO 27001?**

Para responder a la pregunta anterior se realizó una selección de controles de seguridad de información mostrados en la tabla N° 26, de las cuales se obtuvo el despliegue de controles que se deben tomar para reducir los riesgos de seguridad de información de seguridad de información en la tabla N° 33, se muestra los principales controles que se tomaran en cuenta en la política de seguridad e información.

Tabla N° 33, Número de riesgos que reducen los controles de seguridad

Código	Controles	Numero de riesgos que reducen
A.9.1.1	Política de control de acceso	54
A.11.2.4	Mantenimiento de equipo	32
A.11.1.4	Protección contra amenazas externas y ambientales	22
A.11.2.2	Servicios públicos	19
A.9.2.6	Eliminación o ajuste de derechos de acceso	17
A.9.4.1	Restricción al acceso a la información	16
A.7.1.2	Términos y condiciones de empleo	14
A.12.1.1	Procedimientos documentados de operación	11
A.12.2.1	Controles contra software malicioso	11
A.12.3.1	Copia de seguridad de la información	9
A.11.2.1	Ubicación y protección del equipo	8
A.5.1.1	Políticas para seguridad de la información	8
A.14.2.8	Prueba de seguridad del sistema	6
A.14.2.9	Prueba de aceptación del sistema	6
A.13.1.1	Controles de red	5
A.13.1.2	Seguridad de los servicios de red	5
A.6.2.1	Política sobre dispositivos móviles	5
A.9.4.5	Control de acceso al código fuente del programa	5
A.11.1.1	Perímetro de seguridad física	4
A.12.4.1	Registro de eventos	4
A.9.2.5	Revisión de los derechos de acceso del usuario	4
A.12.1.4	Separación de ambientes de desarrollo, prueba y operacional	3
A.18.2.3	Revisión de cumplimiento técnico	3
A.11.2.9	Política de pantalla y escritorio limpio	1

A.14.2.1	Política de desarrollo seguro	1
A.15.1.2	Tratamiento de la seguridad en contratos con proveedores	1
A.7.3.1	Terminación o cambio de condiciones del empleo	1
A.9.1.2	Acceso a redes y a servicios de red	1

Fuente: Elaboración propia

En la figura N° 25, se muestra cuáles son los controles de seguridad de información que tienen la mayor cantidad de riesgos que pueden reducir. Podemos observar que los primeros 9 controles de seguridad de información tienen la mayor cantidad de riesgos que pueden reducir.

Figura N° 25, Controles de seguridad de información

Fuente: Elaboración Propia

Concluimos que: La mayor cantidad de riesgos que reduce los controles de seguridad de información encontrados en la tabla N° 33, pertenece sólo a 9 controles de seguridad según la gráfica, de manera que si se realiza la política de seguridad e información se tiene que tomar en cuenta estos 9 controles de seguridad e información, tomando énfasis en el control de política de control de acceso, mantenimiento de equipos.

El presente trabajo de investigación como se mencionó en los apartados anteriores, se realizó en la empresa Loyaty Peru SAC, el cual laboro durante 2 años, desde el año 2017 hasta la actualidad, para validar esta información se muestra el *Anexo B*, donde se muestra la constancia de trabajo. El área donde me desempeño es el area de sistemas como operador de sistemas.

En el Anexo C nuestra los documentos utilizados para poder desarrollar el plan de seguridad de información y comprender la interconexión de las áreas y los sistemas utilizados.

En el Anexo D se muestra la data center de la empresa Loyalty Peru SAC en el cual se encuentran los distintos equipos que soportan el negocio de la empresa y toda las demás áreas.

CONCLUSIONES

Se consiguió diseñar un plan seguridad de informaciones basadas en los apartados de la norma ISO 27001, los cuales son asignados a los equipos responsables para su implementación, con la estimación de tiempos y los recursos destinados para cada plan de seguridad de información.

Se identificar y valorar los activos de información según las dimensiones de relevancia tales como confidencialidad, disponibilidad e integridad de la empresa Loyalty Perú SAC, de esta manera se sabe que los activos que tienen mayores sumas de dimensiones se encuentran en los tipos de activos de hardware, software y los activos esenciales, el cual necesitan de una particular atención.

Se logra reconocer las posibles amenazas de los activos de información y se consigue estimar el nivel de riesgo para cada amenaza, obteniendo resultados, que los activos que tiene mayor riesgo son: registro de base de datos, la Data Center, la base de datos de IBM AS400, los servidores, el aire acondicionado de la data center, el cableado eléctrico, las computadoras, los laptop, Genexus, Windows, Correos electrónicos, la base de datos SQL server, los manuales los códigos fuentes de los programas, las copias de respaldo, los archivos de Backup, los protocolos de transferencia de datos entre otros, estos activos necesitan mayor pronta atención.

Se logra descubrir las vulnerabilidades y de esa manera se proponen los controles de seguridad de información en base a la norma ISO 27001, obteniendo controles de mayor prioridad las cuales son: Política de control de acceso, mantenimiento de equipo, protección contra amenazas externas y ambientales, servicios públicos eliminación o ajuste de derechos de acceso restricción al acceso a la información, términos y condiciones de empleo, procedimientos documentados de operación, Controles contra software malicioso, copia de seguridad de la información, ubicación y protección del equipo.

RECOMENDACIONES

Se recomienda que una vez planificado se tiene que proseguir con la continuación de las fases del Ciclo de Deming que corresponden a la implementación, el monitoreo y revisión y para lo cual se necesita aprobación de la alta gerencia, el cual debe autorizar al comité de seguridad de información que es el responsable de la planificación e implementación de un Sistema de Gestión de Seguridad de Información.

Se recomienda realizar periódicamente el inventario de los activos para llevar un registro de control de patrimonio de la empresa y de esa manera valorar los activos en las tres dimensiones de seguridad de información, además el inventariado también permitirá identificar a los activos que se encuentran en desgaste, o también perdidos, esto ayudara a reducir costos para la toma de decisiones.

Se recomienda mantener o establecer otra opción de modelo de gestión de riesgos en el cual se aprecie la mayor probabilidad de suceder un evento que pueda perjudicar los activos de información, y de esa manera establecer tratamientos para su respectivo control riesgos.

Se recomienda también adoptar las buenas prácticas de la norma ISO 27002 para tener un mayor control de los activos, e ubicar y corregir los puntos más vulnerables de la empresa, y de esa manera reducir los costos con la prevención de seguridad de información.

BLIBLIOGRAFÍA

Anticona Tupia, M. (2013). *Administración de la seguridad de información*. (2013. Callao : Tupia Consultores y Auditores, Ed.) (2a ed). Lima: Tupia Consultores y Auditores (Lima).

Asociación Española de Normalización. (2016). Las certificaciones, *566*, 32-35.

Berrío López, J. P. (2016). *Metodología para la evaluación del desempeño de controles en sistemas de gestión de seguridad de la información sobre la norma ISO/IEC 27001*.

Berríos Mesía, C. A., & Rocha Cam, M. A. (2018). *Propuesta de un modelo de Sistema de Gestión de la Seguridad de la Información en una pyme basado en la norma ISO/IEC 27001*. (Tesis de grado). Universidad de Ciencias Aplicadas, Lima, Perú.

BSI Group México. (2013). Pasando de ISO / IEC 27001 : 2005 a ISO / IEC 27001 : 2013. Recuperado de https://www.bsigroup.com/es-PE/seguridad-de-la-informacion-isoiec-27001-/transicion-isoiec-270012013/

Carpentier, J.-F. (2016). *La seguridad informática en la PYME: Situación actual y mejores prácticas* (Ediciones). Barcelona, España: Colecciones Data pro. Recuperado de https://books.google.com.pe/books?id=LKE5_6gzBmgC

Comité Técnico de Normalización de Codificación Norma Técnica Peruana, N. (2014). Peruana Ntp-Iso / Iec 27001 Tecnología De La Información ., *2a Edición*, 45.

Electrónica Dirección General de Modernización Administrativa Procedimientos e Impulso de la Administración. (2012). *MAGERIT - versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información* (Vol. 13). Madrit, España: Ministerio de Hacienda y Administraciones Públicas. https://doi.org/10.1016/S0248-8663(05)81005-7

GTDI Tecnología de información y consultoria. (2018). Número de certificados válidos ISO/IEC 27001 en Perú - año 2017.

Guzman, J. (2015). *Elaboración de un marco de referencia para la implementación de la norma ISO/IEC 27001:2013 y ley de protección de datos personales en la*

dirección de admisión de la UNS. (Tesis de ingeniero) Universidad Nacional del Santa, Chimbote, Perú.

Hintzbergen, J., Hintzbergen, K., Smulders, A., & Baars, H. (2015). *Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002*. (Brasport, Ed.). Rio de Janeiro: 2018. Recuperado de https://books.google.com.pe/books?id=1CVFDwAAQBAJ

ISOTools Excellence. (2014). ISO 27001 y el inventario de activos de la información.

ISOTools Excellence Chile. (2016). 12 Beneficios de Implantar un SGSI de acuerdo a ISO 27001 - ISOTools Chile.

Kersten, H., Reuter, J., & Schröder, K.-W. (2013). *IT-Sicherheitsmanagement nach ISO 27001 und Grundschutz*. (H. Kersten & K.-D. Wolfenstetter, Eds.) (Cuarta Edi). Wiesbaden: Springer Fachmedien Wiesbaden. https://doi.org/10.1007/978-3-658-01724-8

López Neira, Agustín; Ruiz Spohr, J. (2012). ISO27000.es -ISO 27001 en español. Gestión de Seguridad de la Información. Recuperado 10 de febrero de 2019, de http://www.iso27000.es/iso27000.html

Manuel Muñoz, M. (2015). *Guía de implantación de un SGSI basado en la norma UNE-ISO/IEC 27001*. (Trabajo de Grado). Universitat Oberta de Catalunya, Cataluña, España.

Moyano, L., & Suárez, Y. (2017). *Plan de implementación del SGSI basado en la norma ISO 27001:2013 para la empresa Interfaces y Soluciones*. Universidad distrital Francisco José de Caldas.

Organización Internacional de Normalización ISO. (2013). ISO/IEC 27001:2013(en), Information technology, Security techniques, Information security management systems, Requirements. Recuperado 24 de febrero de 2019, de https://www.iso.org/obp/ui/#iso:std:iso-iec:27001:ed-2:v1:en

Portal de Administración Electrónica España. (2013). PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

Ruperto, G. (2016). Semana Económica. *30 de agosto 2016*. Recuperado de http://semanaeconomica.com/article/sectores-y-empresas/tecnologia/197847-bonus-tarjeta-de-pago-busca-captar-a-los-jovenes/

Tavalera, R. (2015). *Diseño de un Sistema de Gestión de Seguridad de la Imformación para una Entidad Estatal de la Salud de acuerdo a La ISO/IEC 27001-2013*. Pontificía Universidad Cátolica del Perú.

Vázquez, J. (2018). *Implementación del sistema de gestión ISO 27001:2013, para proteger la información en los procesos de TI*. (Tesis de ingeniería). Universidad Nacional Mayor de San Marcos, Lima, Perú.

Vinod, V., Anoop, M., Firosh, U., Sachin, S., Sangita, P., & Siddharth, A. (2015). *Application security in the ISO27001:2013 Environment* (Segunda Ed).

ANEXOS

Anexo A:

ENTREVISTA 1

Gerente de área de sistemas:

- **¿En qué consiste la seguridad de información?**

  La seguridad de información consiste en proteger la fuga de información de la empresa a través programas, software o políticas de acceso de personas malintencionadas, que tienen sus propios fines de obtener algún beneficio.

- **Llamase activo a los bienes y derechos de propiedad de la empresa. ¿Cuáles crees que son los activos más importantes que están bajo tu responsabilidad y que deben ser protegidos de cualquier amenaza?**

  El Servidor AS 400, es uno activos más importantes que tenemos que proteger, también está la base de datos donde se encuentra alojado toda la información para el desarrollo de las actividades, las tablas donde están los registros de los clientes, sus datos, sus movimientos, los canjes, la facturación de los socios de la empresa, todas estos registros son importantes para la protección.

  No solo esta base datos también esta los servicios la que brindamos la web Service, la data center todos estos activos son importantes para nuestra actividad que necesitan la protección.

- **¿Qué medidas de seguridad propones para proteger estos activos de información?**

  Realizar una auditoría y adoptar una Norma para seguridad de información para plantear medidas controlar el acceso de información y así mejorar nuestra seguridad.

  También tenemos un comité de seguridad de información que estamos planteando para adoptar alguna norma internacional.

ENTREVISTA 2

Jefe de Soporte y Operaciones:

- **¿En qué consiste la seguridad de información?**

  La seguridad de información es proteger activos ante cualquier amenaza, hacker, virus, daño físico, etc.

- **Llamase activo a los bienes y derechos de propiedad de la empresa. ¿Cuáles crees que son los activos más importantes que están bajo tu responsabilidad y que deben ser protegidos de cualquier amenaza?**

  En primer lugar están los servidores son los que almacén información y que se encuentran en aquí en nuestro local principal, la base datos, los computadoras que pueden sufrir daños de cualquier hacker, los equipos como los switch, la data center, los firewall, las conexiones de red, etc.

  En segundo lugar ya están los que se encuentran en los módulos de canje que tenemos muchos equipos que también necesitan su protección.

- **¿Qué medidas de seguridad propones para proteger estos activos de información?**

  Proponer políticas, control de acceso, instalar cámaras de seguridad, los equipos deben estar bajo contraseñas, las contraseñas deben estar encriptadas.

  Las contraseñas se deben cambiar mensualmente, la base de datos deben tener control de acceso, el acceso a la data center solo debe ser para personas autorizadas.

ENTREVISTA 3

Jefe de desarrollo:

- **¿En qué consiste la seguridad de información?**

  La seguridad de información son medidas y políticas para la protección de los datos de una empresa.

- **Llamase activo a los bienes y derechos de propiedad de la empresa. ¿Cuáles crees que son los activos más importantes que están bajo tu responsabilidad y que deben ser protegidos de cualquier amenaza?**

  Los activos importantes que están bajo mi responsabilidad son los programas que desarrollamos para nuestros socios de la empresa, tales como Asignación de Puntos, Módulos Canje de Puntos, Cuentas por Cobrar, Cuentas por Pagar. Y para el control interno desarrollamos los Sistemas como: Alicorp, Esquemas Terceros, San Fernando, Punto Cash, Sistema para las planillas, Control de Asistencia, Supervisores, Comercial, Contabilidad, Marketing, Logística, Servicios para el cliente, recursos humanos, para la Gerencia entre otros.

  Todos sistemas que se desarrolla para nuestra empresa son importantes, y que deben estar en protección de las amenazas.

- **¿Qué medidas de seguridad propones para proteger estos activos de información?**

  Para control de usuarios, todos los sistemas están desarrollados con usuario y contraseña, para tener acceso al sistema cada usuario tiene su usuario y contraseña.

  Tener un log de control de cambios, log de control de accesos, control de modificaciones de desarrollo. Permisos de acceso a la base de datos.

Anexo B:

Se muestra la data center de la empresa Loyalty Peru SAC en el cual se encuentran los distintos equipos que soportan el negocio de la empresa y toda las demas areas.