



**FACULTAD DE INGENIERIA ARQUITECTURA Y
URBANISMO
ESCUELA PROFESIONAL DE INGENIERIA DE SISTEMAS
TESIS**

**MODELO DE GESTIÓN DE RIESGOS PARA
SEGURIDAD INFORMATICA BAJO ISO/IEC
27001:2013 EN EMPRESA DE ENTRETENIMIENTO
Y JUEGOS DE AZAR, LIMA-2021**

**PARA OPTAR EL TÍTULO PROFESIONAL DE
INGENIERO DE SISTEMAS**

Autor:

**Bach. Villon Guerrero, Pablo Leonardo
ORCID: <https://orcid.org/0000-0002-2514-0275>**

Asesor:

**Mg. Atalaya Urrutia, Carlos William
ORCID: <https://orcid.org/0000-0002-2761-4868>**

Línea de Investigación:

Infraestructura, tecnología y medio ambiente

Pimentel – Perú

2021

Aprobación del Jurado

**MODELO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD INFORMATICA
BAJO ISO/IEC 27001:2013 EN EMPRESA DE ENTRETENIMIENTO Y
JUEGOS DE AZAR, LIMA - 2021**

Bach. Villon Guerrero, Pablo Leonardo
ORCID: 0000-0002-2514-0275
Autor

Dra. Heredia Llatas, Flor Delicia
ORCID: 0000-0001-6260-9960
Asesor Metodológico

Mg. Atalaya Urrutia, Carlos William
ORCID: 0000-0002-2761-4868
Asesor Especialista

Dr. Ramos Moscol, Mario Fernando
Presidente de Jurado

Mg. Mejía Cabrera, Heber Iván
Secretario del Jurado

Mg. Atalaya Urrutia, Carlos William
Vocal del Jurado

Dedicatoria

A Dios, porque me dio la fortaleza y paz en momentos que todo era confuso.

A mis padres Hugo y Elsa, por los consejos, ejemplo de vida y constantes ánimos para lograr mi objetivo.

A mi esposa Carla, por todo el apoyo y cariño brindado durante cada ciclo académico de la carrera y el tiempo que conllevó el presente trabajo de investigación.

Pablo Villon

Agradecimiento

Mis agradecimientos sinceros a la USS por acogerme y permitirme realizar uno de mis mayores retos, terminar la universidad.

A mis asesores: Dra. Heredia Llatas, Flor Delicia y Mg. Atalaya Urrutia, Carlos William por el apoyo y orientación brindada durante el curso.

A mis amigos y amigas, que en mayor o menor medida siempre me instaron a culminar mis estudios.

Pablo Villon

Resumen

En términos de seguridad informática, se percibe un alto nivel de criticidad en los recursos informáticos de la empresa en estudio, dado al ineficaz control de acceso a los equipos y sistemas de información, y siendo así, el presente trabajo tiene como objetivo, implementar un modelo de gestión de riesgos para la seguridad informática bajo la norma ISO/ IEC 27001:2013 en una empresa de entretenimiento y juegos de azar, lima - 2021. A nivel metodológico este trabajo se desarrolló como una investigación de tipo cuantitativa, de campo y descriptiva, enmarcada en un diseño experimental de corte transversal, utilizando una muestra de 679 activos que están integrados a la seguridad informática de la empresa en estudio. El método propuesto se basa en la norma ISO/IEC 27001/2013, que se basa en las fases del modelo Deming, y que además contempla aspectos metodológicos de MAGERIT. Como resultado del trabajo se obtuvo el diagnóstico actual de la empresa en estudio, se diseñó el modelo de gestión en la seguridad informática, siendo validado por juicio de expertos y obteniendo un apego *Muy Bueno*. En la implementación progresiva se demostró una eficacia del 80% en la gestión de disminución de incidentes presentes en el entorno tecnológico de la empresa en estudio, y por lo tanto en esa misma proporción es su mejora, certificándose así la hipótesis alterna de la investigación. Se recomienda al respecto, la revisión periódica de las amenazas, y riesgos detectados, considerando los diferentes factores que afectan su incidencia, tales como cambios tecnológicos, implementación de nuevos proyectos, entre otros.

Palabras Clave:

Gestión de riesgos, análisis de riesgos, evaluación de riesgos, normas ISO/TEC 27001:2013, seguridad informática, TI.

Abstract

In terms of computer security, a high level of criticality is perceived in the computer resources of the casino under study, due to the ineffective control of access to equipment and information systems, and thus, the present work aims to implement a model of risk management for computer security under ISO / IEC 27001: 2013 in an entertainment and gaming company, Lima - 2021. At the methodological level, this work was developed as a quantitative, field and descriptive research, framed in a non-experimental cross-sectional design, using a sample of 679 assets that are integrated into the computer security of the company under study. The proposed method is based on the ISO / IEC 27001/2013 standard, which is based on the phases of the Deming model, and which also includes methodological aspects of MAGERIT. As a result of the work, the current diagnosis of the company under study was obtained, the computer security management model was designed, being validated by expert judgment and obtaining a Very Good adherence. In the progressive implementation, an 80% efficiency was demonstrated in the management of the reduction of incidents present in the technological environment of the company under study, and therefore its improvement is in the same proportion, thus certifying the alternative hypothesis of the investigation.

In this regard, it is recommended to periodically review the threats and risks detected, considering the different factors that affect their incidence, such as technological changes, implementation of new projects, among others.

Keywords

Risk management, Risk analysis, risk assessment, ISO/IEC 27001:2013 Standards, IT security, IT.

Índice

Aprobación del Jurado	ii
Dedicatoria	iii
Agradecimiento	iv
Resumen	v
Palabras Clave:	v
Abstract	vi
Keywords.....	vi
Índice.....	vii
I. INTRODUCCIÓN	9
1.1. Realidad problemática.....	9
1.1.1. Trabajos previos	12
1.2. Teorías relacionadas al tema	22
1.2.3. Seguridad de la información	22
1.2.4. Seguridad informática.....	23
1.2.5. Gestión de riesgos.....	24
1.2.6. Metodologías para el análisis de riesgos y seguridad informática	26
1.2.7. ISO 27001	28
1.2.8. Normas Técnicas Peruanas de Seguridad de la Información	31
1.3. Formulación del Problema	31
1.4. Justificación e importancia del estudio	31
1.5. Hipótesis	32
1.6. Objetivos	33
1.6.3. Objetivo general.....	33
1.6.4. Objetivos específicos.....	33
II. MATERIAL Y MÉTODO.....	34
2.1. Tipo y diseño de investigación	34
2.2. Población y muestra.....	35
2.3. Variables, operacionalización.....	35
2.3.1. Variable independiente	35
2.3.2. Variable dependiente.....	35
2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad	

2.5. Procedimientos de análisis de datos.....	39
2.6. Criterios éticos	40
2.7. Criterios de rigor científico.....	41
III. RESULTADOS	42
3.1. Resultados en tablas y figuras	42
3.2. Discusión de resultados	69
3.3. Aporte práctico	73
IV. CONCLUSIONES Y RECOMENDACIONES.....	122
REFERENCIAS.....	124
ANEXOS	130

I. INTRODUCCIÓN

1.1. Realidad problemática

Actualmente con la globalización, mundialmente ha trascendido la seguridad informática en las redes de comunicación, y ha pasado a ser el elemento más importante en las grandes y medianas organizaciones que manejan franquicias, clientes, proveedores y colaboradores a lo extenso de una localidad o país Gonzales (2018), quienes ameritan darle uso a bases de datos y procesos comunes que se manejan a través de servidores y otros canales de interconexión donde estos deben contar con un resguardo estratégico ante riesgos Morales y López (2018), a partir de la gestión de métodos basados en normas internacionales, como las ISO/IEC 27001:2013 que promueven políticas para evitar que los sistemas inmersos sean vulnerados.

Bajo ese contexto, se han aplicado en muchos países de América y Europa, a nivel mundial para llevar a cabo el manejo, control y seguimiento de riesgos en la seguridad informática (SI), apuntándose la aplicación de la norma ISO/IEC 27001:2013 el primer lugar en el 94% de la Pymes, comercios y negocios que involucran en sus procesos operativos un alto volumen de equipos tecnológicos Guevara y Mayorga (2017), como es el caso de casinos, salas de diversiones y centro de apuestas que fortalece la economía turística de países como Estados Unidos, España y Francia, cuyas máquinas son manejadas con el apoyo de robustos sistemas automatizados que se exponen frecuentemente a ser violentados por ataques cibernéticos o a ser hackeados Miranda et al. (2016).

Bajo esta misma idea, en América Latina se ha dado la iniciativa de fortalecer la seguridad de la información ante riesgos informáticos a partir de los estándares de ISO, en sus versiones 27001, 27005 y 31000 Figueroa et al. (2017), extendiéndose con línea principal los sistemas de gestión de riesgos basados en esta primera norma, donde en pymes de Chile ha alcanzado un 93% el éxito de su implementación, en Ecuador un 65% y en Venezuela un 63% Mesa (2016).

En tanto, en las diversas empresas del ramo del entretenimiento de Perú, tales como casinos, sala de video juegos, establecimientos de apuestas y juegos de azar, entre otras, la seguridad informática no está exenta de alinearse al 84% de otras Pymes García et al. (2018), que se enfocaron a adoptar la gestión de la seguridad de la información mediante el establecimiento de estándares basados en la norma ISO/IEC 27001:2013, y así mantener de forma fiable los riesgos a los que está expuesta, es decir, tener claro hasta qué nivel está inmersa y que efectos podría generar ese contexto Berrios y Rocha (2015).

Bajo este precepto, en muchas empresas públicas y privadas, establecidas a lo largo de Perú, se han implementado, para garantizar la seguridad informática, los sistemas de gestión de seguridad de la información (SGSI) enmarcados en las normas ISO/IEC 27001:2013 como estrategia garante de aminorar el menoscabo de los riesgos, de manera que estos se asuman y gestionen de manera documentada en términos de calidad y eficacia Justino (2015).

Ante este escenario, son varios los casinos y centros de diversiones concentrados en la región de Lima, que se han enfocado a implementar estrategias para reforzar la seguridad de la información, y así proteger sus activos tangibles e intangibles Corda et al. (2017), desde donde pueden identificar sus riesgos a partir de métodos definidos y normas estandarizadas de seguridad informática dado que ninguna de estas organizaciones están libres de sufrir vulneraciones por muy buena que sea su estrategia de protección Carrión et al. (2021), estando en un mundo donde la tecnología intensifica métodos para infiltrar de manera desmedida redes y sistemas en general Marchand (2016).

Es entonces que, bajo los criterios de confidencialidad, integridad y disponibilidad, la seguridad de la información que se respalda bajo el enfoque de la seguridad informática en las pymes peruanas se sitúa en el hecho de preservar todos los activos bajo la figura de sistemas vinculados al procesamiento de datos de una organización. Así pues, este trinomio de términos forja la base de la infraestructura de la información Rodríguez et al.

(2020).

De esta situación no escapa la empresa en estudio, establecida en la ciudad de Lima, que por ser una mediana empresa orientada al sector de servicio de entretenimiento y juegos de azar, y distinguirse dentro de los casinos que son parte del rubro de la economía que fortalece las atracciones y el turismo dentro de la localidad, cuenta hasta ahora con una amplia plataforma tecnológica e importante capital humano que le dan soporte a un cuantioso conjunto de equipos y máquinas informáticas interconectadas para llevar a cabo los procesos operativos que implican su razón social donde se maneja desde apuestas, transacciones con monedas virtuales, juegos, entre otros.

No obstante, en la Gerencia General de la empresa en estudio, se pudo evidenciar que actualmente existe un deficiente manejo de la seguridad de la información crítica, al observarse la utilización indebida de esta, así como de los recursos informáticos o de red organizacional que claramente están prohibidos, inadecuado control de acceso, constante hackeo, intento de violación de la privacidad de las máquinas de apuestas y pérdida de dinero virtual (moneda o billetera virtual) tanto de los apostadores que asisten al local, como de la propia casa, sabiendo que en esta se ejecutan hoy en día aproximadamente unas 320 transacciones diarias; pérdida de información, limitaciones de alcance a la misma de manera oportuna, por interrupción prolongada en la red; modificaciones no autorizadas de los sistemas informáticos, daños por efectos de virus, y en todo caso, inseguridad en puntos de accesos remotos, los cuales carecen de vigilancia.

Lo antes señalado se debe, a que la empresa en estudio no cuenta con políticas orientadas a garantizar la disponibilidad, integridad y confidencialidad de la información debido a que no se han canalizado estrategias con base a estándares y normas internacionales para evaluar primeramente las necesidades de seguridad que amerita su caso de acuerdo a los riesgos, así como cuál es la más eficiente, y en consecuencia hasta ahora se desconoce los riesgos a la que se ve expuesta dicha información, ni de las acciones a

tomar ante estos.

Por tal motivo, se hace necesario desarrollar un modelo de gestión de riesgos que garantice la seguridad informática de la empresa, fundamentado en normas estandarizadas y comprobadas con las ISO/IEC 27001:2013, ya que su método de uso mediante políticas ha sido de gran apoyo a la labor de protección de redes e infraestructura informática de este tipo de empresas.

1.1.1. Trabajos previos

Se exponen aquí, las investigaciones previas de autores que hacen referencia al tema, entre los cuales se tiene a:

Morales y López (2018). En el artículo científico: *Sistemas de gestión de seguridad de la información para empresas KPO: una aproximación*, Colombia. La gestión de riesgos para garantizar la integridad, confiabilidad y disponibilidad de la información como activo relevante de toda organización, necesita a priori de estrategias que aseguren su estabilidad, tal como acontece en las empresas KPO (Knowledge Process Outsourcing) que poseen muchos activos que forman parte de la vida empresarial de sus clientes, surgiendo aquí una imperiosa tarea ante la protección de activos de terceros. Se concluye que en los modelos de SGSI se pueden encontrar falencias al estar enfocados solamente en procesos y no en personas, cuando uno de los principales retos de la seguridad informática es prevenir los ataques de ingeniería social.

Esta tesis ayudó a tener un mejor enfoque sobre cómo utilizar una de las metodologías que caracteriza la ISO 27001, que es la PDCA, la cual se adecúa en la evaluación en este trabajo de investigación, siguiendo paso a paso las recomendaciones.

Gonzales (2018). En el artículo científico: *Design of a strategic information security plan, through the application of risk analysis with the ISO / IEC*

27005 standard. INAMHI case study, Ecuador. La organización en estudio requería de la adecuación de medidas para la seguridad de la información, por lo que fue necesario evaluar su plataforma tecnológica, y los procesos organizacionales que la complementan. Ante ello, fue necesario aplicar una auditoría junto a un análisis del riesgo bajo el enfoque de la norma ISO/IEC 27005:2012 de donde se obtuvieron finalmente los controles que permitan una óptima y una mejor gestión del riesgo fundamentado en un Plan Estratégico de Seguridad de la Información para el cual se definió normas y procedimientos para la seguridad informática, que estuviesen en consonancia con las metas organizacionales.

El estudio de Gonzales (2018) se relaciona con el presente informe de investigación, debido a que ambos utilizan como política de calidad las ISO 27000, la cual demanda a evaluar la gestión de seguridad de la información a partir de herramientas que garanticen la confiabilidad y consistencia de su aplicación.

Guevara y Mayorga (2017). *Sistema De Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001 para el departamento de Tecnologías de la Información Y Comunicación del Distrito 18D01 de educación, en Ambato, Ecuador.* Concluyeron que en esa institución no es eficiente la gestión de seguridad de la información de los activos informáticos; tanto, la información que se procesa es altamente vulnerable.

El estudio fue un gran punto de apoyo para esta tesis porque existe procedimientos y políticas definidas para salvaguardar la información las cuales sirvieron para adaptarlas a la problemática.

Miranda et al. (2016). En el artículo científico: *Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática.* Cuba. El trabajo tuvo como objetivo general desarrollar una metodología para la implementación de la gestión automatizada de controles de seguridad informática, a fines de garantizar la protección de la

información. Como resultado se obtuvo un modelo que integra la gestión de riesgos siguiendo el esquema del estándar internacional ISO/IEC 27002 considerando un enfoque de automatización para la fase operativa, de monitoreo y revisión, debido a que casi el 30% de los controles que se adaptaron son automatizables, y de esta manera hacer estos procesos más fáciles de manejar y más eficaces, en cuanto a variables de tiempo y esfuerzo.

En la tesis consultada se analizan diferentes modelos de metodologías, normas de gestión de riesgos de la seguridad de la información, beneficiando de esta manera al mejoramiento de la organización con ayuda de su factor humano.

Figuroa et al. (2017). En su investigación: *La seguridad informática y la seguridad de la información.*, Ecuador. La investigación de tipo documental estuvo orientada a diferenciar y relacionar la seguridad informática y la seguridad de la información. Los autores concluyeron sobre la gran diferencia existente entre estas dos terminologías, y su estrecha relación, donde una depende de la otra. En este sentido, se dice que la seguridad informática tiene una función protectora de factores internos y externos de las TI, mientras que la seguridad de la información sólo de lo que representa los datos, independientemente del medio en el que esté almacenado.

Este trabajo considera una teoría interesante que permite evidenciar el compromiso que debe haber por parte de la gerencia y personal de fomentar la cultura de conciencia de seguridad para así poder tener mejores resultados.

Mesa (2016). *Propuesta para la Implementación de un Sistema de Gestión de Seguridad de la Información aplicando la norma ISO 27001 para Industrias Ales. Guayaquil – Ecuador.* Tuvo como objetivo general desarrollar un plan de Gestión de Seguridad de la Información aplicando la norma ISO 27001 para los equipos y sistemas informáticos, partiendo del

análisis y gestión de riesgos desde su localización, y así poder detallar los eventos que generan impacto en la vulnerabilidad ante amenazas. Se concluye sobre lo común que ha resultado en las empresas la ocurrencia de fallas en sus plataformas tecnológicas que la vinculan a grandes pérdidas que afectan su estabilidad. Siendo así, en este trabajo se proponen lineamientos y políticas para poner en marcha un plan de gestión estratégico en el proceso de TI.

El citado trabajo sirve de aporte a esta investigación, por cuanto utiliza como medio de estudio la herramienta OCTAVE para una Pyme, intermediando con la norma 27001:2013, siendo una guía para conocer su enfoque tanto de uso como de análisis.

García et al. (2018). En el artículo científico: *Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas*. Lima - Perú. De acuerdo a los autores, a partir de los resultados se redujo el riesgo de seguridad de la información sobre los activos más críticos de la Pyme, teniendo como punto a favor la identificación de los mismos, para los cuales se direccionaron controles e indicadores que les permita mejorar con respecto al riesgo y provea un monitoreo del mismo.

En la tesis consultada se analizan diferentes modelos de metodologías, normas de gestión de riesgos de la seguridad de la información, beneficiando de esta manera al mejoramiento de la organización.

Carrión et al. (2021). En el artículo científico: *Modelo de seguridad informática para un medio de conexión pública, Peru*. Comentan que, entre organizaciones privadas de la educación, la aplicación de modelos de SGSI con base a los estándares ISO 31000 e ISO/IEC 27001, se tuvo a disposición un conjunto de instrumentos adaptados a los riesgos con

probabilidades de ocurrir, bajo un contexto de prevención y medidas de control para enfrentarlos. Se concluye que estas empresas incurren en riesgos extremos para la comunidad académica, ya que afectan la integridad, disponibilidad y confidencialidad, se encomendaron medidas correctivas alineadas a la gestión de seguridad de la organización.

El estudio fue un gran punto de apoyo para esta tesis porque existen procedimientos y políticas definidas para salvaguardar la información las cuales sirvieron para adaptarlas a la problemática.

Corda et al. (2017). En el artículo científico: *Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinaria para su abordaje*. Perú. Los nuevos avances que abundan en el mundo de la tecnología de la información, se ven inmersos en constantes riesgos en cuanto a su disponibilidad por vulnerabilidad a los que están expuestos, en el caso de las instituciones como bibliotecas, donde se maneja alta data e inventario de activos, es importante tener bajo control los riesgos que amenazan los sistemas de información, bajo modelos de control de la gestión de la seguridad tecnológica de los procesos del negocio, de manera de minimizar los daños a los que se enfrentan. Ante ello, los autores concluyen que es muy importante sensibilizar en el campo de la prevención de seguridad y riesgos, ya su vez canalizar estrategias para que los miembros de la organización se integren al cumplimiento de los objetivos de resguardos de los SI.

Este trabajo tuvo un efecto en el que se presenta, ya que el impacto que genera la evaluación conduce a recomendar buenas prácticas de resguardo de los sistemas de información, además de apoyar con conocimientos respecto a la metodología MAGERIT como enfoque de gestión de riesgos informáticos.

Marchand (2016). En el artículo: *Modelo de un Sistema de Gestión de Seguridad de la Información. Caso: Universidad Nacional Agraria de la*

Selva. Perú. Esquematiza un prototipo aproximado a un método que persigue el cumplimiento del enfoque que concentra las normas ISO/IEC 27001:2013 y que debe cumplir toda organización ya sea pública o privada. Igualmente enlaza la metodología de análisis y evaluación de riesgos basado en MAGERIT V.3, a partir de la aplicación de instrumentos, encuestas, entrevistas, entre otros necesarios para conocer la situación actual. Igualmente se adaptó una lista de chequeo para verificar los controles existentes, y desde las necesidades desarrollar los que serán requeridos en la posterioridad.

El citado trabajo será de gran ayuda en el desarrollo de los objetivos de la presente investigación, en cuanto a la idea que aporta para diseñar los instrumentos y formatos necesarios para la recolección de datos.

Berrios y Rocha (2015). *Propuesta de un Modelo de Sistema de Gestión de la Seguridad de la Información en una Pyme basado en la Norma ISO/IEC 27001. Peru.* Concluyó, que todas las unidades departamentales de la empresa son responsables de mantener y aplicar estrategias de forma conjunta a la seguridad de la información, por lo tanto, deben estar comprometidas a partir del uso de instrumentos gerenciales, tales como planes, programas, entre otros, que sistematice la ejecución de acciones para tal fin.

Este trabajo considera el compromiso por parte de la gerencia y personal que es muy importante ya que ayuda a fomentar la cultura de conciencia de seguridad para así poder tener mejores resultados.

Cruz y Fukusaki (2017). *Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la Clínica MEDCAM Perú SAC. Lima-Peru.* El SGSI desarrollado medió con los pasos de la metodología Deming a la que exhortan las normas ISO 27001 inherente a la gestión y mejora continua de los procesos, y con ello aminorar los peligros que acechan los activos de

información de MEDCAM Perú S.A.C. y evitar que estos sean violentados de manera de concertar confidencialidad, disponibilidad e integridad de la información.

El citado trabajo hace referencia a aspectos importantes a considerar para diseñar los instrumentos de recolección de datos del presente informe de investigación y así poder evaluar la seguridad en función de la norma ISO 27001.

Rodríguez et al. (2020). En el artículo científico: *Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. Lima. Perú.* De la aplicación de su metodología cuantitativa, se usó un estudio pre experimental en el que se confirmó la influencia de la aplicación del ISO 27001. Para esto se consideró la muestra de 30 colaboradores de la empresa en estudio. Indica la conclusión cuantitativa que si se tiene una influencia de la aplicación del ISO en la seguridad de la información y en los pilares de la seguridad informática: confidencialidad, integridad y disponibilidad.

Justino (2015). *Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013.* En su trabajo canalizó soluciones mediante la administración de la seguridad de la información en una empresa del sector inmobiliario, y en función de ello cumplió con su objetivo de encausar la eficiencia a través de gestión de la información en la alta dirección, y proyectar así una perspectiva del estado de los sistemas de información, así como sus medidas de seguridad aplicadas que fueron utilizadas para la toma de decisiones estratégicas.

El estudio de Justino (2015) se relaciona con el presente informe de investigación, debido a que ambos utilizan como política de calidad las ISO/IEC 27001:2013, la cual demanda a evaluar la gestión de seguridad de la información a partir de herramientas que garanticen la confiabilidad y

consistencia de su aplicación.

Leiva (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015.* Los resultados fueron encaminados desde la aplicación de la metodología que enfoca la norma ISO, donde se siguió metódicamente sus literales en cada proceso de negocio, donde se pudo detallar cada una de las limitaciones que obstaculizan la seguridad de los sistemas y de los activos en general dentro de la institución, ante la carencia de un control que evite riesgos latentes.

Esta tesis ayudó a tener un mejor enfoque sobre el utilizar una de las metodologías que caracteriza la ISO 27001, que es la PDCA, la cual se adecúa en la evaluación en este trabajo de investigación, siguiendo paso a paso las recomendaciones.

Zeña (2015). *Estándar Internacional ISO 27001 para la gestión de seguridad de la información en la oficina central de informática de la UNPRG en Lambayeque - Perú.* Como resultante se obtuvo que el trabajo enfocado a métodos y el seguimiento de políticas y lineamientos de normas ISO 27001, facilitan la detección de dificultades que afectan los procesos de negocio, en cuanto a la seguridad de los sistemas y de los activos presentes la organización.

De esta tesis se puede resaltar lo importante que es en realizar una buena Gestión de Seguridad de la Información, utilizando la metodología COBIT, Magerit III en unión con la ISO 27001 ayudan a concientizar al personal de la Oficina Central de Informática sobre la existencia de riesgos y la necesidad de resolverlos.

Fonseca et al. (2021). En el artículo científico: *A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. Colombia.* El presente trabajo nace de la necesidad de cuidar y proteger la información, como activo más importante, de una empresa que brinda soporte técnico en el sector hidrocarburos; se plantea crear un modelo de gestión de seguridad de la información alineado al ISO/IEC 27001:2013, como resultado mediante el modelo se logró definir su estructura de seguridad, políticas de seguridad de la información y una guía y manual detallado para su posterior certificación.

La relación del presente trabajo con esta investigación es muy estrecha dado que en ambos se busca crear un modelo que permite fijar políticas de seguridad de la información y brindar un manual para su futura certificación.

Aquino Cruz et al. (2021). En el artículo científico: *Implementation of an Information Security Management System Based on the ISO/IEC 27001: 2013 Standard for the Information Technology Division. Apurimac-Perú;* los autores exponen que la Universidad Nacional Micaela Bastidas (UNAMBA) de Apurimac no cuenta con ningún plan, estándar o directiva que permita proteger correctamente sus activos informáticos y su información. Por tal motivo plantean implementar un SGSI basado en la norma ISO/IEC 27001:2013 y vinculando el método Deming y la metodología Magerit. Obteniendo como resultado más significativo una disminución del 75% del nivel de riesgo luego de aplicados los controles y políticas de seguridad de la información.

La relación con el presente trabajo es amplia, ya que usamos las mismas metodologías buscando proteger los activos de la empresa en estudio.

Jaya Putra S. et al (2020). En el artículo científico: *Information Security Risk Management Analysis Using ISO 27005: 2011 for the Telecommunication Company. Tangerang – Indonesia,* plantea que la implementación de la gestión de riesgos de seguridad de la información busca llevar a cabo una gestión sistemática en el proceso empresarial. Usa

la ISO 27005 en relación con los requisitos de ISO/IEC 27001:2013 para controlar el riesgo, teniendo como principal resultado ocho objetivos de control de ISO/IEC 27001:2013 para respaldar la seguridad de la información, así mismo, los resultados servirán para planificar decisiones y programas de trabajo de control de riesgos.

La relación de este artículo con el presente trabajo se orienta por el uso de la norma ISO/IEC 27001:2013 para todo el análisis de riesgos.

Tariq M. I. et al (2020). En el artículo científico: *Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks*, describen la necesidad de proteger las redes informáticas dado que actualmente todo se maneja en la nube y gran parte de los equipos son inalámbricos, viendo el constante incremento en los ciber ataques proponen seleccionar controles de seguridad adecuados para proteger los activos informáticos. Además, indican que los controles de seguridad se deben dar en base a ciertos criterios, como niveles adecuados de seguridad y una investigación previa referente a vulnerabilidades, amenazas, riesgos, implementación, mitigación.

La relación con el presente trabajo va por considerar la red informática un activo clave dentro, además de la necesidad de cuidar todos los activos y por último coincidimos en implantar controles de seguridad traducidas en políticas que sean de cumplimiento masivo.

Mirtsch Mona et al (2021). En el artículo científico: *Information security management in ICT and non-ICT sector companies: A preventive innovation perspective*, describe que la ISO/IEC 27001:2013 ayuda a las empresas a proteger sus activos de información logrando los niveles de seguridad necesarios para tal fin; aborda la creciente necesidad de empresas portuguesas que buscan certificarse en la norma y las complicaciones mismas de la implementación de cara a últimos ataques de ciberseguridad que se llevaron a cabo, además menciona como la certificación en la norma ISO/IEC 27001:2013 es una herramienta eficaz para dar confianza a clientes, proveedores y partes interesadas que los

componentes de seguridad están verificados y validados.

La relación directa con la presente investigación se da por la norma ISO/IEC 27001:2013 orientada a proteger los activos de las empresas en mención, misma situación que se da en la presente investigación, proteger todos los activos de la empresa en estudio.

1.2. Teorías relacionadas al tema

Mientras menos expuesta esté la información en un equipo de computación es mayor su seguridad. En eso se basa uno de los principios principales que fundamentan la teoría de la información que se vincula con la seguridad basada en la oscuridad, y en todo caso con uno de los principios de Kerckhoff para la protección del código en donde se establece que no hay seguridad por oscuridad, al que le sigue el “principio de fortificación”, donde se hace referencia a que la víctima tiene que defenderse ante todos los agentes externos de ataque, mientras que el atacante certeramente es único. Ante esto, se cubren las bases de la encriptación, como acción para resguardar la información sin necesidad de esconderla Oliván (2017).

De allí surge la principal teoría que sustentan el tema de estudio, mejorada en los años cuarenta por el ingeniero Claude E. Shannon, quien concertó una teoría de la información que surgió a consecuencia de un estudio articulado a la comunicación donde abordaba las variables del mensaje, la señal, los medios de transmisión, el origen y destino con el fin de codificar los datos a procesar, y así asegurar la seguridad de la información sin que exista obstáculos de interferencia en la transmisión Oliván (2017).

1.2.3. Seguridad de la información

Para conocer con más exactitud lo que significa la seguridad de la información Oliván (2017) comenta en primer lugar que el término información atiende todos los datos que maneja una organización producto de su labor de servicio y producción. Esta puede ser de índole escrita, gráfica o visual, de audio, entre otras, que en todo caso es almacenable en

medios digitales con fines de transmisión a través de sistemas de telefonía o vía correo electrónico.

En conjugación con el término anterior, la ISO/IEC27001:2013 afirma que la seguridad de la información se enfoca a brindar garantías sobre la confidencialidad, integridad y disponibilidad de la información en la institución, junto a los sistemas que integran el compendio de recursos tecnológicos para su procesamiento. Para Zeña (2015), las características que dimensionan la seguridad de la información se pueden expresar de la manera siguiente:

- a. Confidencialidad: la información solo está disponible a personas y procesos autorizados.
- b. Integridad: la información es veraz y confiable, sin errores ni fallas.
- c. Disponibilidad: la información se obtiene en el momento requerido, sin limitación de acceso y alcance.

Estas tres denominaciones son los principios que ocupan la seguridad informática para garantizar la eficiencia en la gestión de seguridad de la información, y es por ello que las instituciones deben sustentar sus operaciones informáticas mediando con herramientas que les permitan evitar su exposición a riesgos.

1.2.4. Seguridad informática

La seguridad informática (SI) como doctrina plantea el desarrollo y establecimiento de normativas procedimentales que estructuran un método o modelo con el propósito de garantizar la seguridad y confiabilidad de un sistema de información para que este se encuentre disponible en el momento requerido Aguilera (2011).

Por su parte, Oliván (2017) refiere que la seguridad informática es la base de políticas orientadas a alcanzar de manera eficiente el desempeño de un sistema de información seguro y confiable a partir de lineamientos de protección, así como todos los componentes que este integra para su correcto desempeño; y surge con el propósito de proteger la infraestructura integral de los sistemas tecnológicos de la organización, tales como los activos o recursos que forman parte del sistema (como hardware, software y datos).

El objetivo primordial de la SI se enfoca a la minimización de los riesgos que se manifiestan desde la admisión de datos, procesamiento y hasta en su salida, vinculándose en ello los equipos de hardware que soporta tal proceso de la información. De allí que se destaque que esta disciplina ocupe la seguridad de los usuarios, la seguridad de la información, y la seguridad de la infraestructura Aguilera (2011).

1.2.5. Gestión de riesgos

Todo riesgo se traza de manera incierta sobre un evento que se puede deslindar en un efecto adverso (amenaza) o no (oportunidad) en las metas que se fijan en un proyecto Granadino (2019). El riesgo es concebido como la posibilidad de exposición de un sistema ante la materialización de una amenaza en los activos de una organización, los cuales son susceptibles a su impacto negativo.

Se puede decir entonces que la gestión de riesgos son un conjunto de acciones alineadas y orientadas a la dirección y control de riesgos en una compañía. Se fundamenta en un prospecto cuanti-cualitativo que caracteriza todos los activos pertenecientes a la institución, se valoran, se determinan las amenazas y vulnerabilidades para que estas se desarrollen, así como su probabilidad de ocurrencia Alvarado et al. (2018).

1.2.5.1. Etapas de la gestión de riesgos

En este sentido, se pueden diferenciar las siguientes etapas de la gestión de riesgos:

- a. **Identificación de las amenazas y riesgos:** al centrarse esencialmente en la protección de la información, las amenazas podrían discriminarse de tres formas:
- **Entrada ilegal al sitio de los datos:** donde es conveniente preguntarse sobre el daño que provocaría que se dieran a conocer por personal que no debería estar al tanto de ello (confidencialidad).
 - **Cambio no autorizado de los datos:** inherente al perjuicio ocasionado al dañarse o modificarse malintencionadamente (integridad).
 - **Exclusión de los datos:** referido al perjuicio que genera carecer de la información requerida en el momento solicitado (disponibilidad). Agencia Española de Protección de Datos (2018).

Se puede decir, que mayormente toda amenaza está vinculada a un riesgo articulado, razón por la que siempre el hecho de identificar los riesgos estará asociado a tener clara su causa de origen.

- b. **Evaluación de los riesgos:** se orienta a la estimación y tasación del impacto al que está expuesta la amenaza ante la posibilidad de que esta se concrete o se cumpla. Cabe destacar, que el impacto se establece en función del menoscabo visualizado ante el ataque de una amenaza, por lo que según la probabilidad y potencial efecto vinculado a la misma es que se puede determinar el poder del riesgo Agencia Española de Protección de Datos (2018).

- c. **Tratamiento de los riesgos:** en esta etapa se finaliza el proceso de gestión de riesgos, con el objeto de buscar las medidas de control que permita reducir y evitar el grado de exposición de los activos

ante las amenazas circundantes Agencia Española de Protección de Datos (2018).

1.2.6. Metodologías para el análisis de riesgos y seguridad informática

Con relación a la seguridad informática y seguridad de la información, se consolidan una serie de metodologías de análisis y gestión de riesgos, cuya elección óptima se realizará en función de su correcta posibilidad para practicar la misma de manera eficaz, de forma que se lleve a cabo hasta donde se pretende lograr.

Sin embargo, cabe destacar que aún con métodos muy bien desarrollados y comprobados, es difícil conseguir la seguridad total en lo que a gestión de riesgo se refiere, pero con la puesta en marcha de políticas para el tratamiento y control se puede alcanzar eficacia en los niveles de seguridad, de manera de reducir los riesgos tal como lo afirma Alvarado et al. (2018).

De acuerdo con Alvarado et al. (2018) entre las metodologías de gestión de riesgos más conocidas pertinentes a la función de servicios de medianas y pequeñas organizaciones privadas, se encuentran: OCTAVE, MEHARI, CRAMM, EBIOS y MAGERIT, de las cuales se proporciona un preámbulo a continuación:

MAGERIT, por ahora en su versión 3, es una metodología propuesta por el Consejo Superior de Administración Electrónica para el análisis y gestión de riesgos de los Sistemas de Información a los fines de minimizarlos cuando se implantan en las Administraciones Públicas Alvarado et al. (2018).

López (2018), agrega que es una metodología sencilla de utilizar, y por lo tanto no necesita de especialización en conocimientos para aplicarla; en función de ello puede ser aplicada por una o dos personas, pertenecientes

al ente gubernamental, ya sea grande o pequeño su factor humano, igualmente a pequeñas y medianas empresa Pymes.

OCTAVE (Operationally Critical Threat, Asset, And Vulnerability Evaluation), la cual es muy usada para abordar los riesgos de seguridad de la información aplicable a las TI en las grandes empresas con un volumen mayor a 300 empleados, permitiendo analizarlos y evaluarlos por capas de infraestructura informática y jerarquías, para su posterior plan de mitigación. Esta les permite garantizar a las empresas medidas ante riesgos operativos que afecten las finanzas del negocio, y por lo tanto una monitorización que vincule un gran equipo de trabajo López (2018).

MEHARI, desarrollada en Francia en 1996 por CLUSIF (Club Francés de la Seguridad de la Información) cubre un método que articula el análisis con la gestión de riesgos para todo tipo de organizaciones, y que requieran su control, manejo y seguimiento, utilizando sistemáticamente una estructura en módulos. Por lo que requiere un grupo de trabajo especializado López (2018).

CRAMM (CCTA Risk Analysis And Management Method), creada desde el Central Communication and Telecommunication Agency (CCTA) que es un organismo gubernamental de Inglaterra, maneja dentro de su procedimiento el análisis de riesgos más usado en países europeos tanto por grandes industrias y organizaciones gubernamentales o públicas con más de 300 personas. Entre estas grandes organizaciones se encuentran las de componentes militares, la OTAN, entre otras. Maneja a gran escala un proyecto de aplicación, diseño de políticas de seguridad ante riesgos, luego el análisis de riesgos, y por último estudio de los controles necesario para mitigarlos López (2018).

EBIOS (Expresión de las Necesidades e Identificación de los Objetivos de Seguridad), creada en Francia, esta metodología al igual que mucha se centra en analizar y gestionar el riesgo de seguridad de un sistema de

información de manera justificada, bajo un esquema que permite conocer su impacto en los procesos del negocio y a nivel económico financiero López (2018).

1.2.7. ISO 27001

Solarte et al. (2015) acotan que la norma ISO/IEC 27001:2013 declara las pautas para esquematizar la política integral de la seguridad de la información en cualquier clase de empresa o institución, ya sea pública o privada, pequeña o grande. Mediante este conjunto de normas se busca gestionar el riesgo considerando los siguientes elementos.

Activos: es el componente central que resguardar, y están representados por los diferentes recursos que integran una entidad y forman parte de su sistema de información. Son el todo poblacional, en el contexto de estudio.

Amenazas al activo: son los peligros en los que se ven inmersos los activos de la organización, ante alguna eventualidad. Al materializarse se incurre en daños tangibles e intangibles de algún activo institucional.

Vulnerabilidad del activo: es la probabilidad de que se lleve a cabo o se concrete una amenaza sobre un activo.

Impacto de un activo: es la consecuencia de que se concrete una amenaza sobre un activo.

1.2.7.1. Fases de la gestión de riesgos considerados en el modelo de la norma ISO/IEC 27001:2013

De acuerdo con Cuervo (2017), se amolda al siguiente esquema en dos (02) subprocesos bases:

- a. **Análisis de Riesgos:** se aproxima metódicamente a establecer el riesgo presente, tal como se señala a continuación:

- Identificación de activos a proteger.
- Valoración de los activos.
- Identificación de amenazas a las que se encuentran expuestos estos activos.
- Cálculo de Impacto bajo la cuantificación del daño que puede sufrir sobre un activo ante algún evento subestándar. Este se estima mediante la ecuación:

$$\text{Impacto} = \text{Valor del activo} \times \text{Porcentaje de Impacto}$$

- Cálculo del riesgo ante el impacto potencial considerando la frecuencia en que se puede dar.

$$\text{Riesgo} = \text{Frecuencia} \times \text{Impacto}$$

- Selección adecuada del tratamiento de los riesgos identificados a través de acciones pertinentes.
- Reducción del riesgo y riesgo residual ya que, al reducirse cierta cantidad de riesgos, se disminuye su margen inicial, el cual se denomina riesgo residual.
- Estimar el riesgo, definido como el impacto por probabilidad.

Cabe destacar, que los criterios de valoración de los activos, amenazas, vulnerabilidades y los riesgos, son Bajo cuando es igual a 1, Medio cuando es igual a 2 y Alto cuando es igual a 3.

- Tratamiento de riesgos:** donde se planifica y programa los controles ante los incidentes de inseguridad, y así garantizar la continuidad de las operaciones.

1.2.7.2. Modelo de gestión de riesgos basado en la norma 27001;2013

Cuervo (2017), comenta que su Sistema de Gestión de Riesgos (SGR)

se basa en vinculación con la norma ISO 27001, y contienen:

Tabla 1

Contenido del Sistema de Gestión Bajo la norma 27001:2013

Dominio	Descripción
Definición de la política de seguridad	Abarca los objetivos, el marco general, los requerimientos legales, los criterios de evaluación de riesgos.
Definición del alcance del SGR	Delimita hasta dónde llega el plan de acción dentro de la organización considerando los activos, las TI, con sus respectivas descripciones.
Identificación de los riesgos	Describe las amenazas a las que están expuestos los activos de la organización, los responsables directos, a qué son vulnerables y el impacto en los activos en caso de que se vean afectada su confidencialidad, integridad y disponibilidad.
Análisis y evaluación de los riesgos	Corresponde a estimar el impacto de algunos de los riesgos si se llega a materializar. Se percibe allí la probabilidad de ocurrencia y cómo esto afectaría los controles implementados.
Tratamiento de riesgos	Se sugieren o aplican aquí los controles necesarios, de acuerdo a los riesgos identificados. También se clasifican los niveles de riesgo.

Tabla 1

(Cont.).

Dominio	Descripción
Políticas de Gestión para la seguridad en TI	Se define el tratamiento de los riesgos, vinculados a los controles, y ante esto se diseñan los indicadores para medir la eficiencia y eficacia de la gestión. Igualmente se plantea el plan de comunicación del SGR para promover la concientización y fomentar una cultura organizacional sobre el cumplimiento del mismo.
Monitoreo	Se lleva a cabo el diseño de estrategia de verificación y revisión periódica del SGR a través de la formulación de indicadores de gestión para determinar hasta qué nivel se está cumpliendo con la normativa.

Fuente: Cuervo Álvarez (2017)

Una vez concretado el análisis y evaluación de riesgos, será necesario desarrollar un sistema de gestión para garantizar la seguridad de la información, aplicando el esquema de elaboración del modelo de gestión planteado, y con ello conllevar a la empresa en estudio a mejorar su seguridad informática al aminorar los riesgos a los cuales están expuestos todos sus activos.

1.2.8. Normas Técnicas Peruanas de Seguridad de la Información

1.2.8.1. 2NTP- ISO/IEC 27001:2013

Tal normativa fue preparada para consolidar los requisitos esenciales en la implementación, organización y adecuación de una estructura de gestión de seguridad de la información; ya que está sustentada ante las necesidades organizacionales, los elementos de seguridad y los asuntos propios del negocio Indecopi (2014).

Según Indecopi (2008), indica que la ISO cumple con las siguientes fases de planificación, implementación, actuación y monitoreo que es indispensable a considerar en el diseño de un sistema de gestión de riesgos. Se observa con anterioridad, que esta última fase cumple con el modelo del ciclo Deming o modelo de mejora continua, mediante el cual se aplican, luego de las evaluaciones, los sistemas de gestión de seguridad informática (SGSI).

1.3. Formulación del Problema

¿Cómo el modelo de gestión de riesgos bajo el ISO/IEC 27001:2013 puede mejorar la seguridad informática en una empresa de entretenimiento y juegos de azar, Lima-2021?

1.4. Justificación e importancia del estudio

Al presente, es usual que las pequeñas y medianas empresas del sector privado utilicen la información en la mayor parte de sus procesos operativos y administrativos a partir del uso de sistemas informáticos y las infraestructuras que estos implican. Es así, como ha cobrado relevancia poner en marcha herramientas que permitan ver el alcance de los riesgos a los que se encuentran expuestos los datos manejados, identificando amenazas, vulnerabilidades y efectos en las actividades de la organización, donde la mejora continua en gestión de la seguridad que enfoca la norma ISO/IEC 27001:2013 en materia de seguridad informática es sinónimo de garantía de continuidad y disponibilidad de la eficacia que pueda brindarse en este aspecto.

La empresa en estudio en Lima, utiliza una gran cantidad de información en sus procesos, que van desde documentos en físico y otros de manera electrónica vinculadas a muchos sistemas y equipos de tecnología de la información, cuya seguridad para tales activos de la información es importante, y es allí que se justifica el presente trabajo de investigación, donde se diseña un modelo de gestión de riesgos a los fines de proteger la actividad empresarial a partir de la seguridad informática, y elevar el nivel de eficiencia de la misma, ante su cumplimiento con la norma ISO/IEC 27001:2013.

Igualmente, a partir del conocimiento de la herramienta más efectiva, la gerencia podrá tomar decisiones más acertadas acerca de la estrategia más conveniente de protección y salvaguarda de la información, garantizando la confidencialidad, integridad y disponibilidad de los activos informáticos en la empresa en estudio.

1.5. Hipótesis

Ha: La implementación de un modelo de gestión de riesgos basado en la norma ISO/IEC 27001:2013 mejora la seguridad informática de una empresa de entretenimiento y juegos de azar, en Lima - 2021.

Ho: La implementación de un modelo de gestión de riesgos basado en la

norma ISO/IEC 27001:2013 no puede mejorar la seguridad informática de una empresa de entretenimiento y juegos de azar, en Lima - 2021.

1.6. Objetivos

1.6.3. Objetivo general

Implementar un modelo de gestión de riesgos para la seguridad informática bajo ISO/ IEC 27001:2013 en empresa de entretenimiento y juegos de azar, lima-2021.

1.6.4. Objetivos específicos

1. Diagnosticar la gestión de riesgos de la seguridad informática en la actualidad; de la empresa en estudio.
2. Diseñar el modelo de gestión de riesgos para la empresa en estudio.
3. Validar por juicio de expertos el modelo de gestión de riesgos propuesto para la empresa en estudio.
4. Implementar el modelo de gestión de riesgos propuesto en la empresa en estudio.

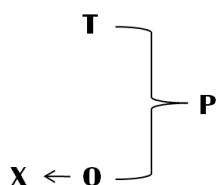
II. MATERIAL Y MÉTODO

2.1. Tipo y diseño de investigación

El presente estudio se destaca como una investigación con un enfoque cuantitativo, experimental, dado que se orienta a la cuantificación de datos provenientes de variables de estudios de campo, descriptivos y/o documentales que caracterizan las situaciones que sobresalen en cuanto a la gestión de riesgos asociados a la seguridad informática de la empresa en estudio, así como las amenazas a los que se ven expuestos y su vulnerabilidad ante estas, permitiendo obtener un diagnóstico más cercano a la realidad, referente a la situación actual del área de estudio Hernández et al. (2018)

Asimismo, se tomó como guía para la contrastación de la hipótesis el documento de metodologías de la investigación de los autores Hernández et al. (2018), quien refiere que un diseño no experimental de corte transversal, no concibe manipulación sobre variable alguna, tal como sucede en este trabajo; el cual además es transeccional o trasversal porque se realizó en un solo momento y; propositivo, debido a que se construyó un constructo referencial y luego se elaboró la evaluación de la gestión de riesgo y el diseño del modelo, para mejorar la seguridad informática de la empresa en estudio.

En el esquema que se presenta está considerada la relación de los factores antes planteados:



Donde:

X: Realidad de la institución

O: Observación

T: Modelo teórico

P: Propuesta de soluciones y recomendaciones basadas en la norma ISO/IEC 27001:2013.

2.2. Población y muestra

La unidad de análisis está conformada por todos los activos de la empresa en estudio, es decir, 679 activos o elementos. En este sentido, la muestra está compuesta por la totalidad de la población, ya que serán identificados los 679 activos que forman parte en la función de manejo de información de esta empresa en estudio.

2.3. Variables, operacionalización

2.3.1. Variable independiente

Modelo de Gestión de Riesgos basado en la norma ISO/IEC 27001:2013.

Definición: conjunto de acciones alineadas y orientadas a la dirección y control de riesgos en una empresa.

2.3.2. Variable dependiente

Seguridad Informática de la empresa de entretenimiento y juegos de azar.

Definición: es la que tienen como propósito proteger la infraestructura integral de los sistemas tecnológicos de la organización

Tabla 2
Operacionalización de variables

Variable de Estudio	Dimensiones	Indicadores	Índices	Técnicas e Instrumentos
Variable dependiente: Seguridad Informática de la empresa de entretenimiento y juegos de azar	- Diagnóstico de situación actual de la gestión de riesgos	- Índice de frecuencia	Tipo de riesgo x Cantidad de ocurrencias al año	Análisis Documental /Guía de análisis de documentos sobre registros históricos de la empresa 2020
	- Identificación de activos	- Cantidad de Activos	Unidades	Observación/ Guía de observación (lista de registros)
	- Análisis de riesgos	- Disponibilidad - Integridad - Confidencialidad - Amenazas - Vulnerabilidad	1 = Baja 2 = Media 3= Alta	
	- Evaluación de amenaza y vulnerabilidad de los activos	- Índice aritmético de vulnerabilidad - Índice aritmético de impacto - Índice de Riesgo	- Promedio \sum nivel de eventos/mes - Promedio \sum nivel de eventos/mes - Probabilidad x Impacto	Observación/ Guía de observación (lista de chequeo)

Tabla 2

(Cont.).

Variable de Estudio	Dimensiones	Indicadores	Índices	Técnicas e Instrumentos
Variable Independiente: Modelo de Gestión de Riesgos basado en la norma ISO/IEC 270001:2013	- Modelo Lógico	Eficacia del modelo a partir de controles de incidentes (Ei)	$Ei = \left(1 - \frac{IDA}{IAA}\right) \times 100$ Donde: IAA = Incidentes antes de aplicación de políticas SI IDA = Incidentes después de aplicación de políticas SI	Análisis Documental /Guía de análisis de documentos sobre registros históricos de la empresa 2021
	- Modelo Documental	<ul style="list-style-type: none"> - Definición de la política de seguridad - Definición del alcance del SGR - Identificación de los riesgos - Análisis y evaluación de los riesgos - Tratamiento de riesgos - Políticas de Gestión para la seguridad en TI - Monitoreo 	Acciones ejecutadas/ Acciones programadas	

Fuente: Elaboración propia

2.4. Técnicas e instrumentos de recolección de datos, validez y confiabilidad

- **Guía de análisis de documentos:** para el registro histórico de la gestión de seguridad informática (SI) del último trimestre del año 2020 (anexo 1), este instrumento permite responder el objetivo específico 1.
- **Guía de observación:** También se aplicó un instrumento tipo lista de registros donde se registraron los activos identificados (Ver anexo 3), este instrumento permite responder el objetivo específico 1, para conocer los bienes asociados a la seguridad informática (SI) de la empresa en estudio.
- **Guía de análisis de documentos:** para el registro histórico de la gestión de seguridad informática (SI) de los últimos 3 meses (marzo y abril del año 2021) en los que se ha venido trabajando con la seguridad informática en la empresa. Es decir, de marzo a abril 2021 (ver anexo 2), este instrumento permite responder el objetivo específico 2.

Esto, a fin de comparar la gestión del último trimestre del año 2020, (antes de aplicar la política de seguridad), con la gestión de este año luego que se empezara a hacer charlas sobre SI en la empresa en estudio (después de informar y evaluar la SI). Con ello se pretende medir la eficacia del modelo y comprobar la hipótesis de si mejora o no, la gestión.

- **Guía de observación:** este instrumento permite responder el objetivo específico 3, y en función de ello se aplicó un formato diagnóstico para el análisis y evaluación de riesgos basado en un guión de observación bajo la modalidad de lista de chequeo (Check List, ver anexo 4), para valorar el nivel de Disponibilidad, Integridad y Confiabilidad de cada activo (Anexo 4.1). Seguidamente, se evaluó

con otra plantilla el nivel de riesgo (Anexo 4.2).

- **Guía de observación:** Se aplicó un guion de observación bajo la modalidad de lista de chequeo (Check List, formato de validación de expertos), este instrumento permite responder el objetivo específico 4, para validar el modelo de gestión de riesgo por parte de tres (03) expertos en el área de SI.

Validez del instrumento / modelo:

Se validó los instrumentos de investigación con tres (03) expertos, concluyendo que esta apto para su aplicación con una validez promedio de 93.33%.

En el caso de la validez del modelo propuesto, de igual manera se hizo con tres (03) expertos a los cuales se solicitó por separado evaluar y analizar mediante un instrumento de diagnóstico (lista de chequeo), siendo aprobado y calificado con (4,90) en una escala del 1 al 5.

2.5. Procedimientos de análisis de datos

Para el análisis de datos se usó la estadística descriptiva usando promedios y cálculos simples. Se usó la técnica de *observación*, para evaluar los activos por un tiempo continuo del quehacer diario de todos los activos involucrados dándose una idea de la situación actual del problema de la gestión de riesgos en la seguridad informática y así familiarizar con los procesos que más adelante fueron motivo de estudio

También se usó la técnica de *Análisis de documentos*, para extraer los datos históricos; se revisó los que manejan en todo el proceso de seguridad de la información y gestión de eventos ocurridos en el año.

Todo esto se dio junto al Departamento de Sistemas, la reunión fue de manera grupal, con ellos se pudo establecer la identificación de activos, la discusión de la valoración de los activos, de las amenazas y las vulnerabilidades de los mismos.

Además, se usó el método Delphi y el coeficiente de correlación de Pearson para validar el modelo, el primero requiere la participación de expertos para responder un cuestionario o formato check list (ronda 1 y ronda 2); el segundo indica la relación entre las dos variables.

Se elaboró el modelo de gestión considerando todos los aspectos de seguridad física y de redes ante riesgos y amenazas a la confiabilidad, integridad y la disponibilidad de la información, así como de las políticas de seguridad por las que se rigen los objetivos de control de la ISO/IEC 27001:2013.

- Definición de la política de seguridad
- Definición del alcance del SGR
- Identificación de los riesgos
- Análisis y evaluación de los riesgos
- Tratamiento de riesgos
- Gestión
- Monitoreo

2.6. Criterios éticos

- a) Es importante el respeto por la confidencialidad de la información no autorizada que la empresa en estudio facilita al investigador, tanto como la que el investigador recauda de fuentes informáticas allegadas a la empresa. Sin embargo, ante esto fue necesario la autorización de la empresa por medios escritos para hacer uso de su razón social en este estudio Norena et al (2012).
- b) De igual modo la protección de los datos de los involucrados en la investigación. Ante esto, se les solicitó a los informantes una carta de consentimiento informado, para respaldar su aceptación en la participación en el estudio Norena et al. (2012).

2.7. Criterios de rigor científico

Se tomaron como criterios de rigor científico la credibilidad, la confirmabilidad y la transferibilidad Norena et al. (2012).

Credibilidad, que puede obtenerse al momento que los resultados son certificados por el autor del trabajo, así como por otros colaboradores con los cuales se han discutido los hechos encontrados. En la presente investigación se logró dicho criterio dado que cada entrevista fue una charla en la que no solo eran preguntas y respuestas sino un intercambio de opiniones, dudas, comentarios, que permitieron analizar y valorar los activos, amenazas y vulnerabilidades. Siendo en todo momento un escenario de confianza para ambas partes (Entrevistador y entrevistado). Norena et al. (2012).

La confirmabilidad, se entiende como la habilidad de otro investigador de seguir el camino o la ruta del investigador original llegando a las mismas conclusiones; siempre y cuando todo esté documentado, tantas ideas, decisiones, métodos de recopilación de datos, entre otras. En la presente investigación toda la documentación brindada permitirá que otro investigador pueda trazar un camino similar al que se está realizando, por ende, llegar a tener conclusiones similares o aproximadas Norena et al. (2012).

La transferibilidad, siendo este criterio el que permite ampliar los resultados del estudio a otras poblaciones, examinando en qué medida los resultados se aproximan a los nuevos escenarios. En la presente investigación se detallarán adecuadamente los resultados con los datos verídicos, al haber tenido acceso a la información de parte de los involucrados en esas labores Norena et al. (2012).

III. RESULTADOS

3.1. Resultados en tablas y figuras

En cuanto al **objetivo específico 1**, se obtuvo que en la actualidad la gestión de seguridad informática de la empresa en estudio es crítica ya que no cuenta con los controles necesarios que ayuden a mitigar los incidentes y dar frente a las amenazas y vulnerabilidades que se presentan para preservar la seguridad de la información.

Ante ello, se ha visto como resultado un alto índice de incidencias y hallazgos que menoscaban los resultados de su actividad operativa, lo cual se puede visualizar en la tabla 3, donde se clasificó de acuerdo al factor de riesgo los hechos imprevistos que se presentaron en los meses de octubre, noviembre y diciembre del año 2020 durante la gestión productiva de los activos informáticos de la empresa en estudio.

Tabla 3

Riesgos evidenciados en la gestión de seguridad informática de la empresa en estudio.

IV Trimestre año 2020

Factor de riesgo	Hallazgo	Oct	Nov	Dic	Total	Total factor riesgo
Industrial	1. Recalentamiento de equipos informáticos por exceso de temperatura	33	27	45	105	146
	2. Caída de los sistemas por corte eléctrico	7	4	3	14	
	3. Daños en aplicaciones informáticas por corte eléctrico	3	1	3	7	
	4. Daños en componentes de equipos informáticos por corte eléctrico	2	2	2	6	
	5. Desconexión de red por corte eléctrico	7	4	3	14	
	6. Pérdida de información por mala restauración de los respaldos	6	5	8	19	
Personas (por causa accidental)	7. Caída de los sistemas por falta de depuración	5	4	2	11	37
	8. Daños en aplicaciones informáticas por falta de actualización	3	2	2	7	

Personas (provocadas intencionalment e)	9. Daños en equipos informáticos por falta de mantenimiento y actualización de software	26	18	29	73	295
	10. Distribución de virus en aplicaciones informáticas por desactualización de software de protección	12	21	16	49	

Tabla 3
(Cont.)

Factor de riesgo	Hallazgo	Oct	Nov	Dic	Total	Total factor riesgo
Personas (provocadas intencionalment e)	11. Caída de los sistemas por agotamiento de los recursos ante su uso en equipos obsoletos	5	6	5	16	
	12. Daños en el equipo ante su agotamiento por obsolescencia	12	18	20	50	
	13. Escape de información confidencial por falta de políticas de control de almacenamiento	3	4	3	10	
	14. Hackeo de los sistemas por falta de políticas de control	4	2	3	9	
	15. Modificaciones de información por falta de políticas de control de cambios	15	18	9	42	
	16. Pérdida de componentes de equipos informáticos por falta de estrategias de control de entrada y salida de los recursos	18	7	21	46	
Total		161	143	174	478	

Fuente: Informe de Gestión del Departamento de Sistemas de la empresa en estudio (2021).
Elaboración propia.

La tabla anterior, muestra en relación a los riesgos evidenciados en el IV trimestre del año 2020 en la gestión de seguridad informática de la empresa en estudio, en el lapso comprendido entre el mes de octubre hasta el mes de diciembre del año 2020, en el cual ocurrieron **478** hallazgos, donde el principal incidente detectado se debió al recalentamiento de equipos informáticos por exceso de temperatura, hecho que se repitió en 105 ocasiones durante esos tres (03) meses.

Le siguen los hallazgos por daños en equipos informáticos por falta de mantenimiento y actualización de software, daños en el equipo ante su

agotamiento por obsolescencia, distribución de virus en aplicaciones informáticas por desactualización de software de protección, pérdida de componentes de equipos informáticos por falta de estrategias de control de entrada y salida de los recursos, y modificaciones de información por falta de políticas de control de cambios. Por tales motivos, la empresa tuvo que sustituir 14 equipos informáticos que sufrieron daños, según información aportada en el informe de gestión del Departamento de Sistemas (DSI).

Es importante señalar, que los seis (06) primeros hallazgos antes mencionados son considerados como riesgos críticos, dado que ocasionaron daños graves en los activos donde se presentaron, a tal punto de dejarlos inoperativos, lo cual en cierto momento se trasladó a toda la red y provocó la caída de todos los sistemas instalados de la empresa en estudio, lo cual afectó las operaciones de trabajo de las máquinas del casino, las actividades administrativas hasta por un lapso de inactividad de una semana, hasta su parcial restitución y nueva reinstalación de los mismos.

Así, se puede deducir, que los incidentes registrados develan el alto índice de incidencias que afectan la seguridad informática de la empresa en estudio, debido a que la empresa no cuenta con políticas para el control, manejo y seguimiento de la seguridad de la información, y en función de ello, nunca ha tomado acciones para este fin, tal como gestionar el análisis de riesgos, realizar la evaluación de amenazas y vulnerabilidades

Si esta situación persiste, la empresa perderá competitividad en el mercado, así como utilidades económicas, por lo que impera aquí implementar políticas de seguridad informática, que integren medidas preventivas para proteger los software y los equipos informáticos ante eventuales sucesos de: recalentamientos de equipos, ataques con software maliciosos, mantenimiento, renovación y/o repotenciación de equipos, entre otros.

En cuanto al **objetivo específico 2**, una vez diagnosticado el contexto, se procedió a diseñar el modelo de gestión de riesgos para la seguridad informática de la empresa en estudio, bajo el marco de la norma ISO/IEC

27001:2013. En función de ello fue pertinente su comprobación, cuyas políticas comenzaron a difundirse de manera informal en febrero del año 2021, de acuerdo con el plan de trabajo e implementación de un modelo de gestión de riesgo presentado a la gerencia general (ver tabla 17), que comenzó con la charla donde se dio a conocer dicho plan en todas las áreas que conforman el casino, utilizándose para su revisión y verificación de eficiencia en la práctica el siguiente indicador:

$$\% Ei = \left(1 - \frac{Ida}{Iaa}\right) \times 100$$

Donde:

$\% Ei$ = Porcentaje de eficacia del modelo.

Iaa = Número de incidentes antes de la aplicación de políticas de SI, reportados en el último trimestre (octubre, noviembre y diciembre) del año 2020.

Ida = Número de incidentes después de la aplicación de políticas de SI, reportados al comienzo de difusión de políticas de seguridad, es decir en marzo y abril del 2021.

Para el análisis de este indicador de eficacia fueron considerados los reportes históricos de incidencia hechos por los usuarios y el responsable del Departamento de sistemas (DSI), quien para tal fin realizó actividades de indagación, observación, inspección, supervisión, muestreo y consultas al sistema. En la tabla 4, se muestra un registro comparativo de ambos periodos, y su diferencia.

Tabla 4

Evaluación de eficiencia del modelo propuesto para la gestión del riesgo

Meses en estudio	Año 2020	Año 2021	Diferencia entre incidentes	Porcentaje de Eficiencia del Modelo
Oct 2020 / Mar 2021	161	36	125	78%
Nov 2020 / Abr 2021	143	24	119	83%
Total incidencias por año	304	60	244	80%

Fuente: Elaboración Propia

Como resultado de la medición se tuvo 304 incidentes reportados “antes” del comienzo de este estudio; y 60 incidentes después de comenzarse las charlas que dieron inicio al presente trabajo, evidenciándose una diferencia de 244 incidentes en este año, con respecto al año anterior, lo que quiere decir, que luego de la puesta en marcha de acciones para abordar el tratamiento de la seguridad informática la gestión mejoró en un 80%, que al aplicar el Coeficiente de Pearson es relativo a 0,903.

Ante este contexto, se observa en las estadísticas un significativo descenso sobre la cantidad de incidentes que ocurrieron entre el periodo estudiado en el año 2020 y el año 2021, siendo más palpable la diferencia en la comparación del mes de noviembre 2020 y abril 2021 donde ocurrieron 143 y 24 eventos, respectivamente, bajando mucho las cifras gracias a que se comenzó en el mes de febrero la concientización a los usuarios de los activos informáticos que asistieron a sus labores administrativas y de soporte durante la pandemia, sobre los riesgos relativos a la SI. Esto indica que, aplicando los controles propuestos, reducen en un 80% los riesgos que afectan la seguridad informática, aun cuando no se ha entrado a formalizar totalmente las políticas de control. Por lo tanto, se rechaza la hipótesis nula y se acepta la hipótesis alterna.

Lo anterior quiere decir que el desarrollo de un modelo de gestión de riesgos basado en la norma ISO/IEC 27001:2013 mejora la seguridad informática de la empresa en estudio. Sin embargo, es importante resaltar que el efecto que pueda causar el modelo diseñado puede incrementarse con posteriores mediciones que coincidan con la consecuente puesta en marcha del mismo.

En cuanto al **objetivo específico 3**, luego de diseñado el modelo de gestión de riesgos propuesto, se llevó a cabo la validación por juicio de expertos de dicho modelo, en el cual se le solicitó el valioso apoyo de tres (03) profesionales de Ingeniería de Sistemas, a los cuales se les planteó que opinaran sobre su perspectiva acerca de la correspondencia del prototipo diseñado con la Norma ISO/IEC 27001:2013, a manera de reforzar su confiabilidad. Ante ello, se

plantearon en el check list (ver anexo 5) los siguientes aspectos a validar:

IT1. Se establece un modelo de gestión de riesgos para la SI basado en la Norma ISO/IEC 27001:2013 de acuerdo con la teoría expuesta.

IT2. Se establece un modelo de gestión de riesgos para la SI basado en la Norma ISO/IEC 27001:2013 de acuerdo con lo señalado en la Norma.

IT3. El modelo gestión de riesgos basado en las normas ISO/IEC 27001:2013 cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.

IT4. El modelo gestión de riesgos propuesto cumple con las fases de las normas ISO/IEC 27001:2013.

IT5. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 sigue una secuencia lógica de los procesos que lo integran.

IT6. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente graficado.

IT7. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente explicado de manera que pueda guiar su implementación.

En la figura 1 se muestra el nivel de coherencia y apego del modelo propuesto de acuerdo con la perspectiva de los expertos.

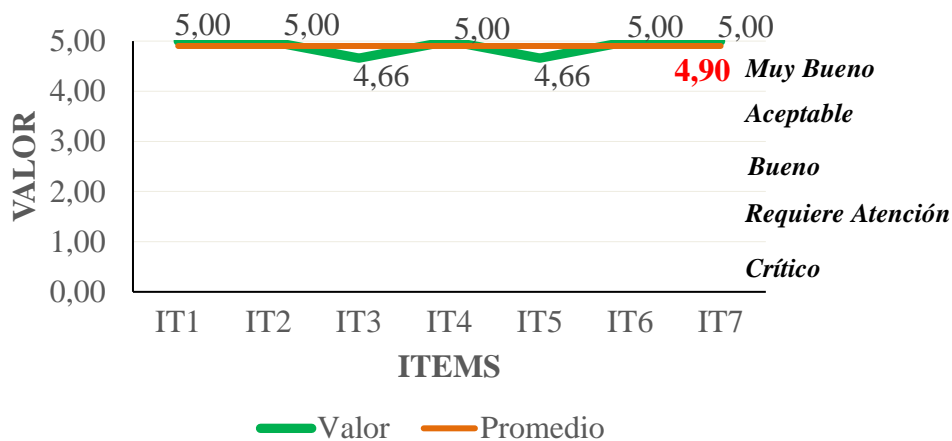


Figura 1. Nivel de coherencia y correspondencia del modelo propuesto con la Norma ISO/IEC 27001:2013
Fuente: Elaboración Propia

Se deslinda de la figura 1, que la perspectiva de los expertos acerca de la coherencia y correspondencia del modelo de gestión de riesgos para la SI propuesto con respecto a la norma ISO/IEC 27001:2013, alcanzó un nivel *Muy Bueno* al adjudicarse 4,90 puntos como promedio, contribuyendo a este resultado general los promedios alcanzados por los indicadores que lo integran, al validar el hecho de que dicho modelo cumple con los parámetros expuestos sobre cada una de sus fases y sus políticas, y siendo así, el modelo diseñado está alineado con sus fases, integrando medidas de control ante cada uno de los riesgos identificados en sus etapas claves, las cuales se presentan en procesos secuenciales bien estructurados, expresados a través de un diagrama de flujo que detalla todos los procesos inmersos, y que posteriormente son explicados detalladamente en la sección 3.3.

En cuanto al **objetivo específico 4**, inherente a la implementación progresiva del modelo propuesto de gestión de riesgos para la seguridad informática, de acuerdo al plan estructurado expuesto en la tabla 17 de la sección 3.3 de este trabajo, que fue aplicado a pesar de las limitaciones de la pandemia, gracias a que el investigador forma parte del talento humano como activo personal del casino en estudio, a la cual tiene libre acceso, por lo que la ejecución ya lleva un avance del 77,7% del plan, lo cual conllevó al resultado anterior en cuanto a eficacia del modelo, donde aplicando cada uno de los pasos del prototipo se

pudo identificar y valorar los activos que posee la empresa en estudio, siendo esto importante para tener presente cuáles son los equipos críticos y de más importancia dentro de lo que supone es la seguridad informática en esta organización.

Al valorarse los activos en función de las dimensiones de *Disponibilidad*, *Integridad* y *Confidencialidad*, se obtuvo lo siguiente en la tabla 5:

Tabla 5

Valoración de los activos de SI de Inversiones Fortunia. Año 2021

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Personas (P)	P1	Trabajadores del Casino	41	2			2	M
Personas (P)	P2	Trabajadores del DSI	2	3			3	A
Instalaciones (L)	L1	Gerencia General (GG)	1	2			2	M
Instalaciones (L)	L2	Departamento de Marketing (DM)	1	2			2	M
Instalaciones (L)	L3	Departamento de Administración (DA)	1	2			2	M
Instalaciones (L)	L4	Departamento de Contabilidad (DC)	1	2			2	M
Instalaciones (L)	L5	Departamento de Logística (DL)	1	2			2	M
Instalaciones (L)	L6	Departamento de Sistemas (DSI)	1	3	3	3	3	A
Instalaciones (L)	L7	Departamento de Mantenimiento (DM)	1	2			2	M
Instalaciones (L)	L8	Departamento de Recursos Humanos (RRHH)	1	2			2	M
Instalaciones (L)	L9	Departamento de Operaciones (DO)	1	2			2	M
Equipos Informáticos (HW)	HW1 – HW20	Laptop	20	3	2	3	3	A
Equipos Informáticos (HW)	HW21- HW25	Desktop	5	3	2	3	3	A
Equipos Informáticos (HW)	HW26- HW33	All In One	8	3	2	3	3	A
Equipos Informáticos (HW)	HW34- HW36	Switch	3	3	2	3	3	A
Equipos Informáticos (HW)	HW37- HW39	Impresora	3	2			2	M
Equipos Informáticos (HW)	HW40- HW41	UPS	2	3			3	A
Equipos Informáticos (HW)	HW42	Proyector Multimedia	1	2			2	M
Equipos Informáticos (HW)	HW43- HW44	Server	2	3		3	3	A
Equipos Informáticos (HW)	HW45	Router	1	3		3	3	A

Tabla 5
(Cont.)

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Equipos Informáticos (HW)	HW46	Antena	1	3		3	3	A
Equipos Informáticos (HW)	HW47- HW62	Pantallas TV	16	2			2	M
Equipos Informáticos (HW)	HW63- HW332	Máquinas Tragamonedas	270	2			2	M
Equipos Informáticos (HW)	HW333- HW603	Smib	270	3		3	3	A
Software y aplicaciones	SW1	Sistema Operativo: Microsoft Windows 10 Professiona1	1	2	2	2	2	M
Software y aplicaciones	SW2	Sistema Operativo: Microsoft Windows 8.1 Professional	1	2	2	2	2	M
Software y aplicaciones	SW3	Sistema Operativo: Microsoft Windows 7 Professional	1	2	2	2	2	M
Software y aplicaciones	SW4	Navegador web: Microsoft Edge	1	2	2	2	2	M
Software y aplicaciones	SW5	Navegador web: Google Chrome	1	3	2	3	3	A
Software y aplicaciones	SW6	Navegador web: Mozilla Firefox	1	2	2	2	2	M
Software y aplicaciones	SW7	Antivirus: ESET End Point Protection Standard	1	3			3	A
Software y aplicaciones	SW8	Ofimática: Microsoft Office 2013 Standard	1	2	2	2	2	M
Software y aplicaciones	SW9	Compresor de Carpetas y Archivos: WinRAR	1	2	2	2	2	M
Software y aplicaciones	SW10	Asistencia Remota: AnyDesk	1	3	2	3	3	A
Software y aplicaciones	SW11	Lector de PDF: Adobe Reader DC	1	2	2	2	2	M
Software y aplicaciones	SW12	Web: Aplicativos de Inversiones Fortunia	1	2	2	2	2	M
Software y aplicaciones	SW13	Sistema DR Gaming Technology™ (DRGT) (Usado en DSI, DO)	1	3	3	3	3	A
Software y aplicaciones	SW14	Windows Server 2012 R2 Standard (Usado en DSI)	1	3	3	3	3	A
Software y aplicaciones	SW15	SQL Server 2008 Express (Usado en DSI)	1	3	3	3	3	A
Servicios (S)	S1	Correo Electrónico	1	3	3	3	3	A

Servicios (S)	S2	Telefonía Fija	1	2			2	M
----------------------	----	----------------	---	---	--	--	---	---

Tabla 5
(Cont.)

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Servicios (S)	S3	Internet	1	3	3	3	3	A
Servicios (S)	S4	Soporte Técnico	1	3	3	3	3	A
Servicios (S)	S5	Creación de usuarios	1	3	3	3	3	A
Servicios (S)	S6	Redirección de Archivos	1	2			2	M
Redes de comunicaciones (COM)	COM1	Cableado Estructurado, Integrado por: Cables UTP, Categoría 6. Puntos de Red	1	3	3	3	3	A
Redes de comunicaciones (COM)	COM2	Conexión inalámbrica, Señal Wi-Fi de 150	1	3	3	3	3	A

Fuente: Elaboración Propia

De acuerdo con los datos registrados en la tabla 5, hay 327 activos con un nivel Alto de valoración ante la seguridad informática de la empresa en estudio.

Estos equipos son los que se tomaron en consideración en lo sucesivo para la identificación de amenazas y vulnerabilidades, y posterior evaluación de riesgos, por considerarse equipos con alto nivel de criticidad.

Con base a los resultados de valoración de activos cuyo resumen se expuso en la tabla 5, se presenta el mapa de valoración de riesgos de los activos en la tabla 6, donde dicho reporte fue realizado con ayuda del formato para el Análisis y Gestión de Riesgo basada en MAGERIT, que formó también parte del modelo que se centra en la norma ISO/IEC 27001/2013, el cual detalla la identificación de la amenaza de cada tipo de activo, la vulnerabilidad, el valor de cada una de estas variables, la estimación de la posibilidad de ocurrencia de la amenaza y la estimación del riesgo.

Tabla 6

Valoración del riesgo de los activos

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
P2	Trabajadores del DSI	Perdida de personal clave	Falta de políticas óptimas de retención de personal	3	3	3	3	9	Mayor	Evitar
		Accidentes Laborales	Falta de políticas de seguridad industrial	3	2					Evitar
		Fuego	Carencia de sistemas de protección contra incendios	2	3					Evitar
L6	Departamento de Sistemas (DSI)	Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización	3	3	3	3	9	Mayor	Reducir
		Robo de información	Falta de mecanismos eficaces de control de entrada y salida de recursos	3	3					Reducir

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
HW1 – Laptop HW20		Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización	1	2	2	2	4	Significativo	Reducir
			Falta de dispositivos de enfriamiento	3	1					Reducir
		Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	2	2					Reducir
		Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	2					Reducir
HW21- Desktop HW25		Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización	1	2	2	2	4	Significativo	Reducir
			Falta de dispositivos de enfriamiento	3	1					Reducir
		Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	2	2					Reducir

Tabla 6

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
HW21- HW25	Desktop	Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	2					Reducir
		Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización	1	2					Reducir
HW26- HW33	All In One		Falta de dispositivos de enfriamiento	3	1	2	2	4	Significativo	Reducir
		Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	2	2					Reducir
		Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	2					Reducir
HW34- HW36	Switch	Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2	2	2	4	Significativo	Evitar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
HW34- HW36	Switch	Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy poca capacidad de procesamiento	2	2					Aceptar
		Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2	2	2	4	Significativo	Evitar
HW40- HW41	UPS	Corte de servicio eléctrico	Falta de generadores eléctricos	2	2					Aceptar
		Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización	3	2					Evitar
HW43- HW44	Server	Falta de dispositivos de enfriamiento	Falta de dispositivos de enfriamiento	3	3	3	3	9	Mayor	Reducir
		Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	3	2					Reducir

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
HW43- HW44	Server	Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	3	3					Reducir
		Manipulación de equipos informáticos	Falta de mecanismos eficaces de control de cambios y manipulación de equipos informáticos	3	3					Evitar
		Hackers	Falta de mecanismos eficaces de control de cambios de información	3	3					Reducir
		Expansión de software dañino	Falla o carencia de software de protección o antivirus	3	3					Evitar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
HW45	Router	Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2	2	2	4	Significativo	Evitar
		Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy poca capacidad de procesamiento	2	2					Aceptar
HW46	Antena	Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2	2	2	4	Significativo	Evitar
		Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy poca capacidad de procesamiento	2	2					Aceptar
HW333- HW603	SMIB		Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2	2	2	4	Significativo	Evitar
		Corte de servicio eléctrico	Fallas del equipo auxiliar	2	2					Aceptar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
SW5	Navegador web: Google Chrome	Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	3	3	3	3	9	Mayor	Reducir
		Hackers	Falta de mecanismos eficaces de control de cambios de información	3	3					Reducir
SW7	Antivirus: ESET End Point Protection Standard	Expansión de software dañino	Falla o carencia de software de protección o antivirus	3	3	3	3	9	Mayor	Evitar
		Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	3	3					Reducir
SW10	Asistencia Remota: AnyDesk	Hackers	Falta de mecanismos eficaces de control de cambios de información	3	3				Mayor	Reducir
		Expansión de software dañino	Falla o carencia de software de protección o antivirus	3	3	3	3	9		Evitar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
SW13	Sistema DR Gaming Technology ™ (DRGT) (Usado en DSI, DO)	Hackers	Falta de mecanismos eficaces de control de cambios de información	3	3					Reducir
		Expansión de software dañino	Falla o carencia de software de protección o antivirus	3	3					Evitar
		Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	3	3	3	3	9	Mayor	Evitar
		Corte de servicio eléctrico	Falta de generadores eléctricos	3	3					Reducir
		Usurpación de identidad	Falta de mecanismos eficaces de control de acceso de usuario	2	3					Evitar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
		Hackers	Falta de mecanismos eficaces de control de cambios de información	2	2					Reducir
SW14	Windows Server 2012 R2 Standard (Usado en DSI)	Expansión de software dañino	Falla o carencia de protección o antivirus	2	2	2				Evitar
		Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	2	2		2	4	Significativo	Evitar
		Corte de servicio eléctrico	Falta de generadores eléctricos	2	2					Reducir
		Usurpación de identidad	Falta de mecanismos eficaces de control de acceso de usuario	2	3					Evitar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
SW15	SQL Server 2008 Express (Usado en DSI)	Hackers	Falta de mecanismos eficaces de control de cambios de información	2	2	2	2	4	Significativo	Reducir
		Expansión de software dañino	Falla o carencia de software de protección o antivirus	2	2					Evitar
		Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	2	2					Evitar
		Corte de servicio eléctrico	Falta de generadores eléctricos	2	2					Reducir
		Usurpación de identidad	Falta de mecanismos eficaces de control de acceso de usuario	2	3					Evitar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
S1	Correo Electrónico	Hackers	Falta de mecanismos eficaces de control de cambios de información	3	3					Reducir
		Expansión de software dañino	Falla o carencia de software de protección o antivirus	3	3	3	3	6	Mayor	Evitar
		Corte de servicio eléctrico	Falta de generadores eléctricos	3	3					Evitar
		Usurpación de identidad	Falta de mecanismos eficaces de control de acceso de usuario	2	3					Reducir

Tabla 6

(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
S3	Internet	Corte de servicio eléctrico	Falta de generadores eléctricos	3	3					Evitar
		Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	3	3	3	9	Mayor	Reducir
		Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy capacidad de procesamiento y de almacenamiento	3						Aceptar
S4	Soporte Técnico	Corte de servicio eléctrico	Falta de generadores eléctricos	3	3					Evitar
		Indisponibilidad de personal	Poco o nulo control de de las políticas de control del personal	1	2	2	3	6	Significativo	Evitar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
		Usurpación de identidad	Falta de mecanismos eficaces de control de acceso de usuario	3	3					Evitar
S5	Creación de usuarios	Cambio intencional de contenido informativo	Falta de mecanismos eficaces de control de cambios de información	2	2	3	3	9	Mayor	Evitar
		Manipulación de equipos informáticos	Falta de mecanismos eficaces de control de cambios y manipulación de equipos informáticos	3	3					Evitar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
COM1	Cableado Estructurado, Integrado por: Cables UTP, Categoría 6. Puntos de Red	Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2					Evitar
		Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy capacidad de procesamiento	2	2	2	2	4	Significativo	Aceptar
		Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2					Evitar
		Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy capacidad de procesamiento	2	2					Aceptar

Tabla 6
(Cont.)

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Índice de impacto (Probabilidad de ocurrencia de la amenaza)	Índice de vulnerabilidad (Valor del activo en riesgo ante vulnerabilidad)	Índice de riesgos (Total riesgo)	Nivel del riesgo	Acción
COM2	Conexión inalámbrica, Señal Wi-Fi de 150 2	Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2	2	2	4	Significativo	Evitar
		Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy capacidad de procesamiento	2	2					Aceptar
		Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	2	2					Evitar
		Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy capacidad de procesamiento	2	2					Aceptar

Fuente: Elaboración Propia

En la tabla 6, los activos que están en un nivel *mayor* de exposición son los del tipo persona (P), correspondiente a los trabajadores del DSI, por ser personal clave en el proceso de seguridad informática, al ser el único, y de desestabilizarse este o no estar disponible la empresa y sus activos quedarían desasistidos en cuanto a soporte técnico en general en ese momento, por lo tanto, esta situación debe *evitar*.

Asimismo, el DSI, donde se acogen los equipos de transmisión de datos de la empresa en estudio, también presentó un nivel *mayor* de riesgo dado que por la falta de políticas TI es muy vulnerable ante las amenazas del entorno, tanto a nivel interno como externo, ya que es un punto débil de ataque a la información de esta empresa, por lo tanto, sus riesgos se deben *evitar y reducir*.

En cuanto a los activos del tipo equipos informáticos, aun cuando todos son importantes al presentar un nivel de riesgo *significativo*, los que tienen *mayor* exposición en el proceso operativo y administrativo de la empresa son los servers, ya que si estos se paralizan se pierde la continuidad de los procesos generales que se prestan en la misma. Estos activos son los que procesan y almacenan la información clave de los servicios que se llevan a cabo en la empresa. Ante ello, resulta primordial evitar y reducir las amenazas ante las cuales poseen debilidad, al igual como sucede con los activos tipo software y aplicaciones, de orden administrativo, como son los sistemas (DR Gaming Technology™), tanto instalados en la red como los que están disponibles vía web (navegador y los antivirus), que también tienen un nivel *mayor* de riesgo.

Por su parte, los activos inherentes al tipo servicios, el de correo electrónico e internet resultaron ser los de *mayor* impacto y riesgo durante el estudio, por ser dos recursos indispensables como base de continuidad en todos los procesos y actividades que se llevan a cabo en la empresa.

Asimismo, es importante darle atención a todos los activos informáticos que integran la organización, ya al estar en un nivel *significativo*, el cual se considera aceptable a su vez, ya que de llegar a materializarse una amenaza

de igual forma genera un *efecto negativo en sus operaciones*; mientras que los de nivel mayor tendrían un impacto adverso de elevada envergadura, y se insta a ser reducidos en todas las circunstancias.

3.2. Discusión de resultados

De acuerdo a lo investigado, el incidente más resaltante que afecta la seguridad informática en la empresa en estudio fue el recalentamiento de equipos informáticos por exceso de temperatura, debido a que muchos de estos se encuentran ubicados en zonas donde los equipos de climatización tienen poco alcance, asimismo, la empresa poco ha hecho para mejorar su sistema de aire acondicionado, tal como sucede en otras organizaciones como las estudiadas por García et al. (2018), quienes destacan que importante mantener en un buen ambiente a los equipos de computación, en especial los servidores, y agregan un mecanismo de refrigeración de los mismos, así como un plan para el mantenimiento de los aires acondicionados de cada uno de los departamentos.

De la misma manera García et al. (2018), aborda estrategias para evitar daños en equipos informáticos, así como la distribución de virus en aplicaciones, por ser estos aspectos los que más cobran protagonismo en la seguridad informática de las Pymes, tal como sucede en la empresa en estudio, donde impera la falta de mantenimiento de las PCs e inadecuada planificación de la actualización de software que puedan causar daños a otros sistemas. Ante esto, es muy frecuente ver en los equipos informáticos del casino la presencia de programas maliciosos que de manera inmediata dañan el sistema operativo del equipo donde se hace presente, motivo por el cual deja de funcionar la estación de trabajo, afectando ante esto el proceso que se esté manejando desde el mismo.

De igual manera, se distinguieron seis rubros en cuanto a activos informáticos en este trabajo, los cuales se consideraron críticos y factibles de estudios, entre ellos: los equipos informáticos, software y aplicaciones, servicios y redes de comunicación, coincidiendo esto con el estudio de Carrión et al. (2021),

quienes detallaron y codificaron los equipos considerando los rubros que acoge MAGERIT, en consonancia con lo que establece la norma ISO/IEC 27001:2013 que sugiere el uso de una metodología que delimite el enfoque de trabajo. De manera muy diferente fue lo abordado en la investigación de Berríos y Rocha (2015), quienes solo trabajaron con dos (02) rubros de activos informáticos, y dieron prioridad a los equipos informáticos y software, es decir, lo que ellos consideran propiamente como elementos de las TICs. Aquí, en el presente trabajo, claramente se integra todos los elementos, incluyendo los servicios de soporte y las redes de comunicación por ser esenciales en el buen funcionamiento a nivel integral de los sistemas informáticos que mueven los procesos básicos de la empresa en estudio.

Igualmente se puede acotar, que este mismo tipo de problema generó una reacción en cadena, generando impactos negativos tanto en los equipos informáticos, como las aplicaciones y sistemas, causando graves daños en los mismos, a tal punto de tener que desincorporar a los primeros, o bien repáralos, lo que significó grandes gastos para la empresa; y los otros volverlos a instalar, aun cuando mucha información clave se perdió, dejando al aire información que era vital para algunos departamentos. Ante esto, Rodríguez et al. (2020) comentan sobre la importancia de los planes de mantenimiento de los equipos informáticos y de climatización, actualización de aplicaciones de protección, que garanticen su trabajo continuo, y con ello mantengan la sostenibilidad de los servicios.

Considerando estas apreciaciones, se estudió y aplicó en el diseño y desarrollo del modelo, el enfoque filosófico que contiene la norma ISO/IEC 27001:2013, el cual fue subdivido en las fases que sistematiza la metodología Deming, que es el que sugiere la misma norma ISO, para diseñar el modelo de gestión de riesgos, tal como se fusionan sus ideas en el modelo presentado por Cruz y Fukusaki (2017) y Carrión et al. (2021), quienes se basan también en varios aspectos que se establecen en la norma ISO 31000 y la metodología MAGERIT; invocando fases para conocer a la organización en estudio, su composición interna, analizar los riesgos, evaluarlos, y tratarlos a través de los

planes de gestión de riesgos que estén en coherencia con sus características y procesos de trabajo.

La implementación del modelo de gestión de SI propuesto se basó en un plan programado, cuya ejecución conllevó a aplicar el prototipo diseñado, siendo en su primera fase de análisis de riesgo donde se detectó que el mayor elemento o activo informático de riesgo son los servers, lo que resultó de manera similar en el estudio de Rodríguez et al. (2020) y Carrión et al. (2021), quienes detectaron que sus activos de más alto índice de riesgos eran los que se encontraban en sus centros de datos, encabezando la situación los servers de procesamiento de datos. Tales coincidencias reafirman el hecho de priorizar políticas de resguardos de estos equipos, cosa que no se consideró de hecho en los citados trabajos, donde solo se limitaron a evaluar los riesgos, sin embargo, en este estudio si se tomó en cuenta.

Una vez difundida la política de seguridad informática, se determinó que mediante la puesta en marcha del modelo propuesto para la gestión de riesgos, hubo un impacto positivo ante la seguridad informática ya que redujo de manera eficaz los incidentes similares que había ocurrido en periodos anteriores, tal como lo determinó Rodríguez et al. (2020), Carrión et al. (2021) y García et al. (2018), cuyos estudios confirmaron su hipótesis ante la eficacia de la ejecución de medidas para aminorar los riesgos e incidencias en las pymes con las que trabajaron, debido a que toda política de gestión de riesgos, permite dar una amplia visión general de cómo actuar ante la seguridad en los distintos elementos que forman las TI, mejorando los aspectos críticos inmersos en las mismas.

En cuanto a la validación del modelo mediante la apreciación y juicio de expertos, se pudo comprobar que el modelo propuesto tiene un nivel *Muy Bueno* de coherencia con respecto a la norma en estudio, y en consonancia con el estudio de Carrión et al. (2021), quienes aplicaron la metodología Delphi para dicha validación, y en la cual se incurrió a una sola ronda de discusión de los resultados para poder aprobarlos, dado a la alta puntuación obtenida ante la

similitud del modelo propuesto con respecto a los pasos que contempla la ISO/IEC 27001:2013, se corroboró que este modelo cumple con todas las expectativas expuestas en el instrumento de evaluación.

3.3. Aporte práctico

En el presente proyecto se busca implementar un modelo de gestión de riesgos para la seguridad informática bajo ISO/IEC 27001:2013 en casino “MERLIN”, para esto se han definido los siguientes objetivos: *1) Diagnosticar la gestión de riesgos de la SI en la actualidad, luego de ello 2) Diseñar el modelo de gestión de riesgos; una vez se tenga el modelo, 3) Validar por juicio de expertos el modelo de gestión de riesgos y por último 4) Implementar el modelo de gestión de riesgos propuesto, este último objetivo implica la ejecución por lo que se cumple en paralelo con el avance de los 3 primeros objetivos.*

Objetivo 1: Diagnóstico actual.

Inversiones Fortunia, es una empresa que opera bajo la figura de casino más de 20 años, con el nombre comercial “MERLIN”, se inició y consolidó en el departamento de Ica, luego se mudó y los últimos 3 años viene operando en el departamento de Lima, cubriendo el área económica de servicio de entretenimiento y juegos de azar, a través de su sala de diversión dotadas con una gran variedad de máquinas tragamonedas y dos ruletas, a los fines de ofrecer al público mayor de edad alternativas de recreación, en términos de calidad de servicio y excelencia operativa.

Es de resaltar, que, para llevar a cabo sus procesos administrativos y operativos, casino Merlín, cuenta con una valiosa plataforma tecnológica que en conjunto con su factor humano y su infraestructura conforman el macrosistema que da soporte a sus obligaciones y responsabilidades, en cuanto a su actividad económica como casino.

Para ello cuenta con una infraestructura de trabajo de 600 m², distribuidos en un edificio de 4 pisos, siendo el primer y segundo piso el eje de su operación, lugar donde aloja en toda su extensión un amplio volumen de activos que se relacionan con la gestión de seguridad informática (SI), lo cuales se pueden dimensionar según su tipo en:

- a. *Instalaciones:* que corresponde a los departamentos y salas de juegos que integran el casino, y donde están ubicados otros activos.

- b. *Personal*: relacionado con el capital humano que manejan los activos en la empresa. Sin embargo, para efecto del estudio solo intervendrán los dos (02) empleados que conforman el Departamento de Sistemas (DSI).
- c. *Equipos Informáticos*: que ocupan todos los elementos de hardware utilizados en la gestión de la información.
- d. *Software y aplicaciones*: que ocupan todos los elementos de software, aplicaciones o sistemas utilizados en el soporte de los procesos.
- e. *Servicios*: referidos a la asistencia que brinda un proceso dentro de los departamentos del casino.
- f. *Redes de comunicación*: son los medios de conexión y enlace de los elementos informáticos entre las diferentes áreas del casino.

En la siguiente hoja se muestra la tabla 7 en la que se presentan los activos de la gestión de SI en estudio.

Tabla 7

Activos relacionados con la seguridad informática en Inversiones Fortunia. Año 2021

Instalaciones (L)	Personal (P)	Equipos Informáticos (HW)	Software y Aplicaciones (SW)	Servicios (S)	Redes de Comunicaciones (COM)
1. Gerencia General (GG)	1. Gerente General	1. Un (01) equipo de computación desktop tipo genérico compatible.	Usados en todos los departamentos: 1. Sistema Operativo: Microsoft Windows 10 Professional 2. Sistema Operativo: Microsoft Windows 8.1 Professional 3. Sistema Operativo: Microsoft Windows 7 Professional 4. Navegador web: Microsoft Edge 5. Navegador web: Google Chrome 6. Navegador web: Mozilla Firefox 7. Antivirus: ESET End Point Protection Standard 8. Ofimática: Microsoft Office 2013 Standard 9. Compresor de Carpetas y Archivos: WinRAR 10. Asistencia Remota: AnyDesk 11. Lector de PDF: Adobe Reader DC 12. Web: Aplicativos de Inversiones Fortunia	1. Correo Electrónico	1. Cableado Estructurado, Integrado por: Cables UTP, Categoría 6. Puntos de Red
	2. Departamento de Marketing (DM)	2. Jefe de Marketing		2. Un (01) equipo de computación desktop tipo genérico compatible.	
3. Asistente de Marketing		3. Una (01) laptop Lenovo.		3. Creación de usuarios	2. Conexión inalámbrica, Señal Wi-Fi de 150
3. Departamento de Administración (DA)		4. Administrador		4. Un (01) equipo de computación desktop tipo genérico compatible.	
	5. Una (01) impresora Cannon color			5. Redirección de Archivos	
	6. Una (01) impresora Cannon monocromática			6. Redirección de Archivos	
	7. Un (01) switch Tp-Link.			6. Redirección de Archivos	
4. Departamento de Contabilidad (DC)	5. Contador	8. Un (01) equipo de computación desktop tipo genérico compatible.		7. Navegador web: Mozilla Firefox	7. Soporte Técnico
	5. Departamento de Logística (DL)	6. Jefe de Logística		9. Un (01) equipo de computación desktop tipo genérico compatible.	8. Navegador web: Mozilla Firefox
7. Comprador		10. Un (01) equipo de computación desktop tipo genérico compatible.		9. Navegador web: Mozilla Firefox	9. Soporte Técnico
8. Asistente de Almacén		11. Una (01) laptop Lenovo.		10. Navegador web: Mozilla Firefox	10. Soporte Técnico

Tabla 7

(Cont.)

Instalaciones (L)	Personal (P)	Equipos Informáticos (HW)	Software y Aplicaciones (SW)	Servicios (S)	Redes de Comunicaciones (COM)
6. Departamento de Sistemas (DSI)	9. Jefe de Sistemas 10. Analista de Soporte Técnico	12. Una (01) laptop Lenovo. 13. Un (01) equipo de computación desktop tipo genérico compatible. 14. Servidor Principal. 15. Servidor Backup. 16. UPS. 17. Un (01) switch TP-LINK. 18. Un (01) Router Cisco. 19. Una (01) Antena Cisco.	Usados en departamentos específicos: 13. Sistema DR Gaming Technology™ (DRGT) (Usado en DSI, DO) 14. Sistema de Control de Administrativo SAINT (Usado en DA, DC)		
7. Departamento de Mantenimiento (DM)	11. Jefe de Mantenimiento 12. Asistente de Mantenimiento 13. Técnico 1 14. Técnico 2 15. Técnico 3 16. Técnico 4	20. Una (01) laptop Lenovo. 21. Una (01) laptop Lenovo. 22. Un (01) equipo de computación desktop tipo genérico compatible. 23. Un (01) equipo de computación desktop tipo genérico compatible. 24. Un (01) switch TP-LINK.	15. Windows Server 2012 R2 Standard (Usado en DSI) 16. SQL Server 2008 Express (Usado en DSI)		
8. Departamento de Recursos Humanos (RRHH)	17. Jefe de Recursos Humanos 18. Asistente de Recursos Humanos	25. Un (01) equipo de computación desktop tipo genérico compatible 26. Una (01) impresora Cannon color. 27. Un (01) proyector multimedia.			

Tabla 7
(Cont.)

Instalaciones (L)	Personal (P)	Equipos Informáticos (HW)	Software y Aplicaciones (SW)	Servicios (S)	Redes de Comunicaciones (COM)	
9. Departamento de Operaciones (DO)	19. Gerente de Operaciones					
	20. Jefe de Sala 1					
	21. Jefe de Sala 2					
	22. Jefe de Sala 3					
	23. Jefe de Sala 4		28. Diez (10) equipo de computación desktop tipo genérico compatible.			
	24. Jefe de Sala 5					
	25. Jefe de Anfitrionas		29. Ocho (08) equipo de computación All In One Lenovo.			
	26. Anfitriona 1					
	27. Anfitriona 2		30. Dieciséis (16) Pantallas de TV.			
	28. Anfitriona 3					
	29. Anfitriona 4		31. Dos (02) UPS.			
	30. Anfitriona 5		32. Doscientos setenta (270) máquinas tragamonedas (TGM).			
	31. Anfitriona 6		33. Doscientos setenta (270) SMIB para conectividad de TGM con el SW de control de juegos DRGT.			
	32. Jefe de Caja					
	33. Asistente de Caja					
	34. Cajera 1					
	35. Cajera 2					
	36. Cajera 3					
	37. Cajera 4					
	38. Cajera 5					
	39. Jefe de Cocina					
	40. Asistente de Cocina					
	41. Ayudante 1					
	42. Ayudante 2					
	43. Lavaplatos					
	9 departamentos	43 personas	603 equipos informáticos	16 software y aplicaciones	6 servicio de informática	2 Redes de Comunicaciones

Fuente: Departamento de Sistemas de Inversiones Fortunia. (2021). Elaboración propia.

Se constató a través del registro presentado en la tabla 7, que actualmente Inversiones Fortunia cuenta con 679 activos en su gestión de SI, entre ellos 603 equipos informáticos, 16 software, 6 servicios de informática y 2 redes de comunicaciones, distribuidos entre 9 instalaciones o departamentos a lo largo de la infraestructura de la empresa para el uso de 43 personas que son sus trabajadores.

No obstante, de acuerdo al Jefe del Departamento de Sistemas (DSI), estos activos se encuentran desprotegidos al no contar con los medios técnicos adecuados, así como los de control para su óptimo resguardo, lo cual fue afirmado mediante el informe de gestión operativa de Inversiones Fortunia, que de acuerdo a la tabla 3 ya expuesta en el punto *3.1 Resultados en tablas y figuras*, arrojó que entre las situaciones de riesgos que impactaron tales activos se encontraban: los riesgos de tipo *industrial*, tales como la caída de los sistemas y desconexión de red por corte eléctrico, daños en componentes de equipos informáticos así como en aplicaciones informáticas por el mismo motivo anterior y constante recalentamiento de equipos informáticos por exceso de temperatura.

Así mismo, se pudo establecer que otros de los riesgos que ocurrieron fueron de tipo *personas (por causa accidental)*, de los cuales fueron a partir de la caída de los sistemas por falta de depuración, daños en aplicaciones informáticas por falta de actualización, pérdida de información por mala restauración de los respaldos, daños en equipos informáticos por falta de mantenimiento y actualización de software.

Por último se determinó que ante el tipo de riesgos *personas (provocadas intencionalmente)*, se presentaron hallazgos de hackeo de los sistemas por falta de políticas de control, caída de los sistemas por agotamiento de los recursos ante su uso en equipos obsoletos, distribución de virus en aplicaciones informáticas por desactualización de software de protección, modificaciones de información por falta de políticas de control de cambios, años en el equipo ante su agotamiento por obsolescencia, pérdida de componentes de equipos informáticos por falta de estrategias de control de

entrada y salida de los recursos, y escape de información confidencial por falta de políticas de control de almacenamiento. Ante lo ya expuesto, se puede observar el índice global de incidentes por factores de riesgos, lo cual arrojó en términos generales:

Tabla 8

Frecuencia de los incidentes por factor de riesgo

Alternativa	Frecuencia	Porcentaje (%)
Industrial	146	30%
Personas (por causa accidental)	37	8%
Personas (provocadas intencionalmente)	295	62%
Total	478	100%

Fuente: Informe de Gestión del Departamento de Sistemas de Inversiones Fortunia. (2021). Elaboración propia.

En la tabla 8, se percibe la ocurrencia de accidentes catalogados por tipo de riesgos “personas (provocados intencionalmente)” (62%) y “personas (por causa accidental)” (8%), dando un acumulado del 70% de impacto básicamente generados sobre los software y equipos informáticos presentes en el ambiente de trabajo, seguido por los riesgos de índole “Industrial” (30%) que son propios de las actividades cotidianas de las personas que laboran el casino.

Ante este contexto, se debe tener en cuenta la elaboración de políticas de control de la seguridad informática, ya que por esta principal razón se obvian los esfuerzos para ser responsables ante los riesgos y amenazas al que son vulnerables los activos. Igualmente, es importante aplicar mejoras en el equipamiento y software, como también en las instalaciones donde se encuentran los mismos, dada la importancia que representan estos activos en el resguardo y procesamiento de la información que maneja la empresa durante sus procesos operativos, que a su vez es de importancia para todos sus clientes apostadores en el momento que utilizan sus servicios, donde cualquier amenaza podría tener un enorme impacto en el momento de estar realizando una jugada exitosa, y por causas externas se le caiga la misma.

Objetivo 2: Diseño del modelo propuesto

Una vez conocido el panorama actual, se busca en este trabajo de investigación, canalizar un enfoque de trabajo para abordar la problemática suscitada ante los riesgos identificados anteriormente, siendo necesario abordar el diseño lógico del modelo de gestión de riesgos para Inversiones Fortunia, para su posterior desarrollo documental y práctico (ejecución de la implementación), y a así adaptar su método al estándar de la norma ISO/IEC 27001:2013 para los siguientes aspectos:

- Definición de la política de seguridad.
- Definición del alcance del SGR.
- Identificación de los riesgos.
- Análisis y evaluación de los riesgos.
- Tratamiento de riesgos.
- Políticas de Gestión para la seguridad en TI.
- Monitoreo.

Cabe destacar, que se selecciona esta norma por pertenecer a las políticas de ISO, y estar certificada de manera exclusiva por las NTP o Normas Técnicas Peruanas de Seguridad de la Información, lo que la hacen una mejor opción para implementarla en este trabajo de investigación.

Así mismo, siguiendo el método de aplicación de mejora continua que demanda el ISO y se basa en la metodología Deming, se destacan las siguientes fases:

Según Indecopi (2008), indica que la ISO cumple con las siguientes fases:

- **P (Plan):** A través del cual se establece el SGSI según el contexto identificado.
- **D (Do):** A través del cual se diseña la mejora del SGSI.
- **A (Act):** A través del cual se ejecuta e implementa la mejora del SGSI, a partir del análisis y evaluación de los factores que afectan la organización.
- **C (Check):** A través del cual se monitorea y revisa el SGSI.

Es así, que acogiéndose al dimensionamiento de estas fases, se pudo construir el modelo de GRSI (Gestión de Riesgos para la seguridad informática) en esta investigación, el cual además se fundamenta en la metodología MAGERIT, en cuanto a su sistema de análisis, evaluación y tratamiento del riesgo, por ser una metodología muy apreciada para trabajar la seguridad informática en pequeñas organizaciones privadas o públicas, además por su versatilidad, flexibilidad y sencillez, al momento de implementarla en empresas donde las exigencias de entrada y acceso a la información no son fáciles de levantar Alvarado et al. (2018).

Asimismo, el citado autor detalla en MAGERIT las siguientes características:

- Metodología documentada en idioma español especialmente para instituciones gubernamentales, así como para Pymes.
- Sus fases cumplen con el orden legal que establecen las normas ISO 27001.
- Cubre con la etapa de análisis, evaluación y tratamiento del riesgo.
- Eficiente aplicación ante entornos críticos.
- Flexibilidad en el ajuste de la codificación de activos.
- Flexibilidad en la escala de valoración de activos, tanto a nivel cualitativo como cuantitativo, donde se establece a juicio del investigador.

Sustentados en los tres puntos ya indicados, ISO, Deming y Magerit, se pudo construir el modelo, que en resumen fusionan los tres métodos anteriores, y todo enmarcado en la norma ISO/IEC 27001:2013, tal como se ilustra a continuación:

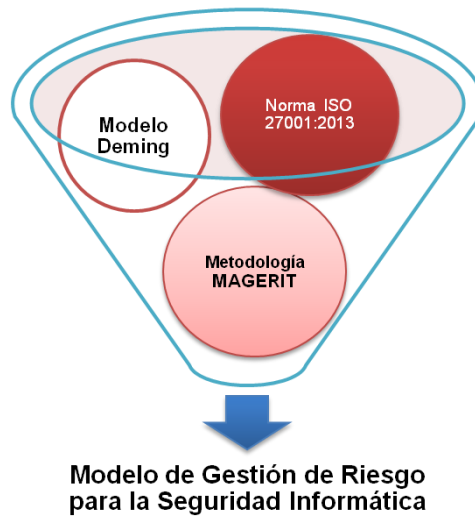


Figura 2. Sustento general del modelo propuesto para la gestión de riesgos en la empresa Inversiones Fortunia

Fuente: Elaboración Propia

Una vez conocidos los fundamentos del modelo que se desarrolla en este trabajo de investigación, se presenta en la figura 3, su diseño lógico:

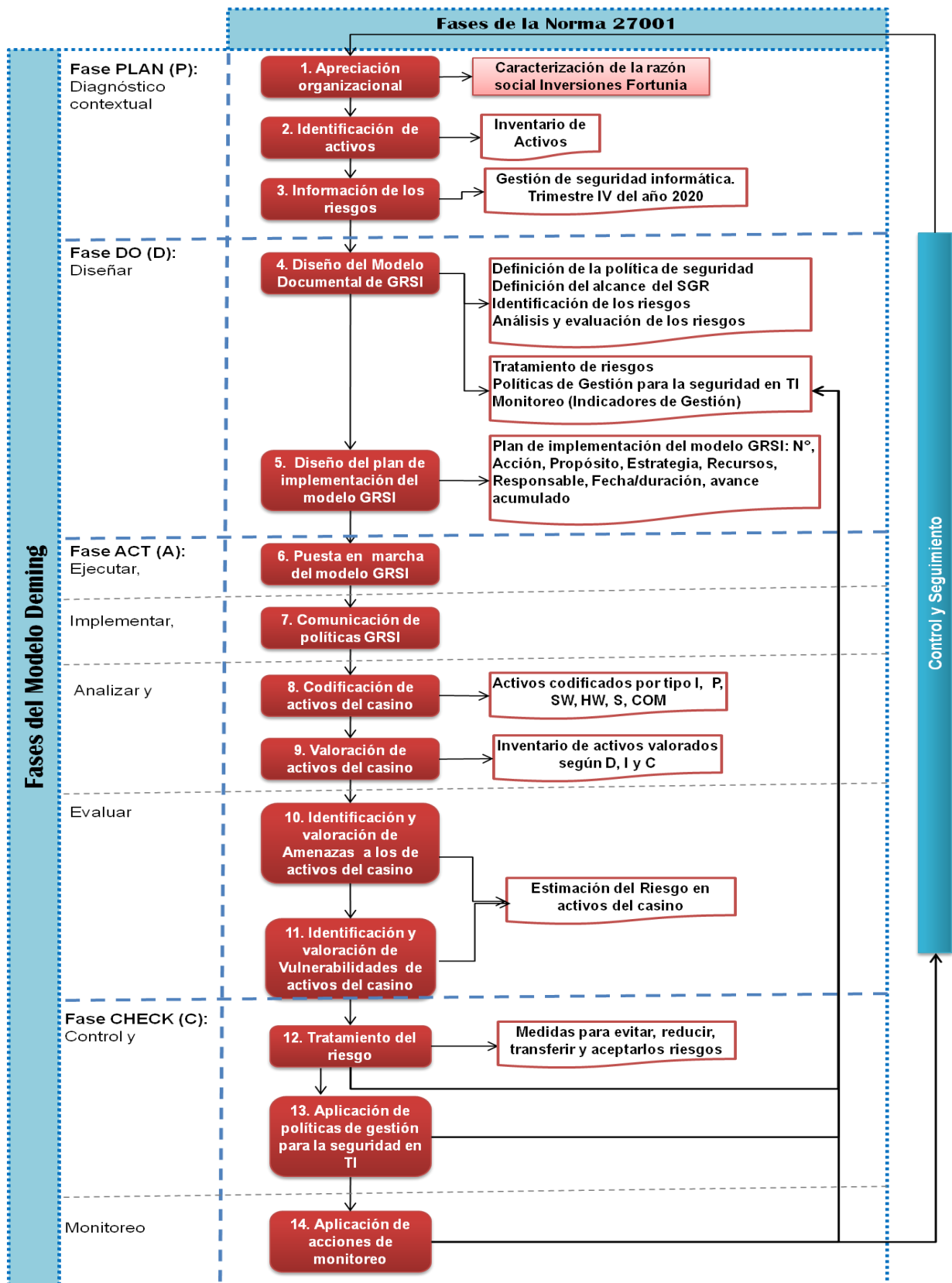


Figura 3. Modelo diseñado para la gestión de riesgos en la seguridad informática de Inversiones Fortunia, basado en la norma ISO/IEC 27001:2013

Fuente: Elaboración Propia

Descripción del Modelo Propuesto

El modelo de la figura 3, está basado en los parámetros estipulados en la norma ISO/IEC 27001:2013, la cual insta a aplicar la metodología MAGERIT para analizar, evaluar y tratar los riesgos para reducir su nivel de potencial; además usa las 4 fases del método Deming señaladas a continuación:

I. Fase PLAN (P): Diagnóstico contextual.

II. Fase DO (D): Diseñar.

III. Fase ACT (A): Ejecutar, implementar, analizar y evaluar.

IV. Fase CHECK (C): Control y monitoreo.

Fase I. PLAN (P), Diagnóstico contextual: en esta fase se lleva a cabo el estudio preliminar del escenario de trabajo, sobre el cual se levantará el plan de trabajo diagnóstico, y que además ya fue dado a conocer en el desarrollo del primer objetivo de esta investigación y contiene las 3 primeras fases de la norma ISO en nuestro modelo lógico, figura 3:

1. *Apreciación organizacional:* Inversiones Fortunia, es una empresa que opera bajo la figura de casino más de 20 años, con el nombre comercial “MERLIN”, se inició y consolidó en el departamento de Ica, luego se mudó y los últimos 3 años viene operando en el departamento de Lima, cubriendo el área económica de servicio de entretenimiento y juegos de azar, a través de su sala de diversión dotadas con una gran variedad de máquinas tragamonedas y dos ruletas, a los fines de ofrecer al público mayor de edad alternativas de recreación, en términos de calidad de servicio y excelencia operativa. Para llevar a cabo sus procesos administrativos y operativos, casino Merlín, cuenta con una valiosa plataforma tecnológica que en conjunto con su factor humano y su infraestructura conforman el macrosistema que da soporte a sus obligaciones y responsabilidades, en cuanto a su actividad económica como casino. Para ello cuenta con una infraestructura de trabajo de 600 m², distribuidos en un edificio de 4 pisos, siendo el primer y segundo piso el eje de su operación, lugar donde aloja en toda su extensión un amplio

volumen de activos que se relacionan con la gestión de seguridad informática (SI).

2. *Identificación de activos*: Se organizó un inventario de todos los activos que fue validado por el DSI, el mismo que se muestra en la tabla 7 del objetivo 1 del presente aporte práctico; la identificación de activos se hizo de acuerdo a la metodología Magerit clasificándolos en 06 categorías: instalaciones (L), personal (P), equipos informáticos (HW), software y aplicaciones (SW), servicios (S) y redes de comunicaciones (COM).

3. *Información de los riesgos*: En este punto buscamos conocer el nivel de exposición a los riesgos, que han sufrido los activos de Inversiones Fortunia, tomando como base la información documental de los registros históricos del IV trimestre del 2020 de la gestión de SI en el DSI de Inversiones Fortunia, donde se detallan los incidentes y hallazgos concernientes a la seguridad informática que ocurrieron a finales del año 2020, detectándose los riesgos potenciales que caracterizan los procesos operativos y administrativos de Inversiones Fortunia.

Clasificamos estos riesgos por su origen:

- *Natural*: como desastres naturales.
- *Industrial*: dado que está en plena zona urbana.
- *Personas (por causa accidental)*: falla del servidor por Falta de mantenimiento programado.
- *Personas (provocadas intencionalmente)*: instalación de software no autorizado.

Así mismo, esta clasificación nos permite identificar las amenazas, vulnerabilidades y los tipos de activos afectados tal y como se ve en el manual que sigue, **Fase II. DO, diseño del modelo, punto "C"**, tabla 9, *identificación de riesgos*.

Fase II. DO (D), Diseño del Modelo: abarcó la presentación del modelo documental, conteniendo la fase 4 y 5 de la norma ISO, modelo lógico, figura 3:

4. *Diseño de modelo documentario de GRSI:* Conforme se avanzó con la implementación del modelo, se realizó un manual ubicado luego de la descripción de la propuesta, donde se aborda paso a paso como realizar el presente diseño, para esto tenemos 07 subprocesos.

A. Definición de la política de seguridad, se abordó en conjunto con la Administración y el Departamento de Sistemas (DSI), coincidiendo en que la política principal de seguridad de Inversiones Fortunia es concientizar al personal para velar por los activos de la empresa y de esta manera garantizar la seguridad de la información, haciendo mayor énfasis en 02 áreas:

i) Clientes: ya que es sumamente crítica para toda la organización, dado que comprenden datos personales, información de juegos, ganancias, perdidas, etc. y ii) Administración, dado que tiene bajo custodia información de usuarios, claves, datos de las máquinas tragamonedas, etc.

En el manual se puede ver el punto “A” donde se brinda la política de seguridad general y en el punto “F” se detallan las Políticas de gestión para la seguridad en TI.

B. Definición del alcance del SGR, este define todo lo que el presente modelo abarca; en reunión con el Departamento de Sistemas y la Administración se definió que se debe considerar todos los activos relacionados con la seguridad informática, los cuales figuran en la tabla 7 y están clasificados en: Instalaciones, personal, equipos informáticos, software y aplicaciones, servicios y redes de comunicaciones.

C. Identificación de los riesgos, en este punto buscamos identificar las amenazas y vulnerabilidades que rodean a los activos de Inversiones Fortunia, al ser una edificación de 4 pisos con servicios básicos de agua/desagüe, luz, internet, tener colaboradores en planilla, además de terceros y por lo datos históricos encontrados; se identificó los siguientes tipos de amenazas: Natural, industrial, personas (por causa accidental) y personas (provocadas intencionalmente), seguido se indica la amenaza

propriadamente dicha y su vulnerabilidad, como también los activos que serían afectados.

- D. Análisis y evaluación de los riesgos, en este punto buscamos conocer los riesgos a los que están expuestos todos los activos de Inversiones Fortunia y los que podrían generar una situación crítica para los activos, ante las amenazas y vulnerabilidades.

Inventario de activos: realizado en la *Fase I. PLAN (P), Diagnóstico contextual*, y denominados según estándar de MAGERIT como se muestra en el manual, punto D, tabla 10.

Valorización de activos, en conjunto con el DSI y la administración se definió los criterios de disponibilidad, integridad y confidencialidad, además se identificó los activos críticos o de alto riesgo que pueden verse afectados negativamente. En el manual que sigue dentro del punto D, tabla 11, 12 y 13 se detalla los criterios de valoración cuantitativa y cualitativa de cada criterio y su descripción.

Además, la administración y el DSI decidió clasificar como activos críticos a las 6 clases de activos: personal, instalaciones, equipos informáticos, software y aplicaciones, servicios y redes de comunicaciones; se detalla los aspectos considerandos por el personal para valorar cada uno de ellos dentro del manual que sigue, punto D, valoración de activos.

Por último, se asigna un valor en cada criterio en función a cada activo, se suma y se divide entre tres (3 criterios), el resultado es el valor del activo; en el manual que sigue, punto D, se tiene una imagen con un ejemplo nítido del cálculo numérico, además la tabla resultante se puede ver en la parte de resultados, 3.1 Resultados en tablas y figuras, objetivo 4, tabla 5 valoración de los activos de Inversiones Fortunia.

Identificación de amenazas y vulnerabilidades, previamente en la *Fase I. PLAN (P), Diagnóstico contextual*; revisamos los todos los datos del diagnóstico actual usando los registros históricos del DSI e identificando tanto amenazas como vulnerabilidades en el manual que sigue, punto C, tabla 9.

Evaluación del riesgo, de forma cuantitativa, indicando medidas para su posterior tratamiento. De acuerdo a MAGERIT se define los criterios de valorización de ocurrencia de la amenaza, criterio de valorización de la vulnerabilidad y criterio de valorización del riesgo, estos 3 puntos se detallan tanto cuantitativa y cualitativamente en el manual que sigue, punto D, evaluación de riesgos. Con los criterios definidos se procede a realizar la tabla de valoración del riesgo, listando los activos y sus respectivas amenazas y vulnerabilidades, se hace el cálculo en primer lugar del índice de impacto: suma de valores de la amenaza referente a cada activo y luego dividiendo el resultado entre el número de riesgos que se tiene para el activo indicado. En segundo lugar, se hace lo mismo con el índice de vulnerabilidad, suma de valores de valor de vulnerabilidad respecto a cada activo y luego se divide entre el número de riesgos de cada activo indicado; en ambos casos si se tiene resultados con decimales se redondea al máximo inferior o superior según corresponda.

Finalmente se calcula el índice de riesgo multiplicando el índice de impacto por el índice de vulnerabilidad, en base al criterio de valoración del riesgo se define el nivel del riesgo. Se detalla un ejemplo grafico en el manual que sigue, punto D, evaluación de riesgos. La tabla resultante se puede ver en la parte de resultados, 3.1 Resultados en tablas y figuras, objetivo 4, la tabla 6 valoración del riesgo de los activos.

- E. Tratamiento del riesgo, se busca establecer un plan para tratar el riesgo. Hasta aquí se tiene en la tabla, el listado de activos con sus amenazas y vulnerabilidades, índice de impacto (amenaza), índice de vulnerabilidad, índice de riesgo y nivel del riesgo; faltaría incluir la acción a tomar como parte del tratamiento del riesgo. Para esto en conjunto con la administración y el DSI se evaluó cada punto de la tabla 6 valoración del riesgo de los activos y se definió la acción seguir, en función de evitar, reducir, transferir y aceptar los riesgos; por ejemplo, para lo que son los riesgos de personas coincidieron ambas áreas en evitar completamente los riesgos. Se detalla cada criterio en el manual que sigue, punto E.

F. Políticas de gestión para la seguridad en TI, una vez detectados los riesgos necesitamos lineamientos y políticas que nos ayuden a mitigarlos de acuerdo a su valoración e importancia. Para esto la administración y el DSI aprobaron las políticas en los siguientes niveles:

- Políticas generales
- Políticas de seguridad a nivel de personas
- Políticas de seguridad a nivel físico
- Políticas de seguridad a nivel lógico
- Políticas de seguridad a nivel de sistemas
- Políticas de respaldos y recuperación de información
- Políticas relacionadas a los equipos de computación
- Políticas de mantenimiento de equipos
- Políticas de actualización de los equipos
- Políticas de accesos remotos
- Políticas del WWW
- Políticas de control de virus, uso de software
- Comunicación de políticas GRSI

En el manual que sigue, punto F, se puede observar todas las políticas planteadas para cada nivel mencionado.

G. Monitoreo (indicadores de gestión), lo primero que se hizo fue plantear 3 políticas de monitoreo base para dejar un lineamiento claro al momento que iniciar el control, pueden ser mejoradas en revisiones futuras; luego se plantearon indicadores que permitan llevar el control y monitorear la efectividad del cumplimiento de las políticas planteadas en todos los niveles. Para este punto se vio por conveniente una reunión con la administración y el DSI, en dicha reunión la administración indico la necesidad de medir la efectividad en un corto, mediano y largo plazo; para esto se acordó incluir indicadores de nivel de efectividad de los controles, para saber si las políticas están siendo efectivas y los riesgos se están mitigando e indicadores para medir el entorno, para ver el comportamiento de ocurrencia y recurrencia de las amenazas, también se plantearon 02 sanciones generales orientadas al personal, con la

intención de enviar el mensaje que toda acción tendrá consecuencia, se puede mejorar en las revisiones futuras. Teniendo el esquema de monitoreo base que se quiere dejar en Inversiones Fortunia se elevó a la Gerencia General para su aprobación, teniendo conformidad de todos los indicadores mencionados. Se puede ver el detalle de las 3 políticas, los indicadores a corto, mediano y largo plazo, así como las sanciones en el manual que sigue, punto G, monitoreo (indicadores de gestión).

5. *Diseño del plan de implementación del modelo GRSI:* Antes de empezar el presente proyecto, se revisó varias veces con el administrador y el DSI los pasos a seguir para la presente implementación, incluso durante el proceso y por la pandemia se ha seguido revisando y ajustando el presente plan para procurar tener todo el cronograma con fechas reales, es así que se decidió que el plan de implementación debía tener en esencia la acción a realizar, el propósito y la fecha de ejecución, por mi parte agregue el resto de columnas dado que considere importante para saber cómo se abordó el presente plan y por ende la investigación:

- Sensibilización de los actores acerca de la Seguridad Informática.
- Diagnóstico del Contexto organizacional con respecto a la seguridad informática.
- Analizar los riesgos.
- Evaluar los riesgos.
- Tratamiento del riesgo.
- Control y seguimiento.

La tabla con el plan de implementación detallado se puede ver en la parte de resultados, 3.3 Aporte practico, objetivo 4, tabla 17.

Fase III. ACT (A): Ejecutar, implementar, analizar y evaluar: En esta fase implementamos en base al modelo documental, siguiendo paso a paso el Plan de Implementación de modelo GRSI tratado en la fase anterior (punto 5).

6. *Puesta en marcha del modelo GRSI:* En este punto se da inicio a todo el proceso contemplado en el Plan de Implementación del modelo GRSI, visto en la fase anterior. A detalle se puede revisar en la tabla 17 en el objetivo 4 del presente aporte práctico. A modo de resumen dejo las acciones consideraras dentro del plan:

- *Sensibilización de actores acerca de la seguridad informática*, con permiso de la Administración y Gerencia, se programan reuniones semanales con todo el personal durante dos meses explicando y abordando temas de seguridad informática tomando como base la data histórica de eventos con los que se armó el diagnóstico actual, usando ejemplos y de alguna manera logrando que los participantes capten los conceptos y consecuencias del referido tema.
 - *Diagnóstico del Contexto organizacional con respecto a la seguridad informática*, este punto abordado como un objetivo específico del proyecto se hizo apoyado en el DSI (Departamento de Sistemas) y en los registros históricos de las incidencias pasadas, siendo esta la base primordial para el proyecto.
 - *Analizar los riesgos*, basados en el objetivo 1, diagnóstico actual, se pudo identificar y analizar los riesgos que más pueden incidir en los activos de Inversiones Fortunia SA, para luego categorizarlos indicando amenazas y vulnerabilidades relacionadas.
 - *Evaluar los riesgos*, con base en Magerit teniendo identificados los riesgos podemos evaluarlos con criterios: nivel de ocurrencia y valoración.
 - *Tratamiento del riesgo*, teniendo identificados y evaluados los riesgos podemos definir cómo tratarlos: evitándolos, reduciéndolos, transfiriéndolos o aceptándolos.
 - *Control y seguimiento*, este punto es importante para ver cómo se comportan los riesgos, si cambian, cambiar las políticas y para medir las mismas en cuanto a su efectividad mejorándolas de ser necesario.
7. *Comunicación de políticas de GRSI*, se procede a comunicar a todo el personal las políticas a implementar, la vigencia y las sanciones por incumplirlas; en este caso por las limitaciones de la pandemia se hizo todo de forma virtual mediante correo electrónico y la intranet de la empresa.
8. *Codificación de activos del casino*, siguiendo el lineamiento de la metodología Magerit, se codificaron los activos identificados. El detalle de la tabla final se tiene en objetivo 1 del presente aporte práctico, tabla 7, activos relacionados con la seguridad informática en Inversiones Fortunia, y la forma

de hacerlo se explica dentro del manual que sigue, punto D, identificación de los activos de la empresa.

9. *Valoración de activos del casino*, para esto se usó los principios de la seguridad informática Disponibilidad, Integridad y Confidencialidad y siguiendo el lineamiento de la metodología Magerit a cada una se le dio un criterio de valorización. Se puede ver el detalle en la tabla final en la parte de 3.1 Resultados en tablas y figuras, objetivo 4, tabla 5; la forma como hacerlo dentro del manual que sigue, punto D, valoración de activos del casino.
10. *Identificación y valoración de amenazas a los activos del casino*, se generó una lista en base al registro histórico y la recurrencia, se designaron las amenazas que caracterizan a cada activo crítico o de alto riesgo; luego basado en la metodología Magerit se definió el criterio de valoración de la ocurrencia de la amenaza. La tabla resultante se puede revisar en la parte 3.1 Resultados en tablas y figuras, objetivo 4, tabla 6. La forma de hacerlo en el manual que sigue, punto D, valoración de amenazas de activos del casino.
11. *Identificación y valoración de vulnerabilidades de activos del casino*, en este punto dado un activo crítico, se asigna diferentes vulnerabilidades que de alguna manera pueda ser un problema de seguridad, siempre en relación con la amenaza del activo crítico; luego en base a la metodología Magerit se definió el criterio de valoración de la vulnerabilidad. La tabla resultante se puede revisar en la parte 3.1 Resultados en tablas y figuras, objetivo 4, tabla 6. La forma de hacerlo en el manual que sigue, punto D, valoración de vulnerabilidades de activos del casino.

Fase IV. CHECK (C): Control y monitoreo: Una vez identificados y evaluados los riesgos, en esta fase se realiza el tratamiento del riesgo que en resumen son las acciones a tomar para mitigar dichos riesgos, además se aplican las políticas de gestión ya difundidas en la fase anterior y por último se implementa las acciones e indicadores de monitoreo y control.


12. *Tratamiento del riesgo*, en conjunto con la Administración y el DSI se revisa la valoración de riesgos de los activos y se define la acción a seguir, tomando como base el Nivel de Riesgo puede ser: Evitar, reducir, transferir o

aceptar. Se puede revisar las acciones tomadas para cada riesgo de cada activo vinculado en la parte 3.1 Resultados en tablas y figuras, objetivo 4, tabla 6 y revisar el detalle de las 4 acciones definidas en el manual que sigue, punto E.

13. *Aplicación de las políticas de gestión para la seguridad de en TI*, en este punto se aplican las políticas que ya se dieron a conocer en la fase anterior, incluyendo las sanciones que se puedan dar producto de la falta cumplimiento por parte de los colaboradores de Inversiones Fortunia. Se puede revisar el listado de las políticas indicadas en el manual que sigue, punto F.

14. *Aplicación de acciones de monitoreo*, en conjunto con la Gerencia, la Administración y el DSI se confirmó la necesidad de controlar el cumplimiento de las políticas, y de igual manera medir la efectividad de las mismas mediante indicadores a corto, mediano y largo plazo.

Seguido, tenemos el manual guía donde en general se muestra ejemplos prácticos para abordar los puntos ya descritos:

	MANUAL Modelo de Gestión de Riesgos para la Seguridad Informática Basado en la Norma ISO/IEC 27001:2013	ID: 00013 Edición: 00 Año: 2021
---	--	--

A. Política de seguridad

Todo el personal debe mantener una posición de compromiso ante la gestión de riesgos y la seguridad informática de todos los activos de Inversiones Fortunia, y en función de ello, cumplir con los preceptos establecidos en la empresa para garantizar y promover que se cumplan las medidas canalizadas a llevar a buen término la gestión, se listan los lineamientos en el punto “F”.

B. Alcance

El presente modelo de gestión abarca a todos los activos identificados en el presente proyecto de Inversiones Fortunia SA, incluyendo el personal propio y de terceros que de una manera u otra entren en contacto con los equipos informáticos de la empresa.

C. Identificación de los riesgos

Mediante este paso, se busca establecer los tipos de amenazas y vulnerabilidades que actualmente afectan la seguridad informática de Inversiones Fortunia para su posterior análisis y evaluación, y por lo tanto se identificaron mediante el formato mostrado en la tabla 9, donde se detalla el *tipo de origen* (de donde proviene) y *tipo de activo* en el cual genera impacto:

Tabla 9

Amenazas y vulnerabilidades que afectan los activos en la empresa Inversiones Fortunia

Tipo de Amenaza por su origen	Amenaza (denominación)	Vulnerabilidad	Tipos de activos afectados
Natural	Fuego	Carencia de sistemas de protección contra incendios	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software, Personas
	Daños por agua	Falta de mecanismos de protección contra el agua	Equipos Informáticos, Instalaciones, Redes de Comunicación
	Desastres naturales (sismos)	Problemas estructurales de mobiliarios e infraestructuras donde se ubica el activo	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software, Personas
Industrial	Desastres industriales (fuga de gases, explosión)	Falta de controles previos del tipo de desastre	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software, Personas
	Corte de servicio eléctrico	Mal funcionamiento de la unidad protección auxiliar, falta de generadores eléctricos	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización, falta de dispositivos de enfriamiento	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
Personas (por causa accidental)	Errores humanos	Poco adiestramiento inducción ante el uso de aplicaciones, equipos y sistemas	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software, Personas
	Expansión de software dañino	Falla o carencia de software de protección o antivirus	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Debilidad de uso del software	Desactualización del software, inadecuada depuración del mismo	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software

Caída del sistema por agotamiento de los recursos	Equipos obsoletos, o con muy capacidad de procesamiento y de almacenamiento	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
---	---	--

Tabla 9
(Cont.)

Tipo de Amenaza por su origen	Amenaza (denominación)	Vulnerabilidad	Tipos de activos afectados
	Mala restauración de respaldos	Inexistencia de mecanismos para garantizar el respaldo o recuperar los mismos	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Fallas gestión de mantenimiento y actualización de equipos	Poco o nulo control de actualización de los equipos	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Indisponibilidad de personal	Poco o nulo control de las políticas de control del personal	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
Personas (provocadas intencionalmente)	Uso no previsto de los recursos	Poco o nulo control de las políticas de control del personal	Equipos Informáticos, Instalaciones, Redes de Comunicación, Software
	Usurpación de identidad	Falta de mecanismos eficaces de control de acceso de usuario	Equipos Informáticos, Personas, Redes de Comunicación, Software
	Cambio intencional de contenido informativo	Falta de mecanismos eficaces de control de cambios de información	Equipos Informáticos, Personas, Redes de Comunicación, Software
	Difusión de información	Falta de mecanismos eficaces de control de cambios de almacenamiento de la información	Equipos Informáticos, Redes de Comunicación, Software
	Robo	Falta de mecanismos eficaces de control de entrada y salida de recursos	Equipos Informáticos, Redes de Comunicación, Software

Cambios de contenidos de software	Falta de mecanismos eficaces de control de cambios y manipulación de programas	Software
Manipulación de equipos informáticos	Falta de mecanismos eficaces de control de cambios y manipulación de equipos informáticos	Equipos Informáticos, Redes de Comunicación

Fuente: Elaboración Propia

Tal como se observa los tipos de riesgos por amenazas que dan origen a los incidentes que afectan los procesos de Inversiones Fortunia se caracterizan por ser de orden natural, industrial o institucional, generados por personas, por causa accidental, o bien provocadas intencionalmente.

D. Análisis y evaluación de los riesgos

Análisis de riesgos: mediante esta etapa se persigue conocer los riesgos y las causas que podrían generar una situación crítica para los activos, ante las amenazas y vulnerabilidades.

- *Identificación de activos de la empresa:* durante esta actividad se lleva a cabo el proceso de denominar según las siglas estandarizadas por MAGERIT en la tabla 10, los activos que posee la empresa, lo cual permite clasificarlos por tipo y a codificarlos mediante una sigla que puede ir seguida de un número o 3 caracteres que estén relacionados con el nombre del mismo.

Tabla 10
Codificación para identificar los activos de la organización

Tipo de activo	Sigla asignada
Instalaciones	(L)
Personal	(P)
Equipos informáticos	(HW)
Software y aplicaciones	(SW)
Servicios	(S)

- *Valoración de activos del casino:* en esta actividad el personal del Departamento de Sistemas de la empresa definió en términos de *Disponibilidad (D)*, *Integridad (I)* y *Confidencialidad (C)*, cuáles son los activos críticos (de alto riesgo) para ellos y la organización, y que pueden verse afectados en caso de que se produzca un impacto negativo en su continuidad del proceso productivo donde interviene.

Tales criterios de valorización, se tomaron de los fundamentos de la metodología MAGERIT a partir de las dimensiones señaladas, y con ayuda del personal responsable de los activos de la organización, se lleva a cabo su valoración cuantitativa o cualitativa establecida en las tablas 11,12 y 13, según la puntuación que crea conveniente.

Disponibilidad: En esta dimensión se insta a certificar el escenario si no es oportuno el acceso de los usuarios a los activos en el momento que lo requieren.

Tabla 11
Criterio de Valorización de la Disponibilidad

Disponibilidad		Descripción
Valor Cuantitativo	Valor Cualitativo	
1	B (Bajo)	Si la información no estuviese disponible no habría efectos en las operaciones.
2	M (Moderado)	Si la información no estuviese disponible, habría algún efecto en las operaciones. Sin embargo, métodos alternativos pueden ser usados en las operaciones.
3	A (Alto)	Si la información no llegara a estar disponible cuando sea necesitada, habría un efecto fatal en las operaciones.

Fuente: libro II-MAGERIT- catálogo de elementos

Integridad: En esta dimensión se insta a certificar el escenario si no es exacta y completa la información procesada por el activo.

Tabla 12
Criterio de Valorización de la Integridad

Confidencialidad	Clase	Descripción
------------------	-------	-------------

Valor Cuantitativo	Valor Cualitativo		
1	B (Bajo)	No necesaria	Usado solo para consultas.
2	M (Moderado)	Necesaria	Si el contenido fuese falsificado habría problemas, pero no afectarían mucho a las operaciones.
3	A (Alto)	Importante	Si la integridad se perdiera, habría un efecto fatal en las operaciones.

Fuente: libro II-MAGERIT- catálogo de elementos

Confidencialidad: En esta dimensión se insta a certificar el escenario si la información accesible es sólo para aquellos autorizados a tener acceso.

Tabla 13

Criterio de Valorización de la Confidencialidad

Confidencialidad Valor Cuantitativo	Confidencialidad Valor Cualitativo	Clase	Descripción
1	B (Bajo)	Pública	Puede ser revelado y proporcionado a terceras personas.
2	M (Moderado)	Uso interno	Puede ser revelado y proporcionado. Si el contenido fuera revelado no tendría mucho efecto en las operaciones.
3	A (Alto)	Secreto	Puede ser solo revelado y proporcionado a partes específicas.

Fuente: libro II-MAGERIT- catálogo de elementos

Cabe destacar, que de antemano el personal de dicho departamento decidió clasificar como activos críticos a los pertenecientes a instalaciones (DSI), personal (de sistemas), equipos informáticos, software y aplicaciones, servicios y redes de comunicaciones tal como lo indica que se puede hacer la metodología MAGERIT. A continuación, los aspectos considerados para valorar su importancia:

(I) Instalaciones: Abarca la gestión de los diferentes departamentos de Inversiones Fortunia.

(P) Personal: Se orienta a la gestión de talento humano que labora en la organización en estudio.

(HW) Equipos informáticos: o bienes materiales de tipo físicos destinados a dar soporte a los servicios que presta la organización, sin estos no ocurre el procesamiento de los datos.

(SW) Software y aplicaciones: gestionan de forma automatizada las actividades funcionales mediante un equipo informático, que en conjunto actúan en el procesamiento de la información para emitir resultados en la prestación de los servicios.

(S) Servicios: la asistencia ante la gestión de información y el procesamiento de datos son la clave de avance de la empresa para prestar de manera continua sus servicios.

(COM) Redes de comunicaciones: Se consideran dispositivos físicos que permiten la transmisión de la información clave dentro de toda la extensión de la empresa.

La valoración del activo se realiza como sigue en la figura 4, con un ejemplo:

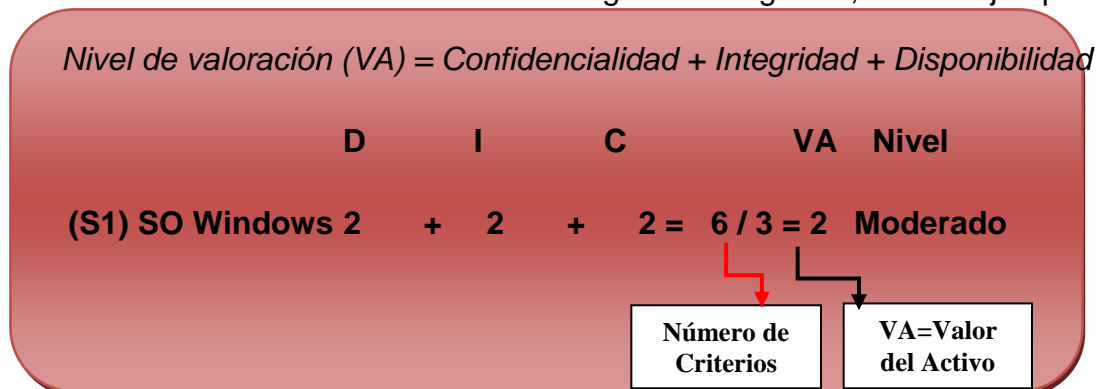


Figura 4. Ejemplo de valoración del activo
Fuente: Elaboración Propia

- *Identificación de amenazas de activos del casino:* en este paso, se generó una lista de riesgos característicos que representan una amenaza para los procesos organizacionales de Inversiones Fortunia, y que coinciden con las ya suscitadas en el año 2020, ya que han sido concurrentes durante los últimos años. Se designaron aquí las amenazas que caracterizan cada tipo de activo crítico o de alto riesgo.
- *Identificación de vulnerabilidades de activos del casino:* en este paso, dado un activo crítico, se le asigna las diferentes vulnerabilidades ante cualquier

situación que pueda desembocar en un problema de seguridad. Esta va en consonancia con la amenaza de cada tipo de activo crítico.

Evaluación de riesgos. En esta etapa se lleva a cabo la evaluación cuantitativa del riesgo, indicando las medidas para su posterior tratamiento. De acuerdo a la metodología MAGERIT, deben ser considerados los siguientes criterios para valorar la ocurrencia de la amenaza, así como su vulnerabilidad, para posteriormente obtener la evaluación del riesgo potencial (ver tabla 14, 15 y 16 respectivamente):

Tabla 14
Criterio de Valorización de la Ocurrencia de la Amenaza

NIVEL		Descripción
Valor Cuantitativo	Valor Cualitativo	
1	B (Bajo)	Es un fenómeno que ocurre rara vez en el año.
2	M (Moderado)	Podría ocurrir con alguna probabilidad.
3	A (Alto)	Existe una gran probabilidad de que ocurra, por lo menos una vez.

Fuente: libro II-MAGERIT- catálogo de elementos

Tabla 15
Criterio de Valorización de la Vulnerabilidad

NIVEL		Descripción
Valor Cuantitativo	Valor Cualitativo	
1	B (Baja)	Sí hay controles y son suficientes.
2	M (Moderada)	Hay algunos controles.
3	A (Alta)	No hay controles o no son suficientes.

Fuente: libro II-MAGERIT- catálogo de elementos

Tabla 16
Criterio de Valorización del Riesgo

NIVEL		Descripción
Valor Cuantitativo	Valor Cualitativo	
1	Insignificante: B (Bajo)	Impacto muy bajo - No requiere acción.
2	Menor: B (Bajo)	Efectos menores en el negocio - No requiere acción.
3	Poco Significativo: M (Moderado)	Algún efecto negativo - No se considera necesario tomar acción.
4 - 6	Significativo: M (Moderado)	Efecto negativo en el negocio. Estos riesgos son considerados aceptables.
7 - 8	Importante: A (Alto)	Tendrían serios efectos negativos en el negocio.
9	Mayor: A (Alto)	Tendrían efectos negativos mayores en el negocio,

y deberían ser reducidos en todas las circunstancias.

Fuente: libro II-MAGERIT- catálogo de elementos

Conocidos los criterios de ponderación para la evaluación, se procede a llevar a cabo las siguientes actividades:

- *Valoración de amenazas y vulnerabilidades en activos del casino:* mediante este paso se mide el efecto adverso vinculado a cada activo crítico en caso de que se concrete un riesgo. Se lleva aquí la sumatoria de las vulnerabilidades y se promedian las mismas, para así conocer el impacto.

15. *Valoración del riesgo en activos del casino:* En este paso se lleva a cabo la multiplicación de valor de activo por el valor de la amenaza y vulnerabilidad. De esta forma se obtiene el nivel de riesgo de cada activo con respecto a una amenaza.

Ante esto, se coloca un ejemplo para calcular el nivel de riesgo del activo en la figura 5:

Código de riesgo	Código de Activo	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor de Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo
R1	(SW1)	Laptop	Exceso de temperatura y humedad	Mal funcionamiento o carencia de equipos de climatización	1	2	2	2	4	Significativo
R2			Exceso de temperatura y humedad	Falta de dispositivos de enfriamiento	3	1		2 x 2 = 4		
R3			Fallas gestión de mantenimiento	Poco o nulo control de mantenimiento de los equipos	2	2				
R4			Fallas gestión de mantenimiento y actualización de software	Poco o nulo control de actualización de los programas	2	2				

$1 + 3 + 2 + 2 = 8/2 = 2$
 $2 + 1 + 2 + 2 = 7/2 = 1,7 \approx 2$

Figura 5. Ejemplo de valoración del riesgo del activo

Fuente: Elaboración Propia

E. Tratamiento del riesgo

En este paso se determina la acción para tratar el riesgo en función de evitar, reducir, transferir y aceptar los riesgos. Donde el cumplimiento de dichas dimensiones debe cubrirse de la siguiente forma:

Evitar, aplicando medidas de salvaguardas.

Reducir, evitando que suceda el evento que produce el riesgo.

Transferir, trasladar a otro entorno la responsabilidad el riesgo, por ejemplo, a un tercero.

Aceptar, no hacer nada al respecto y asumirlo.

F. Políticas de gestión para la seguridad en TI

Esta etapa se delimitan las medidas de mitigación y los lineamientos para administrar los riesgos detectados de acuerdo a su importancia y valoración, a partir de disposiciones adecuadas que garanticen su control y fluidez en los procesos organizacionales.

Políticas generales

1. Para entrar a la intranet de Inversiones Fortunia es necesario contar con una clave de acceso a la misma, cuya responsabilidad es de quien la usa.
2. No se podrá abrir más de una sesión, y si así se requiere, se necesita una autorización del jefe del área en que el usuario se encuentre.
3. Los usuarios tendrán acceso a la PC a las que se encuentran autorizados. En caso de no estar asignado a una PC se hará la solicitud ante esto.
4. Las claves de usuario tendrán una duración de hasta 120 días, sin embargo, el usuario puede cambiarla cuando considere conveniente.
5. Los usuarios dividirán sus aplicaciones bajo tipo pública y tipo privada.
6. Al no darle uso a una clave en un periodo de 90 días la misma será eliminada. Exceptuando situaciones de permisos por maternidad o enfermedad.

7. No se admitirá personas ajenas no autorizadas en el local del Departamento de Sistemas (DSI).
8. La documentación de los softwares pertenecientes a Inversiones Fortunia, tales como tutoriales y manuales estarán resguardados por el responsable del DSI.
9. La Unidad de RR.HH., comunicará al DSI la renuncia o retiro de empleados para que estos sean sacados de la base de datos de usuarios.
10. La limpieza y depuración de los discos duros (DD) se llevará a cabo en equipo con los usuarios de áreas implicadas como Base de Datos (BD).
11. Los usuarios tienen la plena responsabilidad de cuidar y proteger de los equipos informáticos a su cargo.
12. Los usuarios tienen la plena responsabilidad de la información almacenada en los DD de cuidar y proteger de los equipos informáticos a su cargo.
13. Los usuarios son responsables de la información almacenada en sus DD, y en función de ello deben respaldar la misma bajo los estándares establecidos por el DSI.
14. El responsable del DSI será el encargado de comunicar cualquier anomalía en el área, así como cualquier problema eléctrico que surja, o de los equipos de climatización, para su respectiva reparación y/o mantenimiento.
15. Todas las computadoras de escritorio o laptop deberán activar su clave de inicio.
16. Todas las computadoras de escritorio o laptop deberán activar el protector de pantalla.
17. La documentación física en papel inservible en el DSI es conveniente triturarla, o de lo contrario reutilizarla.
18. Para ingresar o sacar hardware o software de propiedad de Inversiones Fortunia se requiere de autorización escrita del Gerente, jefes de área o del responsable del DSI.
19. Para instalar un nuevo software será necesario contar con su licencia original.

Políticas de seguridad a nivel del personal

1. Detallar las responsabilidades de los empleados en relación con la seguridad informática desde la etapa de iniciación en la empresa, de manera que sean incorporadas en las descripciones de cargos y constituyan una de las bases para medir el cumplimiento de su desempeño.
2. Comprometer al empleado ante la Confidencialidad de la información.
3. Establecer los mecanismos requeridos en la difusión de las situaciones subestándares que menoscaban la seguridad informática en su área de trabajo, así como los riesgos que caracterizan a la misma.
4. Poner al tanto al responsable del DSI sobre las amenazas y riesgos inherentes a la SI, para que estos sepan cómo responder ante una eventualidad.
5. Incluir cursos, talleres y seminarios en los planes de capacitación para adiestrar al responsable del DSI sobre la gestión de riesgos en SI.
6. Entrenar personal de contingencia para colaborar con el DSI, en caso de falta o indisposición del responsable.
7. Crear planes de incentivo para aminorar la rotación de empleados en el área del DSI, y garantizar su retención en el puesto.
8. Proveer y garantizar la suficiencia de fuerza laboral para el área del DSI.
9. Todos los empleados de Inversiones Fortunia recibirán una adecuada capacitación y actualización periódica referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo, utilización de dispositivos de almacenamiento entre otros.
10. Incluir cursos, talleres y seminarios en los planes de capacitación para adiestrar a todo el personal en cuanto a la utilización de la plataforma informática de Inversiones Fortunia.

Políticas de seguridad a nivel físico

1. Restringir el acceso al DSI, donde solo se podrá entrar con autorización.
2. Se prohíbe fumar en el DSI.

3. Restringir el acceso a las instalaciones del casino luego de terminar el horario de trabajo, donde solo se podrá entrar con autorización.
4. Cuando suceda algún inconveniente en el DSI por fuego, accidente eléctrico o casos fortuitos o de fuerza mayor, se debe notificar al personal de Seguridad Laboral.
5. No se permite consumir ningún tipo de alimento o bebida cerca de los equipos de computación.
6. Revisar y realizar mantenimiento a los extintores de incendios periódicamente. Del mismo modo se debe proveer y garantizar la localización de un extintor en cada área del casino.
7. Se debe proveer de sistemas contraincendios a todas las instalaciones de Inversiones Fortunia, con prioridad el DSI.
8. Los equipos contra incendios deberán estar ubicados en lugares adecuados y deberán ser revisados de forma periódica para verificar su estado y cambiados cuando sea necesario.
9. Se debe proveer de un generador de energía eléctrica que soporte la carga utilizada en el casino, para garantizar la continuidad de sus funciones caso de corte de esta por la empresa proveedora.
10. Se debe proveer de equipos para respaldar el abastecimiento de energía, tal como los UPS para asegurar el apagado regulado y sistemático o la ejecución continua del equipamiento que sustenta las operaciones críticas.
11. Se debe verificar periódicamente el funcionamiento de los equipos de ininterrupción de suministro de energía (UPS).
12. Se debe asegurar contra todo riesgo los equipos hardware por una compañía de seguros.
13. Se debe contar con servicio de vigilancia permanente para el DSI.
14. Al momento de llevar a cabo las actividades de mantenimiento a los equipos debe estar presente el responsable del DSI.
15. Renovar los equipos de climatización del DSI.
16. Planificar actividades de mantenimiento a los aires acondicionados del DSI, y de las demás instalaciones en general del casino.

17. Se llevará control diario de las condiciones ambientales para verificar que no afecten el funcionamiento de las instalaciones de procesamiento de información y equipos de respaldo eléctrico.

Políticas de seguridad a nivel lógico

1. Las eventualidades que dificultan el buen desempeño del DSI, así como los activos informáticos deben ser registradas en una base de datos de incidentes.
2. Sólo el responsable del DSI podrá instalar y realizar mantenimiento del Sistema Operativo.
3. Sólo el responsable del DSI podrá instalar y actualizar las BD.
4. Sólo el responsable del DSI estará a cargo de la seguridad lógica de la estructura general de la red.
5. Sólo el responsable del DSI estará a cargo de crear y otorgar las claves de usuario.
6. Solo se otorgará claves de acceso a un software si el usuario tiene la habilidad de manejarlo.
7. Para acceder a la navegación de un software el usuario debe hacerlo mediante la secuencia del menú, y en caso de que el mismo no requiera utilizar un módulo dentro del sistema debe comunicarlo.
8. Se deben implementar medios contra ataques maliciosos como hackers o programas malignos.
9. Implementar equipos firewall para el apoyo en la protección de la red.

Políticas de seguridades a nivel de sistemas

1. Es conveniente que las aplicaciones y software orientados a ingresar datos contemplen la opción para validarlos previamente.
2. Es conveniente que las aplicaciones y software orientados a ingresar, modificar y eliminar datos contemplen la opción para generar registro de verificación que permita auditarlos, tales como fecha, hora, entre otros.

3. Se debe considerar el rol de los usuarios según su actividad en los sistemas diseñados, de manera que estos puedan ser agrupados según su clase o tipo.
4. Se debe considerar la recuperación automática de la información en caso de falla del sistema.
5. Se debe considerar las normas del DSI para el diseño y desarrollo de los sistemas.
6. Realizar periódicamente reuniones con los usuarios de software y aplicaciones para el aseguramiento del buen desempeño en el uso de estos.
7. Se debe considerar la ejecución de los sistemas con datos privados a partir del nivel de usuario o un equipo en particular.
8. Se debe hacer entrega al responsable del DSI la documentación de diseño lógico, preliminar y codificado, de los sistemas diseñados para la empresa Inversiones Fortunia. Se insertarán en documentos como:
 - a. Manual Técnico del Sistema.

Asimismo, se complementará la documentación con:

 - b. Manual del Usuario, y
 - c. Manual del Operador.
9. Se debe considerar firmar un acta de entrega y recibimiento del sistema diseñado, como garantía de propiedad del autor, y su cesión para uso legitimado a Inversiones Fortunia.

Políticas de respaldos y recuperación de información

1. Establecer el tiempo estipulado entre un respaldo y otro, de acuerdo con su importancia.
2. Los respaldos serán en distintos dispositivos de almacenamiento para la BD, aplicaciones, usuarios, archivos de documentos y archivos de SO.
3. Se debe mantener en lugares de amplia seguridad y localizados fuera del DSI los respaldos periódicos.
4. Se debe mantener en lugares de amplia seguridad y localizados dentro del DSI los respaldos de archivos permanentes.

5. Los archivos históricos estarán disponibles en línea hasta un lapso de 2 años. Posteriormente se resguardarán en servidores.

Políticas relacionadas a los equipos de computación

1. Todos los equipos informáticos que estén configurados a lo largo y extenso de la infraestructura de la red de la empresa deben estar sujeto a los estándares e instalación del DSI.
2. El DSI en coordinación con el Área de Administración deberá crear una BD que contenga todos los equipos que posee la empresa.
3. Todo equipo informático de la empresa que se considere que interviene en procesos claves y críticos, debe ubicarse estratégicamente en un lugar acondicionado y seguro.
4. El DSI es el responsable de todas las operaciones asignación y rotación de los equipos informáticos.
5. Es responsabilidad del usuario la seguridad física del equipo informático a su cargo.

Políticas de mantenimiento de equipos

1. Es responsabilidad del DSI realizar y controlar el mantenimiento preventivo y correctivo de los equipos informáticos, de manera de garantizar su seguridad y adecuación.
2. Se debe contratar organizaciones externas para complementar la práctica de mantenimiento preventivo y correctivo a los equipos informáticos, cuyo tiempo de garantía haya expirado.
3. Los usuarios no están autorizados para realizar mantenimiento a los equipos informáticos de su responsabilidad.
4. Se debe actualizar y ajustar semestralmente el plan de mantenimiento preventivo a equipos informáticos para verificar su correspondencia ante las necesidades.

Políticas de actualización de los equipos

1. Debe actualizarse periódicamente los equipos informáticos de la empresa, de manera que se conlleva de manera eficaz hacia su conservación y adecuado comportamiento.

Políticas de accesos remotos

1. Es responsabilidad del DSI autorizar a terceras personas para el uso de los recursos informáticos de la red.
2. Se debe cumplir con los lineamientos del DSI para este tipo de servicio.

Políticas del WWW

1. Es responsabilidad del DSI llevar a cabo la instalación y operatividad de los servidores WWW; y solo con páginas autorizadas por la Gerencia de Inversiones Fortunia.

Política de control de virus, uso de software

1. No se debe utilizar software sin licencias adquiridas por la empresa.
2. Garantizar el desempeño permanente y consecutivo de un antivirus instalado en los equipos de computación, cuya adecuación esté disponible en línea.
3. Llevar a cabo la ejecución del programa antivirus antes de usar algún dispositivo de almacenamiento auxiliar.
4. Generar la protección contra escritura de los dispositivos de almacenamiento auxiliar.

Comunicación de políticas GRSI

1. Informar mediante documentos (memorándums) enviados vía e-mail al personal o publicados en cartelera la nueva estrategia de seguridad

informática de Inversiones Fortunia, contentiva de todas las líneas aquí expuestas.

2. Entregar estrategias de difusión a todo el personal, consistente en un tríptico con la información relativa a las medidas de SI.
3. Evaluar periódicamente el conocimiento y concepción de los empleados ante las medidas de SI.

G. Monitoreo (Indicadores de Gestión)

Para esta etapa se generan los indicadores de gestión que permitan llevar el control y monitoreo a partir de la medición de la efectividad del cumplimiento de políticas de seguridad.

Políticas de gestión a nivel de monitoreo

1. Llevar a cabo la identificación de las amenazas que expongan la SI de los activos.
2. Realizar una planificación eficaz de la gestión de los riesgos, donde se incorpore anualmente un análisis y evaluación del riesgo.
3. Llevar un control y seguimiento eficaz de las políticas desarrolladas para garantizar la SI.

Indicadores

1. La reducción del nivel de riesgo en los activos que se integran a la SI en la empresa debe ajustarse en un horizonte de corto, mediano o largo plazo a través de los indicadores que se formulan a continuación:
 - Indicador para medir el nivel de efectividad de los controles: permite saber si las medidas implementadas tienen el funcionamiento esperado.
 - Indicador para medir el entorno: para la verificación del comportamiento de ocurrencia y recurrencias de las amenazas.
2. Los indicadores para implantar son:

A corto plazo:

- a. Cantidad de incidentes de SI reportados.
- b. Porcentaje de incidencias disminuidas, bajo la figura de la “eficacia del modelo de gestión de riesgo diseñado”.

A mediano plazo:

- c. Tiempo sin interrupciones / Tiempo total del servicio.
- d. Tiempo sin violaciones a la seguridad reportadas / Tiempo total del servicio.

A largo plazo:

- e. Valor del riesgo – valor de riesgos reincidentes en nuevo análisis.

3. La disminución del riesgo a corto plazo puede determinarse mediante revisión periódica de los controles implantados y comprobando si cumplen con lo esperado.

Sanciones

1. Se sancionará la violación malintencionada de las medidas de SI de acuerdo con las normativas del ente que le compete la administración de RR.HH. en Inversiones Fortunia.
2. Se suspenderá el servicio que presta el funcionario dentro de la empresa Inversiones Fortunia, dependiendo del nivel del daño causado en su actuación.

Una vez presentado el modelo documental, cabe decir que el mismo fue realizado bajo el marco que utilizan en Inversiones Fortunia para sus documentos oficiales para su respectiva revisión, y aceptación.

Las mencionadas políticas permitirán tener una visión clara de comportamiento y desempeño de todos los miembros de la empresa para lograr su principal objetivo expuesto en su política de seguridad.

Objetivo 3: Validación por juicio de expertos

Una vez diseñado y desarrollado el modelo, y comprobada su eficiencia, se procedió a validar el mismo a través del método Delphi, conformándose el grupo de informantes por tres (03) expertos por grado académico y experiencia, ver tabla 18:

Tabla 18

Grupo de expertos en SI que participaron en la validación del modelo

Nombre y Apellido	Profesión	Especialización/ Conocimiento en SI	Cargo	Ubicación
Carlos Alberto Chirinos Mundaca	Ingeniero de Sistemas	Magister en Informática y Sistemas / Diplomado en delitos informáticos	Perito en sistemas	Orcid: 0000-0002-6733-8992 Perú
Marlo Carranza Gallardo	Ingeniero de Sistemas	Jefe de Sistemas y Redes.	Jefe de TI y sistemas	DNI: 41996716 Perú
Joisy Del Valle Rojas Rojas	Ingeniero de Sistemas	Especialista en Seguridad de la Información / Magister en Educación	Auditor de Sistemas y Docente	CIV: 54207 Venezuela

Fuente: Elaboración Propia

En la tabla antes expuesta, se registran los expertos que fijaron su posición y perspectiva ante la coherencia y correspondencia del prototipo diseñado, con relación a los fundamentos de la norma ISO/IEC 27001/2013, y en este sentido verificar su grado de alineamiento a lo que esta establece.

Ante esto, fue necesario establecer el contacto con los expertos por correo electrónico y darle un preámbulo del modelo de gestión de riesgos y su modo de funcionamiento, para luego enviarle un resumen del informe con el planteamiento del problema o realidad problemática, la teoría que soporta la norma ISO/IEC 27001:2013, el diseño del modelo de gestión de riesgo propuesto (gráfico y descripción de los procesos), y la lista de chequeo inicial (ver anexo 5), con los siete (07) aspectos evaluados de acuerdo a las medias aritméticas en la frecuencia de cada uno de los ítems de estudio, para posteriormente ser relacionadas con el resultado de la escala de Lickert

mostrada en la tabla 19.

Tabla 19

Escala utilizada para el análisis de la lista de chequeo

Alternativas	Criterio de Evaluación
Totalmente de acuerdo (TA)	Muy Bueno (de 4,1 puntos a 5 puntos)
De acuerdo (DA)	Bueno (de 3,1 puntos a 4 puntos)
Neutral (N)	Aceptable (de 2,1 puntos a 3 puntos)
En desacuerdo (ED)	Requiere Atención (de 1,1 puntos a 2 puntos)
Totalmente en desacuerdo (TD)	Crítico (de 0,1 puntos a 1 puntos)

Fuente: Elaboración Propia

Tales resultados, fueron registrados y tabulados para su análisis respectivo, siendo su registro el que se muestra en la tabla 20:

Tabla 20

Medición del nivel de coherencia y correspondencia del modelo con respecto a la ISO/IEC 27001:2013

Ítems	TDA	DA	N	D	TD	Total	Promedio
	5	4	3	2	1		
IT1. Se establece un modelo de gestión de riesgos para la SI basado en la Norma ISO/IEC 27001:2013 de acuerdo con la teoría expuesta.	3	0	0	0	0	3	5,00
IT2. Se establece un modelo de gestión de riesgos para la SI basado en la Norma ISO/IEC 27001:2013 de acuerdo con lo señalado en la Norma.	3	0	0	0	0	3	5,00
IT3. El modelo gestión de riesgos basado en las normas ISO/IEC 27001:2013 cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.	2	1	0	0	0	3	4,66
IT4. El modelo gestión de riesgos propuesto cumple con las fases de la norma ISO/IEC 27001:2013.	3	0	0	0	0	3	5,00
IT5. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 sigue una secuencia lógica de los procesos que lo integran.	2	1	0	0	0	3	4,66
IT6. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente graficado.	3	0	0	0	0	3	5,00
IT7. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente explicado de manera que pueda guiar su implementación.	3	0	0	0	0	3	5,00
Total Promedio de Coherencia y Correspondencia							4,90

Fuente: Elaboración Propia

De acuerdo con los datos arrojados en la lista de chequeo, la concordancia del modelo de gestión de riesgos para la SI basado en la norma ISO/IEC 27001:2013 de acuerdo a la teoría (IT1), el contenido de la norma en sí (IT2), los lineamientos que soportan su diseño (IT3), sus fases (IT4), secuencia lógica

de los procesos (IT5), claridad de graficado (IT6), claridad de explicación (IT7), presenta una calificación cualitativa como *Muy Buena*.

Se puede decir, que el modelo presenta una ***Muy Buena*** concordancia; considerándose procedente su implementación y puesta en marcha en la empresa en estudio.

Objetivo 4: Implementación del modelo de gestión de riesgos propuesto.

Por otra parte, con el propósito de cumplir con el plan trazado para reducir y evitar los riesgos en la seguridad informática en Inversiones Fortunia, se definió un plan de implementación del modelo propuesto, el cual se presenta en la tabla 17.

Tabla 17

Plan de implementación de un modelo de gestión de seguridad informática

N°	Acción	Propósito	Estrategia	Recursos	Responsable	Fecha/Duración	Avance acumulado
1	Sensibilización de los actores acerca de la Seguridad Informática.	Dar a conocer a todos los funcionarios que laboran en la empresa la importancia de la Seguridad Informática para evitar los riesgos a los que están expuestos los activos informáticos del casino.	- Charla	- Proyector - Presentación multimedia - Salón de reunión	- Investigador y responsable del DSI - Gerencia	04 de enero al 26 febrero 2021	11,1%
2	Diagnóstico del Contexto organizacional con respecto a la seguridad informática.	Conocer la razón social y función básica de gestión operativa y administrativa de Inversiones Fortunia, con el fin de conocer su relación con los activos que posee como base de apoyo a sus actividades y los riesgos a los que están expuestos.	- Entrevistas - Revisión de gestión operativa de periodos anteriores	- Grabadora - Lápiz y papel para apuntes	- Investigador y responsable del DSI	20 de febrero al 05 marzo 2021	22,2%
3	Analizar los riesgos.	Conocer los riesgos y las causas que podrían generar una situación crítica para los activos, ante las amenazas y vulnerabilidades.	- Identificación y Valoración de los activos - Identificación y Valoración de las amenazas - Identificación y Valoración de las vulnerabilidades	- Lápiz y papel para apuntes - Office Excel	- Investigador y responsable del DSI	06 al 12 marzo 2021	33,3%

Tabla 17
(Cont.).

N°	Acción	Propósito	Estrategia	Recursos	Responsable	Fecha/Duración	Avance acumulado
4	Evaluar los riesgos.	Estimar de forma cuantitativa los riesgos, indicando las medidas para su posterior tratamiento.	<ul style="list-style-type: none"> - Estimación del impacto de amenazas y vulnerabilidades en activos - Estimación del riesgo en activos 	<ul style="list-style-type: none"> - Lápiz y papel para apuntes - Office Excel 	- Investigador y responsable del DSI	13 al 15 de marzo 2021	44,4%
5	Tratamiento del riesgo.	Determina la acción para tratar el riesgo en función de evitar, reducir, transferir y aceptar los riesgos.	Diseño del plan de implementación de políticas de seguridad.	<ul style="list-style-type: none"> - Lápiz y papel para apuntes - Office Excel - Cartelera 	- Investigador y responsable del DSI	16 al 22 de marzo 2021	66,6%
6			Comunicar la política seguridad	<ul style="list-style-type: none"> - Intranet - Correos 	- Gerencia	23 al 24 de marzo 2021	77,7%
7			Ejecución del plan de implementación de políticas de seguridad			Mayo de 2021	88,8%
8	Control y seguimiento.	Medir la efectividad del cumplimiento de políticas de seguridad.	Aplicar indicadores de gestión	<ul style="list-style-type: none"> - Lápiz y papel para apuntes - Office Excel 	- Investigador y responsable del DSI	Mayo del 2021	100%
Elaborado por:			Revisado por:		Aprobado por:		
Firma:			Firma:		Firma:		
			Revisado por:				
			Firma:				

Una vez conocida las pautas a seguir para ejecutar el modelo propuesto para la gestión de riesgos en Inversiones Fortunia (tabla 17), se procedió a consolidar el cuarto objetivo de esta investigación, dirigido a implementar el modelo de gestión de riesgos propuesto para la SI, de acuerdo al plan propuesto en la tabla 17, que conlleva a la aplicación general del mismo, siguiendo metódicamente lo indicado en la figura 3, y obviando la fase 1, inherente al *diagnóstico contextual*, cuyos resultados ya están expuestos en el primer objetivo orientado al diagnóstico de la situación actual en esta investigación, así como el segundo objetivo, donde se diseña el modelo; tal como se anticipó previamente al iniciar el aporte práctico, el objetivo 4 se desarrolla en paralelo con los 3 objetivos iniciales ya que forman parte de la implementación propiamente dicha.

Tal como se observa en la tabla 17, que forma parte del desarrollo documental del modelo propuesto, hasta ahora va ejecutado un 77,7% de implementación del modelo, considerando que ya se realizó la charla virtual de sensibilización al comienzo del estudio, se concretó la política general y se comunicó vía intranet y correos, posteriormente se llevó a cabo el análisis y evaluación de riesgos, comenzándose ya para este periodo de avance de la investigación que ha sido progresivo, a la fase del tratamiento y aplicación de controles, por el cual se ha llegado solo a la fase de comunicación de la política. Se espera que las operaciones de la empresa en estudio se normalicen el presente año para concluir con la difusión de las políticas detalladas en el manual, ya sea en exposición presencial o virtual.

Dentro de la implementación se tiene la parte ejecutoria del *análisis de riesgos*, que ya se tiene descrito en el apartado **3.1 Resultados en tablas y figuras, objetivo 4, tabla 5 (hoja 46)**.

En resumen:

- Identificar los activos del casino
- Codificarlos y valorarlos, según su nivel de Disponibilidad (D), Integridad (I) y Confiabilidad (C) y los criterios expuestos en las tablas 11, 12 y 13, donde A es igual a nivel "Alto", M a nivel "Moderado" y B a nivel "Bajo".

Los resultados se registran tal como se presenta, a continuación, en la tabla 21 donde solo mostramos los activos con un alto valor, cuya resultante está vinculada a la tabla 5 expuesta en la sección de resultados en tablas y figuras.

Tabla 21

Cantidad de activos críticos y de alto valor en la seguridad informática de la empresa en estudio

Tipo de activo	Nivel	Cantidad	Porcentaje
Instalaciones (L)	Alto	1	0.3%
Personal (P)	Alto	2	1%
Equipos informáticos (HW)	Alto	312	95%
Software y aplicaciones (SW)	Alto	6	2%
Servicios (S)	Alto	4	1%
Redes de comunicaciones (COM)	Alto	2	1%
Total		327	100%

Fuente: Elaboración Propia

De acuerdo a la tabla 5, son 327 los activos con nivel Alto de valoración, dentro de conjunto total de 679 activos de SI que posee la empresa en estudio, resaltándose entre todo el conjunto, que el 95% de los activos con nivel alto de tasación corresponde al tipo de activo equipos informáticos, le sigue en forma consecutiva software y aplicaciones, servicios, redes de comunicaciones, personal y las instalaciones, respectivamente.

Esto quiere decir, que estos son los activos más importantes dentro los procesos atribuibles a la tecnología de la información, donde por supuesto, son básicos para el desarrollo de los procesos informáticos todos los equipos de computación, como desktops y laptops, los software que intervienen en los procesos administrativos y operativos del casino, así como los sistemas operativos, navegadores, los medios de interconexión de la red, como cables de par trenzado y señal wifi, el soporte técnico, el servicio de internet, el personal de soporte técnico y la instalación donde se encuentran los servidores que en este caso es el Departamento de Sistemas (DSI).

Es por ello, que en la actividad de identificar a amenazas y vulnerabilidades expuesta en el modelo propuesto, se buscó conocer estos dos factores

característicos de la situación actual de la gestión de SI del casino, para luego evaluarlos, los cuales se pudieron establecer en la tabla 9 ya expuesta en el modelo documental, en consonancia con los criterios ya conocidos en la lista de elementos de las tablas 14, 15 y 16 que expone MAGERIT, y de allí surgieran las medidas razonables para abordar los riesgos de los activos críticos que aparecen en la tabla 22.

Tabla 22

Activos destacados por su alta (A) valoración de amenazas, vulnerabilidades, impacto y nivel de riesgos

Código	Activo	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Nivel de riesgos	Medidas de acción ante el riesgo
P2	Trabajadores del DSI	Alta	Alto	Mayor	Implementar políticas de motivación al RRHH. Incrementar el grupo de trabajo en la DSI. Reforzar políticas de seguridad industrial.
L6	Departamento de Sistemas (DSI)	Alta	Alto	Mayor	Dotar de sistemas contra incendios todas las áreas del casino. Dotar de aires acondicionados más eficiente el área. Adoptar políticas de seguridad y control para la entrada y salida de recursos.
HW77- HW78	Server	Alta	Alto	Mayor	Dotar de aires acondicionados más eficiente el área. Repotenciar los recursos de los servers. Mejorar y hacer cumplir las políticas de control de mantenimiento de los equipos a nivel hardware y software. Actualizar los programas periódicamente. Referir políticas de control de cambios y manipulación de equipos informáticos. Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada.
SW5	Navegador	Alta	Alto	Mayor	Actualizar los programas

	web: Google Chrome				periódicamente.
SW7	Antivirus: ESET End Point Protection Standard	Alta	Alto	Mayor	Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada. Actualizar los programas periódicamente.
SW10	Asistencia Remota: AnyDesk	Alta	Alto	Mayor	Referir políticas de control de cambios de información. Mantener licencia de software de protección o antivirus actualizada. Actualizar los programas periódicamente.

Fuente: Elaboración Propia

Las medidas planteadas anteriormente, responden a los hallazgos que se especificaron en la tabla 6 expuesta en la sección 3.1. de tablas y figuras, inherente al mapa de evaluación de riesgos de los 679 activos de la empresa que tienen un nivel *mayor* de riesgo, lo cual fue vital para considerar en las políticas de control en la fase de tratamiento de la seguridad informática, estudiada en esta investigación.

IV. CONCLUSIONES Y RECOMENDACIONES

Conclusiones

El trabajo de investigación llevado a cabo, permitió en su diagnóstico dilucidar que actualmente la empresa en estudio carece de medidas de control para garantizar la seguridad informática, aun cuando posee 679 activos por proteger, y en función de ello, no se ha concretado una cultura organizacional al respecto, mucho menos, políticas, procesos y procedimientos documentados para protección de sus equipos y sistemas informáticos.

Se diseñó el modelo propuesto para la gestión de riesgos en la seguridad informática, sustentado en la norma ISO/EIC 27001:2013, la metodología MAGERIT y el modelo DEMING.

El nivel de coherencia y correspondencia validado en el modelo de gestión de riesgos propuesto con respecto a la norma ISO/IEC 27001:2013, obtuvo una firme tendencia al cumplimiento de esta, al arrojar en su evaluación de apreciación por los expertos un apego *Muy Bueno*.

En la implementación progresiva se demostró una eficacia del 80% en la gestión de disminución de incidentes presentes en el entorno tecnológico de la empresa en estudio, y por lo tanto en esa misma proporción es su mejora, certificándose así la hipótesis alterna de la investigación.

Recomendaciones

A la Gerencia General, ante los hallazgos encontrados en el contexto diagnóstico de la empresa, se sugiere integrar dentro de sus procesos operativos y administrativos, el análisis y gestión de riesgos informáticos para aumentar los niveles de seguridad informática, y bajar el índice de incidentes que afectan a los activos informáticos de mayor relevancia, y con ello mejore secuencialmente los índices de eficacia de la gestión mensual del DSI.

Al Departamento de Sistemas (DSI), aunque el modelo de gestión diseñado contempla un método de análisis de riesgos en base a una plantilla que registra los tipos de riesgos existentes, se sugiere que impulsen la creación de un sistema de incidencias que recoja las notificaciones continuas por parte de los usuarios y que permita identificar las nuevas amenazas y vulnerabilidades que se presenten.

Al Departamento de Sistemas (DSI), considerando el plan de implementación del modelo de gestión de riesgos para la SI en ejecución, se sugiere la revisión periódica de las amenazas, y riesgos detectados, considerando los diferentes factores que afectan su incidencia, tales como cambios tecnológicos, implementación de nuevos proyectos, entre otros; a fin de establecer un control perenne.

REFERENCIAS

- Agencia Española de Protección de Datos. (2018). *Guía Práctica de Análisis de Riesgos en los Tratamientos de Datos Personales Sujetos al RGPD*.
Obtenido de <https://www.aepd.es/media/guias/guia-analisis-de-riesgos-rgpd.pdf>
- Aguilera, P. (2011). *Redes seguras (Seguridad informática)*. España - Madrid: Editex.
- Alexander, A. G. (2007). *Diseño de un sistema de seguridad de información*. Colombia: Alfa omega Colombiana S.A.
- Alvarado Meza, E. F. (07 de 06 de 2016). *Propuesta para la implementación de un sistema de gestión de seguridad de la información aplicando la normal ISO 27001 para industrial ALES (Tesis de Grado)*. Obtenido de Repositorio de la Universidad de Guayaquil:
<http://repositorio.ug.edu.ec/bitstream/redug/19804/1/INFORME%20ERICK%20ALVARADO%20TESI.pdf>
- Alvarado, J. P. (2018). *El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT*. Obtenido de Revista Contribuciones a las Ciencias Sociales: <https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html>
- Alvarado, J., Pacheco, J., & Martillo, I. (2018). *El análisis y gestión de riesgos en gobiernos de ti desde el enfoque de la metodología MAGERIT*. Obtenido de Revista Contribuciones a las Ciencias Sociales:
<https://www.eumed.net/rev/cccss/2018/11/gestion-riesgos-magerit.html>
- Arévalo, F., Cedillo, I., & Moscoso, S. (2017). *Agile Methodology for Computer Risk Management*. Obtenido de Revista Killkana Técnica: DOI: 10.26871/killkana_tecnica.v1i2.81.
https://www.researchgate.net/publication/321176840_Metodologia_Agil_para_la_Gestion_de_Riesgos_Informaticos
- Arias, F. (2012). *El Proyecto de la Investigación: Introducción a la Investigación Científica*. Caracas - Venezuela: Epísteme.
- Berrios, C., & Rocha, M. (2015). *Propuesta de un Modelo de Sistema de Gestión*

- de la Seguridad de la Información en una Pyme basado en la Norma ISO/IEC 27001*. Obtenido de https://repositorioacademico.upc.edu.pe/bitstream/handle/10757/581891/berrios_mc-rocha_cm.pdf?sequence=1&isAllowed=y
- Bocanegra, Y. (2015). *Análisis y gestión de riesgos de los sistemas de información de la Alcaldía Municipal De Tuluá aplicando la metodología MAGERIT*. Obtenido de <https://repository.unad.edu.co/handle/10596/3632>
- Cabrera, H. (2018). *Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida*. Obtenido de <https://repositorio.upeu.edu.pe/handle/UPEU/1542>
- Carrión, G., Sánchez, M., Del Castillo, C., Campos, F., & Timaná, M. (2021). Modelo de seguridad informática para un medio de conexión pública. *Revista de la Universidad del Zulia*(32), 344-357. doi:<https://doi.org/10.46925//rdluz.32.21>
- Cisco. (2018). *Cómo fortifica el mercado de empresas medianas y pequeñas sus defensas contra las amenazas actuales*. Obtenido de *Informe Especial de Ciberseguridad* . Recuperado el 18 de Abril de 2020, de https://www.cisco.com/c/dam/global/es_mx/products/pdfs/cisco-2018-smb-report-spa.pdf
- Congreso de la República del Perú. (2011). Ley de Protección de Datos Personales. *Ley N° 29733*. Lima, Perú: http://www.pcm.gob.pe/transparencia/Resol_ministeriales/2011/ley-29733.pdf.
- Cordeiro, M., Viñas, M., & Coria, M. (9 de Octubre de 2017). *Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinaria para su abordaje*. . Obtenido de <https://doi.org/10.24215/18539912e032>
- Cruz, M., & Fukusaki, S. (2017). *Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la Clínica MEDCAM Perú SAC*. Obtenido de <https://hdl.handle.net/20.500.12727/3369>
- Cuervo Alvarez, S. (2017). *Implementación ISO 27001*. Obtenido de <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/64827/8/scuervoT>

FM0617memoria.pdf

- Ferruzola, E., Duchimaza, J., & Ramos, J. &. (2019). Plan de contingencia para los equipos y sistemas informáticos utilizando la metodología MAGERIT. *Revista Científica Y Tecnológica UPSE*, 34-41.
- Figueroa, J., Rodríguez, R., Bone, C., & Saltos, J. (Diciembre de 2017). La seguridad informática y la seguridad de la información. . *Revista Científico-Académica Multidisciplinaria Polo del Conocimiento*, 2(14), 145-155.
doi:10.23857/pc.v2i12.420
- Fonseca-Herrera O.A., R. A. (2021). A Model of an Information Security Management System Based on NTC-ISO/IEC 27001 Standard. *IAENG International Journal of Computer Science*, 48, 1 - 10. Obtenido de <https://www.scopus.com/record/display.uri?eid=2-s2.0-85109172871&origin=resultslist&sort=plf-f&src=s&sid=1b801726882bd5e4994ee85ff8459189&sot=b&sdt=b&sl=41&s=TITLE-ABS-KEY%28management+risks+iso+27001%29&relpos=1&citeCnt=0&searchTerm=>
- García, J., Huamani, S., & Lomparte, R. (2018). Modelo de gestión de riesgos de seguridad de la información para PYMES peruanas. *Revista Peruana De Computación Y Sistemas*, 1(1), 47-56.
doi:<https://doi.org/10.15381/rpcs.v1i1.14856>
- Gonzales, D. (5 de Febrero de 2018). Design of a strategic plan for information security, through the application of risk analysis with ISO / IEC 27005. Case study INAMHI. *INNOVA Research Journal*, 3(2.1), 84-91.
doi:<https://doi.org/10.33890/innova.v3.n2.1.2018.672>.
- Granadino, V. (2019). *Conexion ESAN*. Obtenido de <https://www.esan.edu.pe/apuntes-empresariales/2019/02/el-plan-de-respuestas-a-los-riesgos-las-estrategias-y-acciones-clave/>
- Guevara, R., & Mayorga, F. (2017). *Sistema De Gestión de Seguridad de la Información basado en la Norma ISO/IEC 27001 para el departamento de Tecnologías de la Información Y Comunicación del Distrito 18D01 de educación, en Ambato, Ecuador*. Obtenido de <http://repositorio.uta.edu.ec/jspui/handle/123456789/26932>

- Hernandez, R., Fernandez, C., & Baptista, P. (24 de 05 de 2018). *Metodología de la Investigación*. Obtenido de https://www.esup.edu.pe/descargas/dep_investigacion/Metodologia%20de%20la%20investigaci%C3%B3n%205ta%20Edici%C3%B3n.pdf
- INDECOPI. (2008). Norma Técnica Peruana. *Adaptado en el año 2008*.
- INDECOPI. (2014). *Norma Técnica Peruana "NTP-ISO/ IEC 27001:2014. Tecnología de la Información. Técnicas de seguridad. Sistema de gestión de la seguridad de la información. Requisitos. Segunda edición. Lima, Perú.*
- Jaya Putra, S., Nur Gunawan , M., Falach Sobri , A., Muslimin , J. M., Amilin, & Saepudin , D. (23 de 10 de 2020). Information Security Risk Management Analysis Using ISO 27005: 2011 for the Telecommunication Company. *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*, 9268845. doi:10.1109/CITSM50537.2020.9268845
- Justino, Z. (2015). *Diseño de un sistema de gestión de seguridad de información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013*. Obtenido de <http://hdl.handle.net/20.500.12404/6045>
- Leiva, R. (2016). *Diseño de un Sistema de Gestión de Seguridad de la Información basado en las Normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la Red de Salud de Lambayeque 2015*. Obtenido de https://1library.co/document/qo52650y-diseno-gestion-seguridad-informacion-informacion-suministros-medicamentos-lambayeque.html?utm_source=related_list
- López, M. (2018). Análisis de riesgos en un sistema de gestión de seguridad de la información (SGSI) con las metodologías complementarias. *Revista Especializada en Ingeniería (UNAD)*, <http://polux.unipiloto.edu.co:8080/00004422.pdf>.
- M., A. C., Huallpa Laguna , J. N., Huillcen Baca , H. A., Carpio Vargas, E. E., & Palomino Valdivia , F. L. (2021). Implementation of an Information Security Management System Based on the ISO/IEC 27001: 2013 Standard for the Information Technology Division. *Advances in Intelligent Systems and Computing*, 1302, 264 - 272. doi:10.1007/978-3-030-63665-4_21
- Magerit. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de*

- Información*. Obtenido de <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>
- MAGERIT. (18 de 09 de 2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información*. Obtenido de <https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html>
- Marchand, W. (2016). *Modelo de un Sistema de Gestión de Seguridad de la Información. Caso: Universidad Nacional Agraria de la Selva*. Obtenido de Revista Tecnológica - ESPOL:
https://www.researchgate.net/publication/318224190_Modelo_de_un_Sistema_de_Gestion_de_Seguridad_de_Informacion_Caso_Universidad_Nacional_Agraria_de_la_Selva
- Mesa, E. (2016). *Propuesta para la Implementación de un Sistema de Gestión de Seguridad de la Información aplicando la norma ISO 27001 para Industrias Ales. Guayaquil – Ecuador*. Obtenido de <http://repositorio.ug.edu.ec/handle/redug/19804>
- Miranda, M., Valdés, O., Pérez, I., Portelles, R., & Sánchez, R. (2016). Metodología para la Implementación de la Gestión Automatizada de Controles de Seguridad Informática. *Revista Cubana de Ciencias Informáticas*(10), 14-26. Obtenido de https://www.researchgate.net/publication/317514696_Metodologia_para_la_Implementacion_de_la_Gestion_Automatizada_de_Controles_de_Seguridad_Informatica
- Mirtsch, M., Blind, k., Koch, C., & Dudek, G. (29 de Octubre de 2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Elsevier*, 109(102383).
doi:<https://doi.org/10.1016/j.cose.2021.102383>
- Monsalve, J., Aponte-Novoa, F., & Chaves, D. (2014). *Information Vulnerabilities' Study and Management, for a Private Enterprise in the Boyacá Colombian Department*. Obtenido de Revista Facultad de Ingeniería:
<https://doi.org/10.19053/01211129.2791>. En línea:
<https://revistas.uptc.edu.co/index.php/ingenieria/article/view/2791/4356>
- Morales, E., & López, M. (18 de Setiembre de 2018). Sistemas de gestión de seguridad de la información para empresas KPO: una aproximación.

- Ventana informática*(37).
doi:<https://doi.org/10.30554/ventanainform.37.2723.2017>
- Norena, A., Alcaraz, N., Rojas, J., & Rebolledo, D. . (2012). Aplicabilidad de los criterios de rigor y éticos en la investigación cualitativa. *Aquichan [online]*, vol.12, n.3, pp.263-274.
- Novoa, H., & Rodríguez, C. (2014). *Methodologies for AnAlysis of risks in the isMs*. Obtenido de Revista Especializada en Ingeniería UNAD: DOI: 10.22490/25394088.1435.
https://www.researchgate.net/publication/317149870_Metodologias_para_e_l_analisis_de_riesgos_en_los_sgsi
- Oliván, A. (2017). *Guía de Controles de Ciberseguridad para la Proteccion Integral de la Pyme*. Obtenido de <http://openaccess.uoc.edu/webapps/o2/bitstream/10609/73066/6/aolivan1TFM0118memoria.pdf>
- Rodríguez, L., Cruzado, C., Mejía, C., & Diaz, A. (09 de 2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. Lima. *Propósitos y Representaciones USIL*, 8(3).
doi:<http://dx.doi.org/10.20511/pyr2020.v8n3.786>.
- Solarte, F., Enriquez, E., & Benavides, M. (2015). *Methodology of analysis and risk assessment applied to computer security and information under the ISO / IEC 27001*. Obtenido de Revista Tecnológica - ESPOL:
<https://doi.org/10.37815/rte>. Disponible en:
<http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456>
- Tariq, M., Ahmed , S., Memon , N., Tayyaba , S., Ashraf , M., Nazir , M., . . . Balas , M. (03 de 2020). Prioritization of information security controls through fuzzy AHP for cloud computing networks and wireless sensor networks. *Sensors (Switzerland)*, 20(1310). doi:10.3390/s20051310
- Zeña, V. (2015). *Estándar Internacional ISO 27001 para la gestión de seguridad de la información en la oficina central de informática de la UNPRG* . Obtenido de <http://190.108.84.117/bitstream/handle/UNPRG/166/BC-TES-3899.pdf?sequence=1&isAllowed=y>

ANEXOS

Anexo 1. Resolución de aprobación del proyecto de investigación



FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

RESOLUCIÓN N°0200-2021/FIAU-USS

Pimentel, 24 de marzo de 2021

VISTO:

El Acta de reunión N°2203-2021 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida mediante Oficio N°0087-2021/FIAU-IS-USS de fecha 23 de marzo de 2021, y;

CONSIDERANDO:

Que, de conformidad con la Ley Universitaria N° 30220 en su artículo 48° que a letra dice: "La investigación constituye una función esencial y obligatoria de la universidad, que la fomenta y realiza, respondiendo a través de la producción de conocimiento y desarrollo de tecnologías a las necesidades de la sociedad, con especial énfasis en la realidad nacional. Los docentes, estudiantes y graduados participan en la actividad investigadora en su propia institución o en redes de investigación nacional o internacional, creadas por las instituciones universitarias públicas o privadas.";

Que, de conformidad con el Reglamento de grados y títulos en su artículo 21° señala: "Los temas de trabajo de investigación, trabajo académico y tesis son aprobados por el Comité de Investigación y derivados a la Facultad o Escuela de Posgrado, según corresponda, para la emisión de la resolución respectiva. El periodo de vigencia de los mismos será de dos años, a partir de su aprobación. En caso un tema perdiera vigencia, el Comité de Investigación evaluará la ampliación de la misma.

Que, de conformidad con el Reglamento de grados y títulos en su artículo 24° señala: La tesis es un estudio que debe denotar rigurosidad metodológica, originalidad, relevancia social, utilidad teórica y/o práctica en el ámbito de la escuela profesional. Para el grado de doctor se requiere una tesis de máxima rigurosidad académica y de carácter original. Es individual para la obtención de un grado; es individual o en pares para obtener un título profesional. Asimismo, en su artículo 25° señala: "El tema debe responder a alguna de las líneas de investigación institucionales de la USS S.A.C."

Que, según documentos de Vistos el Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS acuerdan aprobar los temas de las Tesis a cargo de los egresados que se detallan en el anexo de la presente Resolución.

Estando a lo expuesto, y en uso de las atribuciones conferidas y de conformidad con las normas y reglamentos vigentes;

SE RESUELVE:

ARTÍCULO 1°: APROBAR, el tema de la Tesis perteneciente a la línea de investigación de INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE, a cargo de los egresados del Programa de estudios de INGENIERÍA DE SISTEMAS según se detalla en el anexo de la presente Resolución.

ARTÍCULO 2°: ESTABLECER, que la inscripción del Tema de la Tesis se realice a partir de emitida la presente resolución y tendrá una vigencia de dos (02) años.

ARTÍCULO 3°: DEJAR SIN EFECTO, toda Resolución emitida por la Facultad que se oponga a la presente Resolución.

REGÍSTRESE, COMUNÍQUESE Y ARCHÍVESE



Dr. Néstor Fernando Ramos Moscoso
Decano - Facultad de Ingeniería,
Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.



MBA. María Mercedes Siles Rivera
Secretaria Académica / Facultad de Ingeniería,
Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

Cc: Interesado, Archivo

ANEXO

N°	PROGRAMA DE ESTUDIOS	APELLIDOS Y NOMBRES	TEMA DE TESIS
1	INGENIERÍA DE SISTEMAS	VILLON GUERRERO PABLO LEONARDO	MODELO DE GESTION DE RIESGOS PARA SEGURIDAD INFORMATICA BAJO ISO/IEC 27001:2013 EN EMPRESA DE ENTRETENIMIENTO Y JUEGOS DE AZAR, LIMA-2021
2	INGENIERÍA DE SISTEMAS	BURGOS VARGAS DANTE ATILANO	RECONOCIMIENTO DE PLAGAS EN CULTIVOS UTILIZANDO ALGORITMOS DE APRENDIZAJE NO SUPERVISADO: UNA REVISIÓN DE LA LITERATURA

Anexo 2. Carta de aceptación de la institución para la recolección de datos.



Anexo 3.5. Matriz de registro y observación - Inventario de infraestructura y comunicaciones

	
DEPARTAMENTO DE SISTEMAS	
ID Infraestructura	Infraestructura de redes y comunicaciones

Anexo 3.6 Formatos de plantillas de análisis y evaluación - Formato de valoración de activos (VA) en cuanto a Disponibilidad (D), Integridad (I) y Confiabilidad (C)

Tipo activo	Código	Nombre	Cantidad	D	I	C	Valor	Nivel VA
Personas (P)								
Personas (P)								
Instalaciones (L)								
Instalaciones (L)								
Instalaciones (L)								
Equipos Informáticos (HW)								
Equipos Informáticos (HW)								
Equipos Informáticos (HW)								
Equipos Informáticos (HW)								
Software y aplicaciones								
Software y aplicaciones								
Software y aplicaciones								
Software y aplicaciones								
Software y aplicaciones								
Servicios (S)								
Servicios (S)								
Servicios (S)								
Servicios (S)								
Servicios (S)								
Servicios (S)								
Redes de comunicaciones (COM)								
Redes de comunicaciones (COM)								

Anexo 3.7 Formatos de plantillas de análisis y evaluación - Formato de valoración de amenazas y vulnerabilidades en activos para determinar el NIVEL DE RIESGO

Código	Activo	Amenaza	Vulnerabilidad	Valor Amenaza	Valor Vulnerabilidad	Posibilidad de ocurrencia de la amenaza	Valor del activo en riesgo ante vulnerabilidad	Total riesgo	Nivel del riesgo	Acción
P1										
P2										
P3										
P4										
L1										
L2										
L3										
L4										
HW1										
HW2										
HW3										
HW4										
SW1										
SW2										
SW3										
S1										
S3										
S4										
COM1										
COM2										
COM3										
COM4										

Anexo 4. Formato check list para el juicio de expertos del modelo.



FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Lista de chequeo para validar el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de las normas ISO/IEC 27001:2013

Dirigido a:

Expertos en SI

Esta check list a continuación tiene la finalidad de medir el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de las normas ISO/IEC 27001:2013, a quienes se les presenta en las páginas que siguen, bajo una entrevista compuesta de siete (07) preguntas que permitirán obtener información para analizar el cumplimiento de los lineamientos del método, con el fin de que, este análisis sirva como insumo para la sugerencia de mejoras de los ítems en estudio, de tal manera que el entorno productivo sea satisfactorio y conlleve a resultados positivos tanto para la investigación como para el investigador.

Sus respuestas individuales son absolutamente confidenciales y sólo serán utilizadas como insumo para el trabajo de Informe de Investigación.

Instrucciones para la lista de chequeo:

1. Conteste colocando en la sección de preguntas una equis (X) en la descripción que más se aproxime a **su opinión y percepción sobre lo que se indaga**. Las descripciones que se encuentran para escoger son las siguientes:
 - Totalmente de acuerdo (TA)
 - De acuerdo (DA)
 - Neutral (N)
 - En desacuerdo (ED)
 - Totalmente en desacuerdo (TD)
2. Conteste todas las preguntas en orden después de analizar cada elemento, de forma objetiva, es decir contestando lo que observa realmente. No hay respuestas correctas o incorrectas.
3. Se garantiza total confidencialidad de la información proporcionada individualmente.
4. Los resultados se analizarán posteriormente en forma global con el fin de planificar acciones futuras tendientes a mejorar las variables asociadas con el estudio.
5. Use lápiz para que pueda borrar totalmente cualquier respuesta que desee cambiar.

Lista de chequeo:

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
1. Se establece un modelo de gestión de riesgos basado en las normas ISO/IEC 27001:2013 de acuerdo con la teoría expuesta.						<u>RONDA 1:</u> <u>RONDA 2:</u>
2. Se establece un modelo de gestión de riesgos basado en las normas ISO/IEC 27001:2013 de acuerdo con lo señalado en la Norma.						<u>RONDA 1:</u> <u>RONDA 2:</u>
3. El modelo gestión de riesgos basado en las normas ISO/IEC 27001:2013 cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.						<u>RONDA 1:</u> <u>RONDA 2:</u>
4. El modelo gestión de riesgos propuesto cumple con las fases de las normas ISO/IEC 27001:2013.						<u>RONDA 1:</u> <u>RONDA 2:</u>
5. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 sigue una secuencia lógica de los procesos que lo integran.						<u>RONDA 1:</u> <u>RONDA 2:</u>
6. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente graficado.						<u>RONDA 1:</u> <u>RONDA 2:</u>
7. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente explicado de manera que pueda guiar su implementación.						<u>RONDA 1:</u> <u>RONDA 2:</u>

Escala utilizada para el análisis de la lista de chequeo

Alternativas	Criterio Cuanti-cualitativo de Evaluación para calificación	Calificación	
		Cuantitativa	Cualitativa

Totalmente de acuerdo (TA)	Muy Bueno (de 4,1 puntos a 5 puntos)		
De acuerdo (DA)	Bueno (de 3,1 puntos a 4 puntos)		
Neutral (N)	Aceptable (de 2,1 puntos a 3 puntos)		
En desacuerdo (ED)	Requiere Atención (de 1,1 puntos a 2 puntos)		
Totalmente en desacuerdo (TD)	Crítico (de 0,1 puntos a 1 puntos)		

Anexo 4.1. Constancias de Juicio de Experto

CONSTANCIA DE JUICIO DE EXPERTO

Nombre del Experto: _____

Especialidad: _____

C.I.: _____

Por medio de la presente hago constar que realicé la revisión del modelo de gestión de riesgos en SI propuesto para la empresa Inversiones Fortunia, elaborado por Pablo Leonardo Villon Guerrero – Bachiller de Ingeniería de Sistemas de la Universidad “Señor de Sipán”, quien está realizando su tesis: **“MODELO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD INFORMÁTICA BAJO ISO/IEC 27001:2013 EN EMPRESA DE ENTRETENIMIENTO Y JUEGOS DE AZAR, LIMA - 2021”**.

Una vez indicadas las observaciones pertinentes, discutidas y aclaradas considero que dicho modelo es **VÁLIDO** para su aplicación e implementación.

Chiclayo, _____ días de _____ de _____.

FIRMA DIGITALIZADA

Nombre y Apellido _____

DNI: _____

Anexo 5. Validaciones de expertos al modelo – JOISY ROJAS



FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Lista de chequeo para validar el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de las normas ISO/IEC 27001:2013

Indicaciones:

Esta checklist a continuación tiene la finalidad de medir el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de las normas ISO/IEC 27001:2013, a quienes se les presenta en las páginas que siguen, bajo una entrevista compuesta de siete (07) preguntas que permitirán obtener información para analizar el cumplimiento de los lineamientos del método, con el fin de que, este análisis sirva como insumo para la sugerencia de mejoras de los ítems en estudio, de tal manera que el entorno productivo sea satisfactorio y conlleve a resultados positivos tanto para la investigación como para el investigador.

Sus respuestas individuales son absolutamente confidenciales y sólo serán utilizadas como insumo para el trabajo de Informe de Investigación.

Instrucciones para la lista de chequeo:

1. Conteste colocando en la sección de preguntas una equis (X) en la descripción que más se aproxime a **su opinión y percepción sobre lo que se indaga**. Las descripciones que se encuentran para escoger son las siguientes:
 - Totalmente de acuerdo (TA)
 - De acuerdo (DA)
 - Neutral (N)
 - En desacuerdo (ED)
 - Totalmente en desacuerdo (TD)
2. Conteste todas las preguntas en orden después de analizar cada elemento, de forma objetiva, es decir contestando lo que observa realmente. No hay respuestas correctas o incorrectas.
3. Se garantiza total confidencialidad de la información proporcionada individualmente.
4. Los resultados se analizarán posteriormente en forma global con el fin de planificar acciones futuras tendientes a mejorar las variables asociadas con el estudio.
5. Use lápiz para que pueda borrar totalmente cualquier respuesta que desee cambiar.

Lista de chequeo:

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
1. Se establece un modelo de gestión de riesgos basado en las normas ISO/IEC 27001:2013 de acuerdo con la teoría expuesta.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
2. Se establece un modelo de gestión de riesgos basado en las normas ISO/IEC 27001:2013 de acuerdo con lo señalado en la Norma.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
3. El modelo gestión de riesgos basado en las normas ISO/IEC 27001:2013 cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
4. El modelo gestión de riesgos propuesto cumple con las fases de las normas ISO/IEC 27001:2013.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
5. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 sigue una secuencia lógica de los procesos que lo integran.		X				<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
6. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente graficado.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
7. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente explicado de manera que pueda guiar su implementación.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>

Escala utilizada para el análisis de la lista de chequeo

Alternativas	Criterio Cuanti-cualitativo de	Calificación
--------------	--------------------------------	--------------

	Evaluación para calificación	Cuantitativa	Cualitativa
Totalmente de acuerdo (TA)	Muy Bueno (de 4,1 puntos a 5 puntos)	34/7 = 4.85	Muy Bueno
De acuerdo (DA)	Bueno (de 3,1 puntos a 4 puntos)		
Neutral (N)	Aceptable (de 2,1 puntos a 3 puntos)		
En desacuerdo (ED)	Requiere Atención (de 1,1 puntos a 2 puntos)		
Totalmente en desacuerdo (TD)	Crítico (de 0,1 puntos a 1 puntos)		

CONSTANCIA DE JUICIO DE EXPERTO

Nombre del Experto: Mg. Joisy Rojas

Especialidad: Ingeniería de sistemas

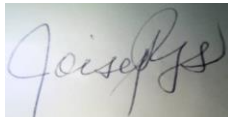
Cédula de Identidad Venezolana: V. 11.511.314

Por medio de la presente hago constar que realicé la revisión del modelo de gestión de riesgos en SI propuesto para la empresa Inversiones Fortunia, elaborado por Pablo Leonardo Villon Guerrero – Bachiller de Ingeniería de Sistemas de la Universidad “Señor de Sipán”, quien está realizando su tesis: **“MODELO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD INFORMÁTICA BAJO ISO/IEC 27001:2013 EN EMPRESA DE ENTRETENIMIENTO Y JUEGOS DE AZAR, LIMA - 2021”**.

Una vez indicadas las observaciones pertinentes, discutidas y aclaradas considero que dicho modelo es **VÁLIDO** para su aplicación e implementación.

Lima, 05 días de mayo del 2021.

FIRMA DIGITALIZADA



Mg. Joisy Rojas
CI: 11.511.314

Anexo 6. Validaciones de expertos al modelo – MARLO CARRANZA



FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Lista de chequeo para validar el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de las normas ISO/IEC 27001:2013

Indicaciones:

Esta check list a continuación tiene la finalidad de medir el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de las normas ISO/IEC 27001:2013, a quienes se les presenta en las páginas que siguen, bajo una entrevista compuesta de siete (07) preguntas que permitirán obtener información para analizar el cumplimiento de los lineamientos del método, con el fin de que, este análisis sirva como insumo para la sugerencia de mejoras de los ítems en estudio, de tal manera que el entorno productivo sea satisfactorio y conlleve a resultados positivos tanto para la investigación como para el investigador.

Sus respuestas individuales son absolutamente confidenciales y sólo serán utilizadas como insumo para el trabajo de Informe de Investigación.

Instrucciones para la lista de chequeo:

1. Conteste colocando en la sección de preguntas una equis (X) en la descripción que más se aproxime a **su opinión y percepción sobre lo que se indaga**. Las descripciones que se encuentran para escoger son las siguientes:
 - Totalmente de acuerdo (TA)
 - De acuerdo (DA)
 - Neutral (N)
 - En desacuerdo (ED)
 - Totalmente en desacuerdo (TD)
2. Conteste todas las preguntas en orden después de analizar cada elemento, de forma objetiva, es decir contestando lo que observa realmente. No hay respuestas correctas o incorrectas.
3. Se garantiza total confidencialidad de la información proporcionada individualmente.
4. Los resultados se analizarán posteriormente en forma global con el fin de planificar acciones futuras tendientes a mejorar las variables asociadas con el estudio.
5. Use lápiz para que pueda borrar totalmente cualquier respuesta que desee

cambiar.

Lista de chequeo:

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
1. Se establece un modelo de gestión de riesgos basado en las normas ISO/IEC 27001:2013 de acuerdo con la teoría expuesta.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
2. Se establece un modelo de gestión de riesgos basado en las normas ISO/IEC 27001:2013 de acuerdo con lo señalado en la Norma.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
3. El modelo gestión de riesgos basado en las normas ISO/IEC 27001:2013 cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
4. El modelo gestión de riesgos propuesto cumple con las fases de las normas ISO/IEC 27001:2013.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
5. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 sigue una secuencia lógica de los procesos que lo integran.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
6. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente graficado.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
7. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente explicado de manera que pueda guiar su implementación.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>

Escala utilizada para el análisis de la lista de chequeo

Alternativas	Criterio Cuanti-cualitativo de	Calificación
--------------	--------------------------------	--------------

	Evaluación para calificación	Cuantitativa	Cualitativa
Totalmente de acuerdo (TDA)	Muy Bueno (de 4,1 puntos a 5 puntos)	35/7 =	MUY BUENO
De acuerdo (DA)	Bueno (de 3,1 puntos a 4 puntos)	5.00	
Neutral (N)	Aceptable (de 2,1 puntos a 3 puntos)		
En desacuerdo (ED)	Requiere Atención (de 1,1 puntos a 2 puntos)		
Totalmente en desacuerdo (TD)	Crítico (de 0,1 puntos a 1 puntos)		

CONSTANCIA DE JUICIO DE EXPERTO

Nombre del Experto: Ing. Marlo Carranza Gallardo

Especialidad: Ingeniería de Sistemas

DNI: 41996716

Por medio de la presente hago constar que realicé la revisión del modelo de gestión de riesgos en SI propuesto para la empresa Inversiones Fortunia, elaborado por Pablo Leonardo Villon Guerrero – Bachiller de Ingeniería de Sistemas de la Universidad “Señor de Sipán”, quien está realizando su tesis: **“MODELO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD INFORMÁTICA BAJO ISO/IEC 27001:2013 EN EMPRESA DE ENTRETENIMIENTO Y JUEGOS DE AZAR, LIMA - 2021”**.

Una vez indicadas las observaciones pertinentes, discutidas y aclaradas considero que dicho modelo es **VÁLIDO** para su aplicación e implementación.

Lima, 05 días de mayo del 2021.



Nombre y Apellido: Ing. Marlo Carranza Gallardo

DNI: 41996716

Anexo 7. Validaciones de expertos al modelo – CARLOS CHIRINOS



FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

Lista de chequeo para validar el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de las normas ISO/IEC 27001:2013

Indicaciones:

Esta check list a continuación tiene la finalidad de medir el nivel de coherencia y correspondencia del modelo de gestión de riesgos propuesto, en función del enfoque de las normas ISO/IEC 27001:2013, a quienes se les presenta en las páginas que siguen, bajo una entrevista compuesta de siete (07) preguntas que permitirán obtener información para analizar el cumplimiento de los lineamientos del método, con el fin de que, este análisis sirva como insumo para la sugerencia de mejoras de los ítems en estudio, de tal manera que el entorno productivo sea satisfactorio y conlleve a resultados positivos tanto para la investigación como para el investigador.

Sus respuestas individuales son absolutamente confidenciales y sólo serán utilizadas como insumo para el trabajo de Informe de Investigación.

Instrucciones para la lista de chequeo:

1. Conteste colocando en la sección de preguntas una equis (X) en la descripción que más se aproxime a **su opinión y percepción sobre lo que se indaga**. Las descripciones que se encuentran para escoger son las siguientes:
 - Totalmente de acuerdo (TA)
 - De acuerdo (DA)
 - Neutral (N)
 - En desacuerdo (ED)
 - Totalmente en desacuerdo (TD)
2. Conteste todas las preguntas en orden después de analizar cada elemento, de forma objetiva, es decir contestando lo que observa realmente. No hay respuestas correctas o incorrectas.
3. Se garantiza total confidencialidad de la información proporcionada individualmente.
4. Los resultados se analizarán posteriormente en forma global con el fin de planificar acciones futuras tendientes a mejorar las variables asociadas con el estudio.
5. Use lápiz para que pueda borrar totalmente cualquier respuesta que desee

cambiar.

Lista de chequeo:

Preguntas/ítems	TDA	DA	N	D	TD	Observaciones
1. Se establece un modelo de gestión de riesgos basado en las normas ISO/IEC 27001:2013 de acuerdo con la teoría expuesta.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
2. Se establece un modelo de gestión de riesgos basado en las normas ISO/IEC 27001:2013 de acuerdo con lo señalado en la Norma.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
3. El modelo gestión de riesgos basado en las normas ISO/IEC 27001:2013 cumple con los lineamientos expuestos en los libros que soportan su diseño por el Consejo Superior de Administración Electrónica.		X				<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
4. El modelo gestión de riesgos propuesto cumple con las fases de las normas ISO/IEC 27001:2013.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
5. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 sigue una secuencia lógica de los procesos que lo integran.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
6. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente graficado.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>
7. El modelo propuesto para la gestión de riesgos basado en las normas ISO/IEC 27001:2013 está claramente explicado de manera que pueda guiar su implementación.	X					<u>RONDA 1:</u> Ninguna <u>RONDA 2:</u>

Escala utilizada para el análisis de la lista de chequeo

Alternativas	Criterio Cuanti-cualitativo de	Calificación
--------------	--------------------------------	--------------

	Evaluación para calificación	Cuantitativa	Cualitativa
Totalmente de acuerdo (TDA)	Muy Bueno (de 4,1 puntos a 5 puntos)	34/7 =	MUY BUENO
De acuerdo (DA)	Bueno (de 3,1 puntos a 4 puntos)	4.85	
Neutral (N)	Aceptable (de 2,1 puntos a 3 puntos)		
En desacuerdo (ED)	Requiere Atención (de 1,1 puntos a 2 puntos)		
Totalmente en desacuerdo (TD)	Crítico (de 0,1 puntos a 1 puntos)		

CONSTANCIA DE JUICIO DE EXPERTO

Nombre del Experto: Dr. Chirinos Mundaca, Carlos Alberto

Especialidad: Ingeniería de Sistemas

DNI: 16721607


Por medio de la presente hago constar que realicé la revisión del modelo de gestión de riesgos en SI propuesto para la empresa Inversiones Fortunia, elaborado por Pablo Leonardo Villon Guerrero – Bachiller de Ingeniería de Sistemas de la Universidad “Señor de Sipán”, quien está realizando su tesis: **“MODELO DE GESTIÓN DE RIESGOS PARA LA SEGURIDAD INFORMÁTICA BAJO ISO/IEC 27001:2013 EN EMPRESA DE ENTRETENIMIENTO Y JUEGOS DE AZAR, LIMA - 2021”**.

Una vez indicadas las observaciones pertinentes, discutidas y aclaradas considero que dicho modelo es **VÁLIDO** para su aplicación e implementación.

Lima, 05 días de mayo del 2021.

Nombre y Apellido: Dr. Chirinos Mundaca, Carlos Alberto
DNI: 16721607

Anexo 8. Resumen de curriculum vitae – Joisy Rojas

Síntesis Curricular		<i>Ing. Joisy Rojas</i>	
1. Datos Personales		3. Adiestramientos y Destrezas	
Nombres:	Joisy Del Valle	Instituto Nacional de Cooperación Educativa (INCE) Certificado: "Dibujo Arquitectónico" 400 h. 1.989	
Apellidos:	Rojas Rojas	Instituto Nacional de Cooperación Educativa (INCE) Certificado: "Operaciones de Micro Básico" 24 h. 1.994	
Cédula de Identidad:	V.-11.511.314	Instituto Universitario Politécnico Santiago Mariño Certificado Obtenido: "Programación Visual Basic" Duración: 16 Horas. 2.001	
Nacionalidad:	Venezolana	FUNDAUDO Certificado Obtenido: "COMPONENTE DOCENTE" Duración: 300 Horas. 2005	
Estado Civil:	Soltera	Destrezas:	
Fecha de Nacimiento:	13 - 12 - 1.971	✓ Metodología y desarrollo de proyectos de Investigación	
Edad:	49 Años	✓ Corrección y tutoría de proyectos de investigación	
Profesión:	Ingeniero de Sistemas	✓ Desarrollo y redacción de artículos, proyectos e Informes de Investigación	
Dirección:	Mzna. 17, casa N° 9, Urb. Manoa, San Félix, Edo. Bolívar	✓ Elaboración de manuales de calidad y Sist. Gestión de calidad	
Teléfono:	Hab. (0286) 9312769 Cel. +58 412 2186547 llamadas, sms y whatsapp	✓ Consultoría y Auditorías de Sistemas	
E-mail:	joisyrojas@hotmail.com joisyrojas@gmail.com		
2. Estudios Realizados		4. Experiencia Laboral	
Educación Primaria:	U.E.N. "Juan Vicente Cardozo". Urb. Manoa. San Félix, Edo. Bolívar. 1ro a 6to Grado. 1.982	Empresa:	EDUCAT Perú, Científica Consultores, GOO EEUU
Educación Secundaria:	U.E. Instituto Combinado "Gonzalo Mendez". Pto. Ordaz, Edo. Bolívar. TÍTULO: Bachiller en Ciencias. 1988	Periodo de Trabajo:	Desde año 2020 – a la actualidad; Modalidad Freelance
Educación Superior:	Instituto Universitario Politécnico "Santiago Mariño". Pto. Ordaz, Edo. Bolívar. TÍTULO: Ingeniero De Sistemas. 05-2002	Cargo:	Asesora de Tesis, Redactora y correctora de proyectos, informes, tesis, manuales de calidad y artículos de diversas ciencias.
Programa de Especialización:	Universidad de Oriente (UDO). San Félix, Edo. Bolívar Ingeniería en Seguridad de Sistemas de Información. Acreditación Ing. de Seguridad SI 11-2002	Empresa:	Universidad Bicentenario de Aragua, UPEL, UCAB y ULA
Postgrado:	Universidad Central de Venezuela (UCV). Caracas, Venezuela. Gestión de Investigación y Desarrollo (I+D) Título: Magister Scientiarum - Año 2010	Periodo de Trabajo:	Desde año 2009 – a la actualidad / Horario Nocturno x Horas
Postgrado:	Universidad Católica Andrés Bello (UCAB). Puerto Ordaz, Edo. Bolívar Sistemas de la Calidad Título: Magister Scientiarum – año 2012	Cargo:	Docente Metodología de la Investigación, Tutora
Postgrado:	Escuela Nacional de Administración y Hacienda Pública (ENDHP). Puerto Ordaz, Edo. Bolívar Control de la Gestión Pública Título: Magister Scientiarum – Año 2019	Empresa:	DUBRAXNET – Empresa Propia de TI
		Periodo de Trabajo:	Desde 12-02-04. Hasta la Actualidad.
		Cargo:	Asesora Externa Metodológica de Proyectos. ULA, UGMA, UNA, USM, UBA, UCAB
		Empresa:	Instituto Universitario de Tecnología "Antonio José de Sucre"
		Periodo de Trabajo:	15-07-02 – 01-07-04/ Horario Nocturno x Horas
		Cargo:	Docente y Tutora Metodológica
		Empresa:	CVG Ferrominera Orinoco, C.A.
		Periodo de Trabajo:	10-11-03 al 15-08-13
		Cargo:	Auditor de Sistemas. Asesor de departamentos en gestión de calidad informática y seguridad en TI.
		Empresa:	RPc Sistemas, C.A.
		Periodo de Trabajo:	15-05-02 al 15-09-03
		Cargo:	Analista de Sistemas e Instructora en capacitación Informática. Administración de Redes. Asesora de proyectos de grado.
		Empresa:	CVG Ferrominera Orinoco, C.A.
		Periodo de Trabajo:	10-02-00 al 15-04-02
		Cargo:	Pasante Tesista Departamento de Sistemas. Actualización Manuales Gestión de SI.

Anexo 9. Resumen de curriculum vitae – Marlo Carranza.



MARLO CARRANZA GALLARDO

INGENIERO DE SISTEMAS

✉ marlocc@hotmail.com

☎ +51-988898079

📍 Lima Perú

📄 Marlo.carranza

HABILIDADES

Excel	★ ★ ★ ★ ★
PowerPoint	★ ★ ★ ★ ★
Word	★ ★ ★ ★ ★
SQL server	★ ★ ★ ★ ★
Qilkview	★ ★ ★ ★ ★
Visual studio .net	★ ★ ★ ★ ★
Sap business	★ ★ ★ ★ ★
Sistema (DRGT)	★ ★ ★ ★ ★
Bizagi	★ ★ ★ ★ ★
Project	★ ★ ★ ★ ★
Otros.	

IDIOMAS

- ✓ Español
- ✓ Inglés básico

HOBBY

- ✓ Jugar Futbol

PERFIL

Compromiso y con vocación de servicio con más de 5 años de experiencia en el rubro de entretenimiento, 8 años en desarrollo e implementación de sistemas. Capacitado para desempeñar eficientemente. Poseo gran criterio personal, capacidad para la recopilación y análisis de un creciente flujo de información, creatividad, confiabilidad, iniciativa, proactivo, capacidad de comunicación clara y fluida, sólida formación en valores, capacidad para tomar decisiones bajo presión, capacidad de planificación y trabajar en equipo.

EDUCACIÓN

2006-I Perú	Título en Ingeniería de Sistemas Universidad N. José Faustino Sánchez Carrión
CIP	128849
2017 Lima	Capacitación de uso de SAP Corporación EW
2015 Ica	Capacitación sistema on-line SID DRGT
2009 Huacho	Curso de capacitación de Oracle 11i UNJFSC
2006 Huacho	Curso de capacitación de SQL Server. CIBERTEC

REFERENCIAS

- Ricardo Aparicio
Gerente/Apoderado
Celular: 942570843
- María Guillinta
Jefe Personal
Celular: 993327680

PROYECTOS REALIZADOS

- Sistema de escritorio (compras, almacenes, ventas, Contabilidad, Activo Fijo, RRHH, Presupuesto, Información Gerencial)
- Sistemas Web Paginas estáticos, dinámicas

EXPERIENCIA PROFESIONAL

De 01/03/2017
Actualidad
(Lima)

INVERSIONES FORTUNIA SA,
ADMINISTRADOR Y JEFE DE TI

Funciones del cargo:

- ✓ Controlar el presupuesto, flujo de caja, EGP.
- ✓ Realizar informe anual del oficial de cumplimiento
- ✓ Realizar las gestiones necesarias con los entes del estado (MINCETUR, INDECI, SBS, SUNAT, Etc.) para garantizar el funcionamiento del giro del negocio.
- ✓ Supervisar y controlar las gestiones de las compras de productos y servicios y control de los inventarios.
- ✓ Supervisar y controlar el correcto funcionamiento de todos los sistemas, proponiendo mejoras alternativas, simplificando procesos y manteniendo un correcto control interno.
- ✓ Supervisar y controlar el correcto cuadro de la caja-bóveda-contadores y recaudos.
- ✓ Proponer mejoras y alternativas en función del análisis de la información para optimizar los procesos y rendimientos de la sala.
- ✓ Supervisar y controlar la gestión del mantenimiento preventivo de los equipos de sala
- ✓ Supervisar y aplicar parámetros de seguridad informática.
- ✓ Controlar y supervisar todos los sorteos, promociones entre otras.
- ✓ Elaboración de proyectos de factibilidad.

De 01/10/2015
28/02/2017
(Ica)

INVERSIONES FORTUNIA SA,
ADMINISTRADOR Y JEFE DE TI

Funciones del cargo:

- ✓ Controlar el presupuesto, flujo de caja, EGP, resultados integrales
- ✓ Realizar informe anual del oficial de cumplimiento
- ✓ Realizar las gestiones necesarias con los entes del estado (MINCETUR, INDECI, SBS, SUNAT, Etc) para garantizar el funcionamiento del giro del negocio.
- ✓ Supervisar y controlar las gestiones de las compras de productos y servicios y control de los inventarios.
- ✓ Supervisar y controlar el correcto funcionamiento de todos los sistemas y manteniendo un correcto control interno.
- ✓ Supervisar y controlar el correcto cuadro de la caja-bóveda-contadores y recaudos.
- ✓ Proponer mejoras y alternativas en función del análisis de la información para optimizar los procesos y rendimientos de la sala.
- ✓ Supervisar y controlar la gestión del mantenimiento preventivo de los equipos de sala
- ✓ Supervisar y aplicar parámetros de seguridad informática.
- ✓ Controlar y supervisar todos los sorteos, promociones entre otras.
- ✓ Seguimiento y evaluación a las campañas de marketing.
- ✓ Apoyo para reclutamiento de personal.

De 01/01/2014
30/09/2015
(Ica)

INVERSIONES FORTUNIA SA

JEFE DE SISTEMAS

Funciones del cargo:

- ✓ Implementación del sistema on-line DRGT
- ✓ Supervisar y aplicar parámetros de seguridad informática.
- ✓ Verificar diariamente el correcto funcionamiento de los sistemas de la empresa
- ✓ Realizar la configuración de las promociones y sorteos.
- ✓ Llevar un control de cambios de accesos a la información.
- ✓ Cambiar periódicamente las claves, verificar accesos según perfil de usuario definido.
- ✓ Realizar backups de la información y enviar mensualmente los backups a la corporación.
- ✓ Mantener actualizado todos los programas de la empresa.
- ✓ Creaciones de usuarios en dominio y sistema on-line utilizando fichas de usuarios.
- ✓ Realizar quincenalmente test a los equipos de comunicación para verificar su correcto funcionamiento
- ✓ Realizar o coordinar los mantenimientos preventivos de los equipos de computo
- ✓ Tener un pleno conocimiento del funcionamiento de los sistemas, garantizando el correcto uso por los usuarios y lanzamiento de productos.
- ✓ Organizar o realizar manuales de usuario.
- ✓ Emitir informes semanales, quincenales de las funciones del puesto o a solicitud de su gerencia.

De 30/12/2013
03/01/2006
(Huacho)

EMPRESA AGRARIA AZUCARERA ANDAHUASI S.A.A,

ANALISTA DESARROLLADOR

Funciones del cargo:

- ✓ Levantamiento de la información y procesarla.
- ✓ Elaborar procesos de negocios usando herramientas de modelamiento de procesos
- ✓ Elaboración de proyectos de sistemas.
- ✓ Elaboración de prototipos de software
- ✓ Desarrollo y despliegue de software.
- ✓ Mantenimiento de funcionalidad ERP SIGERP.
- ✓ Desarrolle e implemente los módulos de contabilidad, análisis de laboratorio, gestión agrícola y gestión de control gerencial.

Anexo 10. Resumen de curriculum vitae – Carlos Chirinos.

CURRICULUM VITAE



1. DATOS GENERALES

1.1. Nombres y Apellidos	: CARLOS ALBERTO CHIRINOS MUNDACA
1.2. Lugar de nacimiento	: Chiclayo
1.3. Fecha de nacimiento	: 14 de abril de 1974
1.4. Tipo de documento de identidad	: DNI
1.5. Número de documento de identidad	: 16721607
1.6. Domicilio	: Calle Yen Escobedo Garro 220 - Chiclayo
1.7. Teléfonos	: 991799575 – (074) 223443
1.8. Correo electrónico	: carlos.chirinosmundaca@gmail.com
1.9. Estado Civil	: Casado
1.10. Código ORCID	: 0000-0002-6733-8992

2. FORMACIÓN ACADÉMICA

2.1 Grados y Títulos

Grados y Títulos	Centro de estudios	Fecha de obtención
DOCTOR EN EDUCACIÓN	UNIVERSIDAD CESAR VALLEJO	2019
MAESTRO EN CIENCIAS CON MENCIÓN EN INFORMÁTICA Y SISTEMAS	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	2011
BACHILLER EN INGENIERÍA DE COMPUTACIÓN Y DE SISTEMAS	UNIVERSIDAD PRIVADA ANTENOR ORREGO	1996
INGENIERO INFORMÁTICA Y DE SISTEMAS	UNIVERSIDAD PARTICULAR DE CHICLAYO	2001

3. EXPERIENCIA PROFESIONAL

Nombre de la Institución	Tipo de Institución	Cargos desempeñados	Fecha de inicio	Fecha de término
Corte Superior de Justicia de Lambayeque - Perito Judicial	Pública	Perito en Sistemas	Abril 2010	2021
Centro de Peritaje y Arbitraje del Colegio de Ingenieros del Perú – Consejo Departamental de Lambayeque	Privada	Perito en Sistemas	Noviembre 2010	Noviembre 2011
Universidad Particular de Chiclayo. Facultad de Ingeniería Informática y de Sistemas	Privada	Profesional Consultor de Mantenimiento de Hardware y Software	Abril 2006	Julio 2010
Empresa Comercializadora Santa Ana – COINSA S.R.L.	Privada	Asistente Profesional	Julio 2003	Junio 2004
Empresa Grafica y Talleres de Arte Inga – Publi 360	Privada	Asesoría y Mantenimiento de Sistemas Informáticos	Octubre 2001	Noviembre 2002
Universidad Particular de Chiclayo	Privada	Labor Administrativa	Julio 1999	Mayo 2002

2.2 Diplomados

Nombre	Centro de estudios	Fecha de obtención
DISEÑO E IMPLEMENTACIÓN DE CURSOS VIRTUALES 204 Horas Lectivas (12 Créditos)	UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO	Junio 2012
DIPLOMADO EN DELITOS INFORMÁTICOS Y LEGISLACIÓN INFORMÁTICA 480 Horas Lectivas (24 Créditos)	UNIVERSIDAD TECNOLÓGICA DE LOS ANDES – FACULTAD DE DERECHO Y CIENCIA POLÍTICA	Octubre 2015
DIPLOMADO EN INFORMÁTICA FORENSE 480 Horas Lectivas (24 Créditos)	UNIVERSIDAD TECNOLÓGICA DE LOS ANDES – FACULTAD DE DERECHO Y CIENCIA POLÍTICA	Setiembre 2015
GESTIÓN DE LA PRODUCCIÓN CIENTÍFICA 400 Horas Académicas (20 Créditos)	UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO	Abril 2007

2.3 Estudios en curso o concluidos

Nombre	Centro de Estudios	Fecha de inicio	Estado	
			En curso	concluido
DOCTORADO - TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES	UNIVERSIDAD NACIONAL DE PIURA	2019	X	
MAESTRÍA - INGENIERÍA DE SISTEMAS CON MENCIÓN EN SISTEMAS DE INFORMACIÓN	UNIVERSIDAD PRIVADA ANTENOR ORREGO	2018		X
SEGUNDA ESPECIALIDAD - INGENIERÍA WEB	UNIVERSIDAD NACIONAL PEDRO RUIZ GALLO	2008		X
SEGUNDA ESPECIALIDAD - TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN APLICADAS AL PROCESO DE ENSEÑANZA APRENDIZAJE	UNIVERSIDAD CATÓLICA SANTO TORIBIO DE MOGROVEJO	2008		X