UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

TESIS

IMPLEMENTACIÓN DE UN MODELO AD HOC DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA EDITORA DE DIARIO REGIONAL PERUANO

PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

Autor(a) (es):
Bach. Castro Medina Miguel Angel
ORCID: https://orcid.org/0000-0002-2573-4559

Asesor(a):
Dr. Tuesta Monteza Victor Alexci
ORCID: https://orcid.org/0000-0002-0007-0928

Línea de Investigación:
Infraestructura, Tecnología y Medio Ambiente

Pimentel – Perú 2021

APROBACIÓN DEL JURADO

IMPLEMENTACIÓN DE UN MODELO AD HOC DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA EDITORA DE DIARIO REGIONAL PERUANO

_____

Castro Medina Miguel Angel

Autor

_____

Dr., Tuesta Monteza Victor Alexci

Asesor

_____ _____

Dr., Vasquez Leiva Oliver

Presidente de Jurado

Mg., Bravo Ruiz Jaime Arturo

Secretario de Jurado

_____

Mg., Aguinaga Tello Juan

Vocal de Jurado

Dedicatorias

A mis padres por brindarme la mejor formación a nivel educacional y moral, muchos de mis objetivos cumplidos se los debo a ustedes, incluido este trabajo. También quiero dedicar este trabajo a mi pequeña hija, que, desde su nacimiento, es un impulso muy grande para poder cumplir con todos los objetivos que me proponga, tanto en lo personal como en el aspecto académico.

Agradecimientos

Agradezco enormemente a todos los ingenieros que me apoyaron con las inquietudes durante todo el desarrollo de este trabajo, así mismo también agradezco a la empresa editora de diario regional peruana seleccionada para este trabajo, debido a que me brindo todas las facilidades para el tratamiento de su información.

Resumen

La información es uno de los recursos más importantes dentro de una empresa u organización, por ende, esta debe ser protegida de manera adecuada. Según Forbes el 41% de empresas a nivel mundial ha sufrido ataques informáticos en el año 2020, y el 82% de ellas están interesadas en proteger sus datos. Existen novedosas técnicas de hacking que permiten extraer datos de una determinada empresa, que no tiene los requisitos mínimos de seguridad para salvaguardar su información. Actualmente existen diversas metodologías que nos permiten desarrollar un modelo de seguridad que este a nivel de la información que la empresa maneja. Sin embargo, las implementaciones de estos modelos son costosos y se alejan de la realidad de las empresas en nuestro país. Es por ello que se optó por desarrollar un modelo que está compuesto por la norma ISO/IEC 27001:2013, y la metodología Magerit. El modelo está compuesto por cuatro fases, la fase 1, corresponde al compromiso de la empresa, la fase 2 está relacionada al tratamiento de los riesgos, la fase 3 abarca el proceso de ejecución y por último la fase 4 se dedica exclusivamente a la mejora continua. Para la creación de las políticas de seguridad se tomaron en cuenta las amenazas que tuvieron una probabilidad de ocurrencia de alta y muy alta, esto debido a que la empresa necesitó implementar políticas de seguridad que se adapten a sus necesidades actuales. Después de haber implementado las políticas de seguridad seleccionadas, se obtuvo un 24% de efectividad después de realizar la aplicación del modelo ad hoc, este porcentaje se obtiene debido a que antes de la aplicación, la empresa no contaba con ninguna norma ni política de seguridad para proteger su información. Sin embargo, es necesario considerar que se debe realizar capacitaciones a los colaboradores que laboran en la empresa, con el fin de que conozcan las vulnerabilidades que existen y puedan hacer frente a la perdida de información ocasionada por cualquier agente externo.

Palabras Clave:
Seguridad, información, modelo ad hoc, gestión, políticas de seguridad, riesgo, amenaza.

Abstract

Information is one of the most important resources within a company or organization, therefore, it must be adequately protected. According to Forbes, 41% of companies worldwide will have suffered cyber attacks by 2020, and 82% of them are interested in protecting their data. There are novel hacking techniques that make it possible to extract data from a given company, which does not have the minimum security requirements to safeguard its information. Currently there are several methodologies that allow us to develop a security model that is at the level of the information that the company handles. However, the implementation of these models is costly and far from the reality of the companies in our country. This is why it was decided to develop a model that is composed of the ISO/IEC 27001:2013 standard and the Magerit methodology. The model is composed of four phases: phase 1 corresponds to the company's commitment, phase 2 is related to risk treatment, phase 3 covers the execution process and finally phase 4 is dedicated exclusively to continuous improvement. For the creation of the security policies, the threats that had a high and very high probability of occurrence were taken into account, because the company needed to implement security policies that adapt to its current needs. After having implemented the selected security policies, 24% of effectiveness was obtained after the application of the ad hoc model, this percentage is obtained because before the application, the company did not have any standard or security policy to protect its information. However, it is necessary to consider that training should be provided to the employees working in the company, so that they are aware of the vulnerabilities that exist and can cope with the loss of information caused by any external agent.

Keywords:

Security, information, ad hoc model, management, security policies, risk, threat.

Índice

I. INTRODUCCIÓN

1.1. Realidad Problemática.

La información constituye uno de los recursos más importantes dentro de una empresa, por consiguiente, ésta debe ser protegida de manera adecuada, y para ello existen políticas de seguridad que se encargan de gestionar de manera adecuada la información. (Vega, 2021) Según Forbes el 41 % de empresas a nivel mundial ha sufrido ataques informáticos en el año 2020, y el 28 % de ellas están dispuestas a proteger sus datos. (Thales, 2021) La gestión de la seguridad de la información se fundamenta en identificar brechas de seguridad y posteriormente plantear las posibles políticas que pueden dar solución a estos inconvenientes de seguridad. La pérdida de información en una organización genera un impacto económico negativo.

A nivel empresarial la información es un activo valioso. Actualmente las empresas consideran a las grandes bases de datos de imágenes, opiniones, compras, etc. el nuevo recurso natural. (Gené & Gallo, 2018) Las empresas creen que invertir en seguridad de la información es un gasto innecesario, ahora con las nuevas técnicas de hacking, usuarios capacitados en esta técnica pueden acceder a los datos de una determinada organización. (Revista Universidad y Sociedad, 2019)

En la actualidad existen distintas metodologías que sirven como referencia para desarrollar un modelo de gestión de seguridad de la información, dentro de estas metodologías podemos encontrar a Octave, Magerit, NIST SP 800-30 y PHVA, es preciso señalar que todas las metodologías trabajan con referencia en la norma ISO/IEC 27001 la cual se encarga de velar por la seguridad, confidencialidad e integridad de los datos y de la información. (ISO Tools excellence, 2021)

La metodología más resaltante que se utiliza actualmente para realizar un adecuado modelo de gestión de seguridad de la información es Magerit, usada mayormente en países de europea y en medianas organizaciones.

(Ministerio de Hacienda y Administraciones Públicas - Gobierno de España, 2012)

El uso de la metodología PHVA se caracteriza por la mejora continua de todas sus etapas, garantizando un mejor control sobre la seguridad de la información de la organización. (Insituto Nacional de Tecnologias de la Comunicación - Gobierno de España, 2021)

Las metodologías mencionadas anteriormente tienen la particularidad de haber sido desarrolladas en su mayoría en países europeos, En la realidad peruana las empresas no cuentan con la solvencia económica para permitirse implementar una serie de normas y políticas de seguridad que cumplan con estándares internacionales, y que a su vez le permitan resguardar su información. (Concytec, 2016)

Baca, (2016) La aplicación de la metodología MAGERIT para realizar una gestión del riesgo adecuada es válida aplicada a una organización peruana, sin embargo, no ha sido personalizada de manera correcta, es importante poner énfasis en la seguridad de la información, la perdida de información puede llegar a poner en problemas legales y económicos a cualquier empresa ya sea del estado o de índole privada, debido a esto es obligatorio realizar una correcta gestión de la seguridad de la información, teniendo en cuenta la dimensión y los recursos de la empresa.

La seguridad informática es la encargada de proteger la información que está presente en un software determinado, muchas veces se tiene la idea de que un sistema informático es perfecto, que nada lo puede vulnerar, lo cual es un grave error. Desde el enfoque de la ingeniería de sistemas esto es un problema que trae como consecuencias perdida de información valiosa tanto para un usuario común y corriente, como para una empresa, independientemente de su tamaño. (Vega, 2008)

Rodríguez, (2020) Los modelos que existen actualmente en el área de la ingeniería de sistemas para poder proteger los datos y activos de una

empresa, pertenecen al área de seguridad informática, y se basan en normativas ISO/IEC, sin embargo, estos modelos son aplicables para coyunturas empresariales totalmente distintas a la realidad peruana. Es por ello que resulta necesario poder adaptar a la realidad peruana estos modelos que han demostrado su eficiencia en el extranjero, quizás el mayor impedimento para permitir desarrollar un modelo de gestión de seguridad de la información sea el dinero.

Contreras, (2003) El extraer información de una empresa es considerado un delito informático, no obstante, muchas empresas peruanas no son conscientes de ello. La ingeniería de sistemas bajo la rama de la seguridad informática, es la encargada de blindar a cualquier empresa que desee proteger sus activos, el inconveniente es que debido a desconocimiento y/o falta de dinero muchas empresas se ven obligadas a obviar este tema tan importante, las soluciones que se presentan actualmente están validadas por la unión europea y otros países pioneros en seguridad informática, no obstante el problema de estas soluciones es que no se adaptan a la realidad empresarial peruana.

Rodriguez, (2020) Otra alternativa de solución para este problema de la perdida de información, es el hacking ético, que tiene como única finalidad, identificar las brechas de seguridad en un sistema de información para posteriormente proponer las alternativas de solución para evitar ataques verdaderos. Sin embargo, este método muchas veces resulta muy costoso, lo cual prácticamente es algo inalcanzable para muchas empresas peruanas. Por otro lado, la ventaja de realizar un modelo personalizado para gestionar la seguridad de la información es que es una propuesta con costos reducidos y lo más resaltante, se adecua a las necesidades de la empresa, y por supuesto, cumpliendo con la normativa internacional.

Muchos de estos modelos de gestión de seguridad de la información se basan en normas internacionales, los cuales garantizan una buena efectividad al momento de implementarse en cualquier organización, sin embargo, no hay muchos estudios científicos aplicados a empresas

peruanas, lo cual evidencia un vacío de conocimiento, no obstante, el reto contemporáneo de la seguridad informática en el Perú, es de extrapolar todos esos conocimientos y normas a la realidad empresarial peruana. Cabe señalar que las políticas de seguridad aplicada a redes informáticas son muy importantes en una organización, debido a que el mayor tráfico de información actualmente circula por internet. (De Freitas, 2009)

1.2. Trabajos previos.

Chierici et al., (2019) realizo la investigación llamada SGSI project at CNAF. Desarrollada en Physics and Astronomy Department, University of Bologna, Italy. El centro italiano Tier1 se dedica a realizar experimentos en el Gran Colisionador de Hadrones (LHC), el área de informática no cuenta con políticas de seguridad personalizadas de grandes volúmenes de datos. Por esta razón se presentó como solución desarrollar un SGSI referenciado en el estándar internacional ISO 27001, así como también estas normas serán adaptadas a los distintos softwares que se usan para realizar los experimentos en el LHC. Los resultados de implementar la normativa ISO 27001 fueron favorables, incluso se han realizado experimentos tras la implementación de este estándar internacional. Es evidente que instituciones de investigación científica requieren tener un control especial con los datos que ellos manejan, avalando la seguridad e integridad de estos.

Poveda et al., (2019) realizó la investigación llamada ISO 50001: 2018 and Its Application in a Comprehensive Management System with an Energy-Performance Focus. Las empresas actualmente no cuentan con una estrategia para lidiar con los riesgos de distintos tipos, así mismo no cuentan con normativas sobre eficiencia energética, los cuales merman la generación de valor agregado por parte de la empresa. Por esta razón de presento como solución la implementación de buenas prácticas que garanticen la disminución de las vulnerabilidades que puede llegar a tener una empresa, así como también la aplicación de un sistema de gestión integral conjuntamente con la aplicación de la norma ISO 5001:2018. Los resultados de implementar estas buenas practicas se aprecia en el mejoramiento de la

eficiencia energética de la empresa, así como también un perfeccionamiento en el sistema de gestión y reducción de riesgos como la perdida de información. Después de haber aplicado todas estas mejoras en distintas empresas, se puede evidenciar una mejora en la gestión de riesgos y eficiencia energética dentro de estas empresas, esto marca un precedente para aquellas medianas y grandes empresas de todo tipo de rubro.

Beckers et al., (2013) realizó la investigación llamada A pattern-based method for establishing a cloud-specific information security management system. La aplicación de un Sistema de gestión de seguridad de la información en la nube, resulta complicado debido a que posee varias partes interesadas, la distribución del almacenamiento en la nube es muy escalable, es dificultoso encontrar los riesgos y encontrar los activos a proteger. Por esta razón se intenta generar un método de gestión de seguridad de la información para la nube referenciado en el estándar ISO 27001. Los resultados de este trabajo de investigación demuestran que es aconsejable implementar estos estándares en seguridad de la información, siempre y cuando se creen patrones para la detección de riesgos y cumplimiento de políticas de seguridad los suficientemente robustas para evitar perdida de datos en la nube. Es de muy importante tener en cuenta que un SGSI puede ser aplicado tanto a una empresa tradicional como a una empresa que tiene sus servicios o productos alojados en la nube, siguiendo métodos que se amoldan a los requerimientos de la empresa.

Ahmad et. al., (2019) realizó la investigación denominada Security monitoring and information security assurance behaviour among employees An empirical analysis. Realizado en Multimedia University, Malasya. La administración de la información en las empresas no está debidamente automatizada, esto conlleva a que los colaboradores no se sientan cómodos al momento de cumplir las políticas establecidas para la custodia de la información dentro de la empresa. Por esta razón se pretende brindar un marco teórico en donde se establezcan cuáles son los motivos por lo cual los trabajadores no cumplen con las normas de seguridad de la información establecidas, así mismo se pretende corroborar el Categoría de insatisfacción de los trabajadores por no

tener sistematizado el control de riesgos en la empresa. Los resultados demuestran que es oportuno brindar capacitaciones a los colaboradores y automatizar los procesos más tediosos para el control de riesgos, evitando de esta manera la incomodidad de los trabajadores, de esto depende que la empresa pueda cuidar de manera adecuada todos sus activos. Es importante señalar que gracias a este estudio es posible determinar los puntos débiles de una organización al momento de establecer normas y políticas de seguridad de la información, llegando a la conclusión que el colaborador es una pieza fundamental para lograr salvaguardar los activos de la empresa.

Pérez et al., (2019) realizó la investigación denominada Organizational practices as antecedents of the information security management performance An empirical investigation. Realizada en University of Cantabria, Santander, Spain. El conocimiento sobre las buenas prácticas de seguridad dentro de la organización está muy limitado, carecen de un modelo que establezca los lineamientos necesarios para realizar con éxito todas las actividades que se vinculan a la vigilancia de datos y activos de la organización. Por esta razón se determinó incrementar los conocimientos acerca de la seguridad en la organización aplicando intercambio de información, y obteniendo datos acerca de las normas de seguridad que establecen los distintos gerentes de 111 empresas. Los resultaros tras aplicar un enfoque de un modelo de ecuación estructural con el software EQS 6.1, son favorables, debido a que gracias a los intercambios de información y validaciones de normas de seguridad de información es posible aumentar el conocimiento que tienen las organizaciones acerca de la seguridad de la información. De esta manera se puede señalar que los conocimientos acerca de las normas de seguridad de la información favorecen no solo a grandes empresas, si no, que también favorecen a las pequeñas y medianas empresas, gracias a este modelo es posible aplicar todos estos lineamientos.

Tagarev, (2012) realizó la investigación llamada Model for information security analyses in information security management system. Realizado en Sofia, Bulgaria. Muchas veces las organizaciones no tienen el conocimiento de cómo actuar después de haber implementado un SGSI. Por tal motivo el

investigador propone un modelo que se basa en análisis de procesos, evaluación por expertos y una integración de salvaguardas y las amenazas que se puedan encontrar en la empresa. Los resultados demuestran que es necesario un ciclo de mejora continua, después de haber implementado un SGSI, es importante mantener actualizado el reporte de incidentes, así como también las nuevas políticas que se pueden implementar de acuerdo al escenario empresarial que se desarrolle en ese momento. Es importante mantener un control de las políticas que se puedan implementar, haciendo un ciclo de mejora continua, esto ayuda a que las empresas puedan predecir que políticas pueden implementar y adelantarse a los hechos para de esta manera tener la seguridad de que están protegiendo sus activos más preciados.

Faizan et al., (2021) realizó la investigación llamada Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. Generalmente los trabajadores de las empresas que cuentan con un SGSI, no cumplen con las normas y lineamientos establecidos por este, ocasionando que este sistema de gestión no logre cumplir los objetivos para los cuales se implementó. Por esta razón el estudio se basa en recopilar información en donde se evalúe el cumplimiento y comportamientos de incumplimiento por parte del trabajador, así mismo se muestra un modelo de proceso de transformación del cumplimiento. Después de haber recopilado toda la información y haber generado un pequeño modelo para transformar el incumplimiento en cumplimiento, se demostró que, aunque la literatura científica es escasa con respecto al tema abordado, se pudieron obtener distintos parámetros los cuales ayudan a los trabajadores a poder cumplir con las normas de seguridad que proporciona la empresa. La investigación acerca de este tema revela que hay ciertos patrones conductuales, los cuales se tienen que estudiar para poder convencer al trabajador de cumplir con las normas que establece el SGSI, es necesario hacer hincapié en este aspecto para poder alinear lo que necesita la empresa con lo que realizan sus trabajadores en materia de seguridad de los activos.

Chan et al., (2005) realizo la investigación denominada Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. Realizado en Naional University of Singapore. El 78% de ataques de virus informáticos tienen como vehículo los correos electrónicos, muchas empresas no tienen conocimiento de cómo actuar frente a una situación así. La propuesta de los autores es generar un modelo en el cual se ponga énfasis al clima laboral y al correcto accionar que deben de tener todos los trabajadores frente a una situación como esta. Así mismo los investigadores mencionan que es importante capacitar al personal y realizar ciclos de concientización en donde los trabajadores puedan ver que sucedería si se logra perder información valiosa para la empresa. Después de haber aplicado el modelo a una determinada organización se llegó a la conclusión de que un 26.5% de éxito para la realización de las normas de seguridad de la información, son gracias a la combinación de factores organizacionales y personales respectivamente. Se puede afirmar después de haber realizado el estudio, que el ámbito personal de los trabajadores de una empresa, influye en el control y prevención de riesgos, así como también la normativa, capacitaciones y alcances que pueda brindar la propia empresa.

Dang et al., (2019) realizó la investigación Explaining the Development of Information Security Climate and an Information Security Support Network: A Longitudinal Social Network Analysis. El clima laboral en la mayoría de las organizaciones es positivo, sin embargo, hace falta conceptualizar y establecer ciertos criterios que permitan a los empleados entender los objetivos de la empresa y colaborar para cumplir con las normativas establecidas con respecto a la seguridad de la información. Los investigadores proponen varias acciones para promover el cumplimento de normas por parte de los trabajadores, la más resaltante es identificar a los trabajadores más influyentes sobre los demás, para poder empezar a contemplar la idea de adoctrinar al colaborador con las normas y estándares que debe de seguir para el beneficio de la empresa, y a su vez este podrá influenciar en sus demás compañeros de trabajo. El clima laboral es sumamente importante en una empresa, ya que de este depende que los

colaboradores se sientan cómodos y así poder cumplir con los objetivos de esta y a su vez incentivar a sus compañeros a hacer lo mismo.

Issa, (2011) realizó la investigación denominada Setting up a Secure Information System Using Information Security Management. Realizado en Taibah University, College of Computer Science & Engineering. En la actualidad los SGSI se encargan de proteger los activos más preciados de una organización, su información, pero siempre surge una pregunta, ¿Quién protege a estos SGSI? Los investigadores proponen enfocarse en establecer políticas de seguridad sólidas para evitar ataques al sistema de prevención en lugar de centrarse en detectar ataques informáticos a la organización. Tras realizarse el estudio y propuesta de implementar políticas de seguridad sólidas, es necesario establecer niveles de seguridad, y seleccionar muy bien las políticas que se van a implementar, debido a que no solo se protegerá la información, sino que, también se protegerá al propio SGSI. Es imprescindible contar con un nivel de concientización adecuado para hacer cumplir todas las políticas de seguridad establecidas, así como también es importante evaluar todos los riesgos que puedan perjudicar tanto al sistema como a los activos que protege el sistema, esa es la clave para que un SGSI sea efectivo al cumplir con su trabajo.

1.3. Teorías relacionadas al tema.

1.3.1. Seguridad de la información

ISO Tools excellence, (2021) La seguridad de la información es la encargada de velar por la confidencialidad, integridad y disponibilidad de la información que resulte importante para una organización o empresa.

El objetivo principal de la seguridad de la información es garantizar que los bienes que tiene la organización o empresa sean empleados de la manera en que la organización o empresa lo estipule.

La seguridad de la información no debe ser un tema ajeno a los participantes de una organización o empresa, con la única intención de poder conservar la

confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad de la información.

1.3.2. Gestión de la seguridad de la información

La gestión de la seguridad de la información es un proceso mediante el cual una organización puede controlar y hacer seguimiento de todas las vulnerabilidades que puedan encontrarse, en oposición de los activos de información. El estándar internacional ISO/IEC 27001 configura diversos procesos y determina responsabilidades dentro de la organización, con el único fin de robustecer las normas y políticas de seguridad de la información dentro de la empresa.

El desarrollo de un SGSI implica elaborar un conjunto de normas de seguridad de la información y por ende asignar responsables de la seguridad y que controles se deben usar en cada situación organizacional. (ISO Tools exellence, 2021)

1.3.3. Sistema de gestión de seguridad de la información (SGSI)

Un SGSI es una agrupación de procedimientos y actividades que poseen como finalidad ratificar la confidencialidad, integridad y disponibilidad de la información.

El principal objetivo de un SGSI es crear y planificar procedimientos óptimos para posteriormente desarrollar controles de seguridad apoyados en una valoración del riesgo y conseguir de esta manera mediciones de eficiencia de los mismos.

Los objetivos de la organización forman parte crucial del desarrollo de un SGSI, de esta manera se garantiza un Categoría de exposición bajo frente al nivel de riesgo que la organización decide asumir. (Pmgssi, 2021) Los principales privilegios de implementar un SGSI son:

- Posee una metodología organizada para la gestión de la seguridad de la información.

- Se reduce el riesgo de pérdida de información de la empresa.
- El cliente tiene entrada a la información, pero con medidas de restricción.
- Revisión periódica de riesgos y controles.
- Auditorías externas para encontrar debilidades en el SGSI.
- Cómoda incorporación con otros sistemas de gestión.
- La prolongación de la empresa está garantizada ante incidentes y accidentes.
- Reducción de costos y mejora continua de procesos.

1.3.4. Metodología Magerit para gestión de riesgos

Ministerio de hacienda y administraciones públicas (2012) La metodología Magerit tiene como objetivo principal, desarrollar el proceso de gestión de riesgos que se adecue mejor a la empresa, de esta manera las áreas de gerencia de una empresa puedan tomar decisiones teniendo en cuenta los posibles riesgos dentro de la organización. Esta metodología se sustenta en la norma estándar internacional lSO/IEC 31000.

Los siguientes informes que se presentan a continuación, reúnen todos los productos de las tareas que se realizan para el análisis y gestión de riesgos.

Modelo de valor: Todas las propiedades que representa un activo para la empresa.

Mapa de riesgos: Relación de vulnerabilidades a las que están comprometidos los activos más importantes de la organización.

Declaración de aplicabilidad: Son todas las políticas que se puedan aplicar al sistema de información que maneja la organización o empresa.

Evaluación de salvaguardas: Evalúa la efectividad de las políticas que existen en la empresa.

Estado de riesgo: Son las propiedades de los activos, clasificados por el riesgo residual.

Informe de suficiencias: Son todas las salvaguardas que aparentemente cumplen con su objetivo de mitigar los riesgos, sin embargo, no son fuertes contra estos.

Cumplimiento de normativa: Es la ejecución de los requerimientos instaurados por las políticas implementadas en la organización.

Plan de seguridad: Conglomerado de salvaguardas que se encargan de brindar los lineamientos para afrontar los riesgos y ataques informáticos que pueda afectar a la organización.

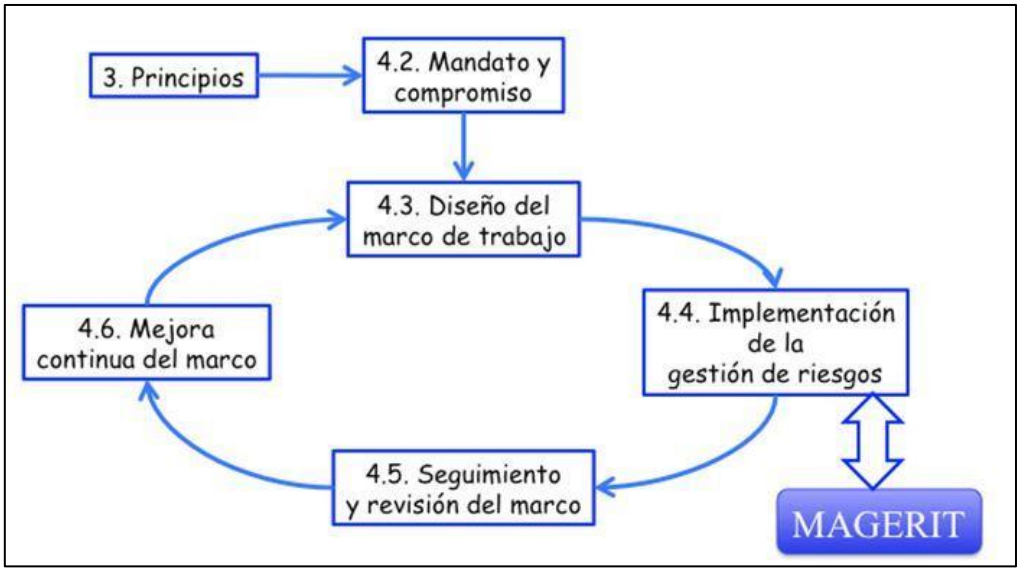


Figura 1. Mapa de procesos del manejo de la metodología Magerit para la gestión de riesgos. Fuente: (Ministerio de Hacienda y Administraciones Públicas - Gobierno de España, 2012)

1.3.5. Metodología Octave para gestión de riesgos

Hurtado, (2020) La metodología Octave (Operationalilty Critical Threat, Asset and Vulnerability Evaluation) cuya traduccion al español seria: Evaluacion operative de amenazas críticas, activos y vulnerabilidades. Esta metodología se aplica específicamente para la valoración de riesgos que puedan existir en

una determinada empresa. Fue desarrollada por el Software Engineering Institute (SEI) en el país de los Estados Unidos. Está compuesta por cuatro principales fases que se presentaran a continuación:

Fase 1
Build asset-based threat profiles
Esta fase está enfocada en el reconocimiento de todos los bienes que posee la empresa, así mismo los recursos que posee la empresa relacionados a la seguridad de la información. (Hurtado, 2020)

Fase 2
Identify infrastructure vulnerabilities
En esta fase se pueden reconocer las flaquezas que afectan a un sistema de información, de igual manera las vulnerabilidades que afectan a los activos que han sido caracterizados en la fase anterior. (Hurtado, 2020)

Fase 3
Develop security strategy and plans
En esta fase se pretende desarrollar los planes y estrategias de seguridad que más se acomoden al estado actual de la empresa. Basándose en las vulnerabilidades encontradas y posibles brechas de seguridad expuestas. (Hurtado, 2020)

Fase 4
Build asset-based threat profiles
Por ultimo en esta etapa se ejecuta la caracterización de los bienes críticos para la empresa y que estrategias se están aplicando para proteger la integridad de los mismos. (Hurtado, 2020)

1.3.6. Normas familia ISO/IEC 27000

La norma internacional ISO/IEC 27000 está conformada por varios estándares, algunos aún se encuentran en desarrollo. Este grupo de normas

están encargadas de proporcionar una estructura para la gestión de la seguridad de la información y puede ser empleado por cualquier empresa. (ISO27000.ES, 2021)

Entre las primordiales normas que conforman el conjunto de normas ISO/IEC 27000 se encuentran.

ISO/IEC 27000: Proporciona el alcance y propósito de todas las normas que conforman esta familia, además menciona descripciones y conceptos acerca de un SGSI. (ISO Tools exellence, 2021)

ISO/IEC 27001: Proporciona requerimientos para robustecer un sistema de información, se sustenta principalmente en brindar los lineamientos para la elaboración de políticas de seguridad. (ISO, 2021)

ISO/IEC 27002: Se encarga de brindar las normas que permitan realizar una correcta implementación de controles de seguridad, así mismo se encarga también de contribuir con la documentación para realizar la selección, desarrollo y la evaluación de las políticas de seguridad. (ISO, 2021)

ISO/IEC 27001: Brinda pautas para implementar de manera correcta la norma ISO/IEC 27000. (ISO, 2021)

1.4. Formulación del Problema.

¿Cómo se mejora la gestión de la seguridad de la información en una empresa editora de diarios regionales peruanos?

1.5. Justificación e importancia del estudio.

Teniendo como marco de referencia las distintas metodologías para la gestión de riesgo, y el estándar internacional ISO/IEC 2701:2013, se instauró varias políticas de seguridad, con la finalidad de efectuar los objetivos estratégicos de la empresa editora de diario regional peruano. El modelo ad

hoc ha sido capaz de fomentar que los colaboradores de la empresa editora de diario regional robustezcan completamente las bases primordiales de la seguridad de la información.

En el ámbito social la presente investigación más allá de contribuir con la empresa en la protección de sus datos, ésta busca concientizar a los colaboradores de la empresa para que conozcan las medidas de protección y seguridad que deben adoptar para salvaguardar la información que ellos manejan diariamente.

Para instaurar políticas de seguridad en una mediana empresa, es necesario tener normativas y procesos que se puedan seguir para garantizar una adecuada protección de la información. Para ello existen metodologías de gestión de riesgos y normativas ISO, que ayudan enormemente a gestionar la protección de los datos dentro de una empresa, sin embargo, en la coyuntura nacional esto no se aplica, debido a que son densas teóricamente y aplicables para otras realidades empresariales.

El trabajo de investigación realizado servirá como modelo para futuras investigaciones e implementaciones de normativas y políticas de seguridad en medianas empresas cuya percepción de seguridad de la información sea prácticamente nula.

La presente investigación tiene como finalidad permitir que la empresa editora de diario regional peruano mejore su enfoque respecto a la seguridad de la información, teniendo políticas de seguridad que salvaguarden la misma, del mismo modo evitar pérdidas de datos y robustecer el área de TI en dicha empresa.

1.6. Hipótesis.

Mediante la aplicación de un modelo ad hoc se mejora la gestión de la seguridad de la información en una empresa editora de diarios regionales peruanos.

1.7. Objetivos.

1.7.1. Objetivo general.

Desarrollar un modelo ad hoc de gestión de la seguridad de la información para una empresa editora de diarios regionales peruanos.

1.7.2. Objetivos específicos.

a) Diagnosticar el estado actual de la seguridad de la información en la empresa editora de diarios regionales previamente seleccionada.

b) Elaborar un modelo de seguridad de la información que más se adecue a la realidad de la empresa.

c) Implementar un modelo apropiado para la aplicación de la norma ISO/IEC 27001.

d) Evaluar los resultados del modelo de gestión de seguridad de la información desarrollado en la empresa editora de diarios regionales seleccionada.

II. MATERIAL Y MÉTODO

2.1. Tipo y Diseño de Investigación.

Cuantitativa -- > cuasiexperimental

2.2. Población y muestra.

La unidad de análisis de esta investigación son los estándares relacionados con la gestión de seguridad de la información y las metodologías para gestión de riesgo, a continuación, se listará la población existente.

Población

1. Modelo de análisis y evaluación de riesgos enfocado a la seguridad de la información referenciado en la norma ISO/IEC 27001 y metodología Magerit para gestión de riesgos.

2. Modelo de análisis y evaluación de riesgos enfocado a la seguridad de la información referenciado en la norma ISO/IEC 27001 y metodología Octave para gestión de riesgos.

3. Modelo basado en la metodología PDCA ISO 27001/2005 para el desarrollo e implementación de un modelo ad hoc para la administración de la seguridad de la información y metodología Magerit para gestión de riesgos.

4. Modelo basado en la metodología PDCA ISO 27001/2005 para el desarrollo e implementación de un modelo ad hoc para la gestión de la seguridad de la información y metodología Octave para gestión de riesgos.

Muestra

Para la correcta elección de la muestra, se realizó un muestreo no probabilístico por conveniencia, de tal manera que se tomaron los 4 modelos encontrados, se analizaron y se tomaron en cuenta los que más se adecuaron a la empresa.

Estándares para la gestión de seguridad de la información y metodologías para gestión de riesgo

Estándares y metodologías	País de origen de la metodología para gestión de riesgo	Entorno	Finalidad	Referencias
Norma ISO/IEC 27001 y metodología Magerit para	España	Medianas y grandes organizaciones	Análisis de los riesgos en los sistemas de seguridad informática	Martha, H. (2020)

gestión de riesgos.			para descubrirlos oportunamente.	
Norma ISO/IEC 27001 y metodología Octave para gestión de riesgos.	Estados Unidos	Pequeñas y medianas organizaciones	Permite que las personas se involucren en las estrategias de protección de la información.	Martha, H. (2020)
PDCA ISO 27001/2005 para el desarrollo e implementación de un SGSI y metodología Magerit para gestión de riesgos.	España	Medianas y grandes organizaciones	Análisis de los riesgos en los sistemas de seguridad informática para descubrirlos oportunamente.	Martha, H. (2020)
PDCA ISO 27001/2005 para el desarrollo e implementación de un SGSI y metodología Octave para gestión de riesgos.	Estados Unidos	Pequeñas y medianas organizaciones	Permite que las personas se involucren en las estrategias de protección de la información.	Martha, H. (2020)

Según el análisis se determinó que de acuerdo a selección por conveniencia se seleccionó un modelo con su respectiva metodología para gestión de riesgos, se descartó trabajar con ciclos PDCA debido a que no se encontró literatura en la cual hable de la eficiencia al aplicar esta metodología.

1. Modelo de análisis y evaluación de riesgos enfocado a la seguridad de la información referenciado en la norma ISO/IEC 27001 y metodología Magerit para gestión de riesgos.

2.3. Variables, Operacionalización.

La variable independiente es el modelo ad hoc de gestión de la seguridad de la información. Mientras que la variable dependiente es la gestión de la seguridad de la información.

Variables	Dimensión	Indicador	Ítem	Técnica e instrumentos de recolección de datos
Modelo de gestión de la seguridad de la información. (VI)	Modelo de gestión de la seguridad de la información.	Nivel de cubrimiento del modelo ad hoc en activos de información.	(ACS/TAO)*100 Variables que participan: ACS, TAO	Alcance del modelo ad hoc, Inventario de activos, Observación.
		Porcentaje de aplicación del plan de sensibilización.	(NFSP/TPC)*100 Variables que participan: NFSP, TPC	Total de trabajadores en la empresa. Observación
		Porcentaje de tratamiento de sucesos de seguridad y privacidad de los datos	(CIC/CIE)*100 Variables que participan: CIC, CIE	Auditoria interna y observación.
Gestión de la	Gestión de la	Estado de	R = 1 (SÍ se	

seguridad de información. (VD)	seguridad de la información.	cumplimiento de políticas de seguridad de la información en la empresa.	evidencia) R = 0 (NO se evidencia) Variables que participan: EPGSI, DACPI, ERLSPI	Usuarios. Observación.
		Categoría de la seguridad de la información y los equipos de cómputo.	R = 1 (SÍ se evidencia) R = 0 (NO se evidencia) Variables que participan: LRSTCPS ,ENPIF	Usuarios. Observación y entrevista.
		Categoría de verificación de Acceso lógico.	R = 1 (SÍ se evidencia) R = 0 (NO se evidencia) Variables que participan: NAUAS, ECAUA, ENCDM	Usuarios. Observación y entrevista.
		Porcentaje de implementación de controles.	(NCI/NCPI)*100 Variables que participan: NCI, NCPI	Plan de Tratamiento de Riesgos. Observación.

	Evidencia de ataques informáticos a la empresa.	R = 1 (SÍ se evidencia) R = 0 (NO se evidencia) Variables que participan: EAIUA, AIUNPE	Observación y reporte de incidencias.
	Categoría de verificación de la políticas de integridad de la información.	R = 1 (SÍ se evidencia) R = 0 (NO se evidencia) Variables que participan: ELMEI, ELRIM	Usuario. Observación.

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

TECNICA	INSTRUMENTO	INTRUMENTO DE REGISTRO	DETALLE
Análisis documental	Fichas bibliográficas − Referencia	Formato de citas y referencia bibliográfica de esta investigación.	Análisis de material impreso y digital.
Entrevista	Guía de entrevista (Cuestionarios)	Formato: Anexo A	Se realizará entrevistas a los colaboradores para conocer su opinión sobre la seguridad de información.

Encuesta	Cuestionario	Formato: Anexo B, C, D.	Se utilizara esta técnica para recopilar información sobre la naturaleza de la seguridad de la información.
Internet	Fichas bibliográficas - Referencia	Referencia bibliográfica de esta investigación	Se utilizará está técnica para búsqueda de libros, revistas, etc.

2.5. Procedimiento de análisis de datos.

Para el adecuado procesamiento y caracterización de datos se utilizará la herramienta Microsoft Excel, conjuntamente con el software de pago SPSS. Para realizar las validaciones de las encuestas aplicadas.

Para el indicador nivel de cubrimiento del modelo ad hoc en activos de información se necesitan dos variables, ACS y TAO las cuales representan lo siguiente:

Activos cubiertos por el sistema = ACS

Total de activos de la organización = TAO

Formula:

Nivel de cubrimiento del modelo ad hoc = (ACS/TAO) * 100

El resultado de esta operación mostrara el porcentaje de nivel de cubrimiento del modelo ad hoc en los activos de información de la empresa.

Para el indicador porcentaje de aplicación del plan de sensibilización se necesitan dos variables, las cuales se detallan a continuación:

Número de fallas encontradas en las sensibilizaciones programadas = NFSP

Total de personal a capacitar = TPC

Formula:

Porcentaje de aplicación del plan de sensibilización = (NFSP/TPC) * 100
El resultado de la formula será el porcentaje del plan de sensibilización para el personal de la empresa.

Para el indicador de porcentaje de tratamiento de sucesos de seguridad y privacidad de los datos se establecen las siguientes variables:
Cantidad de irregularidades concluidas = CIC
Cantidad de irregularidades encontradas = CIE
Formula:
(CIC/CIE) * 100
El resultado de esta fórmula es el porcentaje de tratamiento de sucesos de seguridad y privacidad de los datos.

Para el indicador estado del cumplimiento de políticas de seguridad en la empresa se utilizarán tres variables con valores dicotómicos, a continuación, se presentarán las variables:
La empresa tiene definido una política general de seguridad de la información = EPGSI
La empresa documenta las actividades de control y protección de la información = DACPI
La empresa cumple con requisitos legales de seguridad y protección de información = ERLSPI
Formula:
EPGSI = 0; EPGSI = 1
DACPI = 0; DACPI = 1
ERLSPI = 0; ERLSPI = 1
En donde el valor 0 representa a una respuesta negativa y el valor 1 representa una respuesta positiva.

Para el indicador Categoría de la seguridad de información y los equipos de cómputo posee dos variables dicotómicas que se explicaran a continuación:
La empresa tiene lineamientos a través del responsable de seguridad para que los trabajadores cumplan las políticas de seguridad = LRSTCPS
La empresa tiene normas para la protección de instalaciones físicas = ENPIF

Formula:
LRSTCPS = 0; LRSTCPS = 1
ENPIF = 0; ENPIF = 1
En donde el valor 0 representa a una respuesta negativa y el valor 1 representa una respuesta positiva.

Para el indicador Categoría de verificación de Acceso lógico tiene tres variables con valores dicotómicos a continuación se especifican:
La empresa tiene normas para controlar el acceso de los usuarios a datos almacenados en los servidores = NAUAS
La empresa tiene estándares para controlar el acceso y uso a las aplicaciones de la empresa = ECAUA
La empresa tiene normas para controlar dispositivos móviles = ENCDM
Formula:
NAUAS = 0; NAUAS = 1
ECAUA = 0; ECAUA = 1
ENCDM = 0; ENCDM = 1
En donde el valor 0 representa a una respuesta negativa y el valor 1 representa una respuesta positiva.

Para el indicador porcentaje de implementación de controles se utilizan dos variables que se definirán a continuación:
Número de controles implementados = NCI
Número de controles que se planearon implementar = NCPI
Formula:
(NCI/NCPI) * 100
El resultado dará el porcentaje de implementación de controles de seguridad de la información.

Para el indicador evidencias de ataques informáticos a la empresa será necesario establecer dos variables con valores dicotómicos las cuales se definirán a continuación:
La empresa recibió ataques informáticos el último año = EAIUA

Ataques que impidieron el uso normal de los programas que posee la empresa = AIUNPE

Formula:

EAIUA = 0; EAIUA = 1

AIUNPE = 0; AIUNPE = 1

En donde el valor 0 representa a una respuesta negativa y el valor 1 representa una respuesta positiva.

Para el indicador Categoría de verificación de las políticas de integridad de la información se establecerán dos variables con valores dicotómicos las cuales se especificarán a continuación:

La empresa tiene lineamientos contra modificación o eliminación de información = ELMEI

La empresa tiene lineamientos para la recuperación de información malversada = ELRIM

Formula:

ELMEI = 0; ELMEI = 1

ELRIM = 0; ELRIM = 1

En donde el valor 0 representa a una respuesta negativa y el valor 1 representa una respuesta positiva.

2.6. Criterios éticos.

Toda la información proporcionada por la empresa, para fines de investigación en el presente trabajo de tesis, no debe prestarse para otros fines que no sean la de lograr resultados en el trabajo de investigación.

2.7. Criterios de Rigor Científico.

Para el presente trabajo de investigación se deben de tomar en cuenta los aspectos de credibilidad y confirmación, dos de los criterios de rigor científico que más se adecuan al presente trabajo. La credibilidad es la verdad sentida y expresada por todos los trabajadores de la empresa al momento de aplicárseles una encuesta o llenar un cuestionario. Por otro lado, la

confirmación hace referencia a las afirmaciones veraces y directas de lo que el investigador a percibido dentro del lugar de estudio, en este caso es una empresa editora de diario regional peruano.

III. RESULTADOS.

3.1. Resultados en Tablas y Figuras.

Como paso previo a la aplicación del modelo desarrollado y la instauración de las políticas de seguridad, se evidenció que la empresa no contaba con ninguna política de seguridad ni normativa que protejan la integridad y accesibilidad de su información.

Después de haber aplicado las políticas de seguridad en la empresa editora de diario regional peruano, se procedió a realizar el cálculo de los indicadores previamente seleccionados.

En primer lugar, el indicador denominado nivel de cubrimiento del modelo ad hoc en activos de información, tiene dos variables, ACS y TAO, las cuales se detallaron a continuación.

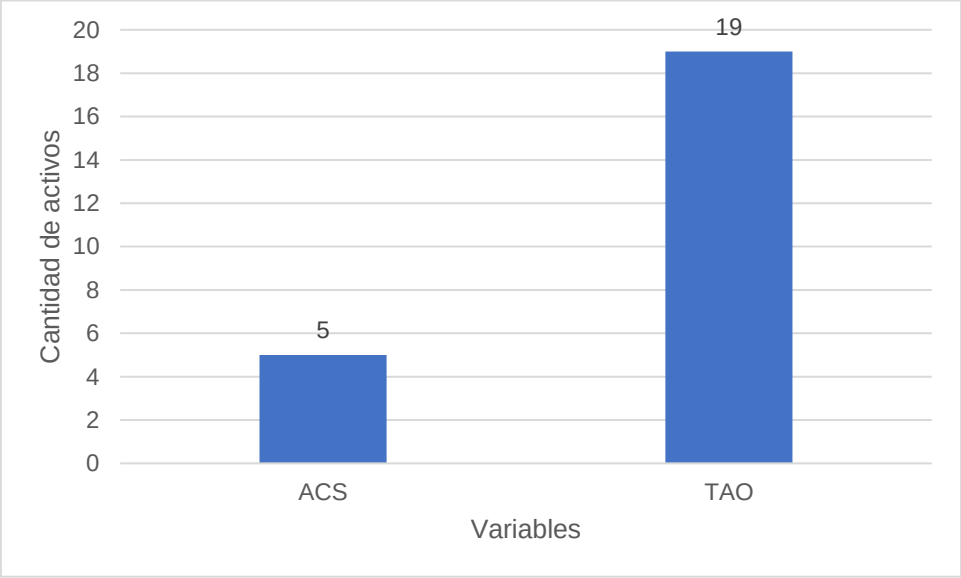


Figura 2. Representación en grafico de barras del nivel de cubrimiento del modelo ad hoc en activos de información. Fuente: *Elaboración propia.*

ACS = Activos cubiertos por el sistema
TAO = Total de activos de la organización

Resultado
ACS = 5
TAO = 19
(5/19)*100 = 26.32%

Después de haber analizado el resultado se evidenció que el nivel de cubrimiento del modelo ad hoc desarrollado alcanza un 26.32%, este resultado evidenció que la empresa mejoró la gestión de la seguridad de información. Cabe señalar que los datos que pertenecen a los activos cubiertos por el sistema y el total de activos que posee la empresa, fueron extraídos gracias a revisión documental proporcionada por la empresa. Posteriormente se calculó el porcentaje de aplicación del plan de sensibilización, el cual tiene dos variables NFSP y TPC que se detallan a continuación.

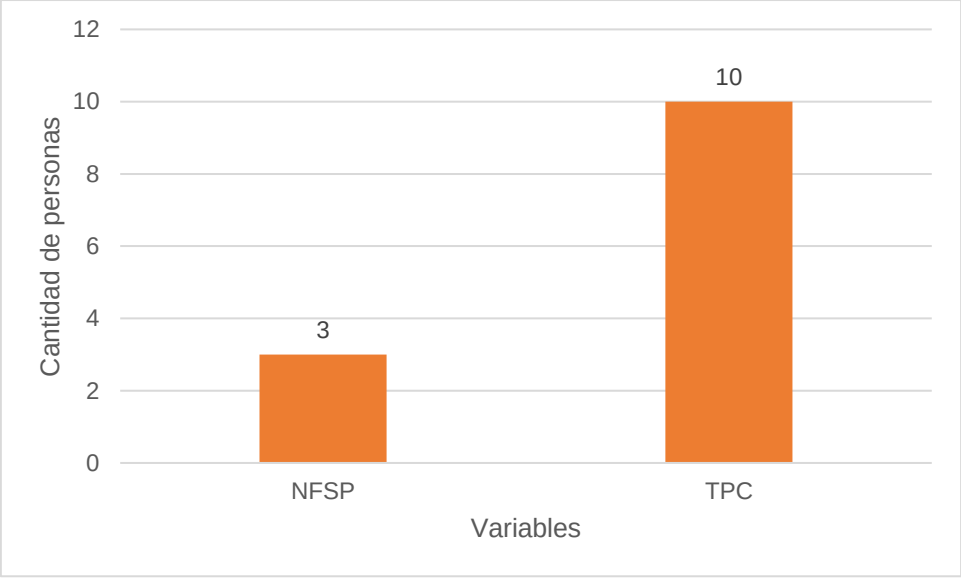


Figura 3. Representación en grafico de barras del porcentaje de aplicación del plan de sensibilización. Fuente: *Elaboración propia.*

NFSP = Número de fallas encontradas en las sensibilizaciones programadas
TPC = Total de personal a capacitar

Resultado

NFSP = 3

TPC = 10

(3/10) * 100 = 30%

Esto demuestra que el plan de sensibilización alcanzo un 30%, teniendo en cuenta que hay trabajadores que se negaron a ser capacitados y omiten los consejos y orientaciones que se les brindo acerca de los riesgos de perdida de información que pueden ocurrir dentro de la empresa. Los datos del número de fallas encontradas en las sensibilizaciones programadas y el total de personal a capacitar fueron procesados a partir de la aplicación de encuestas al personal que trabaja en la empresa. Después de tener esta información se tomó en cuenta el indicador denominado porcentaje de tratamiento de sucesos de seguridad y privacidad de los datos, para la caracterización de este indicador se emplearon dos variables CIC y CIE, las cuales se detallarán a continuación.

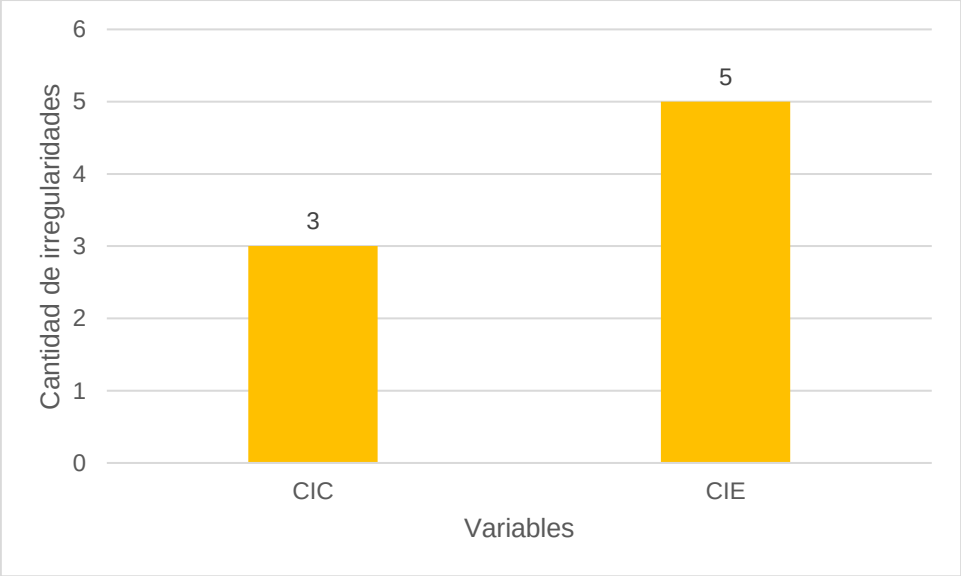


Figura 4. Representación en grafico de barras del porcentaje de tratamiento de sucesos de seguridad y privacidad de los datos Fuente: *Elaboración propia.*

CIC = Cantidad de irregularidades concluidas.

CIE = Cantidad de irregularidades encontradas.

Resultado

CIC = 3

CIE = 5

(3/5) * 100 = 60%

Es importante señalar que un 60% corresponde al porcentaje de tratamiento de sucesos de seguridad y privacidad de los datos, esto se logró contabilizando el total de irregularidades encontradas y hallando la cantidad de irregularidades concluidas, es decir defectos en el entorno de seguridad e integridad de la información que tuvo la empresa. Para la recolección de datos se utilizó revisión documental de carácter virtual, ya que las irregularidades se presentaron en gran parte de los softwares que utiliza la empresa. Seguidamente se procedió a evaluar el estado del cumplimiento de políticas de seguridad en la empresa, para ellos se utilizaron tres variables, EPGSI, DACPI, ERLSPI, las cuales se describirán a continuación.

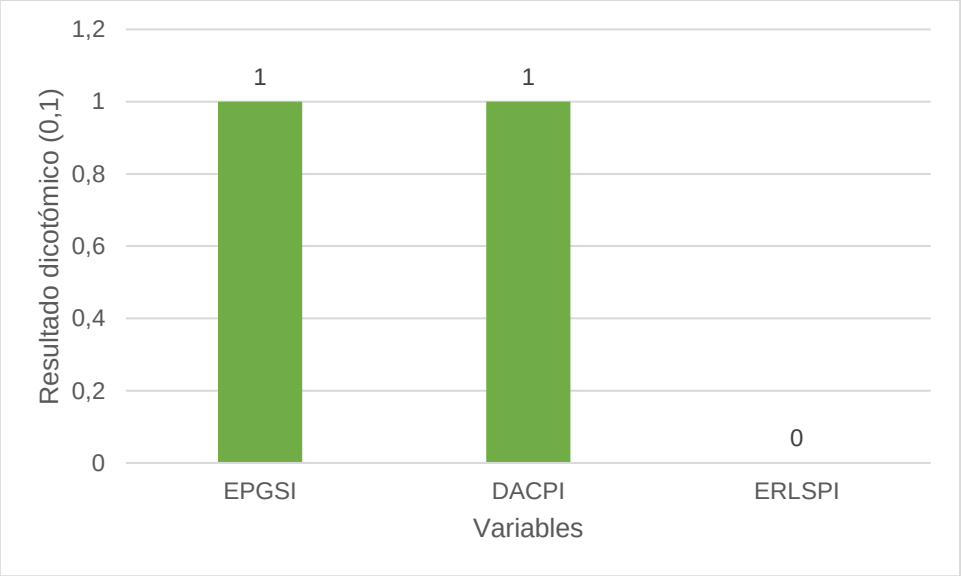


Figura 5. Representación en grafico de barras del nivel de cumplimiento de políticas de seguridad en la empresa. Fuente: *Elaboración propia.*

EPGSI = La empresa tiene definido una política general de seguridad de la información.

DACPI = La empresa documenta las actividades de control y protección de la información.
ERLSPI = La empresa cumple con requisitos legales de seguridad y protección de información.

Resultado
EPGSI = 1
DACPI = 1
ERLSPI = 0

Es preciso señalar que después de haber implementado las políticas de seguridad le empresa cuenta con esta información y a su vez posee un cronograma de actividades de control y supervisión, que ayudan a seguir con el cuidado y protección a los distintos activos de la empresa. Para esto se procedió a revisar los documentos que avalan que efectivamente, la empresa cuenta con documentación de todas las actividades que realiza para proteger su información contable, publicitaria y administrativa. Seguidamente se procedió a evaluar el Categoría de la seguridad de información y los equipos de cómputo, este indicador presenta dos variables, LRSTCPS y ENPIF, las cuales se detallan a continuación.

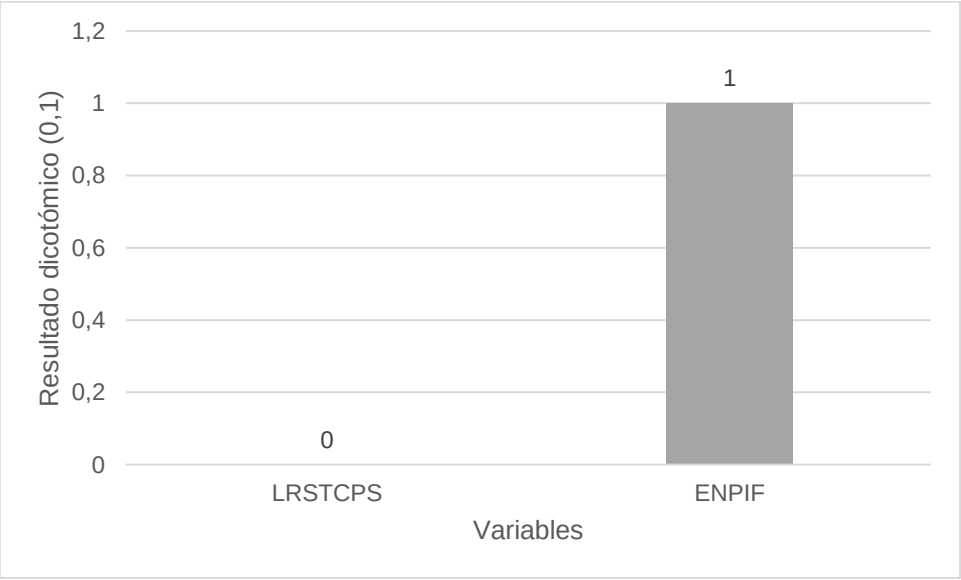


Figura 6. Representación en grafico de barras del Categoría de la seguridad de información y los equipos de cómputo. Fuente: *Elaboración propia.*

LRSTCPS = La empresa tiene lineamientos los cuales están a cargo del encargado de TI, y a su vez hace cumplir las políticas de seguridad a los trabajadores.
ENPIF = La empresa tiene normas para la protección de instalaciones físicas.

Resultados
LRSTCPS = 0
ENPIF = 1

De acuerdo a la medición del presente indicador, se evidencio que la empresa no cuenta con un responsable que supervise a los trabajadores para que efectúen las políticas de seguridad, sin embargo, la empresa posee normas para la protección de sus instalaciones físicas, como SAI y dispositivos anti incendios. Esta información se extrajo gracias a la observación. Para la interpretación del Categoría de verificación de Acceso lógico se necesitaron tres variables, NAUAS, ECAUA y ENCDM, las cuales se detallan a continuación.

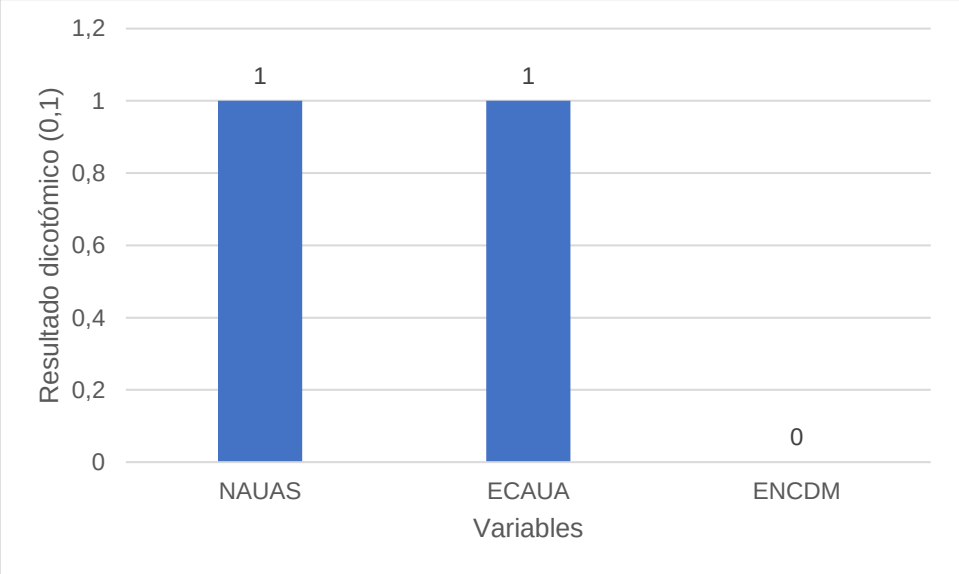


Figura 7. Representación en grafico de barras del Categoría de verificación de Acceso lógico. Fuente: *Elaboración propia.*

NAUAS = La empresa tiene normas para controlar el acceso de los usuarios a datos almacenados en los servidores.
ECAUA = La empresa tiene estándares para controlar el acceso y uso a las aplicaciones de la empresa.
ENCDM = La empresa tiene normas para controlar dispositivos móviles.

Resultado
NAUAS = 1
ECAUA = 1
ENCDM = 0

Después de haber aplicado las políticas de seguridad, los usuarios solo pueden acceder a sus aplicaciones predeterminadas por la empresa, cada área de trabajo tiene sus aplicaciones propias, de esta manera se asegura que no haya inconvenientes al momento de gestionar información sensible, como Información de facturación. La obtención de estos datos fue gracias a la observación y revisión documentaria, estas técnicas permitieron recolectar los datos pertinentes para poder caracterizar el indicador en cuestión. Posteriormente se optó por revisar el porcentaje de implementación de controles, para esto se utilizaron dos variables, NCI y NCPI, que a continuación se detallan.

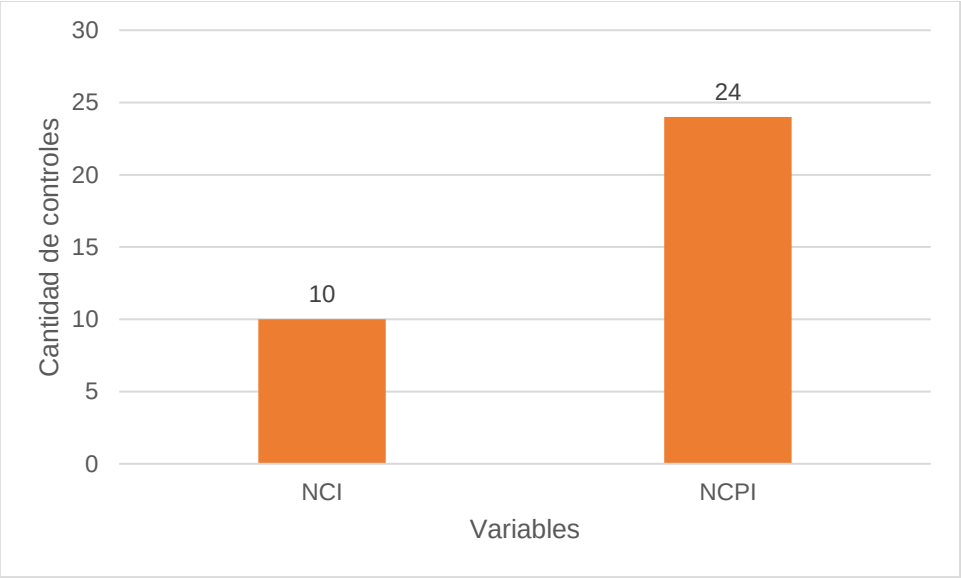


Figura 8. Representación en grafico de barras del porcentaje de implementación de controles de seguridad. Fuente: *Elaboración propia.*

NCI = Número de controles implementados.
NCPI = Número de controles que se planearon implementar.

Resultado
NCI = 10
NCPI = 24
(10/24) * 100 = 41.6%

Según el indicador un 41.6% es el porcentaje de controles implementados, esto debido a que la empresa solicito implementar los controles que sean importantes de acuerdo a la realidad empresarial. Sin embargo, los demás controles están definidos en la presente investigación, los cuales servirán para ser implementados posteriormente. Para llegar a este resultado fue necesario recolectar información documental que permita conocer el número de controles implementados y también el número de controles que se planearon implementar. Seguidamente se evaluó el indicador denominado evidencias de ataques informáticos a la empresa, para realizar el cálculo de este indicador fueron necesarias dos variables, EAIUA y AIUNPE, detalladas a continuación.

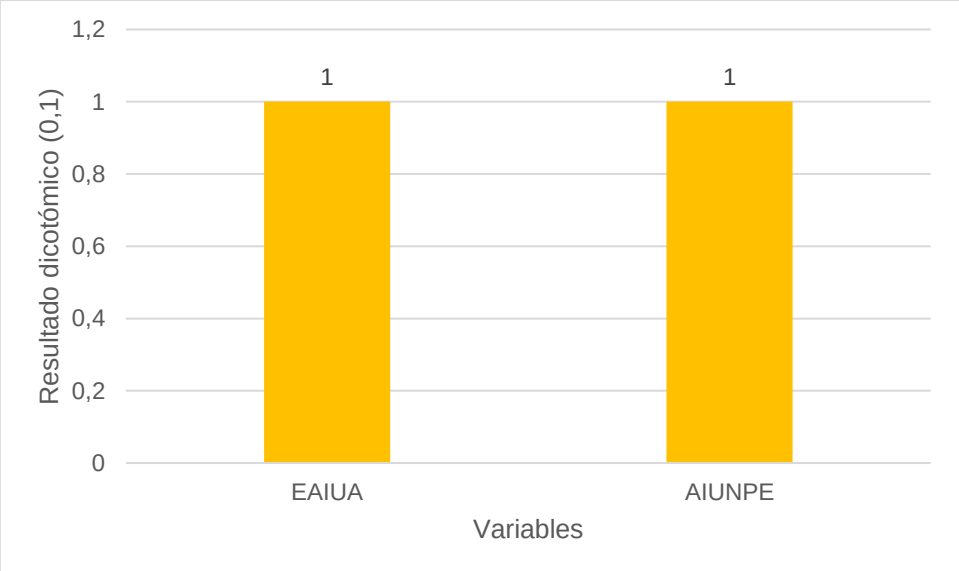


Figura 9. Representación en grafico de barras de evidencias de ataques informáticos a la empresa. Fuente: *Elaboración propia.*

EAIUA = La empresa recibió ataques informáticos el último año.
AIUNPE = Ataques que impidieron el uso normal de los programas que posee la empresa.

Resultado
EAIUA = 1
AIUNPE = 1

En el año 2021, se evidenciaron dos ataques informáticos de regular intensidad, estos provinieron de usuarios que descargaron malware y software mal intencionado, que, al estar todas las computadoras en red, afectaron a gran parte de los activos tecnológicos, en especial al servidor SAP, servidor encargado de almacenar datos sensibles de facturación. Sin embargo, estos problemas fueron resueltos y actualmente gracias a las políticas implementadas no se ha registrado ningún otro ataque hasta el momento. Para recopilar esta información fue necesario revisar los archivos .log del antivirus que utilizo el servidor en ese entonces, cuando sucedió el ataque por parte de virus de tipo malware. Posteriormente se evaluó el Categoría de verificación de las políticas de integridad de la información para cumplir dicho cometido es necesario utilizar dos variables, ELMEI y ELRIM, las cuales se detallarán a continuación.

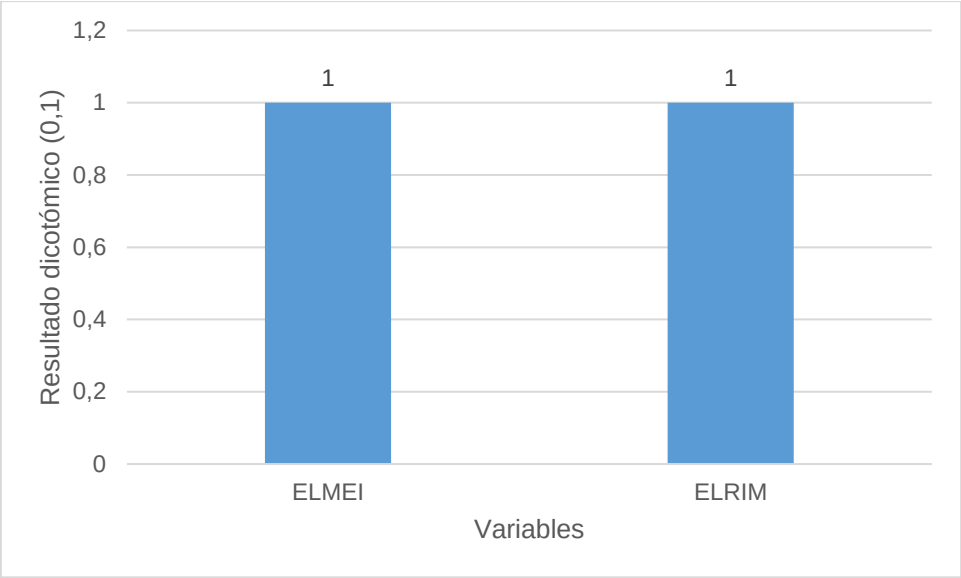


Figura 10. Representación en grafico de barras del Categoría de verificación de las políticas de integridad de la información. Fuente: *Elaboración propia.*

ELMEI = La empresa tiene lineamientos contra modificación o eliminación de información.
ELRIM = La empresa tiene lineamientos para la recuperación de información malversada.

Resultado
ELMEI = 1
ELRIM = 1

Gracias a las políticas implementadas la empresa cuenta con distintos backups que le permiten respaldar su información valiosa, en tal sentido como se aprecia el resultado de este indicador, se considera muy importante tener la información en otro lugar, para que, de esta manera, si llegase a suceder algún contratiempo, poder salvaguardar la información y evitar pérdidas económicas a la empresa. Para el desarrollo de este indicador fue necesario obtener información a través de la ficha de observación y ficha de revisión documental virtual.

3.2. Discusión de resultados.

Según Chan et al., (2005) obtuvo como resultado un 26.5% de Categoría de aceptación de un SGSI para los colaboradores de la empresa, en la presente investigación se obtuvo como resultado un 24.6% de Categoría de implementación del modelo ad hoc para la gestión de la seguridad de la información, dejando en claro que a pedido de la empresa solo se aplicaron las políticas de seguridad prioritarias. Teniendo en cuenta a este autor es claro que ha cierta similitud en los porcentajes.

Para Tagarev, (2012) realizar un ciclo de mejora continua resulto positivo, después de implementar un SGSI, así como también es partidario de que las políticas de seguridad deben ser implementadas de acuerdo al escenario donde se van a desarrollar, en tal medida la empresa editora de diario regional peruano cumple con tener definida las políticas de seguridad que más se adecuen a sus necesidades, tal como lo demuestra el indicador estado de cumplimiento de políticas de seguridad en la empresa.

La capacitación a los colaboradores de una empresa, resulta ser esencial para el cumplimiento delas políticas de seguridad establecida, tal como lo afirma (Ahmad Z., Song T., Hui T., & Norhashim M., 2019). De esta manera haciendo un símil con la investigación realizada, un 30% del personal de la empresa no han acogido las capacitaciones brindadas acerca de la implementación de políticas de seguridad, esto, de acuerdo al resultado del indicador denominado porcentaje de aplicación del plan de sensibilización.

3.3. Aporte práctico.

3.3.1. Diagnosticar el estado actual de la seguridad de la información en la empresa editora de diarios regionales previamente seleccionada.

Para la elección de la empresa en la cual se realizó la implementación de un modelo ad hoc para la gestión de la seguridad de la información. Se tuvo que llevar a cabo un proceso de selección, el cual se describirá a continuación.

En primer lugar, se listó a todos los diarios que se encuentran ubicados en la ciudad de Chiclayo, posteriormente se establecieron tres criterios de evaluación, los cuales son: Procesos, uso de tecnologías y accesibilidad a datos, siento este último criterio, determinante para de esta manera poder implementar correctamente el modelo ad hoc.

Tabla 1.

Relación de empresas editoras de diario en Chiclayo, caracterizadas por sus procesos, uso de tecnologías y accesibilidad a datos.

Empresas editoras de diario en Chiclayo	**Procesos**	**Uso de tecnologías**	**Accesibilidad a datos**
Empresa editora La Industria de Chiclayo S.A.	Compra, Venta, Distribución, Edición.	SAP Bussisnes One; Software de terceros	Permitido
Diario La Verdad	Venta, Distribución.	Redes sociales	Restringido
Diario Oficial El Peruano	Venta, Distribución.	Redes sociales	Restringido
Grupo La Republica	Compra, Venta, Distribución, Edición.	SAP Bussisnes ONE	Restringido
Diario Correo	Venta, Distribución.	Redes sociales	Restringido

Fuente: Elaboración propia.

La empresa editora La Industria de Chiclayo se dedica al rubro de contenidos impresos, de esta manera es importante destacar que los principales activos de información que maneja el área de sistemas y soporte técnico de mencionada empresa están divididos en las siguientes áreas:

Tabla 2.

Tipos de información según las áreas de la empresa.

Tipos de información	
Área	**Descripción**

Información de clientes.	Información y documentos relacionados todos los clientes que tienen un convenio con la empresa.
Información administrativa.	Información usada para el área administrativa, tales como documentos periodísticos, información contable y documentos de gestión interna.
Información relacionada con otras actividades.	Información de sorteos, servicio a la comunidad o actividades fuera del rubro de la empresa.

Fuente: Elaboración propia

La empresa editora La Industria de Chiclayo maneja información de carácter importante, no solo las notas periodísticas, sino que también maneja información de clientes, facturaciones y publicidad en general. Por tal motivo se considera proteger lo siguiente:

- Datos
- Hardware
- Redes de comunicaciones
- Soportes de información
- Software

La empresa en cuestión trabaja con dos tipos de software, uno bajo licencia y otro fue desarrollado por un colaborador externo, es preciso señalar que ambos aplicativos manejan información que resulta de suma importancia para el área de gerencia, ya que esta información permite realizar una correcta toma de decisiones para decidir las futuras estrategias que utilizara la empresa.

Tabla 3.

Caracterización de los sistemas informáticos de la empresa.

Caracterización de los sistemas informáticos	
SAP Business ONE	**Control de movilidades**
Software que trabaja en red local, teniendo un servidor dedicado.	Software de tipo app web que trabaja alojado en una PC, con el programa XAMPP.
Licencia vencida.	No posee licencia.
Versión 2008.	Versión 2014.
Software de pago.	Software gratuito.

Fuente: Elaboración propia

Es oportuno señalar que Magerit brinda una serie de categorías que sirven para identificar de manera clara las amenazas que puedan ocurrir dentro de una organización, a continuación, se listan con su respectiva descripción.

Tabla 4.

Identificación de amenazas con su respectiva descripción.

Identificación de amenazas	
Categoría de amenaza	**Descripción**
Desastres naturales.	Circunstancias que se presentan debido a fenómenos naturales.
Origen industrial.	Sucesos que ocurren accidentalmente debido a actividades humanas.
Descuidos no intencionados.	Descuidos involuntarios causados directamente por las actividades de personas con acceso a los sistemas de información.
Ataques intencionados	Fallos intencionales provocados por la actividad humana.

Nota: Tomado de Ministerio de Hacienda y Administraciones Publicas (2012)

Tomando en cuenta el listado de amenazas propuesto por Magerit, se procedió a recolectar información acerca de las posibles amenazas que puedan afectar a la empresa editora de diario regional peruano, así mismo se caracterizó también los activos afectados y su degradación, la cual está clasificada en cuatro apartados (Confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad) representadas cada una por su letra inicial en mayúscula, de igual manera cada activo está identificado con una letra MA (Muy alta), A (Alta), M (Media), B (Baja), MB (Muy baja) que representa la probabilidad de afectación de ese activo.

Desastres naturales

Tabla 5.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Fuego	
Detalle: Incendio. Probabilidad que las llamas destruyan información tangible de la empresa. **Posibilidad:** Muy Baja	
Activos perjudicados	
Nombre	**Degeneración**
	Dis.
HW1 - Servidor Baltazar	MA
HW2 - Servidor SAP	A
HW3 - Servidor Fileserver	MA
HW4 - Servidor Administrativo	A
HW5 - PC sistemas	MA
Media1 - Disco duro de administración	A
Media2 - Archivos físicos	M

Fuente: Elaboración propia.

Tabla 6.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Agua	
Detalle: Inundación. Puede causar daños irreparables a la información que se encuentra de manera física en la empresa. **Posibilidad:** Muy Baja	
Activos perjudicados	
Nombre	**Degeneración Dis.**
HW1 - Servidor Baltazar	A
HW2 - Servidor SAP	MA
HW3 - Servidor Fileserver	A
HW4 - Servidor Administrativo	MA
HW5 - PC sistemas	M
Media1 - Disco duro de Administración	A
Media2 - Archivos físicos	M

Fuente: Elaboración propia.

Origen industrial

Tabla 7.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Alteración mecánica

Detalle: Daños causados por la suciedad, vibraciones, etc. **Posibilidad:** Alta

Activos perjudicados	
Nombre	**Degeneración**
	Dis.
HW1 - Servidor Baltazar	M
HW2 - Servidor SAP	B
HW3 - Servidor Fileserver	M
HW4 - Servidor Administrativo	MB
Media1 - Disco duro de Administración	MB

Fuente: Elaboración propia.

Tabla 8.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Alteración electromagnética
Detalle: Daños causados por campos electromagnéticos o luz ultra violeta. **Posibilidad:** Baja

Activos perjudicados	
Nombre	**Degeneración**
	Dis.
HW5 - PC sistemas	M

Fuente: Elaboración propia.

Tabla 9.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Corte de la energía eléctrica	
Detalle: Corte de la energía eléctrica.	
Posibilidad: Media	
Activos perjudicados	
Nombre	**Degeneración Dis.**
HW1 - Servidor Baltazar	M
HW2 - Servidor SAP	MB
HW4 - Servidor Administrativo	MB
Media1 - Almacenamiento del área de administración y contabilidad	A

Fuente: Elaboración propia.

Tabla 10.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Fallo de comunicaciones
Detalle: Fallo en la red de transmisión de datos.
Posibilidad: Media

Activos perjudicados	
Nombre	**Degeneración Dis.**
COM1 - Telefonía	A
COM2 - Wifi	A
COM3 - ADSL	MA

Fuente: Elaboración propia.

Tabla 11.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Degradación de soportes
Detalle: Fallos en los dispositivos que brindan información al usuario. **Posibilidad:** Alta

Activos perjudicados	
Nombre	**Degeneración Dis.**
Media1 - Almacenamiento del área de administración y contabilidad y contabilidad	A
Media3 - USB	MB

Fuente: Elaboración propia.

Errores y fallos no intencionados

Tabla 12.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Fallos de usuarios

Detalle: Fallos de los colaboradores al usar el software de la empresa. **Posibilidad:** Muy Alta

Activos perjudicados			
Nombre	**Degeneración**		
	Conf.	**Int.**	**Dis.**
D1 - Información de facturación	MA	A	M
D2 - Documentos pediodísticos	M	A	MB
S1 - Web	MB	MB	MB
S2 - Correo gmail	A	MB	MB
SW1 - SAP Busisness ONE	MB	A	MB
SW2 - Web de movilidad	M	A	MB
Media1 - Almacenamiento del área de administración y contabilidad	MB	M	M
Media3 - USB	A	MB	M
Media2 - Archivos físicos	A	MB	A

Fuente: Elaboración propia.

Tabla 13.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Errores de administrador
Detalle: Fallos de trabajadores encargados de instalación de programas y acceso a data.

Posibilidad: Medio

Activos perjudicados			
Nombre	**Degeneración**		
	Conf.	**Int.**	**Dis.**
S1 - Web			MB
SW1 - SAP Busisness ONE	M	A	MB
SW2 - Web de movilidad	M	A	MB
HW4 - Servidor Administrativo			A
COM2 - Red Wifi			MB

Fuente: Elaboración propia.

Tabla 14:

Caracterización de las amenazas probables que pueden afectar a la empresa.

Desperfectos en la empresa
Detalle: Fallos en las actividades que le corresponde a cada trabajador.
Posibilidad: Muy Alta

Activos perjudicados	
Nombre	**Degeneración**
	Dis.
P1 - Trabajador de sistemas	A
P2 - Trabajador administrativo y logístico	A

Fuente: Elaboración propia.

Tabla 15.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Escape de información		
Detalle: Divulgación de información confidencial.		
Posibilidad: Media		
Activos perjudicados		
Nombre	**Degeneración**	
	Conf.	
D1 - Información de facturación	MA	
D2 - Expediente periodístico	MA	

Fuente: Elaboración propia.

Tabla 16.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Debilidades de los programas			
Detalle: Errores de código fuente.			
Posibilidad: Baja			
Activos perjudicados			
Nombre	**Degeneración**		
	Conf.	**Int.**	**Dis.**
SW2 - Web de movilidad	MA	B	MB
SW1 - SAP Busisness ONE	MA	B	MB
SW3 - Cliente de correo	A	MB	B

Fuente: Elaboración propia.

Tabla 17.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Colapso del sistema por fallo de dispositivos	
Detalle: Recursos insuficientes en servidores. **Posibilidad:** Baja	
Activos perjudicados	
Nombre	**Degeneración**
	Dis.
S1 - Web	MA
HW4 - Servidor Administrativo	MA

Fuente: Elaboración propia.

Tabla 18.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Equipos extraviados		
Detalle: El robo, o la perdida de bienes genera desconfianza en los trabajadores de la empresa. **Posibilidad:** Media		
Activos perjudicados		
Nombre	**Degeneración**	
	Conf.	**Dis.**
HW3 - Servidor Fileserver	MB	MB
HW4 – Servidor Administrativo	B	B
Media3 - Almacenamiento USB	MA	B

Media2 - Archivos físicos	A	MA

Fuente: Elaboración propia.

Ataques intencionados

Tabla 19.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Usurpación de identidad		
Detalle: Personas externas consiguen tener acceso a credenciales autorizadas dentro de la empresa. **Posibilidad:** Muy Baja		
Activos perjudicados		
Nombre	**Degeneración**	
	Conf.	**Int.**
D1 - Información de facturación	B	B
D2 - Documentos pediodísticos	B	B
S2 - Correo gmail	MA	B
SW1 - SAP Busisness ONE	A	MA
SW2 - Web de movilidad	A	MA
COM2 - Red Wifi	MB	MB

Fuente: Elaboración propia.

Tabla 20.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Exceso de privilegios

Detalle: Trabajadores que modifican parámetros determinados por el sistema.

Posibilidad: Baja

Activos perjudicados

Nombre	**Degeneración**		
	Conf.	**Int.**	**Dis.**
D2 - Documentos pediodísticos	B	B	MB
SW1 - SAP Busisness ONE	MA	MB	MB
SW2 - Web de movilidad	A	B	B

Fuente: Elaboración propia.

Tabla 21.

Caracterización de las amenazas probables que pueden afectar a la empresa.

Acceso no vigilado

Detalle: Terceros intentan ingresar de forma fraudulenta a las computadoras de la empresa.

Posibilidad: Muy Baja

Activos perjudicados

Nombre	**Degeneración**	
	Conf.	**Int.**
D1 - Información de facturación	B	MB
D2 - Documentos periodísticos	B	M
S2 - Correo gmail	A	B

SW1 - SAP Busisness ONE	MA	MA
SW2 - Web de movilidad	MA	A
COM2 - Red Wifi	MB	MB

Fuente: Elaboración propia.

Tabla 22.

Frecuencia de amenazas según la metodología Magerit.

Frecuencia de la amenaza		
Valor	**Abreviatura**	**Detalle**
Muy Alta	MA	Diario
Alta	A	Una vez al mes
Media	M	Vez por año
Baja	B	Muchos años
Muy baja	MB	Siglo.

Nota: Tomado de Ministerio de Hacienda y Adminstraciones Públicas, (2012)

Posteriormente se realizó el diagnóstico de la seguridad de la información y a su vez se analizaron los riesgos sindicados a los procesos de la empresa y su entorno. Para ello es importante identificar todos los activos que maneja la empresa en el área de sistemas y soporte técnico, para poder crear una ficha digital que contenga el código del activo, nombre, descripción, tipo y sus Vinculación, es decir activos que dependen de él. También es necesario establecer un Categoría de probabilidad de que el activo pueda ser siniestrado por cualquiera de las amenazas anteriormente caracterizadas. Por ultimo dentro de cada ficha también se realizó una justificación de porque el activo debe estar considerado para esta investigación.

Catálogo de activos

Tabla 23.

Caracterización de activos pertenecientes a la empresa.

Datos					
Código: D1			**Nombre:** Información de facturación		
Detalle: Información del proceso de facturación.					
Tipo: Archivos					
Vinculación					
Activos: SW2			**Categoría:** Muy Alto		
Una vez concluido el periodo de facturación deben introducirse en la aplicación de Efact para que ellos tengan disponibilidad a estos datos.					
Activos: Media1			**Categoría:** Alto		
La información de facturación además de ser colocados en la web de Efact se guardan en los discos duros del área de contabilidad.					
Valor					
Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	Alto	Muy Alto	Bajo	Alto	Alto

Fuente: Elaboración propia.

Tabla 24.

Caracterización de activos pertenecientes a la empresa.

Datos					
Código: D2			**Nombre:** Documentos periodísticos		
Detalle: Información relacionada con los reportajes que se realizan para fines periodísticos.					
Tipo: Archivos					
Vinculación					
Activos: SW2			**Categoría:** Alto		

Todos los datos relacionados con los archivos periodísticos se deben almacenar en un servidor dedicado.

Valor

Total	**Confidencialidad**	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	Muy Alto	Alto	Medio	Alto	Medio

Fuente: Elaboración propia.

Tabla 25.

Caracterización de activos pertenecientes a la empresa.

Servicios	
Código: S1	**Nombre:** Servicio Web
Detalle: Página web del diario La Industria de Chiclayo. .	
Tipo: PHP y Mysql	
Vinculación	
Activos: HW1	**Categoría:** Muy Alto
La web está alojada en un servidor de terceros.	

Valor

Total	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Bajo	Alto	Bajo	Bajo

Fuente: Elaboración propia.

Tabla 26.

Caracterización de activos pertenecientes a la empresa.

Servicios	
Código: S2	**Nombre:** Correo electrónico gmail
Detalle: Correo gmail proporcionado por Xertica para todos los colaboradores de la empresa.	
Tipo: Interno, Email	

Vinculación			
Activos:		**Categoría:**	
Valor			
Total	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	Alto	Alto	Medio

Fuente: Elaboración propia.

Tabla 27.

Caracterización de activos pertenecientes a la empresa.

Software			
Código: SW1		**Nombre:** SAP Busisness ONE	
Detalle: Software de pago para la administración de la información contable de la empresa editora La Industria de Chiclayo.			
Tipo: Desarrollo genérico, Servidor de aplicaciones			
Vinculación			
Activos: COM2, COM3		**Categoría:** Muy Alto	
Para el uso de SAP Busisness ONE, no es necesario internet, pero está conectada a un servidor mediante red local.			
Valor			
Total	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Muy Alto	Muy Alto	Medio	Alto

Fuente: Elaboración propia.

Tabla 28.

Caracterización de activos pertenecientes a la empresa.

Software			
Código: SW2		**Nombre:** Web de movilidad	

Detalle: Herramienta web creada para que los periodistas ingresen sus movilidades, es decir registren el recorrido que hacen para ir al lugar de la noticia, así mismo se registran los pasajes y notas periodísticas a las cuales han sido asignados.

Tipo: Servidor de aplicaciones XAMPP

Vinculación

Activos: COM2, COM3 **Categoría:** Muy Alto

Aplicación web de movilidades, es prioritario tener conexión local.

Valor

Total	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Alto	Muy Alto	Medio	Alto

Fuente: Elaboración propia.

Tabla 29.

Caracterización de activos pertenecientes a la empresa.

Hardware			
Código: HW1		**Nombre:** Servidor Baltazar	
Detalle: Servidor donde se almacena información de periodistas, como galerías de fotos, notas de prensa entre otros.			
Ubicación: Área de sistemas y soporte técnico			
Tipo:			
Vinculación			
Activos:		**Categoría:**	
Valor			
Total	**Disponibilidad**		
Bajo	Medio		

Fuente: Elaboración propia.

Tabla 30.

Caracterización de activos pertenecientes a la empresa.

Hardware	
Código: HW2	**Nombre:** Servidor SAP
Detalle: Servidor donde se almacena el software SAP Busisness ONE, así mismo la base de datos SQL Server 2008.	
Ubicación: Área de sistemas y soporte técnico	
Tipo:	
Vinculación	
Activos:	**Categoría:**
Valor	
Total	**Disponibilidad**
Bajo	Medio

Fuente: Elaboración propia.

Tabla 31.

Caracterización de activos pertenecientes a la empresa.

Hardware	
Código: HW3	**Nombre:** Servidor Fileserver
Detalle: Servidor donde se almacena información sobre edición de noticias, plantillas de adobe indesing, entre otros archivos necesarios para la maquetación del periódico la industria.	
Ubicación: Área de sistemas y soporte técnico	
Tipo:	
Vinculación	
Activos:	**Categoría:**
Valor	
Total	**Disponibilidad**
Bajo	Medio

Fuente: Elaboración propia.

Tabla 32.

Caracterización de activos pertenecientes a la empresa.

Hardware	
Código: HW4	**Nombre:** Servidor Administrativo
Detalle: Servidor donde se almacena información contable, clientes, socios estratégicos e información gerencial.	
Ubicación: Área de sistemas y soporte técnico	
Tipo:	
Vinculación	
Activos:	**Categoría:**
Valor	
Total	**Disponibilidad**
Bajo	Medio

Fuente: Elaboración propia.

Tabla 33.

Caracterización de activos pertenecientes a la empresa.

Hardware	
Código: HW5	**Nombre:** PC sistemas
Detalle: PC que se dedica al host de la web de movilidades y también de la web de control de pesos de bobinas.	
Ubicación: Área de sistemas y soporte técnico	
Tipo:	
Vinculación	
Activos:	**Categoría:**

Valor	
Total	**Disponibilidad**
Bajo	Medio

Fuente: Elaboración propia.

Tabla 34.

Caracterización de activos pertenecientes a la empresa.

Redes	
Código: COM1	**Nombre:** Red telefónica
Detalle: Red telefónica en el área de publicidad.	
Ubicación: Publicidad	
Tipo: Telefonía	
Vinculación	
Activos:	**Categoría:**
Valor	
Total	**Disponibilidad**
Medio	Medio

Fuente: Elaboración propia.

Tabla 35.

Caracterización de activos pertenecientes a la empresa.

Redes	
Código: COM2	**Nombre:** Wifi
Detalle: El Wifi es usado por el área de publicidad, gerencia, redacción LI, redacción EN, diagramación y sistemas.	
Ubicación: Sistemas y soporte técnico	
Tipo: Wifi	
Vinculación	
Activos: HW4	**Categoría:** Muy Alto

Para que el wifi sea accesible desde los diferentes ambientes es
primordial la utilización del PC de sistemas.

Activos: HW5 **Categoría:** Muy Alto

Para acceder al wifi es indispensable el buen funcionamiento del router.

Valor

Total	**Disponibilidad**
Muy Alto	Muy Alto

Fuente: Elaboración propia.

Tabla 36.

Caracterización de activos pertenecientes a la empresa.

Servicio de comunicaciones	
Código: COM3	**Nombre:** Red ADSL
Detalle: Conexión ADSL.	
Ubicación: Área de sistemas y soporte técnico	
Tipo: Red	
Vinculación	
Activos: HW8	**Categoría:** Muy Alto
El servicio ADSL funcionara bien siempre y cuando el router este bien.	
Valor	
Total	**Disponibilidad**
Bajo	Bajo

Fuente: Elaboración propia.

Tabla 37.

Caracterización de activos pertenecientes a la empresa.

Soporte

Código: Media1	**Nombre:** Almacenamiento del área de administración y contabilidad
Detalle: Los discos duros pertenecientes a las computadoras de las áreas de contabilidad, gerencia y publicidad.	
Ubicación: Contabilidad, gerencia y publicidad	
Tipo: Electrónicos, Discos	
Vinculación	
Activos:	**Categoría:**
Valor	
Total	**Disponibilidad**
Alto	Alto

Fuente: Elaboración propia.

Tabla 38.

Caracterización de activos pertenecientes a la empresa.

Soporte	
Código: Media2	**Nombre:** Dispositivo de almacenamiento USB
Detalle: Dispositivos de almacenamiento externo.	
Ubicación:	
Tipo: USB	
Vinculación	
Activos:	**Activos:**
Valor	
Total	**Disponibilidad**
Alto	Alto

Fuente: Elaboración propia.

Tabla 39.

Caracterización de activos pertenecientes a la empresa.

Soporte	
Código: Media3	**Nombre:** Archivos físicos
Detalle: Almacenamiento físico en donde se guardan periódicos, notas de prensa e información contable de años anteriores.	
Ubicación: Contabilidad	
Tipo: Material físico	
Vinculación	
Activos:	**Categoría:**
Valor	
Total	**Disponibilidad**
Alto	Alto

Fuente: Elaboración propia.

Tabla 40.

Caracterización de activos pertenecientes a la empresa.

Personal	
Código: P2	**Nombre:** Personal administrativo y logística
Detalle: Personal encargado de vender publicidad, maquetación, diseño y reparto de periódico.	
Tipo: Usuarios	
Valor	
Total	**Disponibilidad**
Muy Alto	Muy Alto

Fuente: Elaboración propia.

Tabla 41.

Caracterización de activos pertenecientes a la empresa.

Personal	
Código: P1	**Nombre:** Personal de Sistemas

Detalle: Colaboradores relacionados al manejo de sistemas informáticos, redes de comunicaciones y demás apartados tecnológicos dentro de la empresa.	
Tipo: Usuarios internos	
Valor	
Total	**Disponibilidad**
Muy Alto	Muy Alto

Fuente: Elaboración propia.

Después de haber analizado el estado actual de la empresa editora de diario regional peruano, es preciso señalar que, la empresa actualmente no cuenta con un documento formal en el cual se especifiquen normativas de seguridad periódicas, para la eliminación de riesgos con respecto a la seguridad de sus activos.

Según la metodología magerit los riesgos se estiman por su degradación y probabilidad, cuando se habla de degradación hace referencia al porcentaje de tiempo que necesita el riesgo para ser mitigado completamente, por otro lado, cuando se habla de probabilidad, es la frecuencia que tiene el riesgo de presentarse dentro de la empresa u organización.

Tabla 42.

Tabla de degradación de los riesgos según la metodología Magerit.

	Degeneración		
	1%	**10%**	**100%**

	Muy Alto	Medio	Alto	Muy Alto
Valor	**Alto**	Bajo	Medio	Alto
	Medio	Muy Bajo	Bajo	Medio
	Bajo	Muy Bajo	Muy Bajo	Bajo
	Muy Bajo	Muy Bajo	Muy Bajo	Muy Bajo

Nota: Tomado de Ministerio de Hacienda y Adminstraciones Públicas, (2012).

Tabla 43.

Tabla de clasificación de los riesgos según la probabilidad de suceso.

Riesgo	**Posibilidad**				
	Muy raro	**Poco probable**	**Posible**	**Probable**	**Prácticamente Seguro**
Muy Alto	Importante	Crítico	Crítico	Crítico	Crítico
Alto	Apreciable	Importante	Importante	Crítico	Crítico
Medio	Bajo	Apreciable	Apreciable	Importante	Importante
Bajo	Asumible	Bajo	Bajo	Apreciable	Apreciable
Muy Bajo	Asumible	Asumible	Asumible	Bajo	Bajo

Nota: Tomado de Ministerio de Hacienda y Adminstraciones Públicas, (2012).

De esta manera se realizó una estimación de riesgos que permitan saber el Categoría de impacto potencial, impacto acumulado, riesgo potencial y riesgo acumulado dentro de la empresa editora de diario regional peruano. Es preciso señalar que cada apartado esta a su vez dividido en tres sectores: C (Confidencialidad), I (Integridad) y D (Disponibilidad). Cabe señalar que el impacto potencial hace referencia al medio del riesgo en el lapso de un año, por otro lado, impacto acumulado es la medida de implicancia de una amenaza determinada, el riesgo potencial es la medida del probable daño que puede causar la amenaza al sistema, y por último el riesgo acumulado hace referencia a la degradación y a la probabilidad de la amenaza.

Tabla 44.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

Información de facturación						
Amenazas	**Impacto Potencial**			**Riesgo Potencial**		
	Conf.	**Int.**	**Disp.**	**Conf.**	**Int.**	**Disp.**
Fallos de clientes	MB	MA	MB	A	MA	M
Escape de información	MA			MA		
Usurpación de identidad	A	A		A	A	
Acceso no vigilado	A	B		MB	B	
Alteración de información		A	B		A	B

Fuente: Elaboración propia.

Tabla 45.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

Documentos periodísticos						
Amenazas	**Impacto Potencial**			**Riesgo Potencial**		
	Conf.	**Int.**	**Disp.**	**Conf.**	**Int.**	**Disp.**
Fallos de clientes	MA	A	M	MA	MA	B
Escape de información	A			MA		
Usurpación de identidad	MA	A		MB	MB	
Acceso no vigilado	A	MA		M	M	
Alteración de información		A	M		A	M

Fuente: Elaboración propia.

Tabla 46.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

Red de telefonía		
Amenazas	**Impacto Potencial**	**Riesgo Potencial**
	Disp.	**Disp.**
Fallo de las telecomunicaciones	M	MB
Uso inadecuado	M	MB

Fuente: Elaboración propia.

Tabla 47.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

Wifi					
Amenazas	**Impacto Potencial**		**Impacto Acumulado**	**Riesgo Potencial**		**Riesgo Acumulado**
	Conf.	**Disp.**	**Disp.**	**Conf.**	**Disp.**	**Disp.**
Fallo de las telecomunicaciones		MA	A		A	MA
Usurpación de identidad	MB			M		
Uso inadecuado		MB	MB		A	MA
Fallos de administrador		M	M		MB	M

Fuente: Elaboración propia.

Tabla 48.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

ADSL				
Amenazas	**Impacto Potencial Disp.**	**Impacto Acumulado Disp.**	**Riesgo Potencial Disp.**	**Riesgo Acumulado Disp.**
Fallo de las telecomunicaciones	M	MA	MB	A

Fuente: Elaboración propia.

Tabla 49.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

Servidor (Movilidad LI – EN)				
Amenazas	**Impacto Potencial Disp.**	**Impacto Acumulado Disp.**	**Riesgo Potencial Disp.**	**Riesgo Acumulado Disp.**
Prohibición de servicio	MB	M	MB	M

Fuente: Elaboración propia.

Tabla 50.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

Discos duros								
Amenazas	**Impacto Potencial**	**Impacto Acumulado**			**Riesgo Potencial**	**Riesgo Acumulado**		
	Disp.	**Conf.**	**Int.**	**Disp.**	**Disp.**	**Conf.**	**Int.**	**Disp.**
Fuego	MA			M	M			M
Agua	A			MA	M			M
Alteración mecánica	M			M	MA			A
Interrupción de la energía eléctrica	MA			A	A			A
Degradación de soportes	A			MA	A			MA
Fallos de usuarios	M	M	M	M	A	MA	A	A
Alteración de información	MA	A	A	A	M	M	M	M

Fuente: Elaboración propia.

Tabla 51.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

Personal administrativo y logística		
Amenazas	**Impacto Potencial**	**Riesgo Potencial**
	Disp.	**Disp.**
Discrepancias en la empresa	MA	MA

Fuente: Elaboración propia.

Tabla 52.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

Aplicación web		
Amenazas	**Impacto Potencial**	**Riesgo Potencial**
	Disp.	**Disp.**
Fallos de clientes	B	B
Fallos de administrador	MB	B
Caída del sistema	B	MB
Alteración de información	B	B

Fuente: Elaboración propia.

Tabla 53.

Estimación de riesgos que posee la empresa editora de diario regional peruano.

SAP Busisness ONE								
Amenazas	**Impacto Potencial**	**Impacto Acumulado**			**Riesgo Potencial**	**Riesgo Acumulado**		
	Disp.	**Conf.**	**Int.**	**Disp.**	**Disp.**	**Conf.**	**Int.**	**Disp.**
Fallos de los clientes	A	B	B	B	A	B	M	M
Fallos de administrador	A	B	B	M	A	B	B	A
Debilidad del software	B	M	M	M	B	M	M	B
Usurpación de la identidad		M	M			B	B	
Exceso de privilegios	M	M	M B	B	M	M	M B	B
Acceso no vigilado		M	M			B	B	
Negación de servicio	B			M	B			B

Fuente: Elaboración propia.

Así mismo se recopilo información acerca de las amenazas catalogadas en siete sectores, que presenta la empresa editora La Industria de Chiclayo y el impacto potencial que generaría en caso llegara a suceder cualquiera de estos sucesos. De igual manera están clasificados por su impacto potencial y riesgo potencial, cada una con tres características: C (Confidencialidad), I (Integridad) y D (Disponibilidad). Y de esta manera son medidos bajo la siguiente clasificación: MA (Muy alta), A (Alta), M (Media), B (Baja) y MB (Muy baja).

Datos

Tabla 54.

Listado de amenazas caracterizadas por su impacto potencial y riesgo potencial.

Amenazas	**Impacto Potencial**		**Riesgo Potencial**	
	Conf.	**Int.**	**Conf.**	**Int.**
Suplantación de identidad	A	A	MB	MB
Acceso no autorizado	A	B	B	B

Fuente: Elaboración propia.

Redes de comunicaciones

Tabla 55.

Listado de amenazas caracterizadas por su impacto potencial y riesgo potencial.

Amenazas	**Impacto Potencial**	**Riesgo Potencial**
	Disp.	**Disp.**
Fallo de las telecomunicaciones	MB	M
Fallos de administrador	B	B

Fuente: Elaboración propia.

Hardware

Tabla 56.

Listado de amenazas caracterizadas por su impacto potencial y riesgo potencial.

Amenazas	**Impacto Potencial**	**Riesgo Potencial**
	Disp.	**Disp.**
Negación de servicio	M	B
Uso no adecuado	MB	B
Alteración de equipos	B	B
Hurto	MB	B
Equipos extraviados	B	B

Fuente: Elaboración propia.

Soportes de información

Tabla 57.

Listado de amenazas caracterizadas por su impacto potencial y riesgo potencial.

Amenazas	**Impacto Potencial**			**Riesgo Potencial**		
	Con.	**Int.**	**Dis.**	**Con.**	**Int.**	**Dis.**
Uso no adecuado	B	B	M	B	B	M
Hurto	M		M	B		B
Equipos extraviados	B		B	MB		M

Fuente: Elaboración propia.

Personal

Tabla 58.

Listado de amenazas caracterizadas por su impacto potencial y riesgo potencial.

Amenazas	**Impacto Potencial**	**Riesgo Potencial**
	Dis.	**Dis.**
Discrepancias en la empresa	A	A

Fuente: Elaboración propia.

Servicios

Tabla 59.

Listado de amenazas caracterizadas por su impacto potencial y riesgo potencial.

Amenazas	**Impacto Potencial**	**Riesgo Potencial**
	Dis.	**Dis.**
Fallos de usuarios	B	B
Fallos de administrador	M	B
Alteración de información	B	B
Debilidad del software	M	B
Uso no adecuado	M	B

Fuente: Elaboración propia.

Software

Tabla 60.

Listado de amenazas caracterizadas por su impacto potencial y riesgo potencial.

Amenazas	**Impacto Potencial**			**Riesgo Potencial**		
	Con.	**Int.**	**Dis.**	**Con.**	**Int.**	**Dis.**
Exceso de privilegios	MA	M	B	A	B	B
Negación de servicio			A			M
Fallos de usuarios	M	A	B	A	MA	B
Fallos de administrador	M	A	M	M	MA	M
Debilidad del software	A	MA	M	MA	A	M

Fuente: Elaboración propia.

Para poder determinar los requerimientos de seguridad de la información se realizó una caracterización de los tipos de bienes, que según la metodología Magerit, se pueden encontrar en toda organización. Y que para los fines de esta investigación se pudo aplicar perfectamente a la realidad de la empresa editora de diario regional peruano, ya que esta cuenta con todos los activos mencionados.

Tabla 61.

Descripción de las clases de activos según la metodología Magerit.

Clase de activo	**Descripción**
Datos / Información	Información generada por la empresa.
Servicios	Servicios brindados por la empresa para la productividad de los usuarios.
Software	Aplicaciones informáticas destinadas a la productividad de la empresa.

Hardware	Equipo informático para procesamiento de datos.
Redes de Comunicaciones	Redes que actúan como transporte para datos dentro de la empresa.
Soportes de información	Dispositivos capaces de almacenar información.
Equipamiento	Hardware que puede servir para cumplir una determinada función.
Instalaciones	Lugar especializado donde se almacena el hardware de la empresa.
Personal	Trabajadores de la empresa.

Nota: Tomado de Ministerio de Hacienda y Adminstraciones Públicas, (2012).

3.3.2. Elaborar un modelo de gestión de seguridad de la información que más se adecue a la realidad de la empresa.

Para la elaboración del modelo de gestión de seguridad de la información se tomó en cuenta al estándar internacional ISO/IEC 27001:2013 y a la metodología Magerit para la gestión de riesgos, ya que se consideró que ambas tienen fases que se asemejan a lo que la empresa necesita, sin embargo, fue necesario personalizar el modelo y tomar de cada una de ellas lo que más se adecua a la coyuntura actual de la empresa.

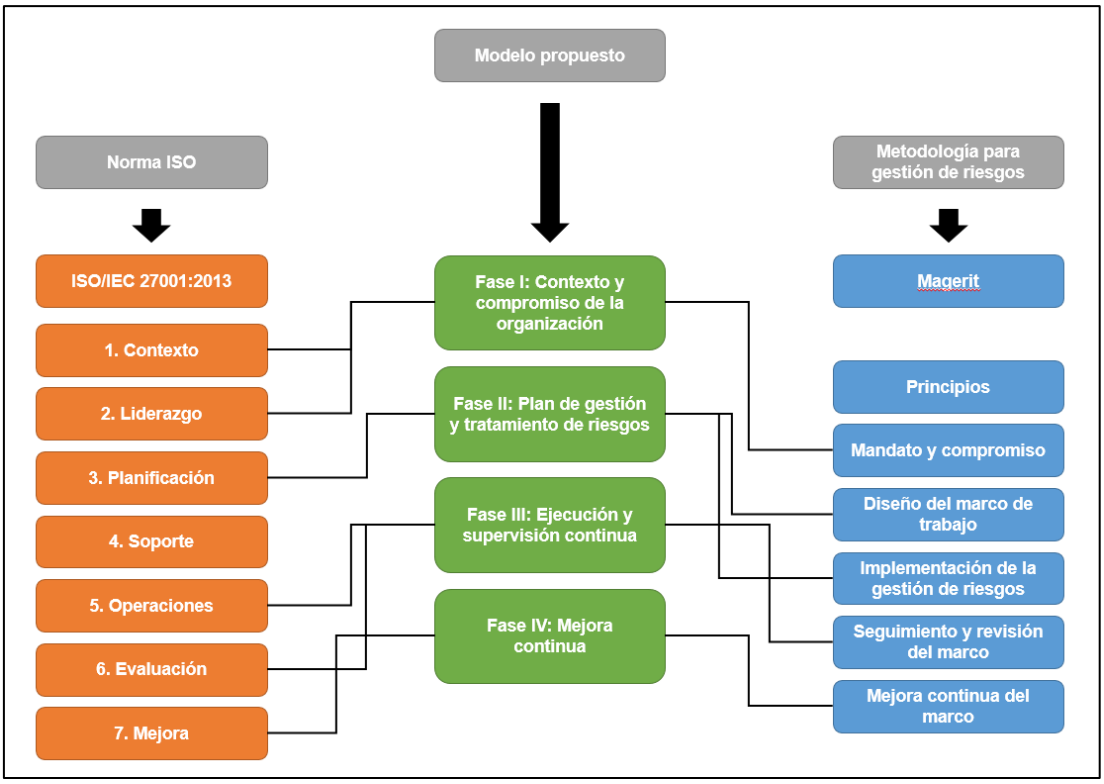


Figura 11. Proceso de elaboración del modelo ad hoc para la gestión de seguridad de la información. Fuente: *Elaboración propia.*

Como se puede apreciar en la ilustración, de la norma ISO/IEC 27001 se optó por tomar todas sus fases a excepción de la fase de soporte, debido a que la empresa en cuestión no cuenta con tecnología e infraestructura que permita tener un sistema propiamente dicho de gestión de seguridad de la información, más sin embargo puede establecer políticas y normas para proteger sus activos. Así mismo de la metodología Magerit para gestión de riesgos se tomaron todas sus fases a excepción de principios, debido a que no es de carácter importante actualmente para la organización.

De esta manera el modelo ad hoc está compuesto por 4 fases, dentro de las cuales, la primera fase denominada contexto y compromiso de la organización se encarga de reunir la fase de contexto y liderazgo pertenecientes a la norma ISO/IEC 27001:2013 con la etapa de mandato y compromiso que se encuentra dentro de la metodología Magerit, siendo estas fases similares, se optó por unirlas.

La segunda fase llamada plan de gestión y tratamiento de riesgos, une la fase de plan de gestión de la norma ISO/IEC 27001:2013 con la etapa de diseño del marco de trabajo e implementación de la gestión de riesgos, para de esta manera enlazar de una mejor forma la parte de planificación con el tratamiento de riesgos y buscar la efectividad al momento de cumplir con lo planificado.

La ejecución y supervisión continua pertenece a la tercera fase del modelo ad hoc, esta etapa rescata de la norma ISO/IEC 27001:2013 la etapa de operaciones y evaluaciones, así como también toma de la metodología Magerit seguimiento y revisión del marco. En esta etapa se prioriza la ejecución de las políticas de seguridad así mismo se debe hacer una retroalimentación de todo lo aplicado para poder mejorar las políticas y ser eficientes al momento de mitigar los riesgos.

Por último la cuarta fase del modelo ad hoc se denomina mejora continua, la cual toma la etapa de mejora de la norma ISO/IEC 27001:2013 y a su vez recoge la fase de mejora continua del marco, perteneciente a la metodología Magerit, Es conveniente señalar que ambas etapas sirven de referencia para el proceso de recojo de información y datos que permitan determinar si se aplicó de manera correcta los salvaguardas y evidentemente dan un buen resultado al momento de presentarse determinados riesgos.

3.3.3. Aplicar el modelo desarrollado en base a la norma ISO/IEC 27001 y la metodología Magerit para la gestión de riesgos.

Fase I: Contexto y compromiso de la organización

El compromiso de la empresa u organización está registrado en el Anexo 5, el cual hace referencia a la voluntad de la empresa de efectuar todas las normas y políticas de seguridad que se puedan aplicar. Así mismo es importante señalar que la empresa trabaja con activos sensibles, que deben

de ser protegidos siguiendo un modelo y un plan de gestión, para de esta manera asegurar la persistencia del negocio en caso se presente cualquier inconveniente ya sea externo o interno.

Fase II: Plan de gestión y tratamiento de riesgos

Según la metodología Magerit los controles se dividen en diez tipos, los cuales a su vez tienen una breve descripción y el efecto que producen. Para efectos prácticos, se determinó que todos estos tipos de control son aplicables dentro de la empresa editora de diario regional peruano, a continuación, se detalla cada tipo de control.

Tabla 62.

Descripción de los tipos de controles y sus efectos, según la metodología Magerit.

Tipo de control	Descripción	Efecto
Preventiva	Reduce la probabilidad de que se presente una amenaza.	Reduce la probabilidad
Disuasoria	Reduce la probabilidad de que se presente un ataque.	
Eliminatoria	Elimina la posibilidad de que ocurra una amenaza.	
Minimizadora	Limitan el impacto de una determinada amenaza.	Reduce la degradación
Correctiva	Medidas que reparan el daño y lo corrigen	
De recuperación	Permiten regresar a un estado anterior.	
De monitorización	Políticas que generan archivos .log para posteriormente ser analizados.	

De detección	Detectan de manera rápida el ataque y proponen alternativas de solución.	Consolida el efecto de las políticas
De concienciación	Concientización a los colaboradores para actuar frente a cualquier imprevisto.	
De administración	Permiten mejorar la seguridad de un determinado sistema.	

Nota: Tomado de Ministerio de Hacienda y Adminstraciones Públicas, (2012).

Referente a lo anterior se procedió a instaurar las políticas de seguridad informática o salvaguardas que se encargaran de proteger todos los activos que posee la empresa. Cabe señalar que las políticas de seguridad están ordenadas en seis apartados los cuales son: Datos, redes, hardware, soporte, personal y software.

Tabla 63.

Políticas de seguridad o salvaguardas.

Datos	
Oficialización de procedimientos de la empresa	Historial de configuración
Backups del servidor	
Desarrollar políticas para el uso de TI	Normas de continuidad

Fuente: Elaboración propia.

Tabla 64.

Políticas de seguridad o salvaguardas.

Redes	
Desarrollar políticas para el uso de TI	Normas de continuidad
Protección de registros	Protección web

Fuente: Elaboración propia.

Tabla 65.

Políticas de seguridad o salvaguardas.

Hardware	
Mantenimiento periódico	Normas de continuidad
Copias de seguridad regulares	Supervisión de acceso mediante malware

Fuente: Elaboración propia.

Tabla 66.

Políticas de seguridad o salvaguardas.

Soporte	
Instalación de equipo SAI	Backups de respaldo
Oficialización de procedimientos de la empresa	Mantenimiento periódico

Fuente: Elaboración propia.

Tabla 67.

Políticas de seguridad o salvaguardas.

Personal	
Formalización de responsabilidades	Oficialización de procedimientos

Fuente: Elaboración propia.

Tabla 68.

Políticas de seguridad o salvaguardas.

Software	
Oficialización de procedimientos de la empresa	Creación de password único
Mecanismos de Acceso lógico	Normativas para uso red wifi

Fuente: Elaboración propia.

Una vez que se establecieron las políticas de seguridad o salvaguardas es importante caracterizarlas, para esto se procedió a construir una tabla en las cuales se encuentran las amenazas, los salvaguardas o políticas de seguridad, así como la posibilidad de que esas políticas sean usadas dentro de la empresa, así mismo también existen los campos de dimensiones, impacto residual y riesgo residual.

Es importante señalar que en los apartados de dimensiones, impacto residual y riesgo residual están clasificados en D (Disponibilidad), I (Integridad) y C (Confidencialidad). Las cuales representan a las características de la información.

Tabla 69.

Caracterización de las políticas de seguridad.

Información de facturación											
Amenazas	**Políticas**	**Posibilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			Co	**In**	**Di**	**Co**	**In**	**Di**	**Co**	**In**	**Di**
Fallas de usuarios	Tratamiento de correos	Alta	B	B	B	M	M	MB	MA	MA	A
	Oficialización de procesos empresariales	Media	B	A	B	M	MA	MB	M	A	A
	Backups de respaldo	Muy Alta	A	B	MB	M	M	MB	A	MA	A
	Manual de uso TI	Media	A			A			M		
Escape de información	Protección de hardware	Media	MB			M			M		
	Restauración de computadoras	Media	B			M			M		
	Implementación de claves originales	Baja	A	B		A	M		M	MB	

Usurpación de identidad	Acceso mediante programación	Muy Baja	A	B		MA	M		M	B
	Claves autorizadas	Baja	A	B		A	M		M	MB
	Protección de hardware	Muy Baja	B	B		M	M		MB	B
Acceso no vigilado	Implementación de claves originales	Muy Baja	M	B		A	M		B	B
	Acceso mediante programación	Baja	M	B		MA	M		B	MB
	Claves autorizadas	Baja	M	B		A	M		B	B
Alteración de información	Protección de hardware	Baja		M	B		A	MB		M B
	Acceso mediante programación	Muy Baja		M	B		A	B		B MB
	Claves autorizadas	Muy Baja		M	B		A	B		B MB
	Backups de respaldo	Baja		M	B		A	MB		M MB
	Normativas de continuidad	Baja		M	B		A	MB		M MB

Fuente: Elaboración propia.

Tabla 70.

Caracterización de las políticas de seguridad.

Wifi											
Amenazas	**Políticas**	**Posibilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			Co	**In**	**Di**	**Co**	**In**	**Di**	**Co**	**In**	**Di**
Fallo de las telecomunicaciones	Normativas de continuidad	Muy Alta			MA			MA			MA
Usurpación de identidad	Implementación de claves originales	Baja	MB	B		M			B		
Uso no adecuado	Acceso mediante programación	Baja	B	B		M			B		
	Normas de uso de TI	Media	MB	B		M			M		
	Eliminar Web	Muy Baja	MB	B		M			M		

Fallos de administrador	Oficialización de procesos empresariales	Muy Baja	B		M		M		
	Historial de configuración	Medio	B	B	M	M	M	M	

Fuente: Elaboración propia.

Tabla 71.

Caracterización de las políticas de seguridad.

Servidor Baltazar									
Amenazas	**Políticas**	**Posibilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			Co	**In**	**Di**	**Co**	**In**	**Di**	**Co**	**In**	**Di**
Fuego	Adquisición de extintores	Baja			A			B			MB
	Adquirir sistema anti incendio	Muy Baja			A			MB			MB
Alteración mecánica	Mantenimiento de computadoras	Muy Baja			M			MB			MB
	Backups de respaldo	Alta			A			A			A
	Historial de configuración	Alta			A			A			A

	SAI	Bajo			B	MB	MB
	Backups de respaldo	Baja			B	MB	MB
Corte de energía eléctrica	Normativas de continuidad	Muy Baja			B	MB	MB
Uso no adecuado	Normas de uso de TI	Media	B	B	B	MB	B
	Eliminar Web	Baja	MB	MB	B	MB	MB
	Protección de hardware	Muy Baja		B	B	MB	MB
Alteración de información	Acceso mediante programación	Muy Baja		B	B	MB	MB
	Backups de respaldo	Baja		MB	B	B	MB
Alteración de equipos	Acceso mediante programación	Muy Baja	B		B	MB	B

Fuente: Elaboración propia.

Tabla 72.

Caracterización de las políticas de seguridad.

Almacenamiento del área de administración y contabilidad										
Amenazas	**Políticas**	**Posibilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			Co	**In**	**Di**	**Co**	**In**	**Di**	**Co**	**In**	**Di**
Fuego	Adquisición de extintores	Baja			A			A			M
	Adquirir sistema anti incendio	Baja			MA			A			M
	Backups de respaldo	Muy Baja			M			MB			B
	Normativas de continuidad	Muy Baja			M			M			B
Alteración mecánica	Mantenimiento de computadoras	Baja			M			M			M
	Backups de respaldo	Alta			B			B			M
	Historial de configuración	Alta			B			B			M
Corte de energía eléctrica	SAI	Baja			A			A			M
	Backups de respaldo	Baja			M			M			M
	Normativas de continuidad	Muy Baja			M			M			M

Fallos de usuarios	Oficialización de procesos empresariales	Media	B	M	M	B	M	M	B	M	M
	Backups de respaldo	Muy Alta	B	B	MB	B	B	B	M	M	M
	Historial de configuración	Muy Alta	MB	B	B	B	B	B	M	M	M
	Normativas de continuidad	Muy Alta	B	B	MB	B	B	B	M	M	M
Alteración de información	Protección de hardware	Baja		M	M			M			M
	Acceso mediante programación	Baja		A	A			A			M
	Backups de respaldo	Baja		B	B			B			B
	Normativas de continuidad	Baja		B	B			B			B

Fuente: Elaboración propia.

Tabla 73.

Caracterización de las políticas de seguridad.

Personal administrativo y logística					
Amenazas	**Políticas**	**Posibilidad**	**Dimensiones Disp.**	**Impacto Res. Disp.**	**Riesgo Res. Disp.**
Discrepancias en la organización	Oficialización de procesos empresariales	Baja	M	A	M
	Oficialización de responsabilidades	Muy Baja	MB	A	MB
	Normas de uso de TI	Muy Baja	M	B	B

Fuente: Elaboración propia.

Tabla 74.

Caracterización de las políticas de seguridad.

SAP Busisness ONE											
Amenazas	**Políticas**	**Posibilidad**	**Dimensiones**			**Impacto Res.**			**Riesgo Res.**		
			Co	**In**	**Di**	**Co**	**In**	**Di**	**Co**	**In**	**Di**
Fallos de usuarios	Tratamiento de correos	Muy Alta	B	B	B	MB	B	B	B	M	M
	Oficialización de procesos empresariales	Muy Baja	MB	A	B	MB	A	MB	MB	A	B
	Normas de uso de TI	Media	MB	A	B	MB	A	B	MB	A	B
	Normativas de continuidad	Muy Alta	MB	MB	B	MB	B	MB	B	M	M
	Oficialización de procesos empresariales	Baja	B	A	M	MB	A	M	MB	M	B
	Normas de uso de TI	Baja	MB	A	M	MB	A	M	MB	A	M
Fallos de administrador	Aplicación RGPD	Muy Baja	B	A	M	MB	A	M	MB	A	M
	Historial de configuración	Media	MB	B	B	MB	B	B	MB	B	B

	Normativas de continuidad	Baja	B	B	MB	MB	B	MB	MB	B	B	
Debilidad del software	Adquisición de antivirus	Baja	A	M	MB	M	M	B	B	B	MB	
Usurpación de identidad	Tratamiento de correos	Muy Baja	A	B		M	B		B	MB		
	Acceso mediante programación	Baja	MA	A		M	A		B	M		
Acceso no vigilado	Implementación de claves originales	Baja	A	A		M	A		B	M		
	Claves autorizadas	Muy Baja	A	A		M	A		B	M		

Fuente: Elaboración propia.

Fase III: Ejecución y supervisión continua

Para la puesta en marcha del plan de seguridad de la información propuesto es necesario recalcar que solo se utilizaron las políticas de seguridad cuya probabilidad de suceso está comprendida entre alta y muy alta, debido a que la empresa optó por minimizar costes y recomiendan que la aplicabilidad del plan propuesta se realice en el menor tiempo posible.

Tabla 75.

Listado de políticas de seguridad o salvaguardas que se implementaran en la empresa de diario regional peruano.

Activos	**Amenaza**	**Salvaguarda**	**Prioridad**	**Entorno de ejecución**
Información de facturación	Errores de los usuarios	Tratamiento de correos	Muy Alta	Suit de google (Xertica)
		Backups de respaldo	Muy Alta	Servidor FileServer
Red WIFI	Fallo de servicios de comunicaciones	Planes de contingencia y continuidad	Muy Alta	Área de sistemas y soporte técnico
Servidor Baltazar	Alteración mecánica	Backups de respaldo	Alta	Servidor Baltazar
		Historial de configuración	Alta	
Almacenamiento del área de administración y contabilidad	Alteración mecánica	Backups de respaldo	Alta	Servidor Baltazar y servidor FileServer
		Historial de configuración	Alta	
	Errores de los usuarios	Backups de respaldo	Alta	
		Historial de configuración	Alta	
		Planes de contingencia y continuidad	Alta	

SAP Busisness ONE	Errores de los usuarios	Tratamiento de correos	Muy Alta	Software SAP Busisnes ONE
		Planes de contingencia y continuidad	Muy Alta	

Fuente: Elaboración propia.

Después de haber identificado las políticas de seguridad, se procedió a aplicar todas las medidas detalladas en la tabla anterior, y las evidencias se adjuntaron en la sección de anexos del presente trabajo, a continuación, se muestra una tabla donde se encontrarán los anexos respectivos a las evidencias de la política de seguridad aplicada.

Tabla 76.

Relación de políticas de seguridad con sus respectivas evidencias.

Activo	Política de seguridad o salvaguarda	Evidencia
Información de facturación	Tratamiento de correos	Anexo 6
	Backups de respaldo	Anexo 7
Red wifi	Planes de contingencia y continuidad	Anexo 8
Servidor baltazar	Backups de respaldo	Anexo 9
	Historial de configuración	Anexo 10
Almacenamiento del área de administración y contabilidad	Backups de respaldo	Anexo 11
	Historial de configuración	Anexo 12
	Backups de respaldo	Anexo 13
	Historial de configuración	Anexo 14
	Plantes de contingencia y continuidad	Anexo 15
	Tratamiento de correos	Anexo 16
SAP Bussisnes ONE	Planes de contingencia y continuidad	Anexo 17

Fuente: Elaboración propia.

Fase IV: Mejora continua

Después de haber aplicado las salvaguardas respectivas se optó por realizar un sondeo a los colaboradores de la empresa, acerca de las medidas

implementadas, cuyo resultado evidencio una mejora significativa en la seguridad de la información de la empresa, tal como se aprecia en el anexo 18.

Se estableció que es importante actualizar las políticas de seguridad aplicadas, debido a que la empresa cada vez tiene un mayor flujo de información, así mismo se creó un precedente dentro de la empresa, debido a que nunca antes había contado con políticas de seguridad formales que protejan sus principales activos.

3.3.4. Medir los resultados de la aplicación del modelo de gestión de seguridad de la información desarrollado en la empresa editora de diarios regionales seleccionada.

Los resultados después de aplicar las políticas de seguridad de acuerdo al modelo ad hoc, reflejaron una mejora en cuanto al aseguramiento de la información dentro de la empresa, no obstante, al ser la primera vez que se aplicó este tipo de controles, es de esperarse que aun sigan existiendo brechas de seguridad, sin embargo, la empresa actualmente ya cuenta con un plan para gestionar sus riesgos y asegurar la data que ellos crean pertinente.

A continuación, se mostrará un breve resumen de los resultados obtenidos.

Tabla 77.

Relación de indicadores con los resultados obtenidos.

Indicador	**Resultado**
Nivel de cubrimiento del modelo ad hoc en activos de información	(5/19)*100 = 26.32%
Porcentaje de aplicación del plan de sensibilización	(3/10) * 100 = 30%
Cumplimiento de políticas de seguridad en la empresa	EPGSI = 1 DACPI = 1 ERLSPI = 0

Categoría de la seguridad de información y los equipos de cómputo	LRSTCPS = 0 ENPIF = 1
Categoría de verificación de Acceso lógico	NAUAS = 1 ECAUA = 1 ENCDM = 0
Porcentaje de implementación de controles	(10/24) * 100 = 41.6%
Evidencias de ataques informáticos a la empresa	EAIUA = 1 AIUNPE = 1
Categoría de verificación de las políticas de integridad de la información	ELMEI = 1 ELRIM = 1

Fuente: Elaboración propia.

El modelo desarrollado sirvió para seleccionar e implementar las políticas de seguridad que más se adecuan a la realidad de la empresa editora de diario regional peruano, para ello fue necesario realizar un documento donde se dejó constancia de todas las políticas de seguridad implementadas, gracias al modelo ad hoc desarrollado, dicho documento se puede apreciar en el anexo 27.

IV. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones.

La seguridad de la información en la empresa editora de diario regional peruano, antes de haber implementado el modelo ad hoc, fue prácticamente nula, esto originó que el área de sistemas y soporte técnico de dicha empresa, sufriera diversos ataques por parte de virus de tipo mallware, poniendo en riesgo la información que maneja la empresa.

El modelo ad hoc desarrollado se caracterizó por rescatar las fases más esenciales de la norma ISO/IEC 27001:2013 y la metodología Magerit para gestión de riesgos, aunados a las necesidades básicas que tiene la empresa para poder salvaguardar su información contable. Este modelo se enfocó en dar

prioridad a la planificación y ejecución de las políticas de seguridad dentro de la empresa.

El modelo ad hoc para la gestión de seguridad de la información, para una empresa editora de diario regional peruano, se implementó de manera satisfactoria, se desarrollaron las políticas de seguridad pertinentes, así como también se llevó a cabo el desarrollo de dichas políticas de seguridad.

Después de haber aplicado las políticas de seguridad, se consideró pertinente interpretar los resultados obtenidos, siendo los más resaltantes el nivel de cubrimiento del modelo ad hoc y el porcentaje de concientización, gracias a estos indicadores se apreció que el Categoría de seguridad de información que tiene la empresa actualmente mejoró en comparación con su situación antes de tener políticas de seguridad instauradas. No obstante, el nivel de concientización de los colaboradores de la empresa resulto un poco bajo, de esta manera se comprobó que es importante trabajar en brindar capacitaciones a los colaboradores para que puedan tener mayor predisposición a cumplir con las normas y políticas de seguridad de la empresa.

4.2. Recomendaciones.

El modelo ad hoc desarrollado en esta investigación ha sido aplicado a una mediana empresa editora de diario regional peruano, para obtener resultados similares a los encontrados en esta investigación, se debe priorizar el tipo de información que maneja la empresa, así como también la cantidad de trabajadores, y por último el flujo de información que manejan.

Es importante señalar que la empresa en cuestión no tenía ninguna política ni norma de seguridad de la información, el modelo desarrollado en esta investigación se usó para implementar políticas que se adecuen a la realidad de la empresa y a sus necesidades, en este caso específico la empresa tiene como prioridad proteger su información contable, administrativa y publicitaria ante cualquier eventualidad.

La prioridad de la empresa editora de diario regional peruano, es la de obtener de manera rápida, protección para la información que se maneja dentro de la empresa, es por ello que el método ad hoc reúne lo más importante y relevante de la norma ISO/IEC 27001:2013 y la metodología Magerit para la gestión de riesgo. La elección de las fases se toma en base a la mera necesidad de la empresa en cuestión, así como también la elección de las políticas de seguridad a implementar dentro de la empresa.

REFERENCIAS.

Ahmad Z., Song T., Hui T., & Norhashim M. (2019). Security monitoring and information security assurance behaviour among employees An empirical analysis. *Information & Computer Security*, 165-188.

Baca, V. (2016). Diseño de un sistema de gestión de la seguridad de la Información para la unidad de gestión educativa local - Chiclayo. *Ingeniería: Ciencia, Tecnología e Innovación*, 42-45.

Beckers K., Coˆte´ I., Faßbender S., Heisel M., & Hofbauer S. (2013). A pattern-based method for establishing a cloud-specific information security management system. *Requirements Eng*, 343-395.

Chan, M., Woon, I., & Kankanhalli, A. (2005). Perceptions of Information Security in the Workplace: Linking Information Security Climate to Compliant Behavior. *Journal of Information Privacy & Security*, 18-41.

Chierici A., Girolamo D., Guizzunti G., Longo S., Maron G., Martelli B., . . . Giampieri E. (2019). SGSI project at CNAF. *EPJ Web of Conferences*, 1-6.

Concytec. (2016). *Política nacional para el desarrollo de la ciencia, tecnología e innovación.* Lima: Concytec.

Contreras, A. (2003). Delitos Informáticos: Un Importante Precedente. *Ius et Praxis*, 515-521.

Dang, D., Kautz, K., Pittayachawam, S., & Bruno V. (2019). Explaining the Development of Information Security Climate and an Information Security Support Network: A Longitudinal Social Network Analysis. *Australasian Journal of Information Systems*, 1-28.

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. *Enlace*, 43-55.

Faizan, R., Dominic, P., Azhar, S., Rehman, M., & Sohail, A. (2021). Information Security Behavior and Information Security Policy Compliance: A Systematic Literature Review for Identifying the Transformation Process from Noncompliance to Compliance. *Applied Sciences*, 1-38.

Gené, J., & Gallo, P. (2018). Big data y seguridad de la información. *Atención Primaria*, 3-5.

Hurtado, M. (2020). Gestión de riesgo metodologías octave y magerit. *Universidad Piloto de Colombia - Metodología de Análisis de Riesgo.*, 1-12.

Insituto Nacional de Tecnologias de la Comunicación - Gobierno de España. (2021). *Implantación de un SGSI en la empresa.* Madrid: Insituto Nacional de Tecnologias de la Comunicación.

ISO. (6 de Mayo de 2021). *ISO*. Obtenido de ISO: https://www.iso.org/isoiec-27001-information-security.html

ISO Tools excellence. (9 de Mayo de 2021). *ISO Tools excellence*. Obtenido de ISO Tools excellence: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISO Tools excellence. (8 de Mayo de 2021). *ISOTools excellence*. Obtenido de ISO Tools excellence: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/

ISO Tools exellence. (6 de Mayo de 2021). *ISO Tools exellence*. Obtenido de ISO Tools exellence: https://www.isotools.org/2016/07/07/sistema-gestion-seguridad-la-informacion-basado-la-norma-iso-27001/

ISO Tools exellence. (6 de Mayo de 2021). *ISO Tools exellence*. Obtenido de ISO Tools exellence: https://www.isotools.org/2015/01/21/familia-normas-iso-27000/

ISO27000.ES. (6 de Mayo de 2021). *ISO27000.ES*. Obtenido de ISO27000.ES: https://www.iso27000.es/iso27000.html

Issa, A. (2011). Setting up a Secure Information System Using Information Security Management. *International Journal of Research and Reviews in Computer Science*, 138-143.

Ministerio de Hacienda y Administraciones Públicas - Gobierno de España. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión.* Madrid: Ministerio de Hacienda y Administraciones Públicas.

Ministerio de hacienda y administraciones públicas - Gobierno de España. (2012). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Ministerio de hacienda y administraciones públicas - Gobierno de España.

Ministerio de Hacienda y Adminstraciones Públicas. (2012). Magerit - versión 3.0, Metología de análisis y gestión de riesgos de los sistemas de información.

Metología de análisis y gestión de riesgos de los sistemas de información, 113-115.

Pérez, D., Trigueros, S., & Solana, P. (2019). Organizational practices as antecedents of the information security management performance An empirical investigation. *Information Technology & People*, 1262-1275.

Pmgssi. (6 de Mayo de 2021). *Pmgssi*. Obtenido de Pmgssi: http://www.pmgssi.com/2015/07/que-es-sgsi/

Poveda P., García J., Pulido A., & Cañón G. (2019). ISO 50001: 2018 and Its Application in a Comprehensive Management System with an Energy-Performance Focus. *energies*, 1-33.

Revista Universidad y Sociedad. (2 de Setiembre de 2019). *Scielo*. Obtenido de Scielo: http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202019000400487

Rodriguez, A. (2020). Herramientas fundamentales para el hacking ético. *Revista Cubana de Informática Médica*, 116-131.

Rodriguez, L., Cruzado, C., Mejia, C., & Diaz, A. (2020). Aplicación de ISO 27001 y su influencia en la seguridad de la información de una empresa privada peruana. *Propósitos y Representaciones*, 8-20.

Tagarev, N. (2012). Model for information security analyses in information security management system. *International Conference on Application of Information and Communication Technology and Statistics in Economy and Education* (págs. 492-500). Sofia: ICAICTSEE.

Thales. (2021). 2021 Data Threat Rport . *Thales Global Edition*, 6-15.

Vega, W. (2008). Políticas y seguridad de la información. *Revista de Difusión cultural y científica de la Universidad La Salle en Bolivia*, 63-69.

Vega, W. (7 de Mayo de 2021). *Scielo*. Obtenido de Scielo: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

ANEXOS.

Anexo 1. Resolución de aprobación del proyecto de investigación.

USS | UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N° 0700-2021/FIAU-USS
Pimentel, 02 de Agosto de 2021

VISTO:
Las Actas de reunión N° 2306 – 2021, N° 1307 - 2021 y la N° 1507 - 2021 del Comité de investigación de la Escuela profesional de INGENIERÍA DE SISTEMAS remitida el 15 de Julio de 2021 mediante oficio N°0250-2021/FIAU-IS-USS de la Dirección de Escuela de INGENIERÍA DE SISTEMAS, 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 acuerda 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, los **Temas de Tesis** perteneciente a la línea de investigación de **INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE**, a cargo de los **alumnos y 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 de los Temas de 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. Mario Fernando Ramos Moscol
Decano - Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN SAC.

Mag. Luis Roberto Larrea Colchado
Secretario Académico (e)
Facultad de Ingeniería, Arquitectura y Urbanismo
UNIVERSIDAD SEÑOR DE SIPÁN S.A.C.

Cc: Interesado, Archivo

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N° 0700-2021/FIAU-USS
Pimentel, 02 de Agosto de 2021

INGENIERÍA DE SISTEMAS	VILCHEZ SILVA OMAR JHONATHAN	ANÁLISIS COMPARATIVO DE ALGORITMO DEVITERBI Y BAM-WELCH DE RECONOCIMIENTO DE VOZ PARA LA IDENTIFICACIÓN DE PERSONAS	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	FERNANDEZ SALDAÑA CARLOS ALDAIR IDROGO CORNEJO LEONCIO	DESARROLLO DE UN MÉTODO DE CLASIFICACIÓN AUTOMÁTICA DE CITRUS AURANTIFOLIA USANDO PROCESAMIENTO DIGITAL DE IMÁGENES	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	SUCLUPE CHAPOÑAN MANUELA DEL ROSARIO	EVALUACIÓN DE LA CALIDAD DE UN SISTEMA DE INFORMACIÓN LOGÍSTICA DE CONTROL DEL PROCESO DE ALMACENAMIENTO DE UNA CONSTRUCTORA DE LA SELVA PERUANA	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	PISFIL JAUREGUI JOSE LAURENT	IMPLEMENTACIÓN DE MICROSERVICIOS PARA MEJORAR LA INTEROPERABILIDAD DEL PROCESO DE CONSULTAS DE ARBITRIOS TRIBUTARIOS EN MUNICIPALIDADES	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	CHIMPEN SERQUEN MERLINA JESSICA	DISEÑO DE UNA MESA DE AYUDA BASADO EN ITIL V3 Y BPM PARA EL AREA DE TI DE UNA MUNICIPALIDAD PROVINCIAL DE LAMBAYEQUE	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	CIEZA CELIS JESUS ABELARDO OJEDA ROMERO ANTHONNY JHONATAN	EVALUACIÓN DEL DESEMPEÑO DE PROTOCOLOS DE SEGURIDAD DE REDES PARA COMBATIR VULNERABILIDADES EN REDES INALÁMBRICAS WI-FI	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	FERNANDEZ RIOJA JUAN NICANOR RIOJA MESIA CHARLES SEGUNDO	IMPLEMENTACIÓN DE UN MODELO DE GESTIÓN BASADO EN ITIL PARA MEJORAR LAS ATENCIONES DE INCIDENCIAS DE TI EN UNA MUNICIPALIDAD DISTRITAL DE LA REGIÓN LAMBAYEQUE	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	TEMOCHE GÓMEZ LENNIN BILLEY	MÉTODO PARA DETECTAR CON EFICIENCIA LOS ATAQUES CROSS-SITE SCRIPTING UTILIZANDO TÉCNICAS DE APRENDIZAJE AUTOMÁTICO	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	BOBADILLA CAMPOS ROLANDO MARTÍN GUEVARA CHAMBERGO JHON DENNIS	IMPLEMENTACIÓN DE UNA METODOLOGÍA DE GESTIÓN DE RIESGOS AD HOC BASADA EN ESTÁNDARES INTERNACIONALES Y BUENAS PRÁCTICAS PARA UNA EMPRESA MANUFACTURERA PERUANA	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	CALDERON YNOÑAN PAMELA DEL CARMEN PRIETO NEIRA FRANCK ALBERSON	DESARROLLO DE UN MÉTODO BAJO EL ENFOQUE ÁGIL Y DISEÑO CENTRADO EN USUARIO (DCU) PARA LA MEJORA DE EXPERIENCIA DE USUARIO (UX)	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	CASTRO MEDINA MIGUEL ANGEL	IMPLEMENTACIÓN DE UN MODELO AD HOC DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA EDITORA DE DIARIO REGIONAL PERUANO	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE

UNIVERSIDAD SEÑOR DE SIPÁN

FACULTAD DE INGENIERÍA, ARQUITECTURA Y URBANISMO
RESOLUCIÓN N° 0700-2021/FIAU-USS
Pimentel, 02 de Agosto de 2021

ANEXO

ESCUELA PROFESIONAL	APELLIDOS Y NOMBRES	TEMA DE TESIS	LÍNEA DE INVESTIGACIÓN
INGENIERÍA DE SISTEMAS	BECERRA SANCHEZ MIGUEL ANGEL	EVALUACION DE RENDIMIENTO DE PROTOCOLOS DE COMUNICACIÓN IOT EN EL MONITOREO DE LA CALIDAD DEL AIRE	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	ÑAÑEZ PEREDO ALEXIS JOEL VELASCO CHERO JUNIOR	ADAPTACIÓN DE UNA METODOLOGÍA DE DESARROLLO ÁGIL DE SOFTWARE PARA MYPES PERUANAS DE DESARROLLO DE SOFTWARE	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	VASQUEZ MUÑOZ DEXTRE ALEXANDER	DESARROLLO DE UN MÉTODO DE CONTEO AUTOMÁTICO DE CAPSIUM ANNUUM GROUP BASADO EN APRENDIZAJE PROFUNDO PARA LA ESTIMACIÓN DE SU PRODUCCIÓN	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	CELIS SANCHEZ SUJEILY PEREZ ROJAS FRANKLIN ALEXI	MODELO DE EVALUACION DE PROCESOS TI CON BASE EN EL MARCO DE REFERENCIA COBIT 5 PAM. CASO DE ESTUDIO SIEMPRESOFT E.I.R.L . CHICLAYO	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	PEREZ SILVA EDWIN WILDOR	RECONOCIMIENTO DE PLACAS VEHICULARES MEDIANTE VISION COMPUTACIONAL PARA MEJORAR EL ACCESO A UN PARQUEADERO	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	LUQUE CONDORI BASILIO	EVALUACIÓN DE LA CALIDAD DE APLICACIONES GENERADAS POR BPM PARA LA GESTIÓN DE TRÁMITES EN UNA GERENCIA REGIONAL DE TRANSPORTE PERUANO	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	BRENIS LLAGUENTO JULIO ANTONIO	COMPARACIÓN DE PROTOCOLOS DE AUTENTICACIÓN EN CONEXIONES DE REDES PRIVADAS VIRTUALES PARA USO EN TRABAJO REMOTO. CASO DEESTUDIO: MUNICIPALIDAD PROVINCIAL DE FERREÑAFE	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	AGUILERA ALVARADO YEISSER FROILAN	EVALUACIÓN DEL PERFORMANCE EN LA COMUNICACIÓN DE APLICACIONES CON ARQUITECTURA DE SOFTWARE QUE UTILIZA SERVICIOS WEB EN EMPRESAS CON PRESENCIA NACIONAL	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	JIMENEZ ESPINOZA LUIS ALBERTO	ANÁLISIS DE MÉTODOS DE RECONOCIMIENTO DE EXPRESIONES FACIALES	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE
INGENIERÍA DE SISTEMAS	CARREÑO GUERRERO SANTIAGO ANIBAL	MODELO PREDICTIVO DEL PROCESO DE VENTAS UTILIZANDO INTELIGENCIA DE NEGOCIOS Y DATA ANALITICS EN LA EMPRESA CENTRO TEXTIL DE LA MATTA S.A.C	INFRAESTRUCTURA, TECNOLOGÍA Y MEDIO AMBIENTE

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

CONSTANCIA DE LEVANTAMIENTO DE INFORMACIÓN Y ACCESO A DATOS

Descripción: Otorgar el permiso para el levantamiento de información y acceso a datos de distintas índoles con fines investigativos.

La Industria

"Año del Bicentenario del Perú: 200 años de Independencia"

EL QUE SUSCRIBE:

MG. ESTELA BEATRIZ MIDDLETON PAICO – GERENTE, EN REPRESENTACIÓN DE LA EMPRESA DIARIO LA INDUSTRIA DE CHICLAYO,

DEJO

CONSTANCIA:

Que, el Sr **(a)**: Miguel Angel Castro Medina, identificado (a) con DNI N° 70304485, tiene autorización para acceder a los datos sensibles de la empresa, ya sean datos de facturación, publicitarios y administrativos. Dicha autorización será válida hasta el 31 de Diciembre del año 2021, con posibilidad a actualizar el permiso de autorización.

Se extiende la presente, a solicitud de la parte interesada para los fines que estime conveniente.

Ciudad, 02 de Junio del 2021

Beatriz Middleton Paico
Gerente General
EMPRESA EDITORA LA INDUSTRIA DE CHICLAYO S.A.

.....

(Firma / sello)

Anexo 3. Instrumentos de recolección de datos, con su respectiva validación de los instrumentos.

FORMATO A

AMENAZAS PROBABILIDAD DE OCURRENCIA	1	2	3	4	5
Fuego		X			
Tormenta eléctrica, rayo	X				
Error de usuario				X	
Errores del administrador				X	
Alteración accidental de la información			X		
Destrucción de la información			X		
Fugas de la información			X		
Vulnerabilidades de los programas (software)		X			
Errores de mantenimiento /actualización de programas software			X		
Errores de mantenimiento / actualización de equipos (hardware)			X		
Indisponibilidad del personal por salud			X		
Manipulación de los registros de actividad			X		
Suplantación de la identidad del usuario		X			
Abuso de privilegios de acceso			X		
Difusión de software dañino			X		
Acceso no autorizado				X	
Modificación deliberada de información			X		
Inestabilidad de la línea de internet			X		
Manipulación de programas			X		
Manipulación de equipos			X		
Robo de equipos		X			
Corte del suministro eléctrico			X		
Condiciones inadecuadas de temperatura o humedad		X			
Degradación de los soportes de almacenamiento de la información			X		
Instalación de software no autorizado			X		

VALOR PUNTUACION	
Prácticamente imposible	1
Poco probable	2
Posible	3
Probable	4
Muy probable	5

La información recaudada mediante este cuestionario es propia de la empresa en cuestión, para esto se aplicó la técnica de observación.

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que ud brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible					X
2	Actualidad: Adecuado al avance de la ciencia y tecnología				X	
3	Objetividad: Permite medir hechos observables					X
4	Organización: Presentación ordenada					X
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo				X	
7	Consistencia: Permite conseguir datos basados en modelos teóricos				X	
8	Coherencia: Hay coherencia entre los items				X	X
9	Metodología: La estrategia responde al propósito de la investigación					X
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

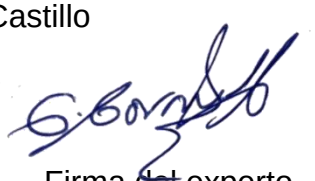
Muchas gracias por su respuesta.

Apellidos y nombres del experto: Gustavo Coronel Del Castillo

DNI: 06914897

Especialidad: Ing. de Sistemas

Grado: Mag. En Ingeniería de Sistemas



Firma del experto

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que ud brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible				X	
2	Actualidad: Adecuado al avance de la ciencia y tecnología				X	
3	Objetividad: Permite medir hechos observables					X
4	Organización: Presentación ordenada				X	
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos				X	
8	Coherencia: Hay coherencia entre los items				X	
9	Metodología: La estrategia responde al propósito de la investigación			X		
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Rojas Ortiz Carlos Antonio

DNI: 16709803

Especialidad: Ing. de Sistemas

Grado: Magister

Firma del experto

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que Ud. brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible					X
2	Actualidad: Adecuado al avance de la ciencia y tecnología					X
3	Objetividad: Permite medir hechos observables					X
4	Organización: Presentación ordenada					X
5	Suficiencia: Comprende los aspectos en cantidad y claridad				X	
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos					X
8	Coherencia: Hay coherencia entre los ítems					X
9	Metodología: La estrategia responde al propósito de la investigación					X
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente				X	

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Fuentes Adrianzén Denny John

DNI: 27858646

Especialidad: Doctorado en Ciencias de la Computación y Sistemas

Grado: Doctor Firma del experto

FORMATO B

CUESTIONARIO SOBRE LA POSIBILIDAD ACEPTACIÓN DEL MODELO AD HOC PARA LA GESTION DE SEGURIDAD DE LA INFORMACION Y DIAGNOSTICO INICIAL DE SEGURIDAD DE LA INFORMACIÓN - MARCA CON UN ASPA (X) NOMBRE: SANTOS GUERRERO CRISANTO CARGO: ADMINISTRADOR

Nº	PREGUNTA	SI	NO
1	¿Sabe Ud. ¿Si dentro de la empresa editora de diario regional peruano existe un sistema de gestión de seguridad de la información?		X
2	¿Cree usted que la implementación de un modelo de seguridad de la información permitirá mejorar la seguridad de la información de su área de trabajo?	X	
3	¿Cree usted que en su área de trabajo se logrará un cambio positivo con la aplicación de este modelo de gestión de seguridad de la información?	X	
4	¿Aprobaría usted la implementación del modelo de gestión de seguridad de la información en su área de trabajo?	X	
5	En su área de trabajo, ¿Aprobaría usted programas dirigidos a todos los empleados para sensibilizar sobre la seguridad de la información?	X	
6	¿Estaría Ud. dispuesto a colaborar para que el diseño e implementación del modelo de gestión de seguridad de la información se lleve a cabo en su área de trabajo?	X	
7	¿Considera Ud. que en su área de trabajo existe información que debe ser protegida?	X	
8	¿Ha recibido Ud. capacitación sobre la seguridad de la información de acuerdo a su función laboral?		X
9	¿Su contrato contempla ítems que estipulen responsabilidades con respecto a la seguridad de la información?		X
10	Dentro de su área de trabajo ¿se considera la seguridad de información cuando se gestiona un proyecto?		X
11	¿Cuenta Ud. con un computador/laptop para realizar sus funciones? (Si la respuesta es No pasar a la pregunta 14)		X
12	¿Cuenta Ud. con una clave de acceso para ingresar a su computador y/o laptop?		
13	Cuando su computador está indefenso ¿Se activa el bloqueo de pantalla con contraseña para proteger la información?		
14	¿En lo que va del año ha sufrido modificación y/o pérdida de información ya sea por virus, acceso de personas no autorizadas, deterioro, tras papeleo, etc.?	X	
15	¿En su área de trabajo se han realizado evaluación de riesgos relacionados con la información?		X
16	¿En su área de trabajo se han realizado una evaluación de vulnerabilidades de la red?		X
17	¿Su área de trabajo cuenta con software antivirus actualizado?	X	
18	¿Considera que su oficina está protegida contra amenazas externas y/o ambientales que ocasionen pérdidas de información?		X

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que ud brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible					X
2	Actualidad: Adecuado al avance de la ciencia y tecnología					X
3	Objetividad: Permite medir hechos observables					X
4	Organización: Presentación ordenada				X	
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos				X	
8	Coherencia: Hay coherencia entre los items				X	X
9	Metodología: La estrategia responde al propósito de la investigación				X	
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Gustavo Coronel Del Castillo

DNI: 06914897

Especialidad: Ing. de Sistemas

Grado: Mag. En Ingeniería de Sistemas

Firma del experto

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que ud brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible					X
2	Actualidad: Adecuado al avance de la ciencia y tecnología					X
3	Objetividad: Permite medir hechos observables					X
4	Organización: Presentación ordenada					X
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos			X		
8	Coherencia: Hay coherencia entre los items				X	
9	Metodología: La estrategia responde al propósito de la investigación			X		
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Rojas Ortiz Carlos Antonio

DNI: 16709803

Especialidad: Ing. de Sistemas

Grado: Magister

Firma del experto

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que Ud. brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible				X	
2	Actualidad: Adecuado al avance de la ciencia y tecnología				X	
3	Objetividad: Permite medir hechos observables					X
4	Organización: Presentación ordenada				X	
5	Suficiencia: Comprende los aspectos en cantidad y claridad				X	
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo				X	
7	Consistencia: Permite conseguir datos basados en modelos teóricos					X
8	Coherencia: Hay coherencia entre los ítems					X
9	Metodología: La estrategia responde al propósito de la investigación					X
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Fuentes Adrianzén Denny John

DNI: 27858646

Especialidad: Doctorado en Ciencias de la Computación y Sistemas

Grado: Doctor

Firma del experto

Validación por método de Xi cuadrado.

El cuestionario anteriormente presentado, está compuesto por una respuesta dicotómica, es decir SI o NO, por lo tanto, el método más recomendable para validarlo es Xi cuadrado, es un método estadístico que se basa en comparar los resultados obtenidos con los resultados esperados. Para ello se le asignó el valor 1 a la respuesta SI y el valor 0 a la respuesta NO.

	Preguntas																	
Sujetos	**P1**	**P2**	**P3**	**P4**	**P5**	**P6**	**P7**	**P8**	**P9**	**P10**	**P11**	**P12**	**P13**	**P14**	**P15**	**P16**	**P17**	**P18**
Trabajador 1	0	1	1	1	1	1	1	0	0	0	0	1	0	0	1	0	0	0
Trabajador 2	0	1	1	0	1	1	1	1	0	0	0	1	0	1	0	1	0	0
Trabajador 3	0	1	1	1	1	1	0	1	1	0	1	1	0	1	0	0	0	0
Trabajador 4	0	1	0	1	1	0	0	1	0	0	0	1	1	0	0	0	0	0
Trabajador 5	0	1	1	1	1	0	1	1	0	0	1	1	0	1	0	1	1	0
Trabajador 6	0	1	1	1	0	1	1	0	0	1	0	1	0	0	1	1	0	1
Trabajador 7	0	0	1	0	0	1	0	0	0	0	0	1	1	0	1	0	0	1
Trabajador 8	1	1	1	1	1	1	1	0	1	1	0	1	1	0	1	0	0	1
Trabajador 9	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	0	1	1
Trabajador 10	0	1	0	1	1	1	1	0	0	1	1	1	0	1	1	0	1	1
Trabajador 11	1	1	1	1	1	1	1	0	1	0	1	1	0	1	1	0	0	0
Trabajador 12	0	1	1	1	1	1	1	0	0	0	0	0	0	0	1	0	0	0
Trabajador 13	1	0	1	0	1	0	1	1	1	0	0	0	0	0	1	0	0	0
Trabajador 14	0	1	1	0	1	0	1	0	0	0	0	1	0	0	1	0	1	0

Trabajador 15	0	0	1	0	0	0	1	1	1	0	0	1	0	0	0	0	1	0
Trabajador 16	0	1	1	1	1	0	0	0	0	0	0	1	0	0	1	1	0	0
Trabajador 17	0	1	1	1	1	1	1	0	1	1	0	1	1	0	1	0	0	0
Trabajador 18	0	0	1	1	1	1	1	0	0	1	0	1	0	1	1	0	0	0
Trabajador 19	0	1	1	1	1	1	1	0	0	0	0	1	0	1	1	1	0	0
Trabajador 20	0	1	1	1	1	1	1	0	0	1	0	1	0	1	1	0	0	0

Después se procedió a generar una tabla en donde se contabilizan la cantidad de respuestas que obtuvieron si y no por cada trabajador de la empresa.

OBSERVADO	SI	NO	TOTAL
P1	3	15	18
P2	16	2	18
P3	17	1	18
P4	14	4	18
P5	16	2	18
P6	14	4	18
P7	16	2	18
P8	6	12	18
P9	7	11	18
P10	6	12	18
P11	4	14	18
P12	18	0	18
P13	4	14	18
P14	8	10	18
P15	15	3	18
P16	5	13	18
P17	5	13	18
P18	5	13	18
	179	145	324
	0.6	0.4	1
	60%	40%	

El valor esperado es el total de respuestas por cada ítem para la respuesta SI es 10 y para la respuesta no es 8, en total suman 18 ítems planteados en el cuestionario.

ESPERADO	SI	NO	TOTAL
P1	10	8	18
P2	10	8	18
P3	10	8	18
P4	10	8	18
P5	10	8	18
P6	10	8	18
P7	10	8	18
P8	10	8	18
P9	10	8	18
P10	10	8	18
P11	10	8	18
P12	10	8	18
P13	10	8	18
P14	10	8	18
P15	10	8	18
P16	10	8	18
P17	10	8	18
P18	10	8	18
	179	145	324
	1	0.4	
	100%	40%	

Para aplicar el método Xi cuadrado se tomó la cantidad observada por cada valor y se restó el valor de la cantidad esperada y se obtuvo un subtotal, posteriormente se realizó la sumatoria por cada valor y la suma dio un resultado de 116.61, lo cual significa que los resultados son asociados, mientras el resultado se aleja más del 0, quiere decir que los datos son asociados y guardan relación.

FORMULA XI CUADRADO	SI	NO	TOTAL
P1	4.85	5.99	10.84
P2	3.69	4.55	8.24
P3	5.01	6.18	11.19
P4	1.65	2.04	3.70
P5	3.69	4.55	8.24
P6	1.65	2.04	3.70
P7	3.69	4.55	8.24

P8	1.56	1.93	3.50	
P9	0.87	1.08	1.95	
P10	1.56	1.93	3.50	
P11	3.55	4.39	7.94	
P12	6.53	8.06	14.58	
P13	3.55	4.39	7.94	
P14	0.38	0.47	0.85	
P15	2.57	3.17	5.74	
P16	2.46	3.03	5.49	
P17	2.46	3.03	5.49	
P18	2.46	3.03	5.49	
	52.18	64.42	116.61	XI CUADRADO

FORMATO C

RELACION DE ACTIVOS - EN CADA TABLA MARQUE (X) LOS ACTIVOS CON LOS QUE CUENTA LA EMPRESA EDITORA DE DIARIO REGIONAL PERUANO

TABLA DE RELACION DE ACTIVOS DE TIPO DATO/INFORMACION

(X) Ficheros o bases de datos
( ) Copias de respaldo
( ) Datos de configuración de los sistemas de información
(X) Datos de gestión interna
(X) Credenciales (Ejem. contraseñas)
( ) Datos de validación de credenciales
( ) Datos de control de acceso
(X) Registro de actividad o de los sistemas de información
( ) Código fuente de los sistemas de información
( ) Código ejecutable de los sistemas de información
( ) Datos de prueba para la implementación de los sistemas de información

TABLA DE RELACION DE ACTIVOS DE TIPO SERVICIO

( ) Anónimo (sin requerir identificación del usuario)
( ) Al público en general (sin relación contractual)
( ) A usuarios externos (bajo una relación contractual)
( ) Interno (a usuarios de la propia organización)
(X) Internet
( ) Acceso remoto a cuenta local
(X) Correo Electrónico
(X) Almacenamiento de ficheros (File Server)
( ) Transferencia de ficheros (FTP)
( ) Intercambio electrónico de datos (EDI)
( ) Servicios de directorio
(X) Gestión de identidades (Servicios que permiten altas y bajas de usuarios de los sistemas)

TABLA DE RELACION DE ACTIVOS DE TIPO SOFTWARE/APLICACIONES INFORMATICAS

(X) Software de desarrollo propio
(X) Software a medida (subcontratado)
(X) Página Web
( ) Intranet
(X) Servidor de aplicaciones
( ) ERP (Enterprise Resource Planning – Planificación de Recursos Empresariales)
(X) Correo electrónico
(X) Sistema de gestión de bases de datos
(X) Ofimática
(X) Antivirus

(X) Sistema operativo
( ) Gestor de máquinas virtuales
( ) Servidor de Terminales
( ) Sistema de backup

TABLA DE RELACION DE ACTIVOS DE TIPO EQUIPOS INFORMATICOS

(X) PCs
(X) Servidor
( ) Equipamiento de respaldo
(X) Medios de impresión (impresoras y servidores de impresión)
( ) Escáneres
(X) Módems
(X) Conmutadores (Swicth)
(X) Encaminadores (Router)
( ) Cortafuegos (Firewall)
( ) Punto de acceso inalámbrico
(X) Teléfono IP
( ) Otros.
……
…..

TABLA DE RELACIÓN DE ACTIVOS DE TIPO REDES DE COMUNICACIONES

(X) Red telefónica
( ) Comunicaciones radio
(X) Red inalámbrica
(X) Telefonía móvil
(X) Red local
(X) Internet

TABLA DE RELACIÓN DE ACTIVOS DE TIPO SOPORTE DE INFORMACIÓN

(X) Discos Duros
( ) Discos virtuales
(X) Almacenamiento en red
( ) Disquetes
( ) Cd (CD-ROM)
(X) Memorias USB
( ) DVD
( ) Cinta magnética
( ) Tarjetas de memoria
( ) Tarjetas inteligentes
(X) Material impreso
( ) Cinta de papel
( ) Otros.
…….

TABLA DE RELACIÓN DE ACTIVOS DE EQUIPAMIENTO AUXILIAR

(X) Fuentes de alimentación
( ) Generadores eléctricos
(X) Cable eléctrico
( ) Fibra óptica
( ) Equipos de destrucción de soportes de información
( ) Suministros esenciales
(X) Mobiliario, armarios, etc.
( ) Otros:
……

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que ud brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible				X	
2	Actualidad: Adecuado al avance de la ciencia y tecnología				X	
3	Objetividad: Permite medir hechos observables				X	
4	Organización: Presentación ordenada				X	
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos					X
8	Coherencia: Hay coherencia entre los items				X	
9	Metodología: La estrategia responde al propósito de la investigación					X
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Gustavo Coronel Del Castillo

DNI: 06914897

Especialidad: Ing. de Sistemas

Grado: Mag. En Ingeniería de Sistemas

Firma del experto

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que ud brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible				X	
2	Actualidad: Adecuado al avance de la ciencia y tecnología				X	
3	Objetividad: Permite medir hechos observables			X		
4	Organización: Presentación ordenada					X
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos			X		
8	Coherencia: Hay coherencia entre los items				X	
9	Metodología: La estrategia responde al propósito de la investigación					X
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Rojas Ortiz Carlos Antonio

DNI: 16709803

Especialidad: Ing. de Sistemas

Grado: Magister

Firma del experto

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que Ud. brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible			X		
2	Actualidad: Adecuado al avance de la ciencia y tecnología				X	
3	Objetividad: Permite medir hechos observables				X	
4	Organización: Presentación ordenada				X	
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo			X		
7	Consistencia: Permite conseguir datos basados en modelos teóricos					X
8	Coherencia: Hay coherencia entre los ítems					X
9	Metodología: La estrategia responde al propósito de la investigación					X
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Fuentes Adrianzén Denny John

DNI: 27858646

Especialidad: Doctorado en Ciencias de la Computación y Sistemas

Grado: Doctor

Firma del experto

FORMATO D

	DESCRIPCCION	MARCA	MODELO
	Teclado	Genius	SLIM STAR310
	Mouse	Genius	GM-04003A XSCROLL
	CPU	Cooler Master	-
	Placa	Intel	DP45SG
1	Procesador	Intel	Intel(R) Core(TM)2 Quad CPU Q6600 @ 2.40GHz
	RAM	-	-
	Disco Duro	Samsung	HD502IJ
	Lectora DVD	LG	HL-DT-ST DVDRAM GH20LS15
	Tarjeta de Red	Intel	82567LF-2 Gigabit Network Connection
	Tarjeta de Video	NVIDIA	GeForce 7300 SE/7200 GS
	Monitor	LG	L1982U
	Teclado	IBM	Y-SU61
	Mouse	Logitech	P90
	CPU	Ciberlink	-
	Placa	Intel	D945GCNL
2	Procesador	Intel	Intel(R) Core(R) i3 6100 3.70Ghz
	RAM	-	-
	Disco Duro	Seagate	ST1000DM003-1CH162
	Lectora DVD	LG	
	Tarjeta de Red		
	Tarjeta de Video		
	CPU	IBM	System Xseries 206m
	Placa		
	Procesador	Intel	Pentium 4 HT
3	RAM		
	Disco Duro	IBM	IBM ServeRAID
	Tarjeta de Red		
	Tarjeta de Video		
	Monitor	LG	Flatrom W19435B
	Teclado	IBM	
	Mouse	Logitech	Micronics
	CPU	Cooler Master	
4	Placa		
	Procesador	Intel	Intel Core 2 Quad 2.40Ghz
	RAM		
	Disco Duro		3 HD de 931 GB c/u
	Tarjeta de Red		
	Tarjeta de Video		
5	CPU	HP	Proilant ML110 Gen9

Placa	HP	
Procesador	Intel	Xeon CPU E5-2602 V4
RAM		
Disco Duro		4 HD. 1 de 80 GB, 1 de 1 TB, 1 de 500 GB, 1 de 3 TB
Tarjeta de Red		
Tarjeta de Video		-

Ficha de observación trabajadores de la empresa

Área	**Número de trabajadores**
Ventas y publicidad	2
Contabilidad	3
Sistemas y soporte técnico	1
Administración	1
Gerencia	1
Diseño y Diagramación	4
Almacén e impresión	4
Redacción	4

Ficha de observación incidencias en servidores y evidencia de ataques informáticos a los servidores de la empresa.

Servidor	**Incidencia**	**Fecha de incidencia**
SAP	Virus Trojan.MultiGenAutorunWHI.a	Enero 2020
	Virus HackTool.MSII.HackKMS.d	Enero 2020
	Virus Trojan.Win32.PcShare.s	Enero 2020
Baltazar	Apagado por falta de energía eléctrica.	Marzo 2020
FileServer	Falta de seguridad en carpetas y archivos	Marzo 2020

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que ud brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible				X	
2	Actualidad: Adecuado al avance de la ciencia y tecnología				X	
3	Objetividad: Permite medir hechos observables					X
4	Organización: Presentación ordenada				X	
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos					X
8	Coherencia: Hay coherencia entre los items					X
9	Metodología: La estrategia responde al propósito de la investigación					X
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Gustavo Coronel Del Castillo

DNI: 06914897

Especialidad: Ing. de Sistemas

Grado: Mag. En Ingeniería de Sistemas

Firma del experto

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que ud brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible					X
2	Actualidad: Adecuado al avance de la ciencia y tecnología				X	
3	Objetividad: Permite medir hechos observables					X
4	Organización: Presentación ordenada					X
5	Suficiencia: Comprende los aspectos en cantidad y claridad					X
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos					X
8	Coherencia: Hay coherencia entre los items					X
9	Metodología: La estrategia responde al propósito de la investigación			X		
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Rojas Ortiz Carlos Antonio

DNI: 16709803

Especialidad: Ing. de Sistemas

Grado: Magister

Firma del experto

FICHA DE VALIDEZ DE CONTENIDO

Título de la investigación:

Implementación de un modelo ad hoc de gestión de seguridad de la información para una empresa editora de diario regional peruano.

Juicio de experto

La opinión que Ud. brinde debe ser personal y sincera.

Marque con un aspa “X” dentro del cuadro de valoración, solo una vez por cada criterio, el que usted considere su opinión sobre el cuestionario.

1. Muy malo
2. Malo
3. Regular
4. Bueno
5. Muy bueno

Nº	Criterio	Valoración				
		1	2	3	4	5
1	Claridad: Esta formulado con un lenguaje claro y comprensible				X	
2	Actualidad: Adecuado al avance de la ciencia y tecnología					X
3	Objetividad: Permite medir hechos observables				X	
4	Organización: Presentación ordenada					X
5	Suficiencia: Comprende los aspectos en cantidad y claridad				X	
6	Pertinencia: Permite conseguir datos de acuerdo al objetivo					X
7	Consistencia: Permite conseguir datos basados en modelos teóricos				X	
8	Coherencia: Hay coherencia entre los ítems				X	
9	Metodología: La estrategia responde al propósito de la investigación					X
10	Aplicación: Los datos permiten un tratamiento estadístico pertinente					X

Muchas gracias por su respuesta.

Apellidos y nombres del experto: Fuentes Adrianzén Denny John

DNI: 27858646

Especialidad: Doctorado en Ciencias de la Computación y Sistemas

Grado: Doctor

Firma del experto

Anexo 4. Acta de compromiso de la empresa para cumplir con las políticas de seguridad a implementar.

La Industria

ACTA DE COMPROMISO DE CUMPLIMIENTO PARA LAS POLITICAS DE SEGURIDAD IMPLEMENTADAS

Chiclayo 08 de Noviembre del 2021

Empresa Editora La Industria de Chiclayo

Area de sistemas y soporte técnico

Estimados Srs.

Por medio de la presente acta hago constatar que, a la fecha actual, las políticas de seguridad ya han sido implementadas, es obligación del responsable del área de sistemas y soporte técnico, así como también del administrador de la empresa, velar por el cumplimiento de estas políticas de seguridad, que tienen como única finalidad, proteger la información contable, publicitaria y administrativa de la empresa.

Atentamente:

Miguel Angel Castro Medina
Responsable del área de sistemas
y soporte técnico

EMPRESA EDITORA LA INDUSTRIA DE CHICLAYO S.A.
C.P.C. Santos Guerrero Crisanto
ADMINISTRADOR

Santos Manuel Guerrero Crisanto
Administrador

Anexo 5. Carta de compromiso de la organización, para la implementación de los controles de seguridad.

La Industria

CARTA DE COMPROMISO PARA LA IMPLEMENTACIÓN DE POLITICAS DE SEGURIDAD DENTRO DEL DIARIO LA INDUSTRIA DE CHICLAYO

Chiclayo 12 de Noviembre del 2021

Empresa Editora La Industria de Chiclayo

Area de sistemas y soporte técnico

Estimado Sr. Miguel Angel Castro Medina

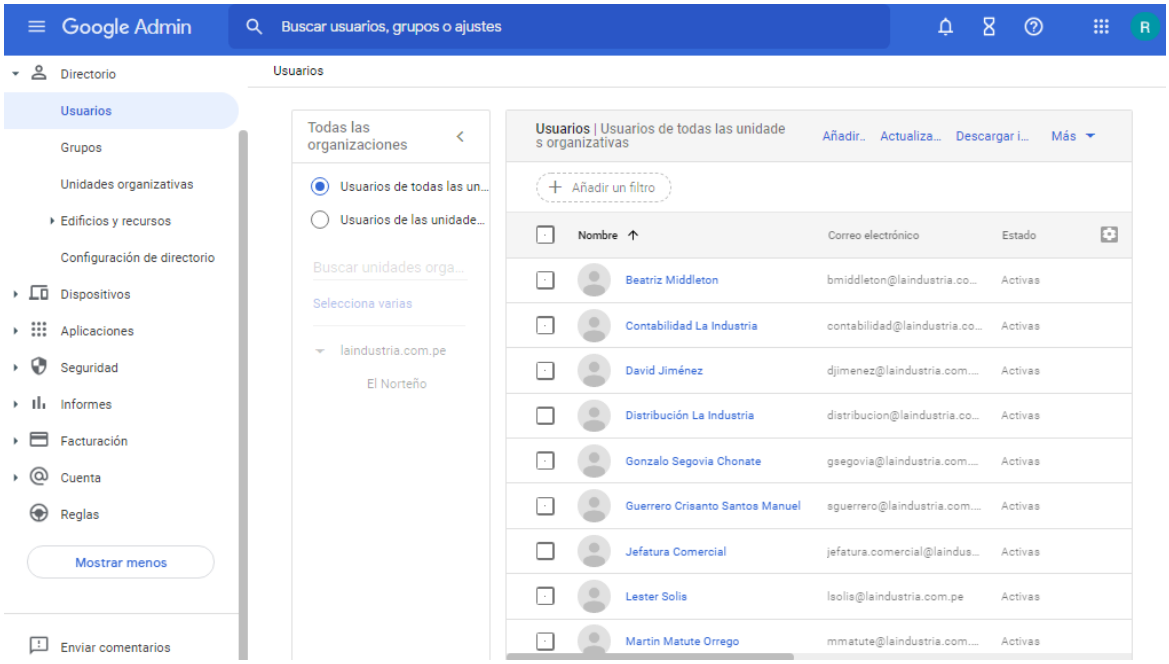
Por medio de la presente carta de compromiso, la empresa editora La Industria de Chiclayo se compromete a participar activamente de la implementación de las políticas de seguridad que Ud. Crea conveniente aplicar. Así mismo la empresa saluda la dedicación y el esfuerzo que su persona realiza constantemente, no solo para cumplir con su universidad, si no en su labor como responsable del área de sistemas y soporte técnico. La empresa se compromete a darle todas las facilidades para el desarrollo de su proyecto de investigación, dentro de nuestra institución.

Atentamente:

EMPRESA EDITORA LA INDUSTRIA DE CHICLAYO S.A.
C.P.C. Santos Guerrero Crisanto

Santos Manuel Guerrero Crisanto
Administrador

Anexo 6. Administración de cuentas de usuarios de todos los colaboradores de la empresa editora de diario regional peruano, la empresa Xertica es la responsable de administrar los correos de todo el personal que labora en la empresa, sin embargo, a través de la opción administración, es posible visualizar distintos parámetros, como el uso de su bandeja Gmail, espacio de almacenamiento en google drive, y gestionar las contraseñas, para ser cambiadas periódicamente.



Anexo 7. Backup realizado a los Información de facturación almacenados en el servidor FileServer, de esta manera se protegen los datos más sensibles pertenecientes al área de contabilidad.

backup_adm.BAT

```
robocopy "\\SERVER\bmilton"          "Z:\backup_serveradm\bmilton_bk"    /MIR     /E /R:3 /W:0 /V /MT:50
robocopy "\\SERVER\Cotizaciones"     "Z:\backup_serveradm\cotizaciones_bk"   /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\SERVER\ddelgado"         "Z:\backup_serveradm\ddelgado_bk"   /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\SERVER\jesus"        "Z:\backup_serveradm\jesus_bk"      /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\SERVER\jjimenez"         "Z:\backup_serveradm\jjimenez_bk"   /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\SERVER\PDT - Sunat"      "Z:\backup_serveradm\pdtsunat_bk"   /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\SERVER\rgaray"       "Z:\backup_serveradm\rgaray_bk"     /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\SERVER\sguerrero"        "Z:\backup_serveradm\sguerrero_bk"  /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\SERVER\Sistem"       "Z:\backup_serveradm\sistem_bk"     /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\FILESERVER\jrenteria"        "Z:\backup_serveradm\jrenteria_bk"  /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\FILESERVER\cotizaciones"         "Z:\backup_serveradm\cotizaciones_bk"   /MIR    /E /R:3 /W:0 /V /MT:50
robocopy "\\FILESERVER\distribucion lesly"       "Z:\backup_serveradm\distribucionlesly_bk"  /MIR    /E /R:3 /W:0 /V /MT:5
log+:C:\BACKUP_INFO.log
cmd.exe
```

Anexo 8. Implementación de un dispositivo SAI para asegurar la continuidad de la red, así como también todos los servidores que maneja la empresa editora de diario regional peruano.

Así mismo se utiliza el archivo hosts protegido con contraseña para evitar que los trabajadores ingresen a páginas web que no corresponden al trabajo que ellos realizan.

backup periodista.bat | hosts

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#      102.54.94.97     rhino.acme.com          # source server
#       38.25.63.10     x.acme.com              # x client host

# localhost name resolution is handled within DNS itself.
#   127.0.0.1       localhost
#   ::1             localhost
```

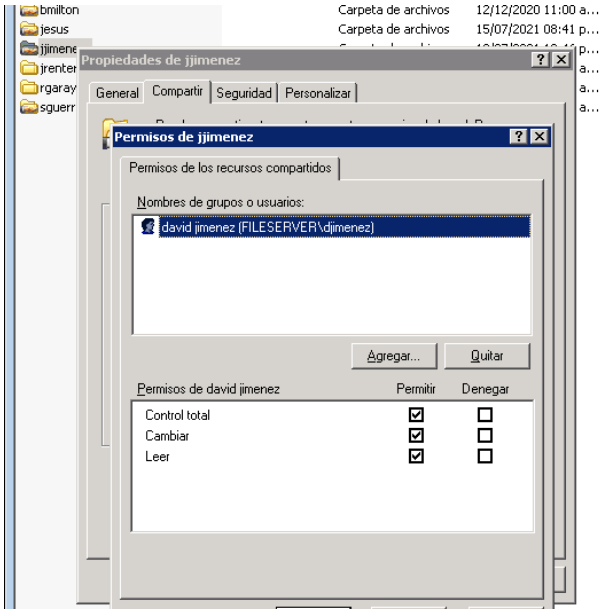
Anexo 9. Backup de los datos de publicaciones y ejemplares que maneja la empresa editora de diario regional peruano, esto aplica al servidor Baltazar y FileServer.

backup_adm.BAT | backup_pp.BAT

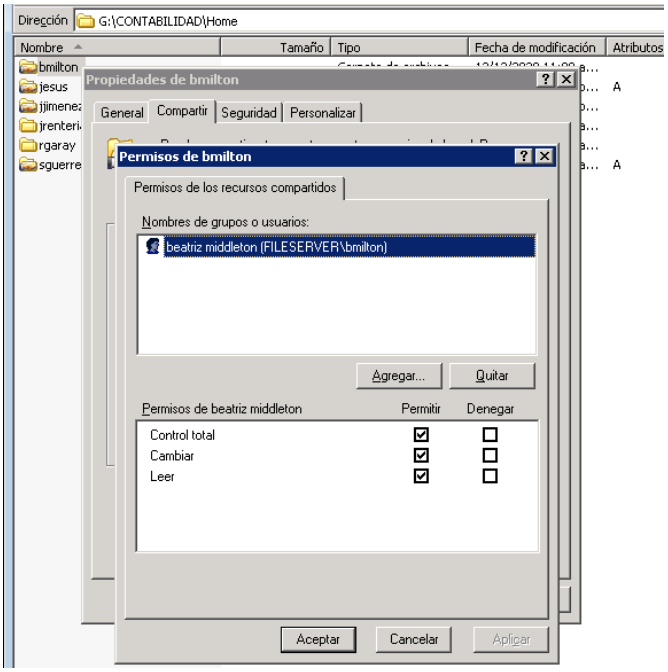
```
1  robocopy "\\Fileserver\pre-prensa" "Y:\backup_preprensa"  /COPYALL /E /R:3 /W:0 /XA:SH /MT:50 /XF *.idlk *.db *.DS_Store
2  cmd.exe
3
```

Anexo 10. Guardado de registros de información de servidores.

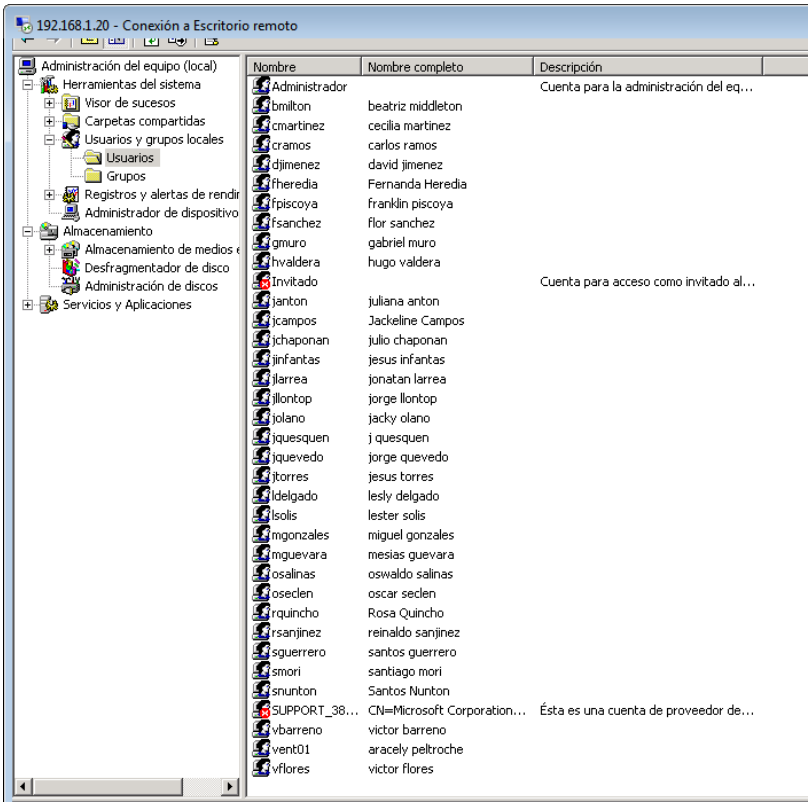
Anexo 11. Gestión de permisos al usuario del Sr. David Jiménez, jefe de contabilidad, para evitar perdida de información valiosa y tener un mayor control en cuanto a información que manejan demás colaboradores.



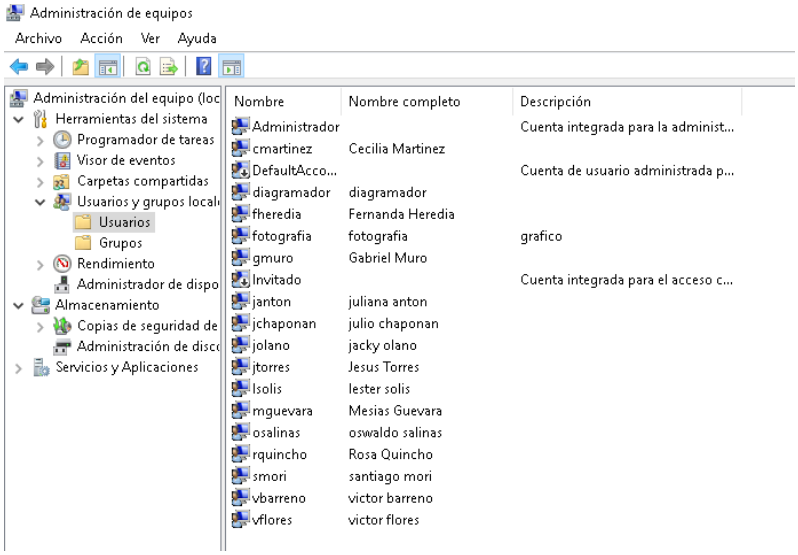
Anexo 12. Gestión de permisos al usuario de la Sra. Beatriz Middleton, gerente de la empresa editora de diario regional peruano, de esta manera nadie podrá acceder a sus datos, así como también poder guardar datos contables de manera segura.



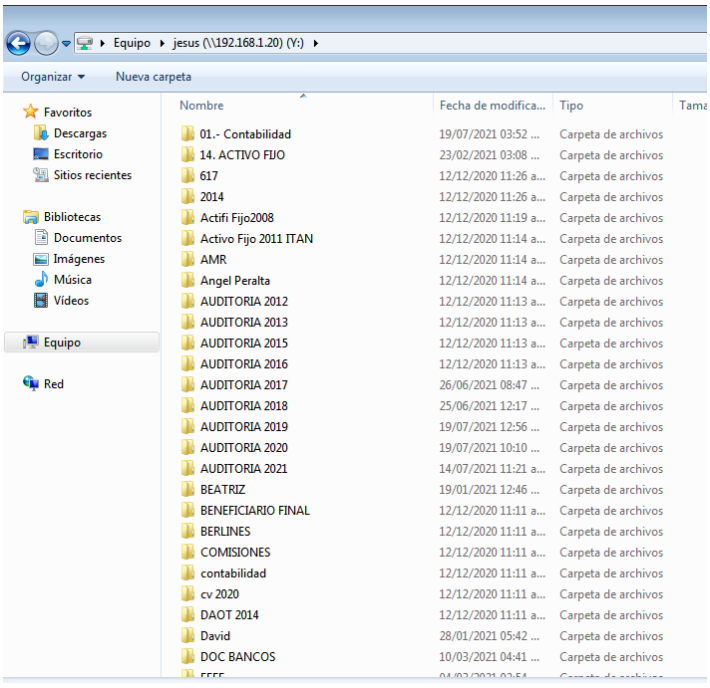
Anexo 13. Administración de usuarios, representados por todos los colaboradores que laboran en la empresa editora de diario regional peruano, de esta manera se pueden brindar y denegar accesos a determinada información.



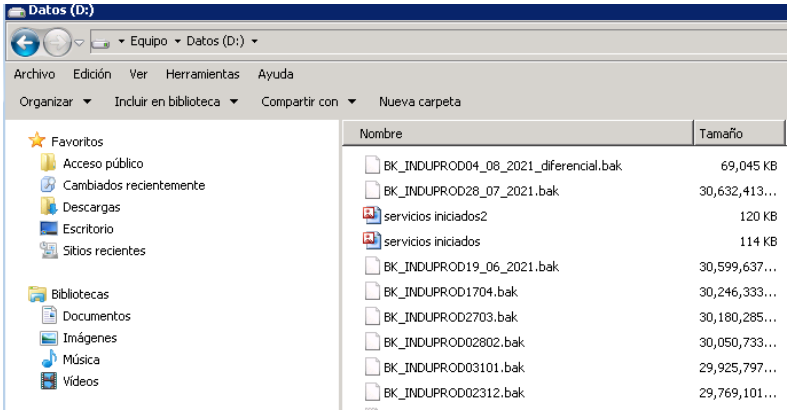
Anexo 14. Administración de usuarios en el servidor FileServer, servidor que se encarga de almacenar toda la información referente a publicidad y medios impresos, así como también almacena todos los archivos en formato pdf, que se generan diariamente para posteriormente ser impresos y distribuidos.



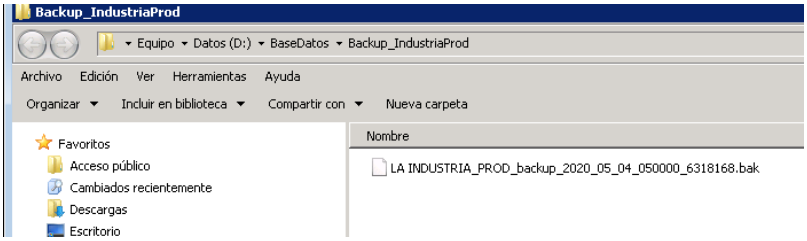
Anexo 15. Unidad de almacenamiento alojada en el servidor FileServer, perteneciente al área de contabilidad.



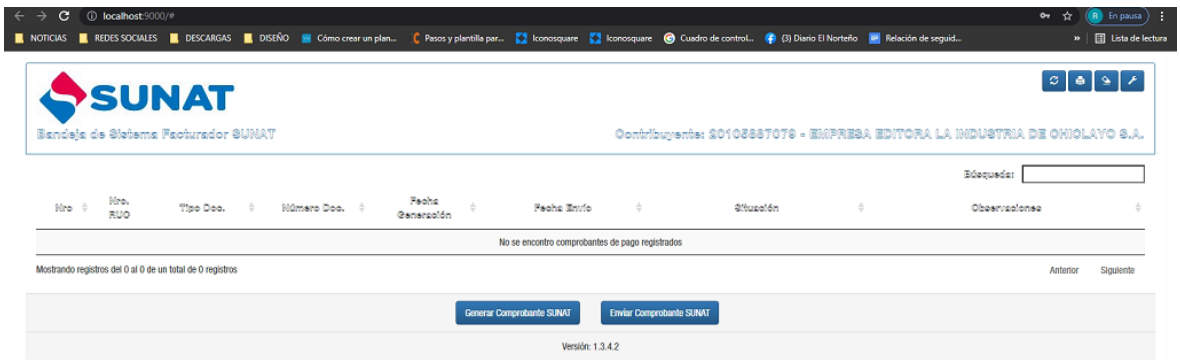
Anexo 16. Backups realizados a la base de datos principal de la empresa editora de diario regional peruano, dicha base de datos tiene por nombre PROD_INDUPROD y se generan una vez a la semana, más precisamente el día domingo.



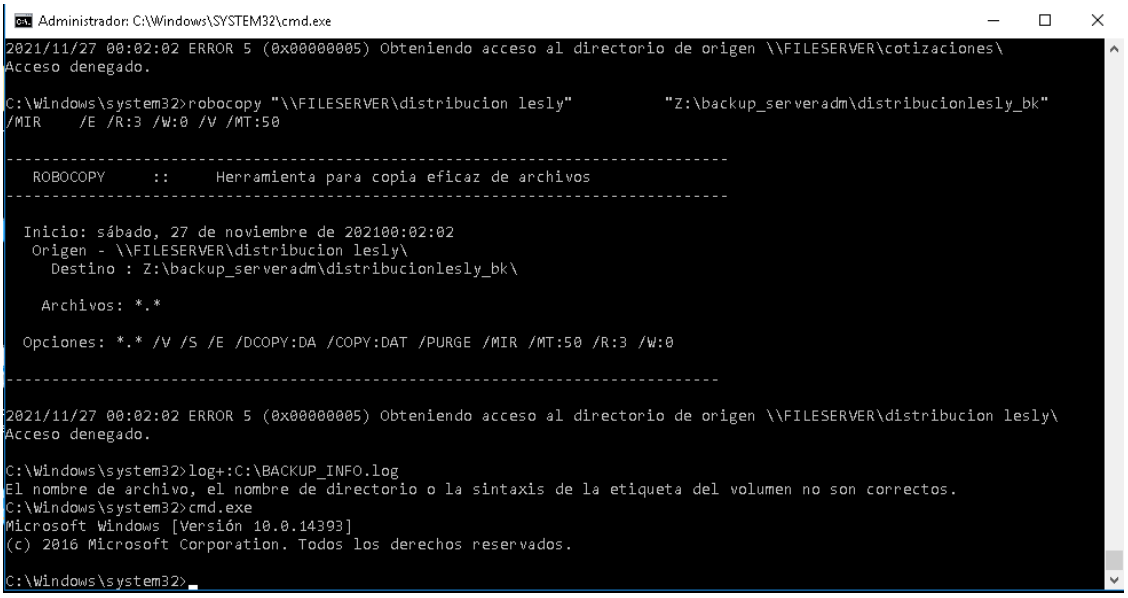
Anexo 17. Backup realizado periódicamente para proteger la información de facturación y contabilidad que maneja la empresa.



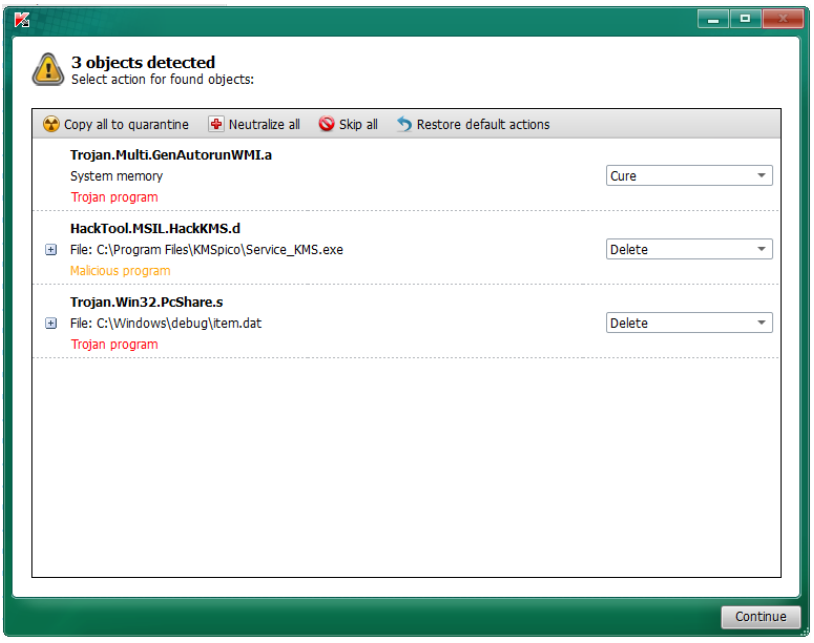
Anexo 18. Aplicación de facturación perteneciente a sunat, como medida de alternativa en caso se presente algún fallo con el software de pago SAP Bussisnes ONE.



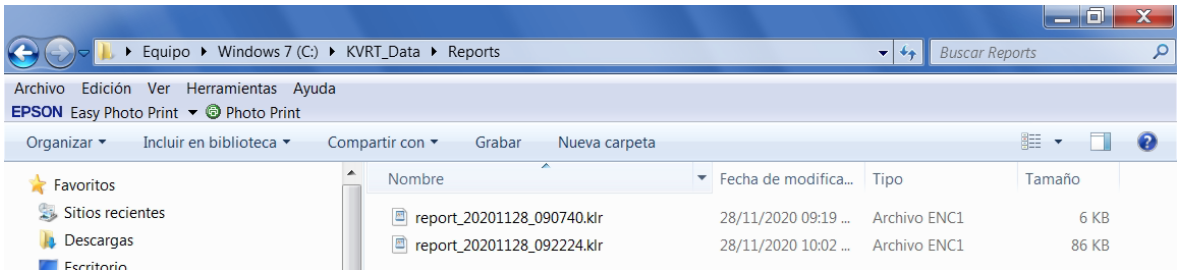
Anexo 19. Backup realizado al área de contabilidad y administración, perteneciente al servidor FileServer, dicho backup se realizó el día 27 de noviembre a las 02:00 de la madrugada.



Anexo 20. Reporte de antivirus Karspersky, dejando en evidencia que se hallaron dos virus en el servidor principal de producción de la empresa editora de diario regional peruano.



Anexo 21. Archivos que contienen reporte de los daños causados por el virus que ataco el servidor FileServer hace aproximadamente 8 meses.



Anexo 22. Documento formal donde se evidencia la implementación de las políticas de seguridad elaborados en el presenta trabajo de investigación.

GESTIÓN DE SEGURIDAD DE LA INFORMACION

La Industria

EMPRESA EDITORA DIARIO LA INDUSTRIA DE CHICLAYO

ELABORADO POR:

MIGUEL ANGEL CASTRO MEDINA

RECIBIDO Y APROBADO POR:

AREA DE GERENCIA Y ADMINISTRACIÓN

SANTOS MANUEL GUERRERO CRISANTO

ADMINISTRADOR

FECHA DE ENTREGA:

26 DE NOVIEMBRE DEL 2021

NORMATIVAS Y POLITICAS DE SEGURIDAD IMPLEMENTADAS EN EL AREA DE SISTEMAS Y SOPORTE TÉCNICO DE LA EMPRESA EDITORA DIARIO LA INDUSTRIA DE CHICLAYO

Objetivo: Con la finalidad de proteger la integridad de la información que maneja el Diario La Industria de Chiclayo, se consideró pertinente y oportuno implementar las siguientes políticas de seguridad.

Alcance: Área de sistemas y soporte técnico.

Datos de facturación	
Política de seguridad	Administración de correos
Detalle	Los usuarios del área de contabilidad guardan su información en correos electrónicos y espacios acondicionados en la plataforma de google drive, es por ello que es conveniente gestionar las contraseñas y permisos, cambiarlos periódicamente, para evitar fuga de información.
Estado	Implementado

Datos de facturación	
Política de seguridad	Backups de respaldo
Detalle	Se realizó la copia de seguridad para todos los datos contables que se almacenan actualmente en el servidor FileServer.
Estado	Implementado

Red wifi	
Política de seguridad	Plan de continuidad
Detalle	La empresa cuenta con 3 routers en general los cuales están adosados a un SAI, asegurando su funcionalidad ante un corte de energía. También se modificaron archivos hosts para evitar el acceso a páginas indebidas y de esta manera evitar la infecciona por virus de tipo malware.

Estado	Implementado

Servidor Baltazar y FileServer	
Política de seguridad	Backups de respaldo
Detalle	Se realizó las copias de seguridad respectivas para salvaguardar toda la información concerniente a los datos de publicaciones y ejemplares que posee el diario.
Estado	Implementado

Servidor Baltazar y FileServer	
Política de seguridad	Registro de configuración
Detalle	Estos registros permiten tener una guía de los parámetros de configuración y servicios que posee el servidor, en caso se agote la batería interna de los SAI y no haya regresado el suministro eléctrico.
Estado	Implementado

Discos duros del área de administración y contabilidad	
Política de seguridad	Backups de respaldo
Detalle	La información correspondiente a las áreas críticas de la empresa, como el área de administración y contabilidad, se encuentran respaldas por copias de seguridad almacenadas en un servidor dedicado. Así mismo si ocurriese un fallo en algún disco duro de las computadoras que maneja esta área, fácilmente de podrá restaurar su información.
Estado	Implementado

Discos duros del área de administración y contabilidad	
Política de seguridad	Registro de configuración
Detalle	Es importante almacenar las configuraciones como el tamaño de las unidades de disco, para de esta

	manera poder restaurar de manera correcta el disco duro.
Estado	Implementado

Discos duros del área de administración y contabilidad	
Política de seguridad	Backups de respaldo
Detalle	Los usuarios de contabilidad, administración, diagramación tienen su información respaldada, gracias a los backups realizados en un horario especifico.
Estado	Implementado

Discos duros del área de administración y contabilidad	
Política de seguridad	Registro de configuración
Detalle	Es importante guardar los registros de configuración tanto de puerto Ethernet, como las distintas configuraciones de permisos que pueda tener cada usuario.
Estado	Implementado

Discos duros del área de administración y contabilidad	
Política de seguridad	Planes de continuidad
Detalle	Los usuarios tienden a tener fallos al momento de laborar con software o archivos que contienen información sensible, es por ello que como plan de continuidad se habilitó una nueva computadora al área de ventas, en caso sea necesario ante alguna falla en la ventanilla número uno.
Estado	Implementado

SAP Bussisnes ONE	
Política de seguridad	Administración de correos
Detalle	Los usuarios al momento de usar el software de pago SAP Bussisnes ONE guardan sus reportes en sus correos, es por ello que las contraseñas se cambiaran periódicamente para evitar fuga de información.

Estado	Implementado

SAP Bussisnes ONE	
Política de seguridad	Planes de continuidad
Detalle	Como plan de continuidad se instaló el facturador sunat, para de esta manera si falla el software SAP Bussisnes ONE, el personal de venta pueda realizar la facturación con esta aplicación gratuita impartida por sunat.
Estado	Implementado

Anexo 23. Documento formal donde se evidencia la recolección de información a través de fichas de observación.

La Industria
EL GRAN DIARIO DEL NORTE desde 1952

FICHAS DE OBSERVACIÓN DIARIO LA INDUSTRIA DE CHICLAYO

FICHA DE OBSERVACIÓN		
FICHA Nº	01	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
4 días	Sala de TI	Se caracterizó todos los componentes informáticos que se ubican en dicha área.

FICHA DE OBSERVACIÓN		
FICHA Nº	02	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
1 día	Empresa	Se contabilizo la cantidad de colaboradores que laboran en la empresa editora La Industria de Chiclayo.

FICHA DE OBSERVACIÓN		
FICHA Nº	03	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
4 días	Sala de TI	Se caracterizan las incidencias en servidores y evidencia de ataques informáticos a los servidores de la empresa.

FICHA DE OBSERVACIÓN		
FICHA Nº	04	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
2 días	Gerencia	La empresa cuenta con normativa para protección de instalaciones físicas, realizadas por un especialista electricista.

La Industria
EL GRAN DIARIO DEL NORTE desde 1952

FICHA DE OBSERVACIÓN		
FICHA Nº	05	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
2 días	Gerencia	La empresa maneja una política de seguridad de utilizar celulares solo con red 3G en sus colaboradores y además no poseen características de celulares de tipo Smartphone.

FICHA DE OBSERVACIÓN		
FICHA Nº	06	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
7 días	Sala de TI	Caracterización de ocurrencias de amenazas y posibles sucesos que atenten contra la integridad y disponibilidad de la información que maneja la empresa.

FICHA DE OBSERVACIÓN		
FICHA Nº	07	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
7 días	Sala de TI	La empresa no cuenta con normativa sobre políticas para asegurar la información y protegerla en caso de algún incidente.
	Empresa	Todas las áreas cuentan con computadoras que no poseen antivirus y todos los usuarios poseen los mismos privilegios de acceso al momento de utilizar carpetas en red en los distintos servidores que están disponibles.

FICHA DE OBSERVACIÓN		
FICHA Nº	08	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
1 día	Empresa	Los correos Gmail no poseen ningún tipo de respaldo.

La Industria
EL GRAN DIARIO DEL NORTE desde 1952

FICHA DE OBSERVACIÓN		
FICHA Nº	09	
ELABORADO POR:	Bach. Miguel Angel Castro Medina	
LUGAR:	Diario La Industria de Chiclayo	
SECTOR:	Área de TI	
TIEMPO	**OBSERVADO**	
7 días	Empresa - requerimientos	La empresa necesita proteger su información. La empresa no cuenta con normativas de seguridad de la información ni ninguna otra medida de protección física ni lógica contra perdida de datos. Formalizar la protección de datos en el área de TI.

Bach. Miguel Angel Castro Medina
Responsable – Área de sistemas LI

EMPRESA EDITORA LA INDUSTRIA DE CHICLAYO S.A.
C.P.C. Santos Guerrero Crisanto

Adm. Santos Manuel Guerrero Crisanto
Administrador