FACULTAD DE INGENIERÍA

CARRERA DE INGENIERÍA DE SISTEMAS COMPUTACIONALES

"USO DE LA NORMA ISO 27001 Y SU INFLUENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA ICO EL AÑO 2021"

Tesis para optar el título profesional de:

Ingeniero de Sistemas Computacionales

Autor:

Henry Alexander Ticona Llerena

Asesor:

Ing. Mg. Rodas Cueva Richard

Lima - Perú

2021

ACTA DE AUTORIZACIÓN PARA PRESENTACIÓN DEL TRABAJO DE INVESTIGACIÓN

El asesor Franchesca Rodríguez Rivera, Docente de la Universidad Privada del Norte, Facultad de Ingeniería, Carrera profesional de INGENIERÍA DE SISTEMAS COMPUTACIONALES, ha realizado el seguimiento del proceso de formulación y desarrollo de la investigación del estudiante:

Ticona Llerena, Alexander Henry

Por cuanto, **CONSIDERA** que el trabajo de investigación titulado: USO DE LA NORMA ISO 27001 Y SU INFLUENCIA EN LA SEGURIDAD DE INFORMACIÓN DE LA EMPRESA ICO EL AÑO 2021 para aspirar al título profesional por la Universidad Privada del Norte, reúne las condiciones adecuadas, por lo cual AUTORIZA al interesado para su presentación.

_____

Ing. /Lic./Mag./Dr. Nombre y Apellido

Asesor

ACTA DE EVALUACIÓN DEL TRABAJO DE INVESTIGACIÓN

El comité del trabajo de investigación, conformado por: El jurado; designados mediante el área de Coordinación de la facultad de Sistemas Computacionales ha procedido a realizar la evaluación del trabajo de investigación del estudiante: Ticona Llerena Henry Alexander para aspirar al título profesional con el trabajo de investigación: Uso de la norma ISO 27001 y su influencia en la seguridad de la información de la empresa ICO año 2021

Luego de la revisión del trabajo en forma y contenido los miembros del jurado acuerdan:

( ) Aprobación por unanimidad

Calificativo:
( ) Excelente [18 -20]
( ) Sobresaliente [15 - 17]
( ) Buena [13 - 14]

( ) Aprobación por mayoría

Calificativo:
( ) Excelente [18 -20]
( ) Sobresaliente [15 - 17]
( ) Buena [13 - 14]

( ) Desaprobación

Firman en señal de conformidad

Ing./Lic/Dr/Mag. Nombre Apellido
Miembro del Comité

Ing./Lic/Dr/Mag. Nombre Apellido
Miembro del Comité

Ing./Lic/Dr/Mag. Nombre Apellido
Miembro del Comité

DEDICATORIA

Dedico esta investigación a mi familia, que gracias a su apoyo incondicional he podido llegar lejos.

AGRADECIMIENTO

Agradezco a todas las personas que me animaron en todo momento y me cuidaron, también a mis compañeros que día a día me ayudaron a ser un mejor profesional.

Tabla de Contenido

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Uso de la norma ISO 27001 y su influencia en la de seguridad de información de la empresa ICO FOOD SERVICE el año 2021

La presente investigación tiene como objetivo determinar en qué medida el uso de norma ISO 27001 influye en la seguridad de la información de la empresa ICO, año 2021.

El enfoque empleado en esta investigación fue cuantitativo. La presente investigación usó para su propósito el diseño experimental del tipo pre-experimental, donde se trabajó con 18 unidades de estudio. A las unidades de estudio de la muestra seleccionada se aplicó un pretest y postest, teniendo como instrumento de recolección de datos un cuestionario y la técnica utilizada fue la encuesta. El instrumento de recolección de datos está constituido por 14 ítems, donde se utilizó la escala de Likert (1-muy bajo, 2-bajo, 3-medio, 4-alto y 5 muy alto). En el cuestionario los responsables de los sistemas de recursos empresariales (ERP) proporcionaron información sobre la variable dependiente ISO 27001 y la variable independiente seguridad de la información, mediante la evaluación de sus distintas dimensiones.

Ahora bien, la presente investigación determina que el uso de la ISO 27001 no influye de manera significativa en la mejora la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021 con un nivel de significancia.

Palabras clave: ISO 27001, Seguridad de la información, Matriz Rasci, Control de Madurez, Magerit, SGSI y MinTic.

CAPITULO 1 INTRODUCCIÓN

1.1 Bases Teóricas

Bases teóricas de ISO

Definición

El término ISO según Del Castillo y Sardi, (2012) proviene de un vocablo griego que significa 'igual', y se aplica a las normas ISO como a la institución que lleva el mismo nombre. Su objetivo es clasificar el sistema de estándares internacionales. En los comités técnicos es donde se realizan las actividades de la ISO, de tal manera que cada uno se encarga de sus áreas respectivamente.

Además de ello, la norma ISO no solamente se enfoca en ciertos rubros, sino que se puede aplicar a diferentes sectores, según Alba (2017) manifiesta que:

> Es la mayor organización mundial desarrolladora de Normas Internacionales voluntarias. ISO como organización, nace en 1947, y desde ese momento han publicado más de 20000 normas internacionales diferentes y de muy variados sectores, de ámbitos tecnológicos y de negocios.

Asimismo, las normas ISO siguen una serie de pasos para que puedan ser empleadas por las diferentes organizaciones. Al respecto la Secretaria Central de la ISO (2010) comenta que:

> Es una red mundial que identifica cuáles normas internacionales son requeridas por el comercio, los gobiernos y la sociedad; las desarrolla conjuntamente con los sectores que las van a utilizar; las adopta por medio de procedimientos transparentes basados en contribuciones nacionales proveniente de múltiples partes interesadas; y las ofrece para ser utilizadas a nivel mundial.

Familias ISO

Cuando se habla de las normas ISO, es imprescindible no comentar de sus tipos, existen al menos 22600 estándares publicados, según Smyth, (2019) menciona que:

> Hay varios tipos de normas ISO, los más conocidos son las normas de gestión de la calidad, la gestión de seguridad alimentaria y ambiental, la gestión de seguridad de la información y la gestión de riesgos.

ISO de la Calidad

Esta Norma Internacional se basa en los principios de la gestión de la calidad descritos en la Norma ISO 9000, según Yzaguirre (2005) comenta que:

> La norma ISO 9001 promueve la adopción de un enfoque basado en procesos para desarrollar, implementar y mejorar la eficacia de un Sistema de Gestión de la Calidad para aumentar la satisfacción del cliente mediante el cumplimiento de sus requisitos, necesidades y expectativas.

Ahora bien, las normas ISO de la calidad no solamente sirven como modelo, sino que es la base para la implementación de sistemas de gestión de la calidad, según Rentería, (2019) menciona que:

> Un Sistema de Gestión de la Calidad es un conjunto de actividades y procesos que interactúan entre sí para lograr unos objetivos orientados a la calidad de la organización asimismo se enfoca a la integración armoniosa de todos los elementos requeridos para desarrollar una gestión encaminada a cumplir los acuerdos y requerimientos establecidos.

Por otra parte, la norma ISO de la calidad sigue una serie de pasos fundamentales, Collado, (2015) comenta que:

Estos principios son las herramientas primordiales para lograr una gran gestión de la calidad, de la misma forma brinda una guía para lograr un desempeño exitoso.

En cuanto al detalle de estos principios, Collado (2015) lo segmenta en 8 principios que son:

Principio 1: Enfoque al cliente

Las organizaciones dependen de sus clientes y por lo tanto deben comprender sus necesidades actuales y futuras, satisfacer sus requisitos y esforzarse en exceder sus expectativas

Principio 2: Liderazgo

Los líderes establecen la unidad de propósito y la orientación de la organización. Ellos deberían crear y mantener un ambiente interno en el cual el personal pueda llegar a involucrarse totalmente en el logro de los objetivos de la organización. El rol del líder en este caso implica el mantener a las personas comprometidas en la labor desarrollada.

Principio 3: Participación del Personal

El personal en todos los niveles, es la esencia de una organización y su total compromiso posibilita que sus habilidades sean usadas para el beneficio de ésta. Es por ello que la organización debe preocuparse por mantener a su personal satisfecho y enfocado en la obtención de resultados.

Principio 4: Enfoque basado en procesos

Un resultado deseado se alcanza más eficientemente cuando las actividades y los recursos relacionados se gestionan como un proceso. Es indispensable identificar tales procesos y la interacción que existe entre ellos.

Principio 5: Enfoque de Sistema para la Gestión

Identificar, entender y gestionar los procesos interrelacionados como un sistema que contribuye a la eficacia y eficiencia de una organización en el logro de sus objetivos.

Principio 6: Mejora Continua

La mejora continua en el desempeño global de la organización debería ser un objetivo permanente de ésta. Esto se refiere a que dentro de la organización siempre se debe buscar alguna oportunidad para seguir mejorando

Principio 7: Enfoque basado en hechos

Las decisiones eficaces se basan en el análisis de los datos y la información. Se debe impedir la toma de decisiones a partir de supuestos o repentinas opiniones.

Principio 8: Relación con Proveedores

Una relación mutuamente beneficiosa aumenta la capacidad de una organización y sus proveedores para crear valor, dado que estos son interdependientes.

Normas ISO del Medio Ambiente

En la actualidad a nivel mundial las normas ISO 9000 y la ISO 14000 son requeridas, debido a que garantizan la calidad de un producto mediante la implementación de controles exhaustivos, al respecto Salas (s.f.) comenta que:

> La ISO 14000 no es solo una norma, sino que forma parte de una familia de normas que se refieren a la gestión ambiental aplicada a la empresa, cuyo objetivo consiste en la estandarización de formas de producir y prestación de servicios que protejan el medio ambiente.

Además de ello, la norma también se puede aplicar a empresas de todos los tipos y tamaños, Cubas y Mendoza, (2018) comentan que:

> ISO 14001 describe la estructura organizativa, la planificación de actividades responsabilidades, prácticas, procedimientos, procesos y recursos para preparar, aplicar revisar y mantener la política ambiental de la organización.

Ahora bien, la ISO del medio ambiente detalla los requerimientos de un sistema de gestión ambiental, al respecto Manzano, (2017) menciona que:

> La ISO 14000 es un conjunto de normas que constituye un modelo uniforme para un sistema de gestión ambiental.

Ahora bien, como se puede observar la ISO del medio ambiente sigue una serie de procedimientos para que este sea aplicado, al respecto Rivera, (2017) comenta que:

> La ISO 14000 es una serie de normas de gestión medioambiental aceptadas internacionalmente. Esta serie, que se ha convertido en uno de los patrones de referencia más acreditados a nivel mundial, la serie de normas ISO 14000 sobre gestión ambiental incluye un conjunto de normas y estándares propuestos.

Normas ISO aplicadas a la Gestión de Riesgos

Las normas ISO para la gestión de riesgos maneja tres componentes fundamentales que son los principios, su estructura y el proceso, según Jose-Marti y Lizarzaburu, (2016) comenta que:

> Es una guía de implementación que pretende ayudar a las organizaciones en el desarrollo de su propio enfoque de gestión del riesgo. Mediante la implementación de la norma ISO 31000, las organizaciones pueden comparar sus prácticas de gestión de riesgos con un punto de referencia reconocido internacionalmente para conseguir una gestión eficaz de los riesgos y un buen gobierno corporativo (p. 35).

Además de ello, como se puede observar las normas ISO de Riesgos tiene como finalidad poder gestionar el riesgo y mitigarlo, según Rodríguez (2016) menciona que:

> La norma ISO 31000 tiene por objetivo el poder gestionar los riesgos en la empresa de forma efectiva proporcionando una colección de términos y definiciones relativas a la gestión del riesgo.

Por otra parte, la norma ISO 31000 para la gestión de riesgo no solamente se enfoca en ciertos rubros o en organizaciones grandes, según Ruiz (2016) menciona que:

> La gestión de riesgos en base a la norma ISO 31000 puede aplicarse a toda una organización, en sus áreas y niveles, en cualquier momento, así en cuanto a funciones específicas, proyectos y actividades. El genérico enfoque descrito en esta norma establece los principios y directrices para la gestión de cualquier forma de riesgo de manera sistemática, transparente y creíble y en cualquier ámbito y contexto.

Además de ello, la norma ISO para la gestión del riesgo recomienda 3 aspectos para optimizar el marco de referencia, según Cervantes, Hernández y Reyes (2017) mencionan que:

> Esta normal internacional recomienda a las organizaciones a desarrollar. Implementar y mejorar continuamente el marco de referencia cuyo propósito es integrar el proceso para gestionar el riesgo en la organización,

englobando la gobernabilidad, estrategias, planeación, documentación de procesos, políticas, valores y cultura

Normas ISO de Seguridad de la Información

La norma ISO 27000 está compuesta por estándares o fases de desarrollo, Chicaiza (2015) en relación a esta norma se refiere como:

> Un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña. Existen distintas normas que componen la serie ISO 27000 con las cuales se pueden implementar un sistema de gestión de seguridad de la información (SGSI) principalmente basado en ISO 27001 en conjunto con las otras normas de la serie 27000 pero también con otros sistemas de gestión. (p. 7)

Dicho de otra manera, la ISO 27000 está compuesta o equipada con herramientas que nos permitirán implantar un sistema de gestión de la seguridad de la información utilizando otras normas para mejorar este SGSI.

Asimismo, la norma 27000 facilita la comprobación de un sistema de gestión de seguridad de la información. Al respecto, Magda (2016) menciona que:

> La norma 27000 permite verificar la importancia de la implementación de un Sistema de Gestión de Seguridad de Información, una introducción a ellos, además de una descripción de pasos a seguir para las empresas u organizaciones que deseen certificarse con esta familia perteneciente a los estándares ISO. (p. 15)

Hay que hacer notar que el uso de la norma 27000 permite comprobar la importancia de un sistema de gestión de seguridad de la información, así como las especificaciones minuciosas que permitirá a una empresa poder certificarse en la familia ISO 27000.

En el proceso de implementación, la ISO 27000 presenta una serie de reglas para poder establecer un sistema de gestión de seguridad de la información, según ISO (como se citó en Imbaquingo y Pusdá, 2015), afirma que: "Es un conjunto de normas que especifican los requisitos para establecer, implantar, poner en funcionamiento, controlar, revisar, mantener y mejorar un SGSI." (p. 13)

Finalmente se puede afirmar que la norma ISO 27000 brinda los fundamentos necesarios para una correcta implementación de un sistema de gestión de seguridad de la información. Según Ortega y Cumbe (2016), el uso de la norma 27000: "Aporta con las bases del por qué es importante la implementación del SGSI y los pasos a seguir para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (p.14).

Definición de la Normas ISO 27001

Cuando se hace mención de la creación de los estándares internacionales de la norma 27001 se debe tomar conciencia en la razón de su aplicación, según Zeña (2015) afirma que: "La creación del estándar internacional ha sido preparado para proporcionar un modelo con el objetivo de establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI)." (p. 29), Así mismo la ISO 27001 se encarga de una serie de obligaciones, para mejorar la seguridad de la información, según Sandoval (2014) afirma que: "El criterio fundamental de la serie contiene las obligaciones del procedimiento de gestión de seguridad de la información. Se fundamenta en la BS 7799-2:2002 y es la política con ajuste a la certificación, por auditores externos." (p. 49), A continuación, una de las funcionalidades de la ISO 27001 es la de gestor de la información, según Vilca (2017) declara que:

> El estándar 27001 ha sido preparado para proporcionar y promover un modelo con el objetivo de establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de Información. La adopción de este estándar debe ser tomada en cuenta como una decisión estratégica para la organización. (p. 12-13).

Cuando se habla de gestionar la seguridad de información es necesario comentar sobre la estructura de la norma ISO 27001.

Por otra parte, la norma ISO está formado por tres conceptos fundamentales, para preservar la información, según Berros y Rocha (2015) manifiestan que: "La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización." (p. 25)

Alcance de la ISO 27001 en la organización

El alcance de la aplicación de la ISO 27001 en la organización puede abarcar desde su uso interno como externo hasta la conformación de un sistema de gestión de seguridad de la información, según INDECOPI C. d. (como se menciona en Encala & Quispe, 2015) afirma lo siguiente sobre el uso de la norma ISO 27001:

> Puede usarse en el ámbito interno y externo de las organizaciones. Esta Norma Técnica Peruana está diseñada para hacer posible que una organización se alinee o integre su SGSI con los requisitos de los sistemas de gestión relacionados. (p. 20)

Se tiene en cuenta que el alcance de la aplicación de la ISO 27001 ayuda de manera considerable a las organizaciones con su uso interno y externo, además de la integración de los requerimientos de los sistemas de gestión con el sistema de seguridad de la información.

Así pues, la implementación de la norma ISO 27001 puede ser llevado por cualquier tipo de organización abarcando la correcta gestión de la seguridad de la información. (Ramírez & Moreira, 2017)

Además, la ISO 27001 en su alcance llega a abarcar un análisis de riesgos evitando un daño perjudicial en la organización, según Guerrero (2016) nos menciona lo que abarca el uso de la ISO 27001:

> Es una norma que ayuda a gestionar la seguridad de la información en cualquier tipo de organización, analizando las amenazas, vulnerabilidades y riesgos laborales que se presentan, permitiendo tener una información segura gracias a la Integridad, Disponibilidad y Confidencialidad que esta

> brinda a todo momento, logrando que se cumplan las políticas establecidas y tener una buena imagen en la empresa. (p. 18)

Como se ha dicho esta norma ISO 27001 llega a abarcar la gestión de seguridad de la organización analizando los riesgos que se puedan presentar asegurando que la información cumpla los 3 principios que son la Integridad, confidencialidad y disponibilidad.

Además de ello, el alcance de la ISO 27001 establece una gestión de riesgos donde se recopila la información necesaria para poder tratar los riesgos asimismo el uso de políticas de control como medida de seguridad, según Cuervo (2017) nos menciona que:

> La norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente. Luego de ello analizar las medidas de seguridad (o controles) que se van a implementar, por lo general, bajo la forma de políticas, procedimientos e implementación técnica. (p. 7)

Hay que destacar que la ISO 27001 busca encontrar y tratar los riesgos a través de su gestión de riesgos e implementa medidas de seguridad en forma de políticas.

Importancia de la ISO 27001

Acerca de la importancia de la ISO 27001:2013 es un pilar importante para la implementación de un sistema de gestión de seguridad de la información usando los procesos que ofrece para salvaguardar la información, según Lema (2017), nos dice que:

> El estándar ISO-IEC 27001:2013 es la columna vertebral de un Sistema de Gestión de Seguridad (SGSI) de la Información, estableciendo procesos para proteger la confidencialidad, integridad y disponibilidad de la información de una organización y mejora continua del sistema de gestión. (p. 22)

Es decir que para poder resguardar la información de una organización es vital que se use la norma 27001 debido a los tres principios que conlleva su uso.

La aplicación de la ISO 27001 conlleva la protección activos con grandes estándares de protección, según Cordero (2015): "Altos niveles de seguridad en temas de datos confidenciales. Especifica los requerimientos para establecer, implantar, documentar, revisar, mantener y evaluar un sistema de gestión de seguridad de la información." (p. 6)

No obstante, cabe mencionar que una de las importancias de la ISO 27001 es proveer una ayuda en el manejo de la seguridad de la información, según Herrera (2015) mención lo siguiente sobre la ISO 27001: "Brinda el apoyo en la gestión de responsabilidades específicas en cuanto a la seguridad de la información, esta debe ser planificada, implementada supervisada, revisada y mejorada con esto se permite disminuir los riesgos." (p. 25)

A continuación, se menciona como la norma 27001:2013 es vital para el tratamiento de los riesgos que presentan las organizaciones, según Palacios (2015) destaca la importancia de la implementación de la ISO 27001 en que:

> Incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza. (p. 31)

Lo más importante del establecimiento de la ISO 27001:2013 es la adaptación de los requisitos y capacidad de tratamiento de los riesgos dentro de las organizaciones.

Bases teóricas de la Seguridad de la información

Definición de la Seguridad de la información

Con respecto a la seguridad de la información esta se ha convertido hoy en día en un tema de importancia estratégica tanto para empresas como para la sociedad. Igual de importante es digitalizar una empresa como lo es mantener segura la información de la compañía. Debido a grandes fallos de seguridad el cuidado de la información se ha convertido en un tema muy delicado y prioritario para las organizaciones (Fresneda, 2017).

A continuación, la seguridad de la información menciona que se debe mantener la confidencialidad, la integridad y la disponibilidad de la información y los datos más relevantes para la organización, indistintamente de la forma que tengan, los cuales pueden ser electrónicos, papel, audio o video. (Isotools, 2015).

Sin embargo, se considera a la seguridad de la información como conjunto de estrategias para gestionar los procesos, las herramientas y las políticas necesarias para prevenir, detectar, documentar y contrarrestar las amenazas a la información digital y no digital. (Rouse, 2016)

Realizar correctamente la gestión de la seguridad de la información requiere de establecer y mantener, los controles y las políticas de seguridad que tienen la obligación de conservar la confidencialidad, la integridad y la disponibilidad de la información de la empresa. (Jansen, 2016)

Según la ISO los tres principios fundamentales en los que se basa la seguridad de la información son la Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados, Integridad mantenimiento de la exactitud y completitud de la información y sus métodos de proceso y la Disponibilidad de acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Gestión de riesgos de seguridad de la información

La gestión de riesgos de seguridad de la información es el proceso de identificar, comprender, evaluar y mitigar los riesgos y sus vulnerabilidades subyacentes y el impacto en la información, los sistemas de información y las organizaciones que dependen de la información para sus operaciones. (Sullivan, 2016)

La gestión de riesgos se presenta entonces como una actividad clave para el resguardo de los activos de información de una organización y en consecuencia protege la capacidad de cumplir sus principales objetivos. Es un proceso constante que permite a la administración balancear los costos operacionales y económicos causados por la interrupción de las actividades y la pérdida de activos, con los costos de las medidas de protección a aplicar sobre los sistemas de información y los datos que dan soporte al funcionamiento de la organización, reduciendo los riegos que presentan los activos de información a niveles aceptables para la misma. (Lujan, 2012)

El proceso de gestión de riesgos involucra cuatro actividades cíclicas como la identificación de activos y los riesgos a los que están expuestos, el análisis de los riesgos identificados para cada activo, la selección e implantación de controles que reduzcan los riesgos y el seguimiento, medición y mejora de las medidas implementadas. En base a lo mencionado no basta con solamente gestionar el riesgo de la seguridad de la información con la ISO 27001, sino que es necesario apoyarse en metodologías que permitan un análisis y gestión de riesgos, una de las muchas que existen actualmente puede ser la Octavo (Espinoza, Martínez y Amador, 2014)

Implementación de un SGSI

El sistema de gestión de la seguridad de la información es vista por la ISO 27001 como parte de un sistema gestión general, según el Instituto colombiano de normas técnicas y certificación (como se citó en Benavides & Blandón, 2017) afirman que:

> Es una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, mantener y mejorar la seguridad de la información, permitiendo el control sobre los sistemas de información y la información que se maneja en la organización. (p. 40)

Es decir que los sistemas de gestión se establecen para tener un mejor control y mejorar la seguridad sobre los sistemas de información de una organización.

Respecto a la implementación de un sistema de gestión de la seguridad de la información, la ISO/IEC 27003:2010 establece una correcta guía para poder utilizarlo. En este mismo sentido, Santos (2016) sostiene que: "Propone una guía de implementación para un SGSI, para lo cual indica etapas, documentos y roles que pueden permitir la adecuada atención de los requisitos establecidos en la ISO/IEC 27001: 2013." (p.7).

Así pues la implementación del sistema de la seguridad de la información (SGSI), según Moyana y Suaréz (2017) afirman que:

> La implementación de un SGSI debe tener en cuenta el tamaño de la organización, los procesos a incluir en el alcance de la norma, la criticidad de la información, la tecnología utilizada por la organización y las disposiciones legales a enfrentar. (p. 20)

Además, la correcta implementación del sistema de seguridad de la información se debe a la definición de los procesos de la organización que deben estar contemplado por la ISO 27001.

Lo más importante sobre la implementación del sistema de gestión de la seguridad de la información es utilizar la metodología recomendada, según Talavera (2015) menciona que:

> Utiliza la metodología Plan-Do-Check-Act también llamado ciclo de Deming para definir las fases de vida y mejora continua del SGSI a través de un seguimiento del mismo que asegura el mantenimiento de los controles y los

> cambios necesarios para poder mitigar los posibles nuevos riesgos que aparezcan luego de la implementación del sistema. (p. 41)

Es decir, usando la metodología recomendada podremos definir correctamente las fases de la vida del sistema de gestión de la seguridad de la información mitigando los posibles riesgos.

Dimensión Integridad

Definición de Integridad

La integridad de la información solo puede ser alterada por el personal autorizado, según Prieto (2016) nos dice acerca de la integridad que:

> Garantiza la modificación, manipulación, borrado y almacenamiento de archivos solo por el personal autorizado de forma controlada, en este sentido provee metodologías de seguridad por niveles y logs de auditoría para salvaguardar la información de las organizaciones, Pymes, empresas y/o compañías. (p. 19)

Es decir, la integridad debe ser controlada por el personal autorizado, de manera que se podrán realizar procedimientos los cuales servirán para auditorias que permitirán resguardar la información.

Después uno de los conceptos de la integridad es proteger completamente los archivos, según Medina (2015) nos afirma sobre la integridad que: "Es la protección del estado completo de los activos. Que se mantenga al 100% en todos sus componentes" (p. 144)

Además, la integridad de la información requiere estar siempre de manera correcta, según Contreras (2016) nos dice que la integridad es un: "Mantenimiento de la exactitud y validez de la información, protegiéndola de modificaciones o alteraciones no autorizadas" (p. 44)

Así pues, la integridad de la información debe ser exacto y completo, según García & Gutiérrez nos dice que la integridad esta: "relacionada con la precisión y

completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio." (p. 40)

Ahora bien, es primordial que la información no sufra ninguna alteración ya que esto puede generar que se decida de manera errónea, al respecto según Romero, Figueroa y Vera (2015) mencionan que:

> "El hecho de trabajar con información errónea puede ser tan nocivo para las actividades como perder la información, de hecho, si la manipulación de la información es lo suficientemente sutil puede causar que se arrastre una cadena de errores acumulativos y que sucesivamente se tome decisiones equivocadas." (p.17)

Además de ello, se conoce que la integridad de la información supone que la información se mantenga inalterada, al respecto Guamán, (2015) menciona que:

> Asegurar que la información recibida sea exactamente igual a la información enviada, es decir que no haya sido dañada por errores de transmisión o alterada intencionalmente en su contenido o en su secuencia. Propiedad de salvaguardar la exactitud y la totalidad de los activos

Ahora bien, la integridad busca entonces prevenir modificaciones no autorizadas de la información, al respecto Calderón, (s.f.) menciona que:

> La integridad hace referencia a la fidelidad de la información o recursos, y normalmente se expresa en lo referente a prevenir el cambio impropio o desautorizado.

Así pues, la integridad de la información se define como el cambio de la información o los datos, según Borghello, (2001) lo define como:

> La característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado y esta modificación sea registrada para posteriores controles o auditorias.

Además de ello, como se puede observar la integridad es una característica fundamental en la información, según Ayala y Gómez, (2011) comentan que:

> Es la propiedad que busca mantener los datos libres de modificaciones no autorizadas.

Dimensión Confidencialidad

Definición de Confidencialidad

La información debe ser entendible por las personas con permisos autorizados, según Costas (2014) menciona que la confidencialidad es la: "Cualidad de un mensaje, comunicación o datos, para que solo se entiendan de manera comprensible o sean leídos, por la persona o sistema que esté autorizado. Comprende por tanto la privacidad o protección de dicho mensaje y datos que contiene." (p. 17)

Luego para preservar la confidencialidad de la información se debe tener procesos definidos y detallados donde indiquen o señalen quien está recibiendo la información, según Baca (2015) nos menciona acerca de la confidencialidad que: "Los procesos deben describir con detalle quién o quiénes son los encargados de la recepción, procesamiento, almacenamiento y envío de la información ya sea dentro o fuera de la empresa. La actividad y responsabilidad en cada etapa es distinta" (p. 174)

Así mismo la confidencialidad de la información una de sus objetivos es que no se permita la propagación de la información, según Joyanes (como se citó en Bernaldo, 2016) afirma que:

> La confidencialidad, es la propiedad de prevenir la divulgación no autorizada de la información. Es decir, es la accesibilidad sólo para los usuarios autorizados y se opone a la divulgación no autorizada. Hace referencia a la necesidad de ocultar o mantener un secreto sobre determinada información o recursos. (p. 23)

Como se ha dicho en esta cita, la confidencialidad vela por evitar que no se filtre y se propague la información sin un consentimiento autorizado, solo se puede tener acceso por usuarios autorizados a esta información.

A continuación, se muestra que la confidencialidad propone a mitigar las distintas amenazas que se presenten que estén en busca de información privada, según Vodia (2015) nos informa sobre la meta de los acuerdos de confidencialidad que: "mitigan las amenazas de ingeniería social, divulgación de información y espionaje interno. Para evitar que personal nocivo ingrese al Data Center con el objetivo de comprometer la seguridad de la información" (p. 25)

Ahora bien, como se ha podido observar, la información es lo más valioso en una organización, al respecto Romero, Figueroa y Vera, (2018) menciona que la confidencialidad de la información:

> "Consiste en asegurar que sólo el personal autorizado accede a la información que le corresponde, de este modo cada sistema automático o individuo solo podrá usar los recursos que necesita para ejercer sus tareas." (p.26)

Asimismo, Romero, Figueroa y Vera, (2018) mencionan que, para garantizar la confidencialidad de la información, se tiene que tener en cuenta tres recursos muy importantes los cuales se detallan a continuación

- Autenticación de usuarios: Sirve para identificar qué quién accede a la información es quien dice ser.

- Gestión de privilegios: Para los usuarios que acceden a un sistema puedan operar sólo con la información para la que se les ha autorizada y sólo en la forma que se les autorice, por ejemplo, gestionando permisos de lectura o escritura en función del usuario.

- Cifrado de información: Según Costas Santos (2011), el cifrado también denominado encriptación, evita que ésta sea accesible a quién no está autorizado, para ello se transforma la información de forma inteligible a una no legible y es aplicable tanto a la información que esté autorizado para ello como para la que no lo está, sólo mediante un sistema de contraseñas puede extraerse la información de forma inteligible y es aplicable tanto a la información que está siendo transmitida como a la almacenada.

Por otra parte, el controlar el acceso a la información es fundamental para poder respetar este principio asimismo este viene de la mano con la confidencialidad de la información, según Guamán, (2015) menciona que:

> El control de acceso y la confidencialidad de la información son dos atributos fundamentales que trabajan de manera conjunta para lograr una protección robusta de la información contra personas o entidades no autorizadas.

Así pues, la ausencia confidencial de la información puede generar que este pierda su valor o que se vuelva inconsistente, al respecto Borghello, (2001) comenta que:

> La confidencialidad de la información es la necesidad de que la misma solo sea conocida por personas autorizadas. En casos de falta de confidencialidad de la información puede provocar severos daños a su dueño o volverse obsoleta.

Dimensión Disponibilidad

Definición de Disponibilidad

La disponibilidad de la información se encarga de que los usuarios siempre tengan acceso a su información mientras estén autorizados, según Cáceres & Mena (2015) mencionan lo siguiente acerca de la disponibilidad: "Garantía que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran" (p. 52)

Así mismo la disponibilidad debe estar funcional cuando la información sea requerida, según el departamento de Defensa de los Estados Unidos de América (mencionado Hincapié, 2017) nos menciona que la disponibilidad es:

> Una medida en la cual el ítem está en un estado operable y puede estar comprometido en el inicio de un uso específico, para el momento en que el servicio sea necesitado o llamado en un punto desconocido en el tiempo (aleatorio). (p. 33)

Hay que hacer notar que el Departamento de Defensa de los Estados Unidos ve a la disponibilidad como un ítem el cual debe estar siempre operable desde un inicio, para cualquier servicio que lo necesite.

Además en la disponibilidad de la información nos indican que se debe a la persistencia de acceso a los diferentes archivos que tengan alojados en un sistema, según García & Villegas citado en Sandoval (2017) menciona lo siguiente acerca de la disponibilidad: "Se refiere a la continuidad de acceso a los elementos de información almacenados y procesados en un sistema informático."(p. 22)

Así pues, la disponibilidad de la información se debe encontrar listo para los usuarios o aplicaciones quieran acceder a la información, según Lemus (2014) citado en Águila (2015) menciona que la disponibilidad es:

> La característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. Grosso modo, la disponibilidad es el acceso a la información y

a los sistemas por personas autorizadas en el momento que así lo requieran. (p. 15)

Lo más importante de la cita mencionada es que la disponibilidad permite que la información siempre sea accesada por personas autorizadas.

Ahora bien, la información y sistemas son seguros si solo accede a la información y recursos quien solamente tenga los permisos correspondientes, al respecto Romero, Figueroa y Vera, (2018) menciona que:

> "Para que la información resulte disponible, este tiene que resultar útil y valiosa para quien la necesite, asimismo se debe implementar las medidas necesarias para que tanto la información como los servicios se encuentren a disposición del personal autorizado" (p.26).

Así pues, la disponibilidad de la información permite a los usuarios acceder a la información en cualquier momento y desde cualquier lugar, según Guamán, (2015) define la disponibilidad como:

> La acción de asegurarse que los sistemas trabajen prontamente con un buen desempeño y garantizar la protección y la recuperación del sistema en caso de ataque o desastre. Propiedad de estar accesible y utilizable bajo demanda de una entidad autorizada.

Ahora bien, tener disponible la información para los usuarios es uno de los propósitos principales de los sistemas de información, según Borghello, (2001) menciona que:

> La disponibilidad de la información es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y software funcionando correctamente.

Asimismo, tener la información de manera disponible para los usuarios permitidos genera que se agilicen los procesos o peticiones, según Guzman, (2015) lo define como:

> La capacidad de acceder a información o utilizar un servicio siempre que lo necesitemos.

Además de ello, lo que se busca con la disponibilidad de la información es prevenir la discontinuidad de las solicitudes, al respecto Calderón, (s.f.) menciona que:

> La disponibilidad hace referencia a que la información del sistema debe permanecer accesible a elementos solamente autorizados.

Dimensión Riesgos

Definición de Riesgos

Los riesgos en la seguridad de la información se enfoca en ciertos factores para perjudicar la información, según Guzmán & Taboada (2015) no dicen acerca de los riesgos que: "Pueden llegar a pasar cuando están de la mano la vulnerabilidad y la amenaza juntas las cuales generan un daño o perdida de la estructura física, material o humana." (p. 78)

Además, los riesgos generan impacto negativo en la seguridad de la información en las organizaciones, según Croatia (2016) menciona que los riesgos son: "Eventos no deseados que pueden tener impacto negativo en la seguridad de la información, y por lo tanto en la empresa, tales como una inundación que podría destruir información en papel" (p. 102)

Luego se menciona que los riesgos poseen factores los cuales su interacción causa distintos impactos, según Santa Cruz (2016) nos menciona que los riesgos son: "En términos generales, podemos definir el riesgo como la posibilidad de que

los eventos, los impactos resultantes, las acciones asociadas, y las interacciones dinámicas entre los tres, pueden ser distintas de lo previsto." (p.23)

Así pues, los riesgos tienen una denominación sobre el daño que causen en los sistemas, según Ministerio de Hacienda y Administraciones Públicas (2012) nos dice que" Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia." (p. 29)

Ahora bien, podemos deducir que cualquier problema que afecte al total funcionamiento de una entidad es considerado un riesgo, al respecto Guzman, (2015) comenta que:

> Los riesgos se pueden definir como aquellas eventualidades que imposibilitan el cumplimiento de un objetivo y según la Organización Internacional por la Normalización (ISO) define riesgo como "La probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de 23 activos, generándole pérdidas o daños.

Así pues, como se puede observar en la cita anterior el riesgo puede materializarse en función a las amenazas que se presenten, según Guamán, (2015) referente al riesgo comenta que:

> El riesgo es la combinación de una amenaza que aprovecha alguna vulnerabilidad de un activo para impactarlo y causarle daño.

Asimismo, Guamán, (2015) comenta que los factores de riesgo que pueden existir son los siguientes:

Activos: Cualquier bien que necesite protección, frente a posibles situaciones de perdida de condiciones como son la confidencialidad, integridad y disponibilidad. Además, al activo se le asigna un valor y por lo tanto la organización debe resguardarlo.

Vulnerabilidades: Son los puntos débiles relacionados con los activos organizacionales, operacionales, físicos, y de sistemas TI en las instituciones.

INDICADORES INTEGRIDAD

Accesos Privilegiados

La ISO 27001 (2014) comenta que el control de acceso "es una actividad técnica que tiene relación con la apertura de cuentas, contraseñas y demás similitudes, además de ello indica que más que el comienzo de algo técnico es una decisión por parte del negocio". Así mismo para la gestión de accesos privilegiados se deben de tener una serie de procedimientos y soluciones, según Gilart Ignacio (2015) afirma

> que los accesos privilegiados, requieren de unas técnicas y soluciones que trasciendan las medidas de control existentes en los sistemas, además de ello se requiere una adecuación entre el nivel de riesgo y el nivel de operación llevada a cabo por los usuarios. (p. 2)

Asimismo, Sánchez Berroso, 2017, auditor de seguridad de la información menciona que:

> El control de acceso a los sistemas es uno de los elementos básicos de cualquier programa de ciberseguridad y privacidad, las gestiones efectivas del control de acceso permiten: Establecer quien puede acceder a los entornos, definir mecanismos de autentificación, establecer permisos, asegurar la segregación de funciones, asegurar el acceso y garantizar la trazabilidad de las actividades en el sistema.

Por otra parte, Florián Malecki, director internacional de Marketing de Dell Security, comenta que:

> Las estrategias de las organizaciones en base a la gestión de accesos privilegiados suelen enfocarse en autorizar, mantener, controlar y dirigir el acceso de los usuarios finales a sus recursos críticos de negocio lo que permite que se cometan errores al momento de aplicar la gestión de accesos.

De esta manera se puede observar que el control de acceso a vital en todo sistema de información, más aún si ello implica brindar ciertos accesos privilegiados.

Usuarios Inactivos

La gestión de cuentas de usuario es muy importante en la administración y configuración de los diferentes sistemas que existen hoy en día, según la corporación de código abierto Red Hat (2003) la define como:

> La forma a través de la cual se identifica y autentifica a un individuo con el sistema. Las cuentas de usuarios tienen diferentes componentes. Primero, está el nombre de usuario. Luego, está la contraseña, seguida de la información de control de acceso

Así mismo López y Villa (2016) en su investigación comentan que

> Los métodos de autenticación se dividen en tres grandes categorías en función de lo que utilizan para la verificación de identidad, las cuales son: algo que el usuario sabe (contraseña), algo que éste posee (tarjeta inteligente), y una característica física del usuario.

Por otra parte, el Instituto Español Puig Castellar comenta que :

> Se pueden declarar diferentes usuarios y asignar un nivel de acceso diferente, o unos privilegios, para cada uno de ellos. Antes de trabajar en el sistema es necesario iniciar una sesión, momento en el que la persona que quiere acceder al sistema se identifica como uno de los usuarios del sistema.

Como se puede observar es muy necesario que se generen políticas que garanticen el cumplimiento de estos procedimientos, tal como menciona la ISO 27001,2014 que

Para la gestión de altas y bajas en el registro de usuario debe de existir un procedimiento forma de alta y baja de usuarios con el objetivo de habilitar la asignación de derechos de acceso.

Discrepancia de Datos

La discrepancia de los datos ocurre cuando existe información contradictoria o incongruente en la base de datos y solamente se produce cuando existe redundancia de data. La inconsistencia consiste en que no todas las copias redundantes contienen la misma información. Además de ello, los problemas que genera esto son la inaccesibilidad de los archivos y la demora en el tiempo de respuesta

Ahora bien, la discrepancia de datos se encuentra ligada directamente con la integridad de la información ya que este evita los datos duplicados, los datos faltantes, los datos alterados y los datos incorrectos los cuales están dentro de la discrepancia, según la Compañía de Tecnologías de la información (2018) menciona que:

Las personas que entran en los registros pueden cometer errores, lo que lleva a variaciones entre los datos originales y los datos almacenados en un sistema. Del mismo modo, pueden cometer errores durante la transferencia o la copia electrónica de datos. Si el sistema aplica integridad a los datos, evitará que el usuario cometa estos errores.

Por otra parte, Sánchez Berroso, 2017, auditor de seguridad de la información menciona en su artículo que:

La integridad de la información está relacionada con el grado en que esta es una representación fidedigna de eventos de la realidad, el tiempo es uno de los factores que más afectan, en la medida en que el paso del tiempo causa cambios en las condiciones de la realidad que pueden no verse reflejadas en la información almacenada en la base de datos

Ahora bien, para que la información se mantenga integra en los diferentes motores de bases de datos que existen, se tienen que tomar medidas pertinentes para la detección de las discrepancias, según la compañía Telefónica (2015) menciona que:

> Para detectar estas inconsistencias, se necesita identificar la sensibilidad de la información, evaluar la configuración de los motores de bases de datos, auditar cada cierto tiempo, realizar un monitoreo continuo de las bases de datos y por último se tiene que controlar el acceso y gestionar de manera eficiente los permisos que se les asigne a los usuarios.

INDICADORES CONFIDENCIALIDAD

Visibilidad de Acciones

Los riesgos de seguridad a los que se enfrentan los Sistemas de Información, cada día cobra mayor importancia el control interno en las organizaciones. Una parte importante del control interno lo constituye la auditoría informática, destinada a evaluar el cumplimiento de normativas, la gestión de los recursos, el funcionamiento y sobre todo la seguridad de los Sistemas de Información, entre otros elementos relacionados con el uso de las TIC en las organizaciones. Según Gonzalo Rivas (1988) define la seguridad informática como:

> Un examen metódico del servicio informático, o de un sistema informático en particular, realizado de una forma puntual y de modo discontinuo, a instancias de la dirección, con la intención de ayudar a mejorar conceptos como la seguridad, la eficacia, y la rentabilidad del sistema que resultan auditados (pg. 40).

Ahora bien, en base a lo mencionado, se puede deducir que la auditoria informática está ligada con la trazabilidad y visibilidad de las acciones que los usuarios puedan realizar en los sistemas permitiendo observar y analizar las acciones que los usuarios cometen en los sistemas ERP, según la compañía de seguridad de la información OptimByte menciona que:

> Para tener una visibilidad de las acciones que realicen los usuarios en el sistema es necesario tener los siguientes tipos de actividades mapeadas que son: Acción de cambios, acciones de organización, acciones de funcionalidad y acciones de seguridad.

Como podemos apreciar es muy importante tener la visibilidad y la trazabilidad de las acciones de los usuarios, ya que eso nos permite saber quién realizo alguna acción con el propósito de dañar la organización. Según el Ministerio de Tecnologías de la información de Colombia (2014), afirma que

> La Trazabilidad permite definir la clasificación de los diferentes tipos de mensajes de error y trazabilidad que deben registrar los Sistemas de Información con el fin de facilitar la identificación, selección y priorización de la información para los procesos de monitoreo, gestión de incidentes y de mejoras.

Asimismo, la compañía española FHios (2011) comenta que

> La globalización de los mercados, donde cada vez se demanda una calidad mayor en los productos que se ofrecen (ya sea por las administraciones y entes reguladores como por los propios consumidores) implica, cada vez más, la necesidad de implantación un control de trazabilidad que nos permita asegurar ese plus de calidad y mejora competitiva de nuestros productos.

Validaciones de Usuario

Existen distintas tecnologías para lograr mejoras en los niveles de seguridad en la validación o autenticación de accesos y de la identidad de usuarios, tales como esquemas PKI usando Certificados Digitales o dispositivos de generación de claves aleatorias tipo ONE TIME PASSWORD (OTP), pero por lo general son soluciones costosas y que requieren largos plazos para su implementación.

Asimismo, según la empresa española QTech (2013) menciona que

> En entornos regulados o cuyo grado de informatización es elevado o crítico es vital establecer una metodología de trabajo para asegurar el correcto funcionamiento y gestión del sistema informatizado a lo largo del tiempo teniendo en cuenta un proceso de validación en los sistemas informáticos.

Además de ello, según Karla Castro (2010) explica en sus tesis que

> Cuando se halla de validaciones de usuarios en los sistemas se define las personas que tienen accesos a que, saber quién tiene acceso o cuales son las personas que tienen el nivel adecuado de acceso a las aplicaciones correctas.

Cifrado de Información

En el mundo de la tecnología vemos que el cifrado se usa de muchas maneras para proteger todo tipo de datos. Por ejemplo, en muchas ocasiones debemos entregar nuestros datos bancarios y personales para hacer compras en Internet, y para que estos estén seguros, las páginas web utilizan métodos de cifrado que proteger las transacciones (aunque algunas veces estos sean descifrados por entes malintencionados). Según Gabriela Gonzales (2014) en su artículo define el cifrado como:

> Un proceso de codificación de información sensible para evitar que esta llegue a las manos de terceros que no están autorizados para verla**.** Y la única forma de poder entender el contenido original sería usando una llave especial que decodificaría la información.

Pero si hablamos de cifrado de información o data, tenemos que hablar de criptología, según el centro de información de la defensa de España define la Criptologia como:

> La ciencia que estudia la ocultación, disimulación o cifrado de la información, así como el diseño de sistemas que realicen dichas funciones, e

inversamente la obtención de la información protegida, comprende la cifra y el criptoanálisis.

Asimismo, Eset Securiy (2014), define el cifrado de la información como:

La alteración, generalmente mediante el uso de una clave, de modo que no sean legibles para quienes no posean dicha clave. Luego, a través del proceso de descifrado, aquellos que sí poseen la clave podrán utilizarla para obtener la información original

Además de ello, la AGESIC (Agencia de gobierno electrónico y sociedad de la información y del conocimiento) define el cifrado como:

un método para evitar que alguien no pueda tener acceso a información que se desea preservar. Este método consiste en alterar un mensaje antes de transmitirlo, generalmente mediante la utilización de una clave, de modo que su contenido no sea legible para los que no posean dicha clave. De esta forma, cualquier persona que tenga acceso al mensaje no podrá entender su contenido a menos que cuente con la clave para descifrarlo

INDICADORES DISPONIBILIDAD

Disponibilidad de la Información

La disponibilidad de la información forma parte del día a día de una empresa**,** por lo que conocer los mecanismos a poner en marcha y las estrategias de seguridad necesarias para poder garantizar la seguridad del proceso son cruciales para cualquier compañía, según la compañía española de TI APSER (2015), comenta que la disponibilidad de la información es

acceso de personas u organismos a los datos con los que se trabaja**.** Además de ello, la compañía Firma A-e(2012) define la disponibilidad de la información como:

Aquella información a la que podemos acceder cuando la necesitamos a través de los canales adecuados siguiendo los procesos correctos.

Esta característica, la disponibilidad, puede en ocasiones chocar frontalmente con la confidencialidad, ya que un cifrado complejo o un sistema de archivado más estricto puede convertir la información en algo poco accesible, por lo que no se trata en absoluto de un punto menor y marca en gran medida el buen hacer del responsable de la seguridad de la información de la empresa u organización.

Asimismo, según la compañía EVERAC (2014) define la disponibilidad como:

> Una de las características de las arquitecturas empresariales que mide el grado con el que los recursos del sistema están disponibles para su uso por el usuario final a lo largo de un tiempo dado. Ésta no sólo se relaciona con la prevención de caídas del sistema (también llamadas tiempos fuera de línea, downtime u offline), sino incluso con la percepción de "caída" desde el punto de vista del usuario.

En concordancia con lo mencionado, según la ISO 27001, define la disponibilidad de la información como:

> El continúo trabajo de un sistema de información sin que ese sufra ninguna degradación en cuanto a accesos. Es necesario que se ofrezcan los recursos que requieran los usuarios autorizados cuando se necesiten. La información deberá permanecer accesible a elementos autorizados**.**

Fiabilidad de la información

Actualmente en internet podemos encontrar prácticamente cualquier información con un mínimo esfuerzo; el principal problema es que, en muchas ocasiones, es difícil distinguir si eso que hemos encontrado es válido, si esa información es veraz y contrastada, por lo que podemos estar fiándonos de determinados contenidos que, en el mejor de los casos, no se ajustan a la realidad o no están lo suficientemente actualizados, según la RAE (2014) define fiabilidad como:

La probabilidad de que un sistema, aparato o dispositivo cumpla una determinada función bajo ciertas condiciones durante un tiempo determinado

Ahora bien, la credibilidad tiene ciertos criterios para que puedan ser medidas y afectos, según Rieh y Beikin (2002) menciona que:

> Los criterios que afectan la credibilidad de la información son: la fuente, el contenido, el formato, la presentación, la velocidad de cara y la precisión de la información.

Asimismo, según Juan Baño (2013) en su artículo enumera los criterios para tener en cuenta al momento de querer buscar información fiable y fidedigna que son el

> Verificar el autor de la información, la presentación y el nivel de profundidad del contenido, el propósito de la información, la objetividad de la información, la pertinencia y si la actualización.

Por otro lado, Jordi Martí (2011) comenta que

> Para considerar la información como válida, debemos tener en cuenta los siguientes factores como: autor de la misma, exactitud y verificación de los detalles y la vigencia.

INDICADORES RIESGOS

Seguridad de cableado

Según la compañía de Telecomunicaciones Antena Comunicaciones (2014) comenta que el sistema de cableado estructurado de redes se refiere a:

> La infraestructura de cable destinadas a transportar, por todas las áreas posibles en un espacio, estas señales se trasladan desde un emisor de algún tipo de señal hasta el receptor.

Por otra parte, un sistema de red física de cable única y completa, existen combinaciones de alambre de cobre (trenzados sin blindaje UTP), bloques de

conexión, cables de fibra óptica y cables con diferentes terminaciones y con distintos usos, además de ello según la Asociación de la Industria de Telecomunicaciones (TIA) define el cableado estructurado como:

> La forma de diseñar, construir y administrar un sistema de cableado que es estructurado, lo que significa que el sistema está diseñado en bloques que tienen características de rendimiento muy específicos. Los bloques se integran de una manera jerárquica para crear un sistema de comunicación unificado.

Asimismo, según Pérez & Gardey (2014) define el cableado estructurado como

> Grupo de cables, conectores, canalizaciones, y dispositivos que permiten escalecer una infraestructura de telecomunicaciones en un sitio determinado. La instalación y las características del sistema deben cumplir con ciertos estándares para formar pare de la condición del cableado estructurado.

En cuanto a la seguridad del cableado, según Alina Bradford (2015) en su artículo comenta que:

> Para garantizar la seguridad en el cableado estructurado es necesario cubrir los cables con tubos de vinilo, enrollarlos en uso de espiral, asimismo colocar sus respectivas canaletas, además de ello se necesitan de sensores que detecten alguna interferencia.

Protección contra amenazas externas y ambientales

La ciberseguridad en una empresa es el aspecto más a tener en cuenta ya que si tenemos un error de seguridad informático podemos perder toda la rentabilidad acumulada e incluso incurrir en cuantiosas pérdidas que lleven irrevocablemente al cierre. Por ejemplo, podríamos tener que indemnizar a clientes que hayan visto sus datos publicados en Internet mientras los creían seguros en los servidores. Según el diario colombiano Portafolio (2017) comenta que:

> Las medidas que tiene que tomar toda organización contra las amenazas externas son: el establecimiento de políticas de seguridad, respaldar la información, cifrar la comunicación de la organización, utilizar antivirus en pc y móviles y adquirir herramientas de seguridad

Ahora bien, para tener en cuenta las medidas que tenemos que tomar, antes tenemos que conocer los tipos de amenazas a las cuales nos estamos enfrentando, según la compañía de TI Work Panamá (2015) clasifica las amenazas de la siguiente manera:

> Los ataques de denegación de servicios, los bots y virus, los accesos no autorizados y el pishing.

Por otra parte, según la ISO 27001, recomienda que para las amenazas externas:

> Se tiene que asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre. Se debiera prestar consideración a cualquier amenaza contra la seguridad presentada por locales vecinos

Como podemos ver la seguridad física es considerada una parte fundamental en lo que a protección de la información se refiere, de esta manera la seguridad

ambiental entra a tallar, según la ISO 27001, menciona que hay 3 aspectos fundamentales en la seguridad ambiental que son:

> La vigilancia natural, el control de acceso natural y el refuerzo territorial.

Nivel de Servicio de Suministro

Existen industrias y empresas que se ocupan de suministrar una serie de artículos y servicios. El concepto de suministro no sólo afecta a los alimentos, aunque sean los más demandados y necesitados por parte de los usuarios, ya que existe una amplia variedad de productos de uso concreto en un sector o de demanda general que también se suministran a los distintos espacios habilitados para que puedan llegar al consumidor final. Según el artículo de la compañía Economía Simple (2016), define suministro como

> Una actividad que se desarrolla con el propósito de satisfacer las necesidades de consumo de una estructura económica, ya sea empresa, familia, etc. Dicho suministro debe efectuarse en tiempo y forma.

> Por otra parte, la organización IT Solutions (2015) define suministro como: La implicancia de una acción en la cual se le provee a alguien de aquello que necesita, no solamente los alimentos son plausibles de esta acción, sí son los que más se necesitan y demandan, pero hay una enorme variedad de otros productos de uso específico de un sector o de demanda general que también son suministrados a aquellos espacios que se encargan de acercarlos al público.

Asimismo, para hablar de suministro, tenemos que mencionar los contratos que existen de por medio, Martínez Grecias (2016) en su columna comenta que

> Se define como contrato de suministro a aquel en el que una parte llamada suministrante se obliga con otra llamada suministrado a proporcionarle una determinada o determinable cantidad de artículos,

objetos, insumos, bienes o servicios durante un lapso o periodo de tiempo a cambio de un precio cierto y en dinero.

Nivel de Control de Ingreso

Cuando hablamos de seguridad es innegable que la tecnología ha puesto a nuestra disposición un gran número de opciones, no sólo destinadas a la protección de espacios y control de acceso sino también a la protección de la información que se alberga en la red o fuera de ella. Segunda la compañía Red Hat, define control físico de la siguiente manera:

> Es la implementación de medidas de seguridad en una estructura definida usada para prevenir o detener el acceso no autorizado a material confidencial

Asimismo, la empresa colombiana ISEC SA define el control de acceso como:

> El control de acceso consiste en un mecanismo que permite verificar la identidad de un usuario u ordenador con el fin de autorizar el ingreso o acceso a recursos físicos o lógicos.

Por otra parte la compañía mexicana HID Global menciona en cuanto al control de acceso:

> El control de acceso es todo mecanismo o sistema que gestiona el acceso autorizando o revocando derechos de acceso a bienes físicos o lógicos dentro de una organización.

Además de ello la organización ISO comenta que el acceso físico es el primer elemento de seguridad de la información que enfrenta las amenazas.

1.2 Antecedentes

Antecedentes Locales

El trabajo de investigación titulado "Propuesta de un modelo de sistema de gestión de la seguridad de la información en una Pyme basado en la Norma ISO 27001" de Mesías, Augusto (2015) publicada por la Universidad Peruana de Ciencias Aplicadas, Lima, Perú. Llegó a la siguiente conclusión: El SGSI propuesto es una solución eficiente frente a riesgos de perdida de data o manipulación indebida de la misma, además de ello gracias a los controles aplicados en la organización en base al SGSI planteado, la información se encuentra mucho más resguardada. Esto permite a la organización tener un mayor nivel de seguridad de la información de los activos en las diferentes áreas. De esta manera la presente investigación nos brinda una estructura de implementación de controles lo cual nos sirve como referencia para la presente investigación.

El trabajo de investigación titulado "Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de la información de la clínica Medcam Perú" de Bayona y Palacios (2017) publicado por la Universidad San Martin de Porres, Lima, Perú. Llegaron a la siguiente conclusión. La implementación del SGSI permitió la mitigación de los riesgos a los que se veía expuesto la clínica a través de los controles aplicados, además de ello se establecieron roles y responsabilidades asignados a los empleados de la organización permitiendo generar el monitoreo y la mejora continua. Este antecedente muestra los beneficios que se obtiene implementando un SGSI a lo que desea alcanzar la presente investigación.

El trabajo de investigación titulado "Metodología de gestión de seguridad de la información para el sector financiero peruano" de Bobadilla y Quijandria (2014) publicado por la Universidad Nacional de Ingeniería, Lima, Perú. Llego a la siguiente conclusión: El SGSI planteado brinda un apoyo metodológico con técnicas y herramientas basadas en estándares y normativas internacionales, además permite asegurar los activos de información más importantes de la organización y gestionar los riesgos que puedan existir, de esta manera la implementación de la metodología generaría un incremento en el cumplimiento de la circular G-140 norma de seguridad de la información decretada por el estado para el sector financiero. Este antecedente indica que los activos de información se tienen que encontrar de manera segura en base a las técnicas y herramientas de la ISO 27001 lo cual hace referencia al dimensionamiento de la variable de la presente investigación.

El trabajo de investigación titulado "Plan de seguridad informática para una entidad financiera" de Córdova. (2014) publicado por la Universidad Nacional Mayor de San Marcos, Lima, Perú, expone su investigación con el objetivo de diseñar un Plan de Seguridad que permita desarrollar operaciones seguras basadas en políticas y estándares claros y conocidos por todo el personal de un determinado Banco. Adicionalmente define la estrategia y los proyectos más importantes que deben ser llevados a cabo para culminar con el Plan de Implementación. Córdova explica también que la infraestructura que soporta estas políticas y reglas puede ser una gran debilidad si este se ve comprometida o corrompidas por personas internas o externas permitiendo que la información y los datos sean vulnerados. Llegando a la conclusión que para ejecutar un plan de seguridad de la información se requiere que las políticas, los estándares y procedimientos de seguridad sean un grupo de documentos relacionados es decir que toda la documentación se encuentre alineado acorde a los procedimientos establecidos, asimismo las organizaciones tienen que identificar las necesidades de implementar una política de seguridad.

El trabajo de investigación titulado "Diseño de un sistema de gestión de seguridad de la información para servicios postales del Perú S.A", de Aguirre (2014), publicado por la Pontificia Universidad Católica del Perú, Lima, Perú. Llegó a la siguiente conclusión: que la necesidad es grande en la propalación de las normas de seguridad que actualmente existen asimismo también es esencial establecer charlas de capacitación y concientización en toda la organización , empezando desde las altas gerencias hasta el personal que realiza actividades operativas y al personal de seguridad ya que se ha detectado que existen controles normados ; sin embargo estos no son conocidos por el personal y no existen métricas que permiten monitorear el cumplimiento de estas normas. El antecedente muestra una estructura del SGSI planteando es por ello a lo que apunta la presente investigación.

El trabajo de investigación titulado "Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo", de Espinoza (2014), publicada por la Pontificia Universidad Católica del Perú, Lima, Perú. Llego a la siguiente conclusión: Que el SGSI presentado permite la adecuada gestión de seguridad de la información, además de ello permitió garantizar la seguridad y continuidad de los activos de información críticos. También mejoro bastante la seguridad física y ambiental debido a la implementación de los controles

y procedimientos basados en la norma 27001. De esta manera se ha implementado un SGSI que permite salvaguardar toda la información crítica de la empresa. Este antecedente brindad la estructura de implementación del SGSI asimismo la mejora que genero los controles aplicados de la ISO 27001 lo cual se pretende dar a conocer en la presente investigación

El trabajo de investigación titulado "Mejora de seguridad de información en la comandancia de operaciones guardacostas basada en la norma técnica peruana NTP-ISO/IEC 27001:2008", de Fernández y Pacheco (2014), publicada por la Universidad San Martin de Porres, Lima, Perú. Llego a la siguiente conclusión: que en base a la evaluación selectiva de los activos de información se halló en un 48 % de activos de información que se encuentran vulnerables, además de ello, gracias a la mejora se logró utilizar un 25 % de controles de la ISO 27001 y por ultimo gracias a esta solución se logró mitigar en un 73 % los riesgos, las amenazas y vulnerabilidades de la comandancia. Este antecedente nos brinda una estructura de selección de activos, como se pretende realizar en el presente trabajo de investigación.

Antecedentes Nacionales

El trabajo de investigación titulado "Plan de seguridad del sistema de información ERP Spring en el grupo Transpesa Sac" de Esquivel y Bobadilla (2017) publicado por la Universidad Privada Antenor Orrego, Trujillo, Perú. Llegaron a la siguiente conclusión. El plan de seguridad estableció 7 políticas de seguridad de la información en base a la ISO 27001 los cuales asentaron los lineamientos generales y procedimientos, además de ello se determinó que el plan garantiza la seguridad de la información del sistema ERP Spring esto en base a los resultados de la evaluación de indicadores y variables , obteniendo un efecto mayor al 80%.Este antecedente nos proporciona una estructura de plan de SGSI y nos muestra los beneficios de aplicar seguridad de la información en un sistema ERP lo cual se pretende dar a conocer en la presente investigación.

El trabajo de investigación titulado "Diseño de un sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001 e ISO/IEC 27002 para proteger los activos de información en el proceso de suministros de medicamentos de la red de salud de Lambayeque 2015" de Leiva (2015) publicado por la Universidad Nacional Pedro Ruiz Gallo, Chiclayo, Perú. Llego a la siguiente

conclusión: El SGSI propuesto en la organización permitió asignar un valor a los activos de información en base a las ISO donde se encontró un total de 47 activos con un nivel enorme de criticidad , además de ello se evaluó los riesgos aplicando las mismas normas ISO , encontrándose con un total de 75 riesgos que se emplearon para trabajar las mitigaciones de las amenazas y vulnerabilidades del proceso de la red de salud a través del plan de tratamiento de riesgos , por otra parte los controles que seleccionaron fueron 20 los cuales se eligieron para disminuir los riesgos con más altos niveles de criticidad dentro del procesos de la red de salud. Este antecedente brinda la estructura de implementación de un SGSI lo cual pretendemos dar a conocer en la presente investigación.

El trabajo de investigación titulado "Plan de mejora de la seguridad de la información y continuidad del centro de datos de la gerencia regional de educación La Libertad aplicando lineamientos ISO 27001 y buenas practicas COBIT" de Yan y Zavala. (2013) publicado por la Universidad Privada Antenor Orrego, Trujillo, Perú. Llego a la siguiente conclusión: Para el plan de mejora planteado se empleó la metodología MAIGTI lo cual permitió dirigir eficientemente las actividades de cada de las fases de la auditoria, facilitando con ello la evaluación y análisis, por otra parte, los procedimientos de control se realizaron correctamente permitiendo una seguridad de información robusta. Las normas de control interno implementados se están aplicando en un 50 % debido a cambios de personal en la organización, además de ello las buenas prácticas en base a COBIT permitieron el mapeo de controles eficientemente. Este antecedente indica los beneficios de implementar las buenas prácticas COBIT y MAIGTI en un SGSI lo cual se desea aplicar de ser factible en la presente tesis.

El trabajo de investigación titulado "Propuesta metodológica para implementar la Norma Técnica Peruana ISO/IEC 27001:2008 de Seguridad de la Información en entidades públicas del estado", de Suca (2014), publicada por la Universidad Católica Santa María, Arequipa, Perú. Llego a las siguientes conclusiones: Que la propuesta permite gestionar y proteger los activos que son parte esencial en la seguridad de la información. Se ha logrado también determinar que los requerimientos dados ayudan con la implementación de la NTP/ISO 27001:2008, además de ello informa que, asignando los controles correctos y designando a los responsables para dichas tareas, ayudan a tener un mejor control sobre los activos

de información en la gestión de riesgos de la propuesta metodológica. Este antecedente nos da a conocer la estructura de implementación del SGSI permitiéndonos dar un amplio panorama en cuanto a la implementación de la presente investigación.

El trabajo de investigación titulado "Gestión de la seguridad de la información para la toma de decisiones en la infraestructura de la red telemática de la Universidad Nacional Pedro Ruiz Gallo utilizando COBIT 5 y software open source", de Santos y Arenas (2017), publicada por la Universidad Nacional Pedro Ruiz Gallo, Lambayeque, Perú. Llego a la siguiente conclusión: Que la herramienta OSSIM permite gestionar la seguridad de la información y administración de eventos, teniendo asociados ciertos controles de la ISO 27001, integrándose con el marco de referencia COBIT 5, proporcionado de esta manera un sistema de gestiona de seguridad de la información alineado a los objetivos que el autor propone en dicha tesis. Este antecedente nos brinda un marco de trabajo para la identificación de objetivos e indicadores lo cual se pretende dar a conoces en la presente investigación.

El trabajo de investigación titulado "Sistema de Gestión de Seguridad de la Información para una Institución Financiera en el Perú", de Díaz y Ramírez (2014), publicada por la Universidad Nacional Del Santa, Chimbote, Perú. Llego a la siguiente conclusión: Que se identificaron normas y estándares pertinentes para ser aplicados en las instituciones financieras del Perú, lo que permitió que mejore en grandes cantidades la gestión de la seguridad de la información, además de ello, la implementación del SGSI permitió mejorar las estrategias de seguridad, la confidencialidad de la información y que la información pueda ser consultada de manera segura. Este antecedente hace referencia al dimensionamiento de la variable de la presente investigación.

El trabajo de investigación titulado "Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la Universidad nacional José María Arguedas", de Ochoa (2017), publicada por la Universidad Nacional José María Arguedas, Apurímac, Perú. Llego a la siguiente conclusión: Se diseñó los procesos y controles de la seguridad de la información para la Universidad, asimismo se construyó, implemento y desplego los controles del sistema de seguridad de la información, todo esto permitió a la Universidad

centralizar sus activos en un aplicativo web categorizándolos y detallándolos, asignándoles un nivel de integridad, confidencialidad y disponibilidad. Este antecedente nos brindó la estructura de implementación de controles, asimismo hace referencia al dimensionamiento de la variable de la presente investigación

El trabajo de investigación titulado "Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte PNP en la ciudad de Chiclayo", de Alcántara (2015), publicada por la Universidad Católica Santo Toribio de Mogrovejo Lambayeque, Perú. Llego a la siguiente conclusión: que gracias a la guía de implementación en base a la ISO 27001 se obtuvo un nivel alto en la seguridad de las aplicaciones informáticas de la institución policial. Permitió también la mejora del proceso para identificar fallas de seguridad de la información, además de ello los niveles de riesgo entre ellos las amenazas y vulnerabilidades respecto a los activos informáticos disminuyo considerablemente. Este antecedente nos brinda los beneficios de implementar un SGSI, lo cual se pretende realizar en la presente investigación.

El trabajo de investigación titulado "Plan de mejora de la seguridad de la información y continuidad del Centro de la gerencia regional de educación La Libertad aplicando lineamientos ISO 27001 y buenas practicas COBIT", de Bach (2014), publicada por la Universidad Privada Antenor Orrego, Trujillo, Perú. Llego a la siguiente conclusión: que la implementación de la mejora genero procedimientos de control alienados a la norma ISO 27001 y las buenas prácticas COBIT, asimismo el Plan de continuidad del negocio aplicado también permitió controlar el destino de la empresa. El antecedente nos indica la mejora que genera el plan de seguridad de la información, lo cual la presente investigación desea apuntar.

Antecedentes Internacionales

El trabajo de investigación titulado "Análisis de riesgos de la seguridad de la información para la Institución Universitaria Colegio Mayor Del Cauca" de Perafan (2014) publicado por la Universidad Nacional Abierta y a Distancia, Cauca, Colombia. Llego a la siguiente conclusión: Los análisis de riesgos permitieron realizar dictámenes para conocer las debilidades y fortalezas internas que nos llevaron a la creación de controles adecuados y normalizados dentro de las políticas de seguridad de la información que hacen parte del SGSI. Se logró identificar y clasificar los activos de información, aplicando una metodología de evaluación de riesgos y mecanismos de control y gestión, además de ello los controles generados permiten mejorar y normalizar los procesos. Este antecedente nos muestra que el análisis de los riesgos, la identificación y clasificación de los activos y la aplicación de controles son partes fundamentales en el diseño del SGSI propuesto brindándonos una estructura de análisis de riesgos para la presente investigación.

El trabajo de investigación titulado "Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría aplicando la Norma ISO 27001", de Tola (2015), publicada por la Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador. Llego a la siguiente conclusión: La adopción de la metodología MAGERIT para el análisis de riesgos, permitió identificar de manera oportuna la probabilidad y el impacto de que se materialicen los riesgos pudiendo establecer controles que nos ayuden a prevenirlos, asimismo en base a la identificación de los riesgos es necesario implementar los salvaguardas con el objetivo de proteger los activos y mitigar los riesgos. Este antecedente aplico la metodología MAGERIT obteniendo buenos resultados la cual se plantea implementar en la presente investigación.

El trabajo de investigación titulado "Modelo de sistema de gestión de seguridad de la información basado en la norma NTC ISO/IEC 27001 para Instituciones públicas de educación básica de la Comuna Universidad de la Ciudad de Pereira", de Benavides y Blandón (2017), publicada por la Universidad Autónoma de Manizales, Manizales, Colombia. Llegaron a las siguientes conclusiones: que el instauramiento del modelo de SGSI proporciona una línea base para el cumplimiento de los decretos en cuanto a la seguridad de la información para instituciones de educación básica públicas se refiere. Además de ello este modelo permite garantizar la confidencialidad, integridad y disponibilidad de la información de los niños, niñas,

adolescentes y personal administrativo procurando el cumplimiento de lo dispuesto por los decretos del estado. Este antecedente hace referencia al dimensionamiento de la variable de la presente investigación.

El trabajo de investigación titulado "Plan de implementación del SGSI basado en la norma ISO 27001:2013", de Salcedo (2014), publicada por la Universidad Oberta de Catalunya, Catalunya, España. Llego a la siguiente conclusión: que la cultura organizacional a nivel de seguridad de la información ha aumentado en un 40 %en consecuencia a las actividades desarrolladas en la investigación, se llevaron comités para la sensibilización de la norma ISO 27001 y sus cambios para que de esta manera se genere concientización en los usuarios en cuanto a esta norma. Además de ello se debe incrementar los testeos de seguridad de forma habitual, asimismo es necesario que se involucren todos los niveles de organización. Este antecedente nos brinda una estructura y beneficios que genera la implementación del SGSI, a lo cual apunta la presente investigación.

El trabajo de investigación titulado "Definición y validación de procesos de gestión de seguridad de la información para la empresa Amisoft", de Molina (2015), publicada por la Universidad de Chile, Santiago, Chile. Llego a la siguiente conclusión: que con la elaboración del proyecto de seguridad de la información se logró obtener un Marco de Proceso de Amisoft mejorado, agregando el marco de seguridad de la información. Esto permitió que, en base a los nuevos documentos de procesos creados, se soporte los procesos de seguridad de la información, además de ello las políticas de seguridad creadas permitió mitigar los problemas de vulnerabilidades y ataques de diferentes tipos. Este antecedente nos brindó la estructura para mitigar las vulnerabilidades, lo cual apunta la presente investigación.

El trabajo de investigación titulado "Estudio de una auditoria en seguridad informática aplicando la norma internacional de calidad total Iso 27001 para la empresa Maint de la ciudad de Guayaquil", de Lara (2015), publicada por la Universidad de Guayaquil, Guayaquil, Ecuador. Llego a la siguiente conclusión: que

tener una estructura formal de políticas de seguridad de la información aplicando la ISO 27001 garantiza el correcto funcionamiento de los procesos de la organización, además de ello, los controles implementados fortalecen las medidas de seguridad que rigen actualmente. Todo esto permitió mejorar continuamente la gestión de la seguridad de la información, se redujo los costos asociados a los incidentes y mejoro la aplicación y participación del personal en la gestión de la seguridad. Este antecedente proporciona la estructura de políticas implementadas, como se pretende realizar en el presente trabajo de investigación

El trabajo de investigación titulado "Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001", de Pardo (2015), publicada por la Universidad Nacional de Loja, Loja, Ecuador. Llego a la siguiente conclusión: que el aprovechamiento de la metodología MAGERIT v3 permitió medir las fallas de seguridad y amenazas asociadas a los mismos con el objetivo de poder determinar el impacto que pueda tener en la institución, además de ello los mecanismos de control seleccionados de la ISO 27001 han permitido una adecuada gestión de activos de información para la disminución de peligros informáticos. El antecedente nos brinda una metodología para el análisis y la gestión de riesgos como se pretende realizar en el presente trabajo de investigación.

El trabajo de investigación titulado "Sistema de gestión de seguridad de la información basado en la norma ISO 27001 y 27002 para la unidad de informática y telecomunicaciones de la universidad de Nariño", de Guerrero y Tabango (2014), publicada por la Universidad de Nariño, Pasto, Colombia. Llegaron a la siguientes conclusiones : que gracias a la aplicación de la norma ISO 27001 y 27002 se puede alcanzar un nivel de calidad en el proceso de seguridad de la información , sin embargo se sabe que no existe la seguridad en su totalidad , de alguna u otra forma siempre existirán maneras de vulnerar estos controles , además de ello la herramienta MAGERIT permitió facilitar el análisis de riesgos asimismo permitió acelerar y facilitar el procesos de análisis mediante las tablas de doble entrada. Este antecedente nos sirve como guía para implementar la metodología MAGERIT y poder alcanzar un SGSI completo.

1.3. Realidad Problemática

A nivel mundial la mayoría de las empresas tienen una gestión para la seguridad de la información; según Lone (2016) afirma que:

> El 58% de las compañías han adoptado una estrategia de gestión ad hoc, mientras que solo el 27% establece metas concretas. No es nada fácil medir aspectos relacionados con la seguridad de la información, como cuantificar el coste de la filtración de datos o la pérdida de los mismos.

Estas compañías hacen grandes esfuerzos para mejorar la seguridad de la información, sin embargo, EY (2017) afirma que

> No tienen un enfoque de gestión sistemático. Motivados por la necesidad de proteger la información, muchas iniciativas se centran en los requisitos esenciales de infraestructura, como la inversión en equipamiento adecuado (41%), o acciones básicas como la contratación de personal adecuado (40%) y la aplicación de los controles (35%).

Con respecto a la mejora de la seguridad de la información, Lone (2016), menciona que "Poco más del 30% identifican el alto coste de la implantación y el mantenimiento como un obstáculo, por delante de la falta de plantilla competente (23 %) y la conciencia de la dirección (19 %).

Asimismo, Lone (2016), afirma que para tener éxito en el uso de un gestor de seguridad de la información que:

> No solo depende de la competencia del especialista de seguridad. La alta dirección tiene un papel importante, y las empresas necesitan trabajar para integrar la gestión de la seguridad de la información como parte de la cultura de la empresa.

La Organización estándar internacional (ISO) a nivel mundial, realizó una encuesta que presenta información de los principales organismos de certificación sobre aquellos que aun mantengan sus certificados, de la cual se tomó como referencia. Datasec (2017) según su análisis afirma que:

Del total de certificados emitidos, un 44% se encuentran en el este de Asia y Pacífico, un 38% en Europa, un 9% en Asia Central y Sur, un 5% en Norte América, un 2 % en el Medio oriente, un 1% en América Central y del Sur y 0.5% en África.

Fuente:(Datasec, 2017).

*Figura 1 SEQ Figura * ARABIC Certificaciones a nivel mundial*

Como se observa en la figura 1 este cuadro estadístico busca mostrar la cantidad de certificaciones que mantienen aún vigente las compañías en los distintos países a nivel mundial.

Ahora bien, con los sistemas de recursos empresariales (ERP) se deben tener cuidado en los accesos que se otorga o entrega a los usuarios, a continuación, se muestra un ejemplo en los sistemas ERP SAP, según Martínez (2018) afirma sobre alguna de las vulnerabilidades de los sistemas SAP que:

> Es una práctica habitual que los usuarios de los sistemas SAP tengan acceso a subir y bajar ficheros en ciertos directorios del servidor SAP (locales o montados desde otra máquina). Este uso no es esencialmente peligroso, pero combinado con otras autorizaciones y permisos puede suponer uno de los mencionados atajos para conseguir privilegios o ejecutar código malicioso. (p. 70)

Es decir, por no tener implementado un control sobre el acceso que los usuarios tienen establecidos pueden perjudicar la información que hay en los sistemas SAP

Asimismo, por dar facilidades a un usuario para que puedan acceder los servicios que necesita, se cometen errores de acceso, como menciona Martínez (2018) acerca de la prestación de funcionalidades a los usuarios:

> Debido a habituales urgencias a la hora de prestar funcionalidad al usuario, a menudo los accesos a los datos se proporcionan asignando directamente el uso de transacciones de consulta a la base de datos, en lugar de programar una transacción controlada por objetos de autorización. (p. 70)

Dicho de otra manera, se entrega acceso a la información, por medio de consultas a la base de datos a los usuarios, en vez de utilizar una tarea programada controlada para brindar los accesos.

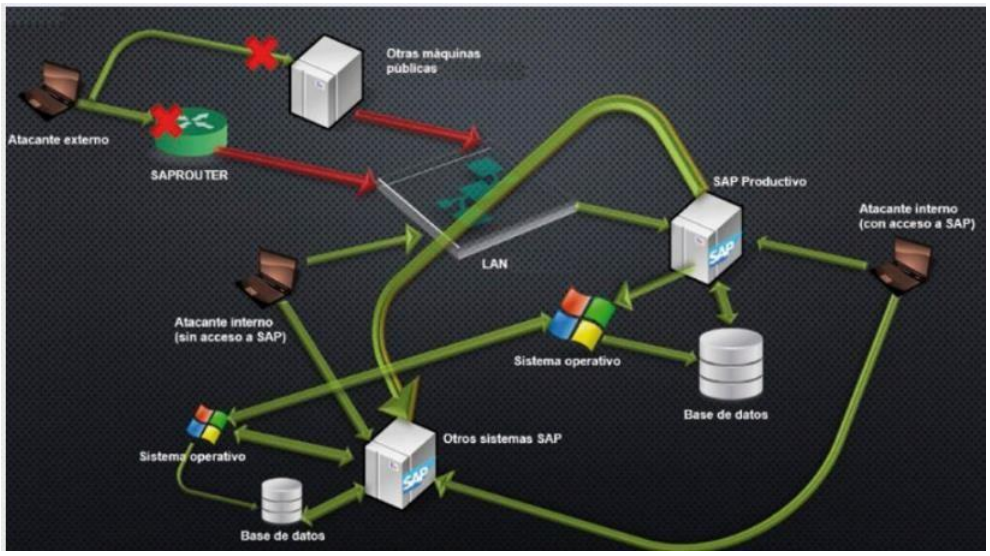


Figura 2 SEQ Figura * *ARABIC* Vías de acceso a los sistemas SAP
Fuente: (Red de Seguridad, 2018)

En la Figura N° 2 se visualiza los diferentes medios de acceso, por donde los usuarios llegan a los sistemas ERP, mostrando que se puede vulnerar por los permisos que poseen.

Además de ello, a nivel nacional en el Perú, los temas de seguridad de la información en las empresas peruanas no tienen entendimientos del rol de seguridad de la información, según Horna (2015) afirma que:

> En el país, un oficial de seguridad se encuentra por debajo del área de TI y esta dependencia está debajo del área de Administración. Por lo tanto, se desvirtúa el rol fundamental de un oficial de seguridad, incluso en otros países existe el rol de oficial de privacidad.

Es decir, que a nivel nacional en el Perú el rol de un oficial de seguridad no es evaluado como un rol de gran importancia para la seguridad de la información.

Además, según lo dicho por Cama (2017) nos dice acerca de la revisión de políticas y los procedimientos de seguridad informática en las empresas que:

> Muchas veces, es la falta de disciplina en la aplicación de controles ya establecidos lo que deja vulnerable a una compañía. Estas revisiones les permiten identificar posibles brechas en sus sistemas, las cuales, dependiendo de su complejidad, podrían ser superadas en el corto, mediano o largo plazo", explica el especialista.

Dicho de otra manera, la ausencia de la disciplina en los controles deja expuesto a la empresa ante cualquier amenaza.

La empresa ICO FOOD SERVICE es una distribuidora exclusiva de la empresa Laive en el Perú con más de 15 años en el mercado, A mediados del año 2017, la distribuidora ICO sufrió un ataque informático a gran escala lo cual género una perdida crítica de información confidencial.

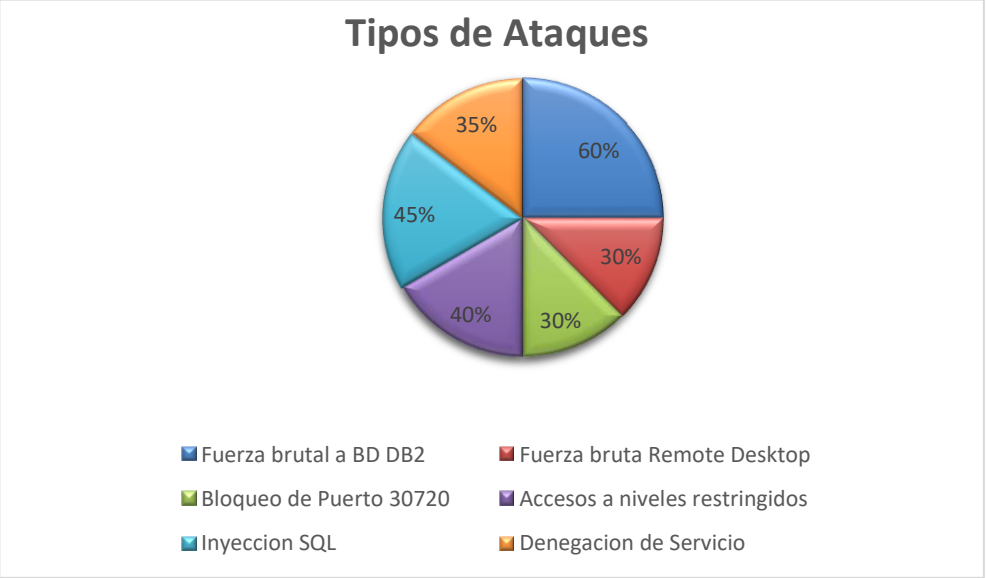


*Figura 3 SEQ Figura * ARABIC* Tipos de Ataques
Fuente (RRHH, 2017)

En la figura 3 observamos que en la empresa ICO presento un 60% de Fuerza bruta a BD DB2, un 30% a la fuerza bruta Remote Desktop, en este cuadro se refleja los métodos que realizaron, para poder sustraer la información y en su proceso causar pérdidas monetarias a la empresa ICO FOOD SERVICE.

Debido a la preocupación de que se vuelva a filtrar información clasificada se determinó implementar un sistema de gestión de seguridad de la información con lo cual se pretende que bajo las normas o políticas que mantiene la ISO 27001 se pueda poner un muro lógico de protección contra agentes externos al área de trabajo o agentes internos de la empresa, poniendo por sobre todo los activos de la empresa, asegurándonos de prevenir los riesgos y a su vez proteger la confidencialidad, la integridad la disponibilidad de la información además se concientizara al personal de los pasos que deben realizar para asegurar su información, por cada una de las personas que utilizan el sistema ERP, con el único fin de minimizar o reducir los riesgos de estos activos que son primordiales para la empresa, estableciendo reglas que puedan ayudarnos a lograr el cometido de reducción de riesgos en la empresa ICO FOOD SERVICE. (Inteco, s.f.)

Actualmente la empresa ICO FOOD SERVICE no cuenta con un sistema de gestión de la seguridad de la información, de manera que la organización se encuentra expuesto a vulnerabilidades que de ser explotadas podrán generar mayores pérdidas, para ello se utilizará las normas de la Organización Internacional

de Normalización (ISO) 27001 usando las buenas practicas que brindan, se mejorara la seguridad de la información en toda la organización, gracias a esta implementación se podrá concientizar el mejor uso de protección para evitar pérdidas grandes de información.

1.1. Formulación del problema

¿En qué medida el uso de la ISO 27001 influye en la seguridad de información en los sistemas ERP de la empresa ICO, año 2021?

1.2.1. Problemas Específicos

¿En qué medida el uso de la ISO 27001 influye en la confidencialidad de la seguridad de información en los sistemas ERP de la empresa ICO, año 2021?

¿En qué medida el uso de la ISO 27001 influye en la integridad de la seguridad de información en los sistemas ERP de la empresa ICO, año 2021?

¿En qué medida el uso de la ISO 27001 influye en la disponibilidad de la seguridad de información en los sistemas ERP de la empresa ICO, año 2021?

¿En qué medida el uso de la ISO 27001 influye en la prevención de riesgos en la seguridad de información de los sistemas ERP de la empresa ICO, año 2021?

1.3. Objetivos

1.3.1. Objetivo general

Determinar en qué medida la ISO 27001 influye en la seguridad de la información, en los sistemas ERP de la empresa ICO, año 2021

1.3.2. Objetivos específicos

Determinar en qué medida la ISO 27001 influye en la confidencialidad de la información, en los sistemas ERP de la empresa ICO, año 2021

Determinar en qué medida la ISO 27001 influye en la Integridad de la información, en los sistemas ERP de la empresa ICO, año 2021

Determinar en qué medida la ISO 27001 influye en la disponibilidad de la información, en los sistemas ERP de la empresa ICO, año 2021

Determinar en qué medida la ISO 27001 influye en la prevención de riesgos en la seguridad de la información, en los sistemas ERP de la empresa ICO, año 2021

1.4. Hipótesis

1.4.1. Hipótesis general

El uso de la ISO 27001 influye de manera significativa en la mejora de la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021.

1.4.2. Hipótesis específicas

El uso de la ISO 27001 influye de manera significativa en la mejora de la confidencialidad de la información en los sistemas ERP de la empresa ICO, año 2021

El uso de la ISO 27001 influye de manera significativa en la de mejorar la integridad de la información en los sistemas ERP de la empresa ICO, año 2021.

El uso de la ISO 27001 influye de manera significativa en la de mejorar la disponibilidad de la información en los sistemas ERP de la empresa ICO, año 2021.

El uso de la ISO 27001 influye de manera significativa en la mejorar de la prevención de los riesgos en la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021.

CAPÍTULO II. METODOLOGÍA

2.1. Tipo de investigación

La presente investigación tiene un enfoque cuantitativo, de tipo aplicada, de nivel explicativo, con un diseño experimental de tipo pre experimental, con pretest y postest.

Hay que destacar que la investigación cuenta con un enfoque Cuantitativo debido a que: Se debe considera para hacer uso de este enfoque cuantitativo los procesos que se tiene se deben desarrollar de manera ordenada en otras palabras cada proceso o etapa debe ser consecuente de la anterior. El orden siempre debe ser implacable, pero se puede volver a definir alguna fase. Este enfoque se toma como punto inicial en la idea que se va mejorar hasta el punto en el cual se haya delimitado, se derivan objetivos y preguntas de investigación, se verifica la literatura y se edifica un marco teórico. De las preguntas nacen en las hipótesis y con estas determinar las variables, se establece un plan para verificarlas, se desarrolla un plan para probarlas (diseño), estas variables deben ser medibles en el contexto, una vez obtenido los valores se hace un análisis de las mediciones adquiridas y da a conocer una serie de conclusiones con respecto a la hipótesis. Hernández, Fernández, y Baptista, (2010) además el tipo de investigación científica cuantitativo es una investigación basada en los datos probabilísticos y recopila información para ser más confiable, este tipo de investigación realiza análisis estadísticos cuando cuantifica los datos y usa los números, para poder mostrar los datos, en base a los resultados se realiza una comparación y busca una relación entre los datos que recolectó (Universidad Naval, 2016).

A continuación, se usa el tipo investigación aplicada de forma que, se utiliza todos los conocimientos que se ha adquirido en la previa investigación básica, de forma que se pueda aplicar los conocimientos que se ha adquirido sobre el tema y poder contentar al cliente con la solución que se plantea. Bejarano (2005)

Ahora bien, la investigación presenta un nivel explicativo, dado que se busca responder preguntas como el ¿porque? de la investigación, también proponen hipótesis explicativas usando la relación de las variables que se tienen, primero usan la variable dependiente, luego usan la variable interviniente y al final usan la variable independiente, de manera que proponen ideas que expliquen el problema y sea verificable (Caballero, 2014). A continuación, la investigación explicativa está enfocado en responder y explicar por qué ocurren los eventos y por qué estos se

originan, este tipo de investigación esta únicamente enfocado a poder responder los orígenes de un problema, de manera que explica el motivo por el cual se haya originado un problema y bajo qué condiciones es que se puede mostrar el problema, esta investigación tiende a ser más estructuradas que los demás estudios (Universidad Continental, 2016).

Sin embargo la investigación cuenta con un diseño experimental, debido a que se tiene variables dependiente e independiente en el tema de investigación este diseño hace que el investigador manipule o maneje una variable experimental que no ha sido verificada, bajo situaciones controladas, de manera que busca detallar de qué forma y por qué motivo es que se puede originar algún evento y gracias a esta información tratar de anticipar el futuro, para poder tener una visión de lo que va a pasar y cuando estén confirmadas poder aumentar el conocimiento, el investigador siempre debe tener el control de las condiciones en las cuales se va a realizar el experimento y modificar las variables independientes para la obtención de resultados(Palella y Martins, 2012).

Hay que hacer notar que la presente investigación tiene un diseño experimental, pero del tipo Pre experimental porque: Este tipo de investigación se observa que es poco conveniente el nivel de control de las variables para definir una relación entre la variable dependiente y la variable independiente, según Palella y Martins (2012), afirma con referente a la investigación pre-experimental que:

Es conveniente utilizarla sólo como prueba de experimento que requieren un mayor control. Puede servir en ocasiones como estudio exploratorio, debido a que es útil como un primer acercamiento al problema de investigación. Se basa en administrar un estímulo a un grupo y después aplicar una medición que permite observar su efecto en una o más variables. (p.89)

Hay que destacar que al usar el diseño experimental del tipo Pre-experimental que se puede realizar mediciones a un grupo de investigación del cual se quiere observar el efecto o cambio que causa la medición en la variable o en más de una variable.

Así mismo este tipo de investigación Pre-Experimental no tiene control sobre las variables desconocidas y no presenta grupos de control, según Bernal (2010) mención que:

> Presentan el más bajo control de variables y no efectúan asignación aleatoria de los sujetos al experimento, y son aquellos en los que el investigador no ejerce ningún control sobre las variables extrañas o intervinientes, no hay asignación aleatoria de los sujetos participantes de la investigación ni hay grupo control. (p.146)

Como se ha dicho en la cita descrita sobre el tipo de investigación Pre-Experimental, esta investigación tiene definida a los sujetos a los cuales estarán presente en la investigación sin utilizar sujetos aleatorios y en el cual los investigadores no poseen autoridad sobre la variable desconocida.

Ahora bien, en la investigación se procederá a realizar un pretest y postest ya que: se va aplicar una prueba de evaluación previa antes de implementar la solución y después de realizar el pretest se aplica un estímulo, para poder proceder a realizar una prueba de evaluación posterior al implementar la solución, de tal manera que deba existir una referencia inicial que nos muestre como fue afectada el grupo con respecto a la variable dependiente antes de la implementación de la solución y no se debe modificar o manipular las variables o grupo de comparación.(Palella y Martins, 2012).

2.2. Población y muestra

La población según Ludwig (como se citó en Universidad Naval, 2016) piensa que el universo o población es "finita cuando tiene un número limitado de elementos (ejemplo: todos los habitantes de una comunidad); una población es infinita cuando no es posible contar a todos sus elementos (ejemplo, la población de insectos en el mundo)" (p. 34).

La población presente en este proyecto de investigación se ve conformado por los 18 módulos que se tiene por cada sistema de recursos empresariales (ERP), de los cuales se seleccionará los 2 únicos sistemas ERP que posee la empresa ICO FOOD SERVICE.

Tabla 1
Ubicación de los módulos en los Sistemas ERP

Sistemas ERP	Módulos
Ant	Ventas
Ant	Compras
Ant	Almacén
Ant	Distribución
Ant	Cubo de Ventas
Ant	Administración
Ant	Configuración
Ant	Reportes
Ant	CRM
Uniflex	Proveedores
Uniflex	Contabilidad
Uniflex	Finanzas
Uniflex	Planilla
Uniflex	Tesorería
Uniflex	Inventarios
Uniflex	Configuración
Uniflex	Gestión Gerencial
Uniflex	Reporte
Total	18

Fuente: Área TI, 2021

La muestra según Silva (como se citó en Universidad Naval, 2016) "Es un sub conjunto o parte de la población seleccionada para describir las propiedades o características; es decir, que una muestra se compone de algunos de individuos, objetivos o medidas de una población" (p. 34).

Debido a que en el presente trabajo de investigación se establece que la población será evaluada en su totalidad, ya que se cuenta con solo 18 módulos, 9 módulos por cada sistema de recursos empresariales, se usó el método censal donde se establece que la muestra posee la misma cantidad que la población.

2.3. Técnicas e instrumentos de recolección y análisis de datos

El instrumento usado en la presente investigación es el cuestionario, según Fidias (2006) menciona que una de las formas de efectuar la encuesta es que: "Se realiza de forma escrita mediante un instrumento o formato en papel contentivo de una serie de preguntas. Se le denomina cuestionario auto administrado porque debe ser llenado por el encuestado, sin intervención del encuestador" (p. 74).

Asimismo, Pallela y Martins (2015) lo definen como:

> Un instrumento de investigación que forma parte de la técnica de la encuesta. Es fácil de usar, popular y con resultados directos. El cuestionario, tanto en su forma como en su contenido, debe ser sencillo de contestar. Las preguntas han de estar formuladas de manera clara y concisa; pueden ser cerradas, abiertas o semiabiertas, procurando que la respuesta no sea ambigua. Como parte integrante del cuestionario o en documento separado, se recomienda incluir unas instrucciones breves, claras y precisas, para facilitar su solución.

Por otro lado, Domínguez, Ernesto y Sánchez (2009) mencionan referente a la utilidad de la encuesta:

> Puede ser muy útil para algunos tipos de objetos de estudio, pero suele requerir personal que no siempre se tiene a la mano. Además, se debe contar con conocimientos de estadística para realizar un análisis apropiado.

Cabe mencionar que el instrumento de recolección de datos se aplica a los administradores de los sistemas y no directamente a los módulos de los sistemas ERP, esto debido a que ellos son las personas que utilizan, configuran y monitorean los módulos en los sistemas ERP.

En cuanto a la técnica utilizada para la presente investigación fue la encuesta, según Palella y Martins (2012), mencionan que:

> Es una técnica destinada a obtener datos de varias personas cuyas opiniones interesan al investigador. Para ello, a diferencia de la entrevista, se utiliza un listado de preguntas escritas que se entregan a los sujetos quienes, en forma anónima, las responden por escrito. Es una técnica aplicable a sectores amplios del universo, de manera mucho más económica que mediante entrevistas individuales

2.4. Confiabilidad

Para establecer el nivel de confiabilidad se utilizó el coeficiente alfa de Cronbach "Es una de las técnicas que permite establecer el nivel de confiablidad que es, junto con la validez, un requisito, minino de un buen instrumento de medición presentado con una escala tipo Likert"(Palella & Martins, p. 162)

Por otro lado Palella & Martins (2012) nos dicen lo siguiente: "El coeficiente Cronbach se utiliza para evaluar la confiabilidad a partir de la consistencia interna de los ítems. El alfa de Cronbach varía entre 0 y 1(0 es ausencia total de consistencia y 1 es consistencia perfecta)" (p. 162)

Además, existen varias formas de poder determinar la confiabilidad del instrumento según Hernández, Fernández & Baptista (2014) nos dice que:

> Todos utilizan procedimientos y fórmulas que producen coeficientes de fiabilidad. La mayoría oscilan entre cero y uno, donde un coeficiente de cero significa nula confiabilidad y uno representa una máxima confiabilidad (fiabilidad total, perfecta). Cuanto más se acerque al coeficiente cero, mayor error habrá en la medición. (p. 207)

Es decir que la confiabilidad de un instrumento es determinada por cuanto este se acerque a 1

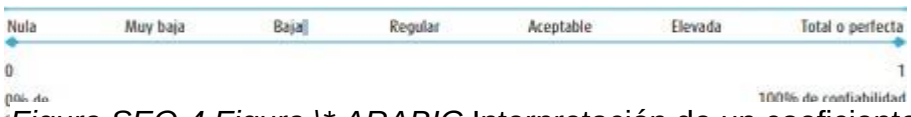


*Figura SEQ 4 Figura * ARABIC* Interpretación de un coeficiente de confiabilidad

Fuente: Metodología de la investigación (Hernández, Fernández y Baptista, 2014)

Como se indica en la figura 4 donde especifica que mientras más se acerque el coeficiente a 1 la confiabilidad del instrumento la medición será más exacto, en cambio sí se acerca el coeficiente a 0 habrá errores en la medición.

$$\alpha = \frac{K}{K-1}\left[1 - \frac{\sum S_i^{\,2}}{S_T^{\,2}}\right]$$

Figura 5 Formula Coeficiente alfa de Cronbach

Fuente: Elaboración propia.

- K: El número de ítems : 14
- Si^2 : Sumatoria de Varianzas de los Ítems : 6.36
- ST^2 : Varianza de la suma de los Ítems : 25.54

= 0,81

*Figura 6 SEQ Figura * ARABIC* *Reemplazando* los valores en la formula

Fuente: Elaboración propia

2.5. Ficha Técnica del Instrumento

CUESTIONARIO ICO

A. Nombre:

Cuestionario para la variable "Seguridad de la información – Ico Food Service"

B. Objetivos:

El siguiente cuestionario tiene como finalidad determinar en qué medida el uso de la norma ISO 27001 influye en la seguridad de la información, de la empresa ICO, año 2021

C. Autor: Henry Alexander Ticona Llerena

D. Administración: Individual

E. Duración: 15minutos

F. Sujetos de aplicación:

Encargados de la seguridad de la información en la Empresa Ico.

G. Técnica:

Encuesta

H. Puntuación y escala:

Tabla 2 Puntuación y Escala

Puntuación Numérica	Rango o Nivel
1	Muy Bajo
2	Bajo
3	Medio
4	Alto
5	Muy alto

Fuente: Elaboración Propia

2.6. Validez

Con respecto a la determinación de la validez del instrumento de recolección de datos cualitativos (cuestionario) se aplicó el "juicio de expertos", lo cual fue revisado y calificado por los siguientes profesionales:

Tabla 3
Lista de instrumento de recolección de datos expertos que certificaron la validez

DNI	Grado Académico	Apellidos y Nombres	Institución donde Labora	Calificación
09536323	Doctor	Flores Macias Edward	Universidad Privada del Norte	Aplicable
42819556	Titulado	Romero Quichiz Denis	RQ Consultores SAC	Aplicable
45286733	Magister	Melgarejo Solís Ronalc	Universidad Privada del Norte	Aplicable

Fuente: Elaboración propia

Los expertos validaron los aspectos de claridad, pertinencia y relevancia de los ítems correspondientes a cada dimensión de las variables de estudio. En ambos

casos los expertos coincidieron en su apreciación determinando como opinión de aplicabilidad "Procede su aplicación".

2.7. Procedimiento

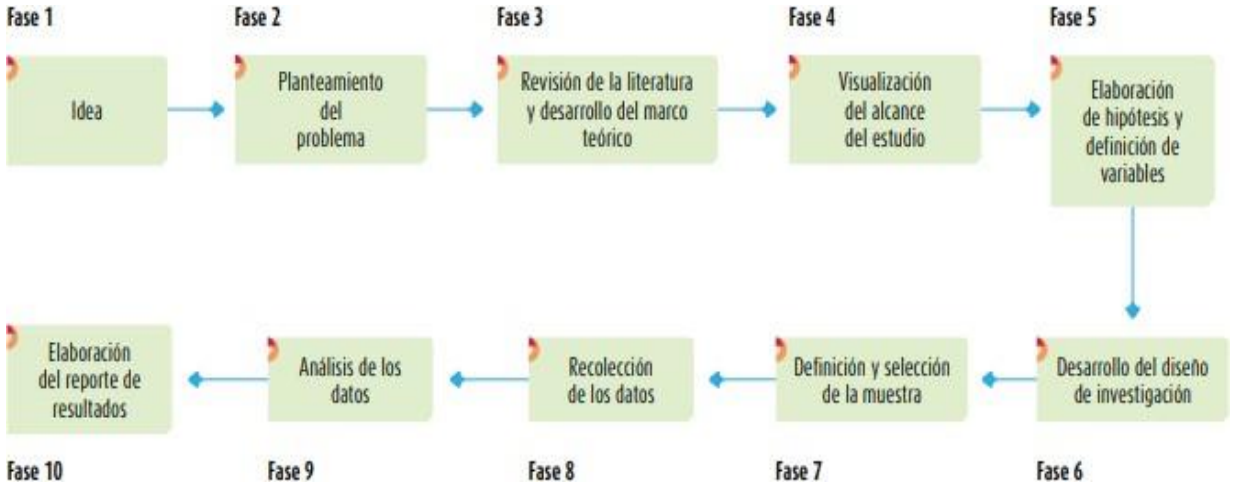


*Figura 8 SEQ * ARABIC 8* Procesos Cuantitativos

Fuente: Metodología de la investigación (Hernández, Fernández y Baptista, 2014)

La presente investigación se basa en el procedimiento de la figura 8 de procesos cuantitativos para analizar datos los cuales se deben realizar de una manera secuencial sin omitir ningún paso, aunque se puede redefinir uno de estos procesos se pueden redefinir y se debe empezar desde el primer proceso.

- Se revisó detalladamente el instrumento de recolección de datos.
- Se depuro los datos recogidos, para detectar y eliminar los errores que se lleguen a presentar.
- Se representó las respuestas de los cuestionarios en indicadores numéricos para facilitar la tabulación. Se utilizó el software SPSS.
- Se registró los datos del cuestionario en una hoja de cálculo tabulándolos con indicadores numéricos agregándole formulas, para hallar la suma total de la variable dependiente, para así re direccionar los datos en el software SPSS para su evaluación estadística.
- Se registró los datos de los resultados del cuestionario elaborado al grupo de control en el software SPSS, para su análisis descriptivo y su prueba de normalidad.

- Se registró los datos de los resultados del cuestionario elaborado al grupo de experimento en el software SPSS, para su análisis descriptivo y su prueba de normalidad.
- Se almaceno los datos de los resultados del cuestionario elaborado al grupo de control y grupo de experimento en un mismo archivo SPSS, para así hallar los resultados de las tablas de contingencia.
- Se almaceno los datos de los resultados del cuestionario elaborado al grupo de control y grupo de experimento en un mismo archivo SPSS, hallando los resultados de las pruebas de estadística, de correlación de Spearman, para comprobar así la valides de las pruebas de hipótesis.
- Se elaboró los Histogramas de estadística descriptiva del grupo de control en el software SPSS así como los del grupo de experimento para observar el comportamiento antes y después de la implementación de la ISO 27001.
- Se elaboró los Histogramas de estadística diferencias del grupo de control en el software SPSS así como los del grupo de experimento.

2.8. Aspectos Éticos

Para la presente investigación se consideró los aspectos éticos en cada proceso de la exploración, manteniendo la confidencialidad de la información brindada por los participantes encuestados y por la organización. Además de ello respetando a las personas, el lugar, la cultura, la estructura y los valores donde se realizó la encuesta. Al respecto Cortina A (1996), señala, "la ética como aquella parte de la Filosofía que se dedica a la reflexión sobre lo moral y como un tipo de saber que intenta construirse racionalmente, utilizando para ello, el rigor conceptual y los métodos de análisis y explicación propios de la filosofía. Como reflexión sobre las cuestiones morales, la ética pretende desplegar los conceptos y argumentos que permitan comprender la dimensión moral de la persona humana."

Por otra parte, las personas que participaron en las encuestas y consultas se les informo del propósito de la investigación, y de los resultados. Asimismo, a la organización se le solicito los permisos pertinentes para dicha investigación, generando de esta forma transparencia en todo el análisis.

CAPÍTULO III. RESULTADOS

3.1. Prueba de Normalidad

En el presente informe se analiza una muestra de 18 módulos de los sistemas ERP, dado que la muestra es menor a 30, se utilizó la prueba de normalidad de Shapiro-Wilk, así mismo se usará para contrastar la normalidad de los datos

Para determinar si existe una distribución normal o en las variables de investigación del presente trabajo se toma como criterio el nivel de significancia menor a 0.05. Al respecto Hernández, Fernández y Baptista (2014) comentan que:

> "El nivel de significancia y el intervalo de confianza son niveles de probabilidad de cometer un error o de equivocarse en la prueba de hipótesis o la estimación de parámetros, los niveles más comunes son 0.05 y 0.01" (p.328).

H0: La variable de la seguridad de la información tiene una distribución normal

H1: La variable de la seguridad de la información no sigue una distribución normal

Tabla 4 Prueba de Normalidad
Prueba de Normalidad

Pruebas de normalidad

	Shapiro-Wilk		
	Estadístico	gl	Sig.
Variable seguridad de la información	,646	13	,000

Fuente: Elaboración propia, 2021

Como se puede observar la tabla 4 la distribución de datos tiene un nivel de significancia 0.000, por lo tanto, es menor a 0.05. En consecuencia, se acepta la hipótesis alterna donde H1 es aceptada como una distribución normal.

3.2. Análisis Descriptivo

3.2.1. Análisis Descriptivo de la variable Seguridad de la información Pre Test

Tabla 5
Análisis Descriptivo Variable Seguridad de la Información

		Pre Seguridad de la Información(Pre test)	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	0	0	0	0
	Media	9	47,4	50,0	50,0
	Alto	9	47,4	50,0	100,0
	Muy Alto	0	0	0	0
	Total	18	94,7	100,0	

Fuente: (Elaboración Propia, 2021)

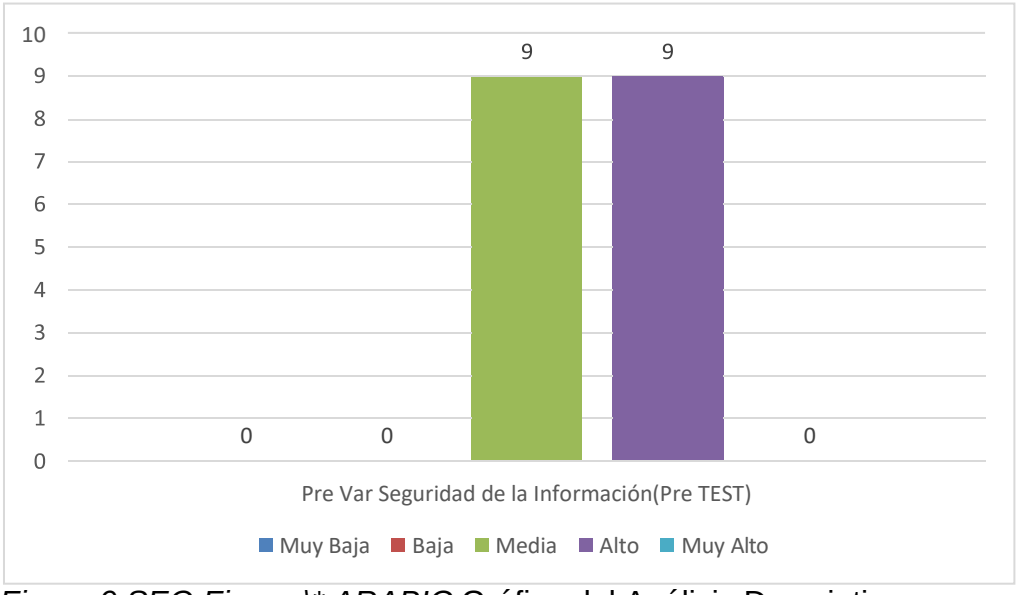


*Figura 9 SEQ Figura * ARABIC* Gráfico del Análisis Descriptivo Variable Seguridad de la Información
Fuente: Elaboración Propia

Como se puede observar en la Tabla 5 y figura 9, sobre el análisis descriptivo del Pre test de la variable Seguridad de la información, evaluado por las personas a cargo del sistema ERP en donde califican a la variable dependiente en 2 categorías: como "Media" y "Alta" siendo representado ambas por un 47.4% del total.

3.2.2. Análisis Descriptivo de la dimensión de Integridad Pre Test

Tabla 6
Análisis Descriptivo Dimensión Integridad
Pre DIM INTEGRIDAD

		Pre DIM INTEGRIDAD(Pre TEST)	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	1	5,3	5,6	5,6
	Media	7	36,8	38,9	44,4
	Alto	10	52,6	55,6	100,0
	Muy Alto	0	0	0	0
	Total	18	94,7	100,0	

Fuente: Elaboración Propia

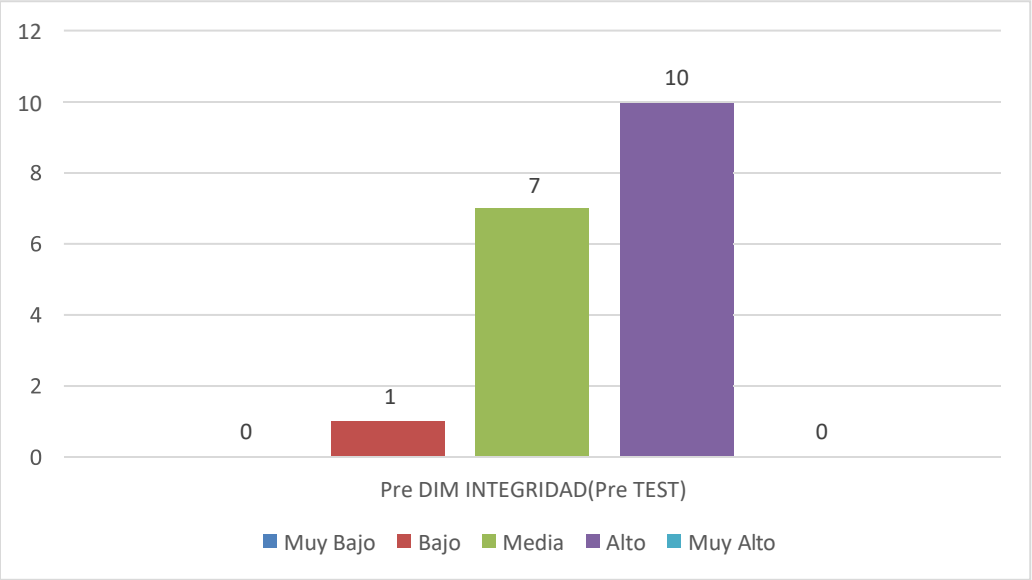


*Figura 10 SEQ Figura * ARABIC* Grafico del Análisis Descriptivo Dimensión Integridad

Fuente: Elaboración Propia

Como observamos en la Tabla 6 y Figura 10, sobre el análisis Pre test de la dimensión Integridad, habiendo sido evaluado por los encargados de los sistemas de planificación de recursos empresariales (ERP), definieron la dimensión en 3 categorías como: "Baja" evidenciado por un 5.3% de total,

"Media" siendo contemplado por un 36,8% del total y "Alta" observado con un 52.6% del total.

3.2.3. Análisis Descriptivo de la dimensión de Confidencialidad Pre Test

Tabla 7
Análisis Descriptivo Dimensión Confidencialidad
Pre DIM CONFIDENCIALIDAD

		Pre DIM CONFIDENCIALIDAD(Pre TEST)	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	3	15,8	16,7	16,7
	Media	12	63,2	66,7	83,3
	Alto	3	15,8	16,7	100,0
	Muy Alto	0	0	0	0
	Total	18	94,7	100,0	

Fuente: Elaboración Propia

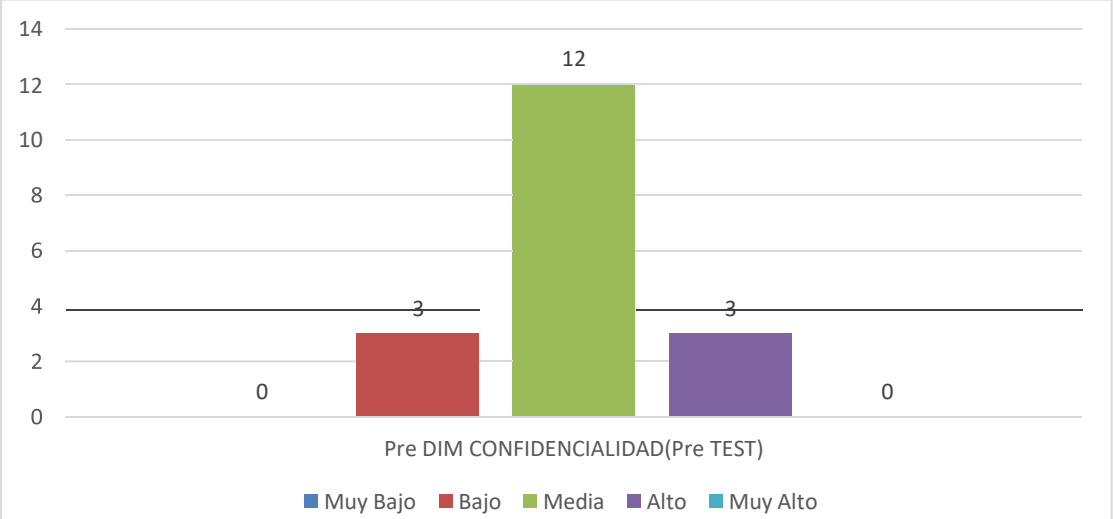


*Figura 11 SEQ Figura * ARABIC Grafico del Análisis Descriptivo*
Fuente:(Elaboración Propia, 2021)

Como podemos observar en la tabla 7 y figura 11, acerca del análisis descriptivo de la dimensión Confidencialidad en los sistemas de planificación de recursos empresariales (ERP), bajo el criterio de las personas encargadas de estos sistemas ERP calificaron a la dimensión en 3 categorías diferentes como: "Baja" la cual está representada con un 15,8% del total, "Media" siendo está demostrado con un 63.2% del total y "Alto" comprobado con un 15.8% del total.

3.2.4 Análisis Descriptivo de la dimensión de Disponibilidad Pre Test

Tabla 8
Análisis Descriptivo Dimensión Disponibilidad

		Pre DIM DISPONIBILIDAD(Pre TEST)	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	0	0	0	0
	Media	0	0	0	0
	Alto	13	68,4	72,2	72,2
	Muy Alto	5	26,3	27,8	100,0
	Total	18	94,7	100,0	

Fuente: Elaboración Propia

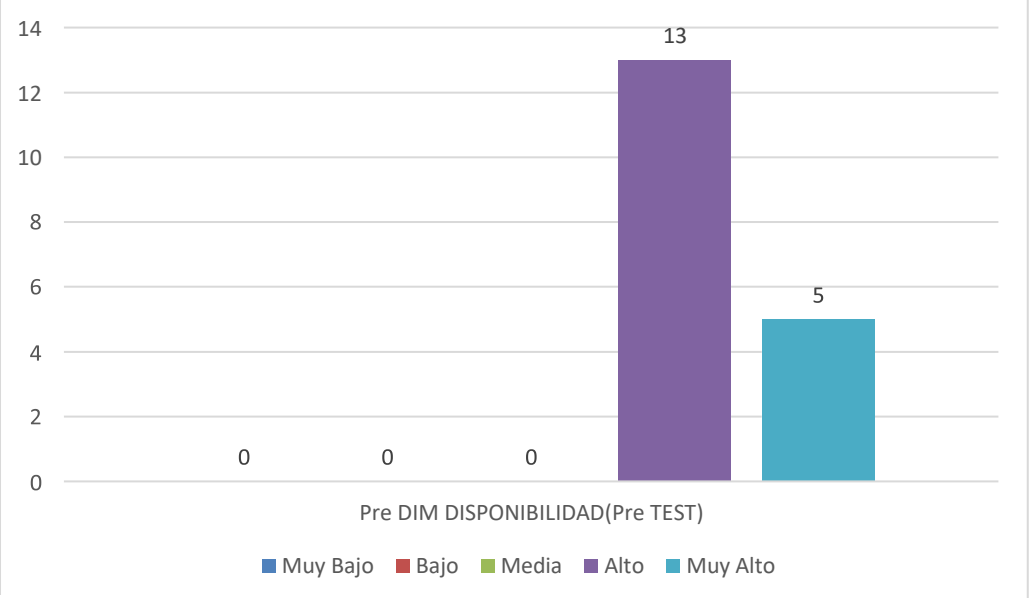


*Figura 12 SEQ Figura * ARABIC* Gráfico del Análisis Descriptivo
Fuente: (Elaboración Propia, 2021)

Como podemos observar en los datos obtenidos en la tabla 8 y figura 12, acerca del análisis descriptivo de la dimensión Disponibilidad en los sistemas de planificación de recursos empresariales (ERP), bajo el criterio de las personas encargadas de estos sistemas ERP calificaron la dimensión en 2 categorías diferentes como: "Alto" la cual está descrito con un 68.4% del total y "Muy Alto" se encuentra definido con un 26.3% del total.

3.2.5 Análisis Descriptivo de la dimensión de Riesgos Pre Test

Tabla 9
Análisis Descriptivo Dimensión Riesgo
Pre DIM RIESGOS

		Pre DIM RIESGOS	Porcentaje	Porcentaje válido	Porcentaje acumulado
-	Muy Bajo	0	0	0	0
Válido	Bajo	0	0	0	0
	Media	11	57,9	61,1	61,1
	Alto	7	36,8	38,9	100,0
	Muy Alto	0	0	0	0
	Total	18	94,7	100,0	

Fuente: (Elaboración Propia, 2021)

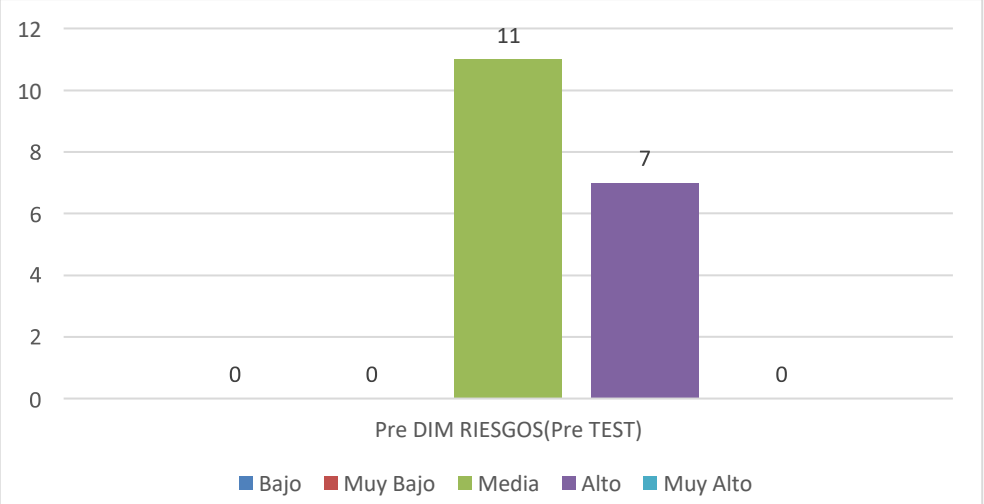


*Figura 13 SEQ Figura * ARABIC* Gráfico del Análisis Descriptivo Dimensión Riesgo
Fuente: Elaboración Propia

Como podemos observar en los datos obtenidos mostrado en la tabla 9 y figura 13, acerca del análisis descriptivo de la dimensión Riesgo en el sistema de planificación de recursos empresariales (ERP), bajo el criterio de las personas encargadas de estos sistemas ERP calificaron la dimensión en 2 categorías diferentes como: "Media" la cual está descrito con un 57.9% del total y "Alto" se encuentra definido con un 36.8% del total.

3.2.6 Análisis Descriptivo de la variable Seguridad de la Información Post test

Tabla 10 Análisis Descriptivo Post Variable Seguridad de la información
Análisis Descriptivo Post Variable Seguridad de la información

Post SEGURIDAD DE LA INFORMACIÓN

		Post Var Seguridad de la información(Post TEST)	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	0	0	0	0
	Media	5	26,3	27,8	27,8
	Alto	13	68,4	72,2	100,0
	Muy Alto	0	0	0	0
	Total	18	94,7	100,0	

Fuente: Elaboración propia

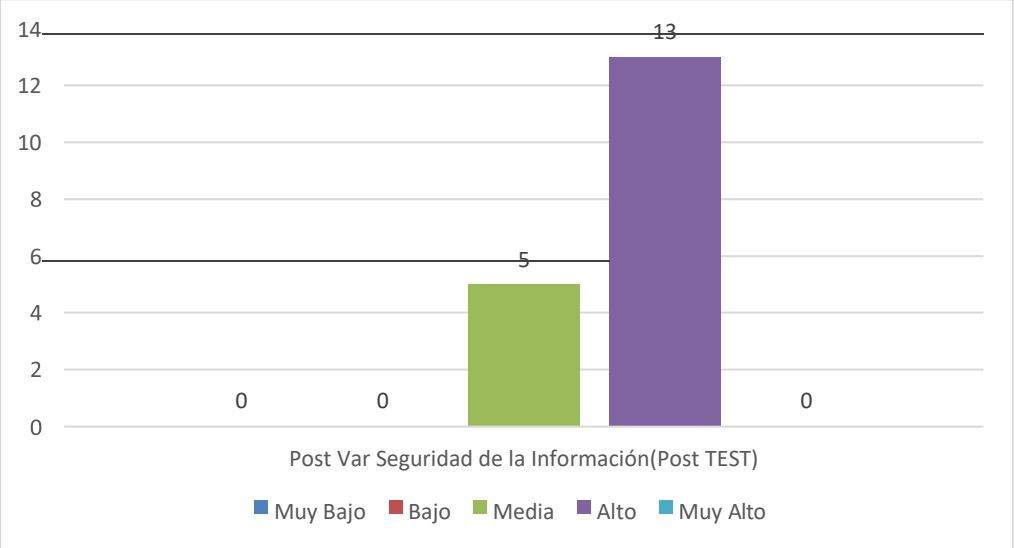


*Figura 14 SEQ Figura * ARABIC* Gráfico del Análisis Descriptivo Post Variable Seguridad de la Información

Fuente: Elaboración propia

Como se puede visualizar en los datos obtenidos en Post Test definidos en la tabla 10 y figura 14, acerca del análisis descriptivo de la variable Seguridad de la información en el sistema de planificación de recursos empresariales (ERP), bajo el criterio de las personas encargadas de estos sistemas ERP calificaron a la dimensión en 2 categorías diferentes como: "Media" la cual está descrito con un 26.3% del total y "Alto" se encuentra definido con un 68.4% del total.

3.2.7 Análisis Descriptivo de la dimensión de Integridad Post test

Tabla 11 Análisis Descriptivo Post Dimensión Integridad

Post DIM INTEGRIDAD(POST TEST)

		Post DIM INTEGRIDAD(Post TEST)	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	3	15,8	16,7	16,7
	Media	12	63,2	66,7	83,3
	Alto	3	15,8	16,7	100,0
	Muy Alto				
	Total	18	94,7	100,0	

Fuente: Elaboración propia

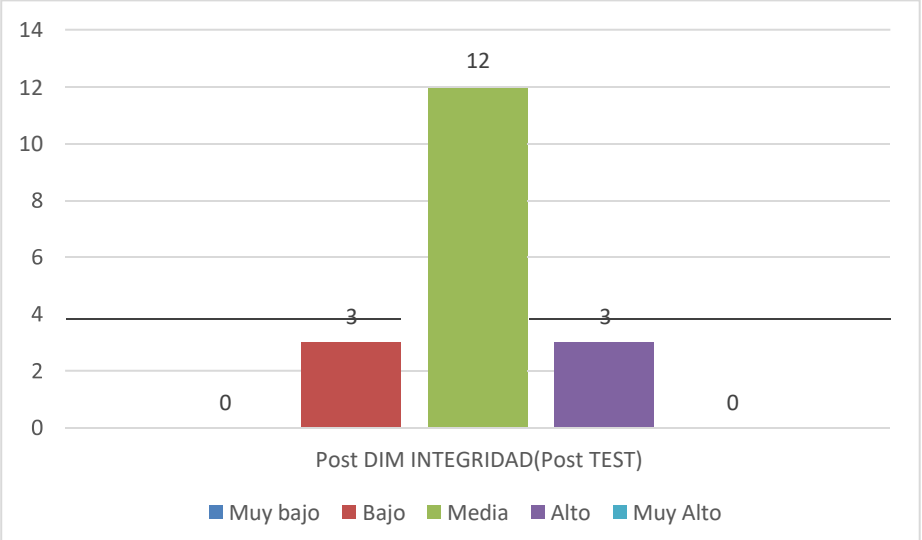


*Figura 15 SEQ Figura * ARABIC* Gráfico del Análisis Post Descriptivo Dimensión Integridad
Fuente: Elaboración propia

Como se observa en los datos obtenidos en el Post Test establecidos en la tabla 11 y figura 15, acerca del análisis descriptivo de la dimensión Integridad en el sistema de planificación de recursos empresariales (ERP), bajo el criterio de las personas encargadas de estos sistemas ERP calificaron a la dimensión en 3 categorías diferentes como: "Bajo" la cual está descrito con un 15.8% del total, "Media" se encuentra definido con un 63.2% del total y "Alto" representado con un 15.8%

3.2.8 Análisis Descriptivo de la dimensión de Confidencialidad Post test

Tabla 12
Análisis Descriptivo Post Dimensión Confidencialidad
Post DIM CONFIFENCIALIDAD(Post TEST)

		Post DIM CONFIDENCIALIDAD(Post TEST)	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	0	0	0	0
	Media	0	0	0	0
	Alto	12	63,2	66,7	66,7
	Muy Alto	6	31,6	33,3	100,0
	Total	18	94,7	100,0	

Fuente: (Elaboración propia, 2021)

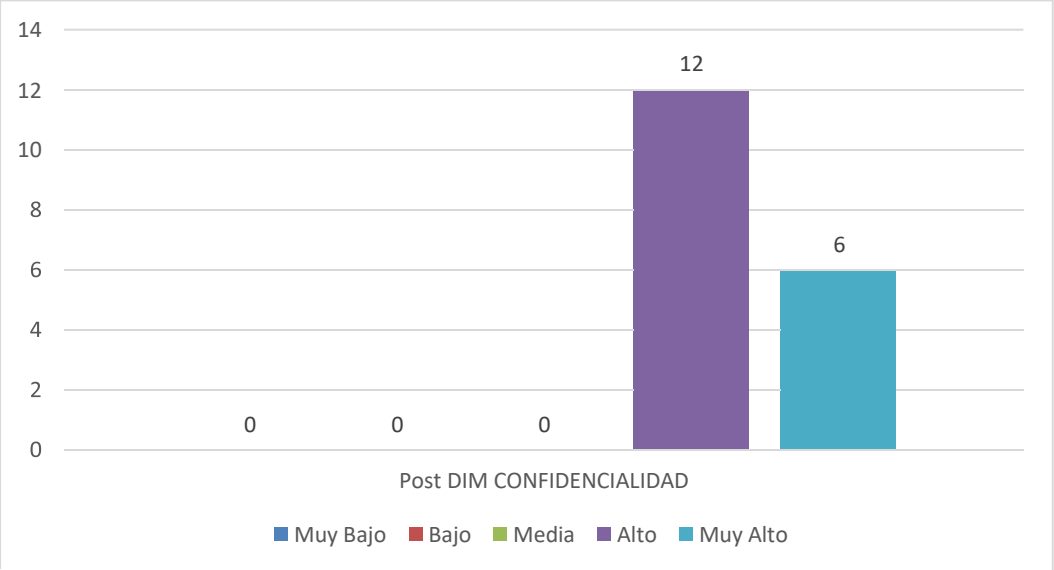


*Figura SEQ Figura * ARABIC 16 Gráfico del Análisis Descriptivo Post Dimensión Confidencialidad*

Fuente: (Elaboración propia, 2021)

Como podemos observar en los datos obtenidos en el Post Test definidos en la tabla 12 y figura 16, acerca del análisis descriptivo de la dimensión Confidencialidad en el sistema de planificación de recursos empresariales (ERP), bajo el criterio de las personas encargadas de estos sistemas ERP calificaron a la dimensión en 2 categorías diferentes como: "Alto" la cual está establecida con un 63.2% del total, "Muy Alto" se encuentra definido con un 31.62% del total.

3.2.9 Análisis Descriptivo de la dimensión de Disponibilidad Post test

Tabla 13
Análisis Descriptivo Dimensión Disponibilidad
Post DIM DISPONIBILIDAD(Post TEST)

		Post DIM DISPONIBILIDAD(Post TEST)	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	0	0	0	0
	Media	2	10,5	11,1	11,1
	Alto	12	63,2	66,7	77,8
	Muy Alto	4	21,1	22,2	100,0
	Total	18	94,7	100,0	

Fuente: (Elaboración propia, 2021)

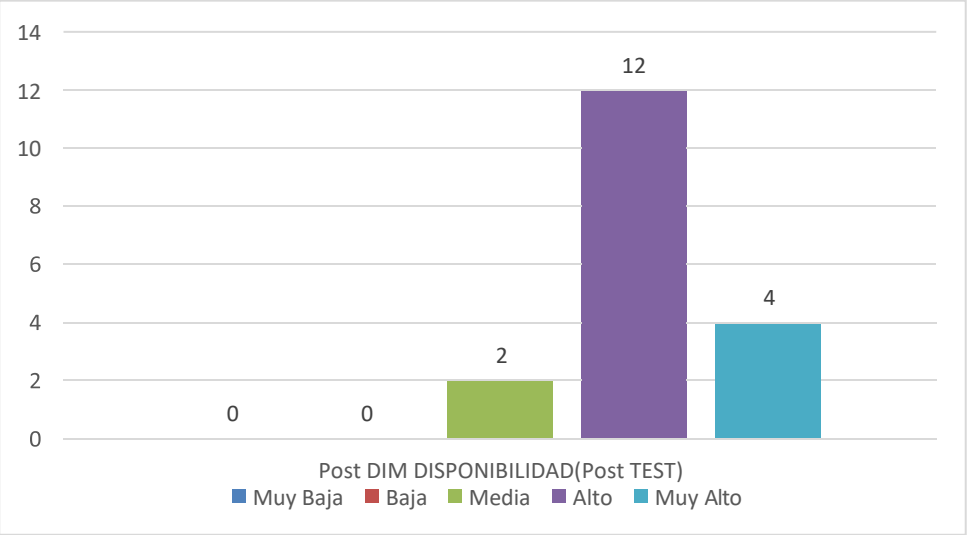


*Figura SEQ Figura 17 * ARABIC Gráfico del Análisis Descriptivo*
Fuente: Elaboración propia

Como se puede observar en los datos obtenidos en el Post Test establecidos en la tabla 13 y figura 17, acerca del análisis descriptivo de la dimensión Disponibilidad en el sistema de planificación de recursos empresariales (ERP), bajo el criterio de las personas encargadas de estos sistemas ERP calificaron a la dimensión en 3 categorías diferentes como: "Media" la cual está descrito con un 10.5% del total, "Alto" se encuentra definido con un 63.2% del total y "Muy Alto" representado con un 21.1% del total.

3.2.10 Análisis Descriptivo de la dimensión Riesgo Post test

Tabla 14
Análisis Descriptivo Post Dimensión Riesgo

Post DIM RIESGOS(Post TEST)

		Post DIM RIESGOS	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Muy Bajo	0	0	0	0
	Bajo	0	0	0	0
	Media	2	10,5	11,1	11,1
	Alto	16	84,2	88,9	100,0
	Muy Alto	0	0	0	0
	Total	18	94,7	100,0	

Fuente: (Elaboración propia, 2021)

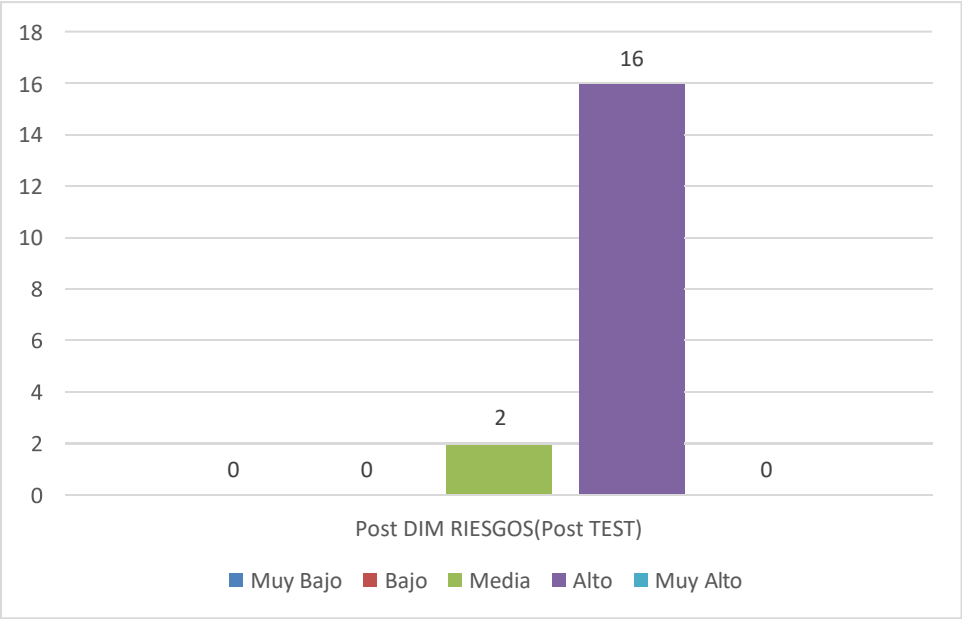


*Figura SEQ Figura * ARABIC 18 Gráfico del Análisis Descriptivo Post Dimensión Riesgos*

Fuente: (Elaboración propia, 2021)

Como se puede observar en los datos obtenidos en el Post Test establecidos en la tabla 14 y figura 18, acerca del análisis descriptivo de la dimensión Riesgos en el sistema de planificación de recursos empresariales (ERP), bajo el criterio de las personas encargadas de estos sistemas ERP calificaron a la dimensión en 2 categorías diferentes como: "Media" la cual está descrito con un 10.5% del total y "Alto" se encuentra definido con un 84.2% del total.

3.2.11 Cruce de Variables Pre Test y Post Test

3.2.12 Análisis Descriptivo de la variable Seguridad de la Información

Tabla N° 15
Análisis Descriptivo del cruce de Variables Pre y Post test de la Seguridad de la Información

		Post SEGURIDAD DE LA INFORMACIÓN(Post TEST)					
		Muy Bajo	Bajo	Media	Alto	Muy Alto	Total
Pre SEGURIDAD DE LA INFORMACIÓN(Pre TEST)	Muy Bajo	0 (0%)	0 (0%)	0 (0%)	0(0%)	0(0%)	0(0%)
	Bajo	0 (0%)	0 (0%)	0 (0%)	0(0%)	0(0%)	0(0%)
	Media	0 (0%)	0 (0%)	3 (17%)	6 (33%)	0(0%)	9 (50%)
	Alto	0 (0%)	0 (0%)	2 (11%)	7 (39%)	0(0%)	9 (50%)
	Muy Alto	0 (0%)	0 (0%)	0(0%)	0(0%)	0(0%)	0(0%)
Total		0 (0%)	0(0%)	5 (28%)	13 (72%)	0(0%)	18 (100%)

Fuente: (Elaboración propia, 2021)

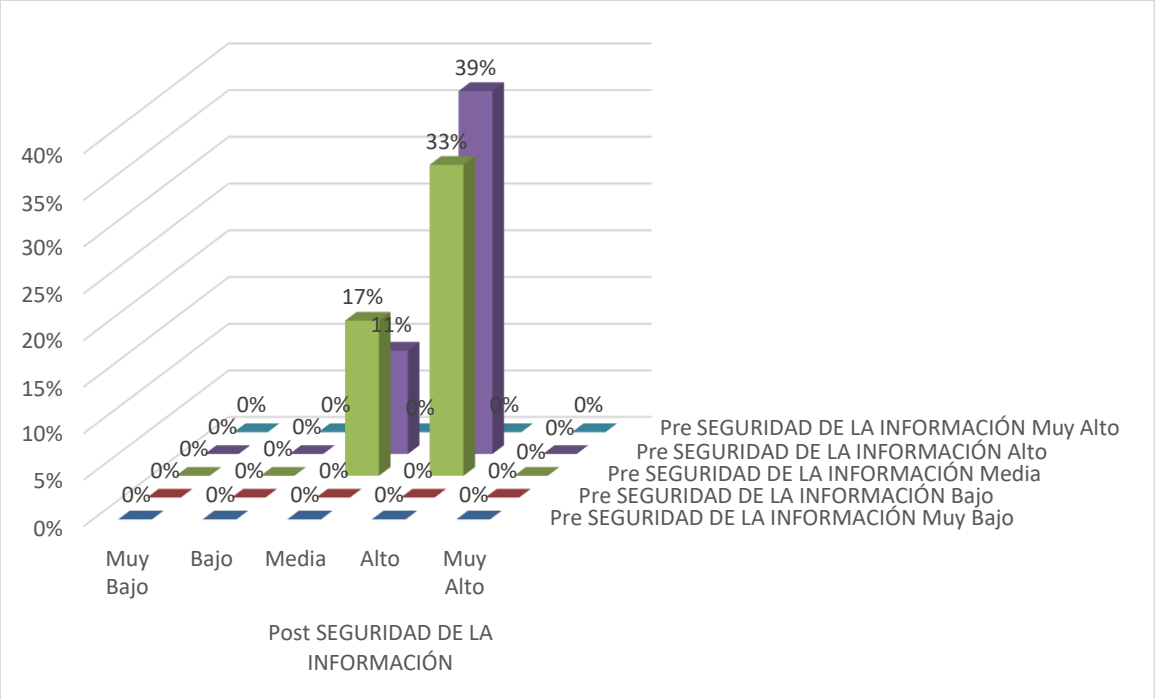


*Figura SEQ Figura * ARABIC 19 Gráfico del cruce de variables Pre y Post test de la Seguridad de la Información*
Fuente: (Elaboración propia, 2021)

Como se puede observar en los datos obtenidos en el cruce del Pre Test y Post Test establecidos en la tabla 15 y figura 19, acerca del análisis descriptivo de la variable Seguridad de la Información en el sistema de planificación de recursos empresariales (ERP), se puede establecer una

diferencia mediante el cruce Pre Test y Post Test en el cual indican lo siguiente: en la categoría "Media" del Pre Test tiene establecido como un valor total de 9 representado por 50%, esta categoría presenta un cambio en el Post test manteniendo en la categoría "Media" con un valor de 3 definido con un 17% y cambiando su categoría a "Alto" con un valor de 6 descrito con un 33% del total, Además en el Pre test la categoría "Alto" con un valor total de 9 descrito con 50%, presento cambios en el Post test su categoría cambia a "Medio" con un valor de 2 representado con un 11%, Así mismo mantiene la categoría "Alto" con un valor de 7 determinado en un 39% del total.

3.2.13 Análisis Descriptivo de la dimensión Integridad Pre Test y Post Test

Tabla 16
Análisis Descriptivo del cruce de Variables Pre y Post test de la dimensión Integridad

		Post DIM INTEGRIDAD(Post TEST)					
		Muy Bajo	Bajo	Media	Alto	Muy Alto	Total
Pre DIM INTEGRIDAD (Pre TEST)	Muy Bajo	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Bajo	0 (0%)	0 (0%)	1 (6%)	0 (0%)	0 (0%)	1 (6%)
	Media	0 (0%)	2 (11%)	4 (22%)	1 (6%)	0 (0%)	7 (39%)
	Alto	0 (0%)	1 (6%)	7 (39%)	2 (11%)	0 (0%)	10 (56%)
	Muy Alto	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Total			3 (17%)	12 (67%)	3 (17%)		18 (100%)

Fuente: Elaboración propia

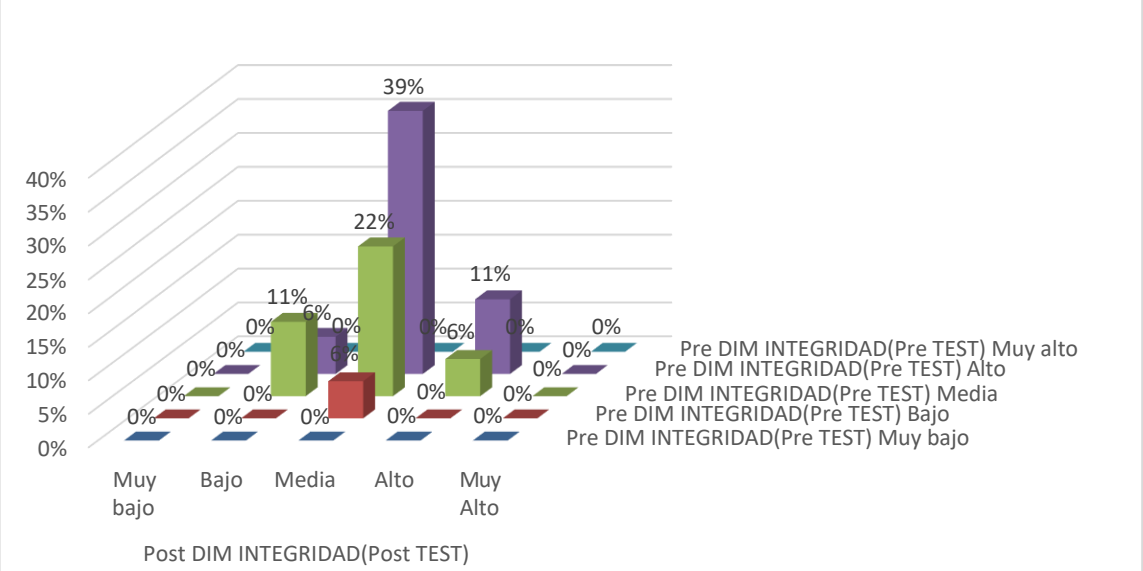


*Figura SEQ Figura * ARABIC 20 Gráfico del análisis descriptivo del cruce de variables Pre y Post test de la dimensión Integridad*
Fuente: Elaboración propia

Como se puede observar en los datos obtenidos en el cruce del Pre Test y Post Test establecidos en la tabla 16 y figura 20, acerca del análisis descriptivo de la dimensión Integridad en el sistema de planificación de recursos empresariales (ERP), se puede establecer una diferencia mediante el cruce Pre Test y Post Test en el cual indican lo siguiente: en la categoría "Baja" del Pre Test tiene establecido como un valor total de 1 representado por 6%, esta categoría presenta un cambio en el Post cambiando su categoría a "Media" con un valor de 1 descrito con un 6% del total, Además en el Pre test la categoría "Media" con un valor total de 7 descrito con 39%, presento cambios en el Post test en su categoría cambia a "Bajo" con un valor de 2 representado con un 11%, Así mismo mantiene la categoría "Media" con un valor de 4 determinado en un 22% del total, la categoría cambia a "Alto" con un valor de 1 representado con un 6%, Después la categoría "Alto" del Pre test con un valor de 10 definido por un 56% del total, muestra el cambio de la categoría a "Bajo" con un valor de 6%, la categoría "Media" con un valor 7 establecido con un valor de 39% y por último la categoría "Alto" se mantiene con un valor de 2 definido por el 11% del total.

3.2.14 Análisis Descriptivo de la dimensión Confidencialidad Pre Test y Post Test

Tabla 17
Análisis Descriptivo del cruce de Variables Pre y Post test de la dimensión Confidencialidad

		Post DIM CONFIDENCIALIDAD(Post TEST)				
		Muy Bajo	Bajo	Alto	Muy Alto	Total
Pre DIM CONFIDENCIALIDAD(Pre TEST)	Muy Bajo	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Bajo	0 (0%)	0 (0%)	2 (11%)	1 (6%)	3 (17%)
	Media	0 (0%)	0 (0%)	9 (50%)	3 (17%)	12 (67%)
	Alto	0 (0%)	0 (0%)	1 (6%)	2 (11%)	3 (17%)
	Muy Alto	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Total				12 (67%)	6 (33%)	18 (100%)

Fuente: Elaboración propia

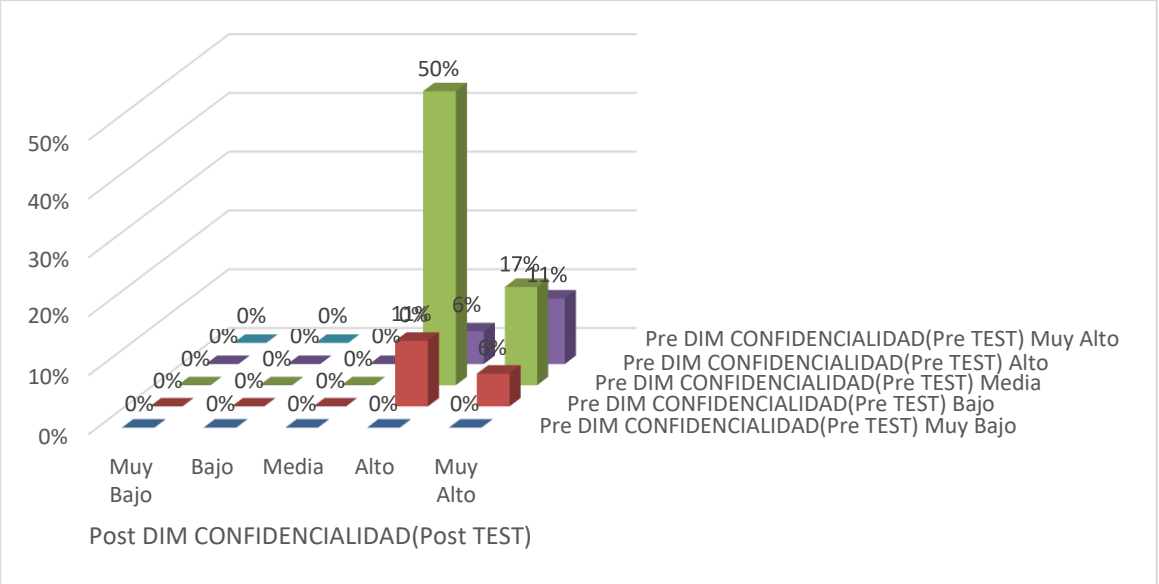


*Figura SEQ Figura * ARABIC 21 Gráfico del análisis descriptivo del cruce de variables Pre y Post test de la dimensión Confidencialidad*
Fuente: Elaboración propia

Como se puede observar en los datos obtenidos en el cruce del Pre Test y Post Test establecidos en la tabla 17 y figura 21, acerca del análisis descriptivo de la dimensión Confidencialidad en el sistema de planificación de recursos empresariales (ERP), se puede establecer una diferencia mediante el cruce Pre test y Post test en el cual indican lo siguiente: en la

categoría "Baja" del Pre test tiene establecido con un valor total de 3 representado por 17%, esta categoría muestra un cambio en el Post cambiando su categoría a "Alta" con un valor de 2 descrito con un 11% del total y a "Muy Alta" con un valor de 1 definido por un 6%, Además en el Pre test la categoría "Media" con un valor total de 12 descrito con 67% del total, presenta cambios en el Post test en su categoría cambia a "Alto" con un valor de 9 representado con un 50% y a "Muy Alto" con un valor de 3 determinado en un 17% del total, así pues la categoría "Alto" del Pre test con un valor de 3 representado con un 17% del total, como se evidencia en el Post test muestra que se mantiene en la categoría "Alto" con un valor de 1 definido con un 6% y en la categoría "Muy Alto" se muestra con un valor de 2 reflejado con 11%.

3.2.15 Análisis Descriptivo de la dimensión Disponibilidad Pre Test y Post test

Tabla 18
Análisis Descriptivo del cruce de Variables Pre y Post test de la dimensión Disponibilidad

		Post DIM DISPONIBILIDAD(Post TEST)					
		Muy Bajo	Bajo	Media	Alto	Muy Alto	Total
Pre DIM DISPONIBILIDAD(Pre TEST)	Muy Bajo	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Bajo	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Media	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Alto	0 (0%)	0 (0%)	2 (11%)	8 (44%)	3 (17%)	13 (72%)
	Muy Alto	0 (0%)	0 (0%)	0 (0%)	4 (22%)	1 (6%)	5 (28%)
Total		0 (0%)	0 (0%)	0 (0%)	12 (67%)	4 (22%)	18 (100%)

Fuente: Elaboración propia

Fuente:

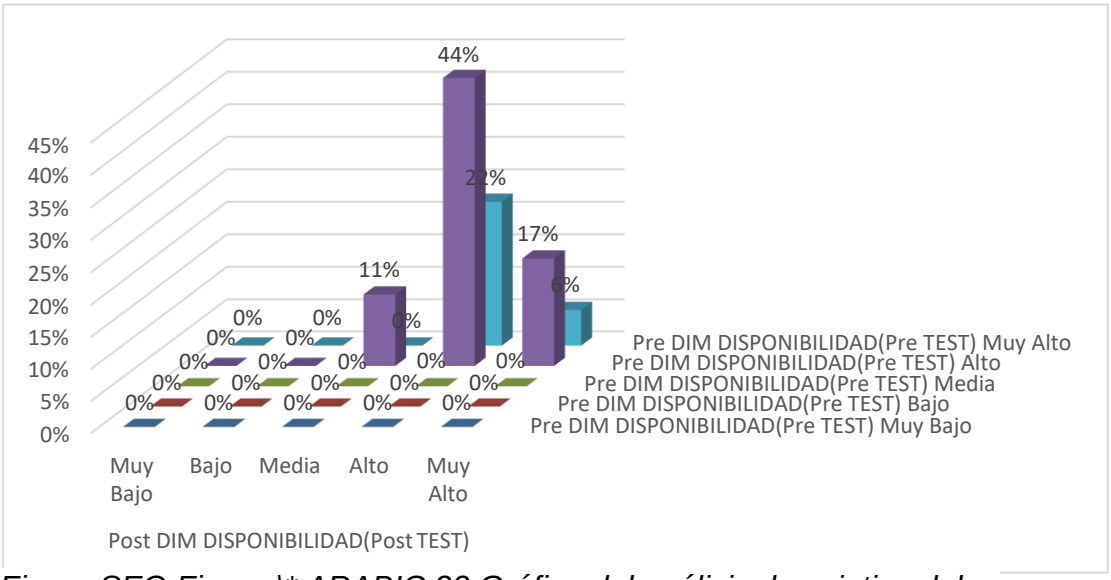


*Figura SEQ Figura * ARABIC 22 Gráfico del análisis descriptivo del cruce de variables Pre y Post test de la dimensión Confidencialidad*
Elaboración propia

Como se puede observar en los datos obtenidos en el cruce del Pre Test y Post Test establecidos en la tabla 18 y figura 22, acerca del análisis descriptivo de la dimensión Disponibilidad en el sistema de planificación de recursos empresariales (ERP), se puede establecer una diferencia mediante el cruce Pre Test y Post Test en el cual indican lo siguiente: en la categoría "Alto" del Pre Test tiene establecido como un valor total de 13 representado por 72% del total, esta categoría presenta un cambio en el Post test cambiando su categoría a "Media" con un valor de 2 descrito con un 11%, así mismo se mantiene en la categoría "Alta" con un valor de 8 establecido con un 44% y por ultima cambia a la categoría "Muy Alto" con un valor de 3 representado por un 72%, en el Pre test la categoría "Muy Alto" con un valor total de 5 descrito con 28%, presento cambios en el Post test en su categoría cambia a "Alta" con un valor de 4 representado con un 22%, además mantiene la categoría "Muy Alta" con un valor de 1 determinado por el 6%, mas no muestra algún en cambio en la categoría "Media" el cual tiene un valor 0 evidenciado por un 0%.

3.2.16 Análisis Descriptivo de la dimensión Riesgo Pre Test y Post Test

Tabla 19
Análisis Descriptivo del cruce de Variables Pre y Post test de la dimensión Riesgos

		Post DIM RIESGOS(Post TEST)				
		Muy Bajo	Bajo	Media	Alto	Total
Pre DIM RIESGOS(Pre TEST)	Muy Bajo	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Bajo	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
	Media	0 (0%)	0 (0%)	0 (0%)	11 (61%)	11 (61%)
	Alto	0 (0%)	0 (0%)	2 (11%)	5 (28%)	7 (39%)
	Muy Alto	0 (0%)	0 (0%)	0 (0%)	0 (0%)	0 (0%)
Total		0 (0%)	0 (0%)	0 (0%)	16 (89%)	18 (100%)

Fuente: Elaboración propia

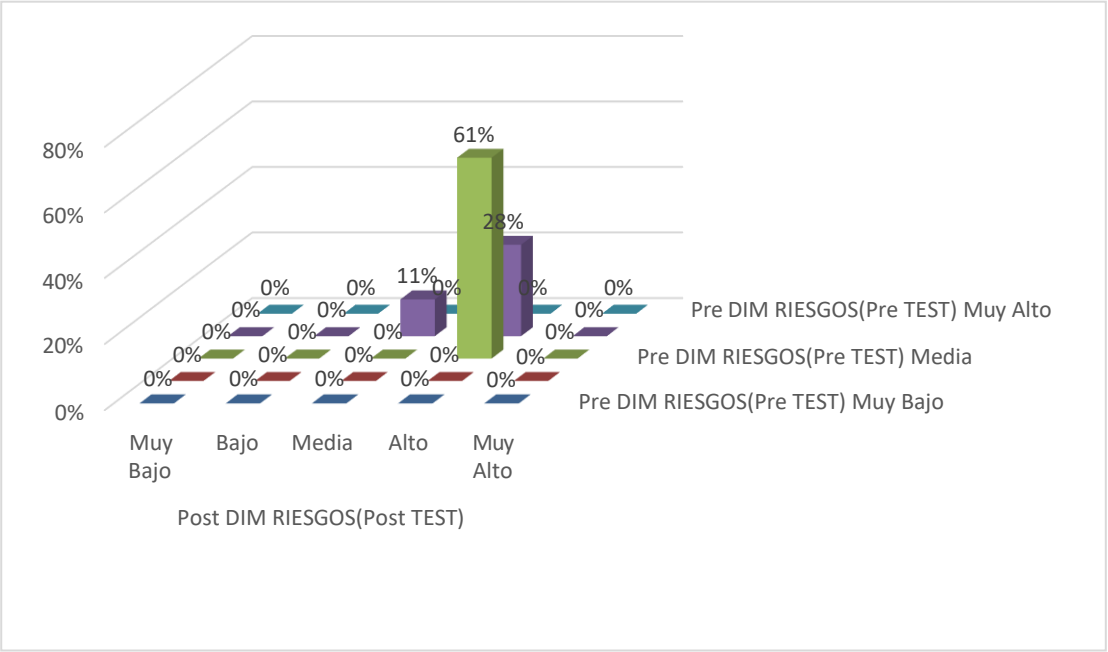


*Figura SEQ Figura * ARABIC 23* Gráfica del Análisis Descriptivo del cruce de Variables Pre y Post test de la dimensión Riesgos

Fuente: Elaboración propia

Como se puede observar en los datos obtenidos en el cruce del Pre Test y Post Test establecidos en la tabla 19 y figura 23, acerca del análisis descriptivo de la dimensión Riesgos en el sistema de planificación de recursos empresariales (ERP), se puede establecer una diferencia mediante

el cruce Pre Test y Post Test en el cual indican lo siguiente: en la categoría "Media" del Pre Test tiene establecido como un valor total de 11 representado por 61% total, esta categoría presenta un cambio en el Post test mostrando ninguna cambio en la categoría "Media" con un valor de 0 definido con un 0% y cambiando su categoría a "Alto" con un valor de 11 descrito con un 61% del total, Además en el Pre test la categoría "Alto" con un valor total de 7 descrito con 39%, presento cambios en el Post test su categoría cambia a "Media" con un valor de 2 representado con un 11%, Así mismo mantiene la categoría "Alto" con un valor de 5 determinado en un 28% del total.

3.3 Prueba de hipótesis

En el presente informe se va a cotejar las dos hipótesis que se han propuesto siendo una de tipo nula y la otra de tipo alterna, este contraste involucra que se tome una decisión sobre las hipótesis planteadas, de esta manera influyendo en el rechazo o no rechazo de una hipótesis en favor de la otra.

Al respecto Hernández, Fernández y Baptista (2014) comentan que:

> "Las hipótesis son las guías precisas hacia el problema de investigación o fenómeno que se estudia, también pueden definirse como explicaciones tentativas sobre las posibles relaciones entre dos o más variables" (p.107).

Además de ello, el nivel de significancia que se tomó en cuenta para la presente investigación es el de 0.05, que repercute en un 95% de seguridad y 5% de error, al respecto Hernández, Fernández y Baptista (2014), mencionan que:

> "Para aceptar una hipótesis el nivel de significancia debe ser menor 0.05, el cual implica que el investigador tiene 95 % de seguridad para generalizar sin equivocarse y solo el 5% en contra" (p.302).

3.3.5 Prueba de hipótesis general

H0: El uso de la ISO 27001 no influye de manera significativa en la mejora de la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021

H1: El uso de la ISO 27001 influye de manera significativa en la mejora de la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021.

Tabla 20 Prueba de contrastación de hipótesis

Correlaciones

			Pre SEGURIDAD DE LA INFORMACIÓN	Post SEGURIDAD DE LA INFORMACIÓN
Rho de Spearman	Pre SEGURIDAD DE LA INFORMACIÓN	Coeficiente de correlación	1,000	,124
		Sig. (bilateral)		,624
		N	18	18
	Post SEGURIDAD DE LA INFORMACIÓN	Coeficiente de correlación	,124	1,000
		Sig. (bilateral)	,624	
		N	18	18

Fuente: Elaboración propia

Como podemos observar en la tabla 20, se obtuvo un nivel de significancia de 0,624 lo cual indica que llega a hacer mayor que el 0.05, así mismo el valor obtenido en el nivel de significancia permite aceptar o rechazar la hipótesis de investigación, es decir debido a que el valor del nivel de significancia es mayor a 0.05, se rechaza la hipótesis alternativa (H1) y se acepta la hipótesis nula (H0), en otras palabras de acuerdo al cuadro estadístico se puede entender que: El uso de la ISO 27001 no influye de manera significativa en la mejora de la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021.

3.3.6 Prueba de hipótesis de la dimensión Integridad

H0: La aplicación de la ISO 27001 no influye de manera significativa en la mejora de la confidencialidad de la información en los sistemas ERP de la empresa ICO, año 2021

H1: La aplicación de la ISO 27001 influye de manera significativa en la mejora de la confidencialidad de la información en los sistemas ERP de la empresa ICO, año 2021

Tabla 21 Prueba de contrastación de hipótesis dimensión Integridad

			Pre DIM INTEGRIDAD	Post DIM INTEGRIDAD
Rho de Spearman	Pre DIM INTEGRIDAD	Coeficiente de correlación	1,000	,179
		Sig. (bilateral)		,476
		N	18	18
	Post DIM INTEGRIDAD	Coeficiente de correlación	,179	1,000
		Sig. (bilateral)	,476	
		N	18	18

Fuente: Elaboración propia

Como podemos observar en la tabla 21, se obtuvo un nivel de significancia de 0,476 lo cual indica que el dato obtenido es mayor que el 0.05, es decir el valor obtenido en el nivel de significancia deja aceptar o rechazar la hipótesis de investigación, en otras palabras debido a que el valor del nivel de significancia es mayor a 0.05, se rechaza la hipótesis alternativa (H1) y se acepta la hipótesis nula (H0), hay que hacer notar que del cuadro estadístico se puede entender que: La aplicación de la ISO 27001 no influye de manera significativa en la mejora de la confidencialidad de la información en los sistemas ERP de la empresa ICO, año 2021

3.3.7 Prueba de hipótesis de la dimensión Confidencialidad

H0: La aplicación de la ISO 27001 no influye de manera significativa en la mejora de la confidencialidad de la información en los sistemas ERP de la empresa ICO, año 2021.

H1: La aplicación de la ISO 27001 influye de manera significativa en la mejora de la confidencialidad de la información en los sistemas ERP de la empresa ICO, año 2021.

Tabla 22 Prueba de contrastación de hipótesis dimensión Confidencial

Correlaciones

			Pre DIM CONFIFENCIALIDAD	Post DIM CONFIFENCIALIDAD
Rho de Spearman	Pre DIM CONFIFENCIALIDAD	Coeficiente de correlación	1,000	,204
		Sig. (bilateral)		,417
		N	18	18
	Post DIM CONFIFENCIALIDAD	Coeficiente de correlación	,204	1,000
		Sig. (bilateral)	,417	
		N	18	18

Fuente: Elaboración propia

Como podemos visualizar en la tabla 22, se obtuvo un nivel de significancia de 0,417 lo que nos da entender que el valor es mayor que el 0.05, como se ha dicho el valor obtenido en el nivel de significancia permite aceptar o rechazar la hipótesis de investigación, es decir debido a que el valor del nivel de significancia es mayor a 0.05, de manera automática se debe rechazar la hipótesis alternativa (H1) y se debe aceptar la hipótesis nula (H0), en otras palabras de acuerdo al cuadro estadístico se puede entender que: La aplicación de la ISO 27001 no influye de manera significativa en la mejora de la confidencialidad de la información en los sistemas ERP de la empresa ICO, año 2021.

3.3.8 Prueba de hipótesis de la dimensión Disponibilidad

H0: La aplicación de la ISO 27001 no influye de manera significativa en la mejora de la disponibilidad de la información en los sistemas ERP de la empresa ICO, año 2021.

H1: La aplicación de la ISO 27001 influye de manera significativa en la mejora de la disponibilidad de la información en los sistemas ERP de la empresa ICO, año 2021.

Tabla 23 Prueba de contrastación de hipótesis dimensión Disponibilidad

Correlaciones

			Pre DIM DISPONIBILIDAD	Post DIM DISPONIBILIDAD
Rho de Spearman	Pre DIM DISPONIBILIDAD	Coeficiente de correlación	1,000	,086
		Sig. (bilateral)		,734
		N	18	18
	Post DIM DISPONIBILIDAD	Coeficiente de correlación	,086	1,000
		Sig. (bilateral)	,734	
		N	18	18

Fuente: Elaboración propia

Como podemos observar en la tabla 23, se obtuvo un nivel de significancia de 0,734 lo cual da a entender que el valor es mayor que el 0.05, hay que tener en cuenta que el valor obtenido en el nivel de significancia indica si se acepta o se rechaza la hipótesis de investigación, como se ha dicho el valor del nivel de significancia es mayor a 0.05, en conclusión se rechaza la hipótesis alternativa (H1) y se acepta la hipótesis nula (H0), además de acuerdo al cuadro estadístico se puede entender que: La aplicación de la ISO 27001 no influye de manera significativa en la mejora de la disponibilidad de la información en los sistemas ERP de la empresa ICO, año 2021.

3.3.9 Prueba de hipótesis de la dimensión Riesgos

H0: La aplicación de la ISO 27001 no influye de manera significativa en la mejora de la prevención de los riesgos en la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021.

H1: La aplicación de la ISO 27001 influye de manera significativa en la mejora de la prevención de los riesgos en la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021.

Tabla 24 Prueba de contrastación de hipótesis dimensión Riesgos

Correlaciones

			Pre DIM RIESGOS	Post DIM RIESGOS
Rho de Spearman	Pre DIM RIESGOS	Coeficiente de correlación	1,000	-,443
		Sig. (bilateral)		,065
		N	18	18
	Post DIM RIESGOS	Coeficiente de correlación	-,443	1,000
		Sig. (bilateral)	,065	
		N	18	18

Fuente: Elaboración propia

Como podemos ver en la tabla 24, se llegó a obtener un nivel de significancia de 0,065, hay que destacar que el valor obtenido es mayor que el 0.05, después de obtener el valor del nivel de significancia nos permite comprender si se acepta o se rechaza la hipótesis de investigación, en otras palabras debido a que el valor del nivel de significancia es mayor a 0.05, se debe rechazar la hipótesis alternativa (H1) y se acepta la hipótesis nula (H0), hay que hacer notar que el análisis del cuadro estadístico se entiende que: La aplicación de la ISO 27001 no influye de manera significativa en la mejora de la prevención de los riesgos en la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

Discusión

En cuanto a los resultados obtenidos en el presente trabajo de investigación, utilizando el análisis descriptivo de la variable Seguridad de la información se puede observar en la tabla de cruce de variables ,una mayor aceptación en el nivel Alto de la variable seguridad de la información, con 7 respuestas representado el 39% de las 14 en total; en la prueba de hipótesis, se ha podido determinar el nivel de significancia igual 0.624 siendo este valor mayor al 0.05,valor límite máximo permitiendo rechazar la hipótesis de investigación, en consecuencia se afirma que no existe una influencia significativa en la mejora de la seguridad de la información en la empresa ICO FOOD SERVICE, año 2021. Estos resultados difieren con los afirmados por Leiva (2015) debido a que su plan del SGSI obtuvo una mayor cantidad de activos que resguardar, los cuales tuvieron un nivel de criticidad muy alto, así mismo tuvieron unos 75 riesgos que se emplearon para trabajar en las mitigaciones(p.202), ahora bien Leiva utilizo uno de los documentos exigido sobre los procedimientos de la continuidad del negocio, no obstante en la presente investigación a diferencia de Leiva los activos identificados para establecer los riesgos no se encontraban definidos y eran menores a lo expuesto por el citado autor, así pues se procedió a comunicarse con los trabajadores con el objetivo de encontrar los activos que no tenían definidos, asimismo lo encontrado por Yan y Zavala (2013) (pág. 131) indica que su plan de mejora empleó dos tipos, el uso de la ISO 27001:2005 y buenas practicas COBIT el cual requiere una participación completa a nivel estratégico, además de usar la metodología MAGERIT permitió dirigir de mejor manera las actividades de cada una de las fases de la auditoría facilitando con ello el análisis y evaluación del centro de datos, asimismo lo encontrado por Córdova (2014) menciona que para establecer los controles adecuados de protección de información se debe tener documentada la información que se quiera proteger a su vez donde se encuentra ubicadas. Asimismo, lo encontrado por el Instituto colombiano de normas técnicas y certificación (como se citó en Benavides & Blandón, 2017) (p. 40) indican que un sistema de gestión de seguridad de la información es un sistema de

gestión general el cual está enfocado en los riesgos empresariales que se establece para crear, implementar, operar, supervisar, mantener y mejorar la seguridad de la información, permitiendo el control sobre los sistemas de información en conjunto con la de la organización.

Acerca de la delimitación en la actual exploración, se encontraron diferentes limitaciones en cuanto a la presente investigación, la primera fue que los activos identificados para establecer los riesgos no se encontraban definidos, como segunda limitación fue que la información no se encontraba documentada y como tercera limitación los archivos de información no se encontraban ubicadas correctamente.

Estas limitaciones se podrían amortizar en una investigación que contemple una clara identificación de los activos, una documentación de la información completa y un orden correcto en los procesos.

Dimensión Integridad

Acerca de los resultados obtenidos en el presente trabajo de investigación, utilizando el análisis descriptivo para la dimensión de la integridad perteneciente a la variable Seguridad de la información podemos observar en la tabla de cruce de variables con una mayor aceptación en el nivel Media de la dimensión Integridad, con 7 respuestas representado el 39% del total; en la contrastación de la hipótesis, según lo mencionado en la tabla 21 se ha determinado que a partir del el nivel de significancia la integridad es igual 47.6%, definiendo de esta manera que no existe una influencia significativa en la integridad de la información en los sistemas ERP de la empresa ICO FOOD SERVICE, año 2021, sin embargo estos resultados difieren de lo afirmado por Cruz & Fukusaki (2017, pp. 132) indicando que la sensibilización del personal sobre los temas de seguridad es vital para la implementación de un SGSI en la organización y a su vez permitiendo que maduren en conjunto, teniendo esto en cuenta los trabajadores son conscientes que la información que manejan debe permanecer integro, a causa de la sensibilización permite una robustez al sistema implementado y generar una mejora continua.

Asimismo, lo encontrado por Alcántara (2015, pp. 146) establece que el uso de la guía de implementación basada en la ISO 27001, logró mejorar el proceso para detectar las anomalías en la seguridad de la información, reflejado en distintos mecanismos de seguridad para salvaguardarla y prevenir su mal uso y divulgación no adecuada que perjudiquen a la institución. Asimismo, lo encontrado por Jansen (2016, pp. 160) aclara que realizar correctamente la gestión de la seguridad de la información requiere de establecer y mantener, los controles y las políticas de seguridad que tienen la obligación de conservar la confidencialidad, la integridad y la disponibilidad de la información de la empresa.

Acerca de la limitación de la dimensión integridad para la presente investigación fue la concientización del uso del SGSI por parte del personal interno ya que no se pudo llevar a cabo en su totalidad debido a que se contaba con un corto tiempo para instruir a los empleados sobre la importancia de la seguridad e integridad de información que debe mantenerse.

Esta limitación se podría retribuir en una investigación que contemple la concientización del uso del SGSI en su totalidad para todo el personal de la organización.

Dimensión Confidencialidad

Acerca de los resultados obtenidos en el presente trabajo de investigación, utilizando el análisis descriptivo para la dimensión de la confidencialidad perteneciente a la variable Seguridad de la información podemos observar en la tabla de cruce de variables con una mayor aceptación en el nivel Alto de la dimensión confidencialidad, con 12 respuestas representado el 67% del total, así mismo se observa en la tabla 22 que el nivel de significancia es igual 41.7% siendo este valor mayor al 0.05 definiendo de esta manera que no existe una influencia significativa en la confidencialidad de la información en los sistemas ERP de la empresa. Estos resultados difieren lo afirmado por

(Esquivel y Bobadilla,2017pp.81-84) mencionando que que el plan de SGSI garantiza la confidencialidad de seguridad de la información en un nivel alto, los cuales permitieron asentar los lineamientos y procedimientos generales. Asimismo, los resultados encontrados por (Benavides y Blandón, 2017,pp. 20-95) indican que el modelo de SGSI implementado permite garantizar la confidencialidad , integridad y disponibilidad de la información de los niños , niñas ,adolescentes y personal administrativo; así mismo lo encontrado por(Ochoa, 2017,pp.30-108) indican que la construcción , implementación y despliegue de los controles del sistema de seguridad de la información permitió a la universidad centralizar sus activos en un aplicativo web asignándoles un nivel de confidencialidad. Según la ISO 27001 los tres principios fundamentales en lo que se basa la seguridad de la información son la confidencialidad, la integridad y la disponibilidad.

Acerca de la limitación de la dimensión confidencialidad para la presente investigación fue la falta de planificación de los controles del sistema de seguridad de la información generando que los activos no se puedan centralizar.

Esta limitación se podría retribuir en una investigación que contemple la planificación de los controles del sistema de gestión de seguridad de la información.

Dimensión Disponibilidad

Acerca de los resultados obtenidos en el presente trabajo de investigación, utilizando el análisis descriptivo para la dimensión de la disponibilidad perteneciente a la variable Seguridad de la información podemos observar en la tabla de cruce de variables con una mayor aceptación en el nivel Alto de la dimensión disponibilidad, con 12 respuestas representado el 67% del total, así mismo se observa en la tabla 23 que el nivel de significancia es igual 73.4% siendo este valor mayor al 0.05 definiendo de esta manera que no existe una influencia significativa en la disponibilidad de la información en los

sistemas ERP de la empresa ICO FOOD SERVICE, año 2021. Estos resultados difieren de (Díaz y Ramirez,2014,pp,16-99) indicando que para que se genere una mejora en grandes cantidades en la gestión de la seguridad de la información se tienen que identificar normas y estándares pertinentes para que puedan ser aplicados a la institución financiera, asimismo lo encontrado por (Berrios y Rocha ,2015,pp.14-138) indicando que el modelo SMESEC permite implementar el SGSI a pequeñas y medianas empresas salvaguardado la disponibilidad de la información; así mismo lo encontrado por(Cruz y Fukusaki,2017,pp,14-132) indican que la implementación se logró a través del diseño e implementación de políticas para gestionar eficientemente el acceso a la información, buscando asegurar la disponibilidad de los activos de información de esta manera logrando minimizar los riesgos de seguridad de la información.

Acerca de la limitación de la dimensión disponibilidad para la presente investigación fue la falta de identificación de normas y estándares pertinentes para que puedan ser aplicados a la organización.
Esta limitación se podría retribuir en una investigación que contemple la identificación correcta de las normas y estándares para un exitoso uso de la norma ISO 27001.

Dimensión Riesgos

Acerca de los resultados obtenidos en el presente trabajo de investigación, utilizando el análisis descriptivo para la dimensión de la disponibilidad perteneciente a la variable Seguridad de la información podemos observar en la tabla de cruce de variables con una mayor aceptación en el nivel Alto de la dimensión Riesgos, con 7 respuestas representado el 39% del total; en la contratación de la hipótesis, según lo mencionado en la tabla 24 se ha determinado que a partir del coeficiente de correlación el nivel de influencia

de la dimensión riesgos es igual – 44.3%, como podemos observar en la tabla 24 el nivel de significancia obtenido es 0.033 siendo este valor menor al 0.05 definiendo de esta manera que existe una influencia significativa negativa en la dimensión riesgos en los sistemas ERP de la empresa ICO FOOD SERVICE, año 2021. Estos resultados difieren de Cruz & Fukusaki (2017, pp. 131) afirmando que las aplicaciones de controles son idóneos para el tratamiento de riegos, debido a que fueron diseñados en base a variables de costo de implementación, la efectividad para mitigación de riesgo identificado y el análisis de costo beneficio, así mismo lo encontrado Berrios & Rocha (2015, pp. 139) nos dice, puesto que la implementación del modelo SMESEC se trabajó con una lista de riesgos de la seguridad de la información los cuales permitirán juntarse con los riesgos establecidos por una empresa teniendo la finalidad de considerar las medidas que se tomaran a futuro para la empresa, además en concordancia con los resultados obtenidos en la investigación, asimismo lo encontrado por Perafan & Mildred (2014, pp. 109) acerca del uso de la metodología MAGERIT es el primer paso para garantizar la seguridad de los activos de información y que gracias al análisis de riesgos se pueden determinar los controles y políticas necesarias para que sean tomados como soporte en el SGSI, asimismo lo encontrado por Sullivan (2016, pp. 162) indica que la gestión de riesgos es el proceso en el cual podremos identificar, comprender, evaluar, mitigar los riesgos, las vulnerabilidades subyacentes y el impacto en la información. En el Perú hace falta la concientización de una gestión de riesgos en los negocios, ya que esta no es tomada muy en cuenta, asimismo lo encontrado por Arellano (2016) indica que en el Perú un 70% de las empresas toma la gestión de riesgos como parte de su agenda a que se va a realizar más adelante, ahora bien en comparación al promedio global de empresas que hacen uso de la tecnología Gobierno, riesgo y cumplimiento (GRC) como herramientas, se evidencia que el Perú el 33% de las empresas encuestadas hace uso de estas herramientas GRC, en cambio se demuestra que un 58% de las empresas peruanas no tienen presente una gerencia de riesgos, en cuanto al 42% restante, únicamente el 9% reporta funcionalmente a algunos de los

comités o al directorio, esto demuestra que en el Perú la empresas no toman como uno de los objetivos principales la gestión de riesgo.

Acerca de la limitación de la dimensión riesgo para la presente investigación fue que no se definió los controles para el tratamiento de los riesgos.
Esta limitación se podría retribuir en una investigación que contemple la definición clara de los controles para la gestión de los riesgos.

Conclusiones

Conclusión 1

Teniendo en cuenta la prueba de hipótesis el valor de la significancia es 0.312 el cual es mayor a 0.05 se rechaza la hipótesis de la investigación y se concluye que no existe influencia positiva en el uso de la norma ISO 27001 en los sistemas ERP, en la variable Seguridad de la información. Asimismo, considerando el coeficiente de correlación Rho de Spearman que arroja la citada prueba de hipótesis 0.312, según la tabla N° 20 se determina que no existe influencia positiva.

Conclusión 2

Teniendo en cuenta la prueba de hipótesis el valor de la significancia es 0.238 el cual es mayor a 0.05 se rechaza la hipótesis de la investigación y se concluye que no existe influencia positiva en el uso de la norma ISO 27001 en los sistemas ERP, en la dimensión integridad de la información. Asimismo, considerando el coeficiente de correlación Rho de Spearman que arroja la citada prueba de hipótesis 0.179 según la tabla N° 21, se determina que no existe influencia positiva en dicha dimensión.

Conclusión 3

Teniendo en cuenta la prueba de hipótesis el valor de la significancia es 0.208 el cual es mayor a 0.05 se rechaza la hipótesis de la investigación y se concluye que no existe influencia positiva en el uso de la norma ISO 27001 en los sistemas ERP, en la dimensión confidencialidad de la información. Asimismo, considerando el coeficiente de correlación Rho de Spearman que arroja la citada prueba de hipótesis 0.204 según la tabla N° 22, se determina que no existe influencia positiva en dicha dimensión.

Conclusión 4

Teniendo en cuenta la prueba de hipótesis el valor de la significancia es 0.367 el cual es mayor a 0.05 se rechaza la hipótesis de la investigación y se concluye que no existe influencia positiva en el uso de la norma ISO 27001 en los sistemas ERP, en la dimensión disponibilidad de la información. Asimismo, considerando el coeficiente de correlación Rho de Spearman que arroja la citada prueba de hipótesis 0.086 según la tabla N° 23, se determina que no existe influencia positiva en dicha dimensión.

Conclusión 5

Teniendo en cuenta la prueba de hipótesis el valor de la significancia es 0.033 el cual es mayor a 0.05 se rechaza la hipótesis de la investigación y se concluye que existe una influencia negativa en el uso de la norma ISO 27001 en los sistemas ERP, en la dimensión riesgo de la información. Asimismo, considerando el coeficiente de correlación Rho de Spearman que arroja la citada prueba de hipótesis -0,443 según la tabla N° 24, se determina que existe influencia negativa en dicha dimensión.

REFERENCIAS

4, R. H. (sf). *Red Hat Enterprise Linux 4*. Obtenido de http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/ch-acctsgrps.html

abox. (sf). Obtenido de https://www.abox.com/PDFM/infohardkey.pdf

acens. (s.f.). Obtenido de https://www.acens.com/wp-content/images/2015/03/vulnerabilidades-bbdd-wp-acens.pdf

acimed. (sf). Obtenido de http://www.acimed.sld.cu/index.php/acimed/article/view/270/232

blogthinkbig. (sf). Obtenido de https://blogthinkbig.com/que-es-el-cifrado

ebookcentral. (sf). Obtenido de http://ebookcentral.proquest.com/lib/upnortesp/reader.action?docID=3160439&query=criptologia+

elpuig. (sf). Obtenido de https://elpuig.xeill.net/Members/vcarceler/c1/didactica/apuntes/ud4/na1

google. (sf). Obtenido de https://books.google.com.pe/books?

mintic. (sf). Obtenido de http://www.mintic.gov.co/arquitecturati/630/articles-9263_recurso_pdf.pdf

optimbyte. (sf). Obtenido de http://www.optimbyte.com/actividad-de-los-usuarios-en-wordpress/

oqotech. (sf). Obtenido de https://www.oqotech.com/servicios/validacion-de-sistemas-informatizados/

rebundancia-e-inconsistencia-de-datos. (sf). Obtenido de https://prezi.com/9rj6pc3grzmn/la-rebundancia-e-inconsistencia-de-datos/

redalyc. (sf). Obtenido de http://www.redalyc.org/html/849/84950866004/

Repositorio U San Martin. (sf). Obtenido de http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/331/1/castro_ke.pdf

(sf). Obtenido de https://www.tecnologias-informacion.com/integridaddatos.html

(sf). Obtenido de https://technologyincontrol2.wordpress.com/2015/02/23/integridad-de-la-informacion-marco-de-referencia/

wikipedia. (sf). Obtenido de https://es.wikipedia.org/wiki/Centro_Nacional_de_Inteligencia

27000, I. (s.f.). Obtenido de http://www.iso27000.es/iso27002_9.html

Aguila, X. (2015). *ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN EL CRITERIO DE LA NORMA NTE INEN-ISO/IEC 27001:2011, DE UN MODELO DE NEGOCIO APLICADO EN LA COMERCIALIZACIÓN Y DISTRIBUCIÓN DE* (4, sf)*PRODUCTOS QUÍMICOS.* Universidad Politécnica Salesiana, Guayaquil Recuperado de : http://dspace.ups.edu.ec/handle/123456789/10283.

Alcantara, J. (2015). *Guía de implementación de la seguridad basado en la norma ISO/IEC 27001, para apoyar la seguridad en los sistemas informáticos de la comisaria del norte PNP en la ciudad de Chiclayo.* Lambayeque: Universidad Católica Santo Toribio de Mogrovejo.

Alvarez, C. (2017). Implementación de la ISO 27001. *(Trabajo fin de Master).* Universitat Oberta de Catalunya.

Arellano, N. (01 de 2016). *ey*. Obtenido de https://www.ey.com/pe/es/newsroom/newsroom-am-gestion-riesgos-gobierno-corporativo

Arenas, C., & De los Santos, D. (2017). *Gestión de la seguridad de la información para la toma de decisiones en la infraestructura de la red telemática de la universidad nacional pedro ruiz gallo utilizando cobit 5 y software open source.* Lambayeque: Universidad Nacional Pedro Ruiz Gallo.

Baca, G. (2015). *Proyectos de sistemas de información.* from http://ebookcentral.proquest.com: Grupo Editorial Patria .

Bach. (2013). *Plan de mejora de la seguridad de la información y continuidad del Centro de la gerencia regional de educación La Libertad aplicando lineamientos ISO 27001 y buenas practicas COBIT.* Trujillo: Universidad Privada Antenor Orrego.

Benavides, A., & Blandon, C. (2017). *Modelo de Sistema de Gestión de Seguridad de la Información Basado en la Norma NTC ISO/IEC 27001 para Instituciones Públicas de Educación Básica de la Comuna Universidad de la Ciudad de Pereira.* Universidad Autonoma de Manizales, Colombia.

Benavides, A., & Blándon, C. (24 de Julio de 2017). *repositorio.autonoma.* Obtenido de http://repositorio.autonoma.edu.co/jspui/bitstream/11182/1117/1/INFORME%20FINAL%20ALEJANDRA%20%26%20CARLOS%20V5.pdf

Bernaldo, N. (2016). *Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016.* Universidad Cesar Vallejo, Lima.

Berríos, C., & Rocha, M. (06 de Noviembre de 2015). *repositorioacademico.upc.* Obtenido de http://repositorioacademico.upc.edu.pe/upc/bitstream/10757/581891/1/berrios_mc-rocha_cm.pdf

Cáceres, C., & Mena, C. (2015). *ELABORACIÓN DE LA GUÍA DE IMPLANTACIÓN DE LAS NORMAS PRIORITARIAS DEL ESQUEMA GUBERNAMENTAL DE SEGURIDAD DE LA INFORMACIÓN EGSI EN LAS ENTIDADES DE LA ADMINISTRACIÓN PÚBLICA CENTRAL.* ESCUELA POLITÉCNICA NACIONAL, Quito.

Campos, G., & Lule, N. (2012). La observación, un metodo para el estudio de la realidad. *Xihmai, VII*(13), 45-60.

Cesar, B. (2010). *Metodología de la investigación administración, economía, humanidades y ciencias sociales.* bogotá d.c. colombia: PEARSON.

Chicaiza, N. (2015). ANÁLISIS Y DESARROLLO DE UNA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27000 PARA EMPRESAS DE DESARROLLO DE SOFTWARE BANCARIO EN ECUADOR. *(Plan de Investigación).* UNIVERSIDAD INTERNACIONAL SEK, Quito.

Cibercamp. (s.f.). Obtenido de https://cybercamp.es/cybercamp2015/ponentes/ignacio-gilart-iglesias.html

Contreras, L. (2017). Diseño de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO/iec 27001 para la dirección de sistemas de la gobernación de Boyacá. *(PROYECTO DE GRADO PARA OPTAR POR EL TITULO DE ESPECIALISTA EN SEGURIDAD INFORMATICA).* Universidad Nacional Abierta y a Distancia, TUNJA: Recuperado de:http: //hdl.handle.net/10596/11895.

Cordero, G. (2015). Estudio Comparativo entre las metodologias MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información. *(Tesis de Grado).* Universidad del Azuay, Cuenca, Ecuador.

Costas, J. (2014). *Mantenimiento de la seguridad en sistemas informáticos.* Retrieved from http://ebookcentral.proquest.com: RA-MA Editorial .

Cruz, M., & Fukusaki, S. (2017). *Diseño e implementación de un SGSI para proteger los activos de información de la clínica MEDCAM Perú.* Lima: Universidad San Martin De Porres.

Datasec. (2017). *datasec-soft*. Obtenido de https://www.datasec-soft.com/es/blog/certificados-isoiec-27001-emitidos-nivel-mundial

Dell. (s.f.). Obtenido de http://www.conocedell.es/seguridad/gestion-segura-de-las-cuentas-privilegiadas-en-tres-pasos

Encala, R., & Quispe, J. (2015). SISTEMA EXPERTO EN AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LAS NTP ISO 27001 Y 27002. *(Tesis).* UNIVERSIDAD PRIVADA ANTENOR ORREGO, Trujillo - Perú.

Espinoza, H. (s.f.). Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo. *2013.* Pontificia Universidad Catolica del Perú, Lima.

EY. (13 de Junio de 2017). *exitosanoticias*. Obtenido de https://exitosanoticias.pe/solo-7-empresas-peruanas-estan-listas-ante-ciberataques/

Fernandez, D., & Oscar, P. (s.f.). MEJORA DE SEGURIDAD DE INFORMACIÓN EN LA COMANDANCIA DE OPERACIONES GUARDACOSTAS BASADA EN LA NORMA TÉCNICA PERUANA NTP-ISO/IEC 27001:2008. *2014.* Universidad De San Martin de Porres, Lima.

Fidias. (2012). *ebevidencia.* Caracas: EPISTEME, C.A. Obtenido de https://ebevidencia.com/wp-content/uploads/2014/12/EL-PROYECTO-DE-INVESTIGACI%C3%93N-6ta-Ed.-FIDIAS-G.-ARIAS.pdf

Garcia, N., & Elkin, G. (2015). *PROPUESTA DE GUÍA METODOLÓGICA PARA AUDITAR EL ESTADO DE LAS TECNOLOGÍAS DE INFORMACIÓN Y LAS TELECOMUNICACIONES - TIC - EN LAS ENTIDADES PÚBLICAS QUE FISCALIZA LA CONTRALORÍA GENERAL DE ANTIOQUIA (COLOMBIA).* Universidad Pontificia Bolivariana Colômbia, Antioquia, Colombia.

Guerrero. (2016). SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27001 SOBRE UN SERVIDOR CENTOS Y SERVICIOS DE RED PARA EL APOYO DE LA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA IMPORTADORA MEGATECH DE LA PROVINCIA DE SANTO DOMINGO DE LOS T. *(Proyecto de Investigación).* UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES, Santo Domingo - Ecuador: Recuperado por : http://dspace.uniandes.edu.ec/handle/123456789/4994.

Guerrero, Y., & Tabango, R. (2014). *Sistema de gestión de seguridad de la información basado en la norma ISO 27001 y 27002 para la unidad de informática y telecomunicaciones de la universidad de Nariño.* Pasto: Universidad de Nariño.

Guzmán, G., & Taborda, C. (2015). *Diseño de un sistema de gestión de la seguridad informática –SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C., a través de la auditoría.* Universidad Nacional Abierta y a Distancia, Bogota recuperado de: http://hdl.handle.net/10596/3448.

Hernàndez Sampieri, R., Fernández Collado, C., & Baptista Lucio, P. (2010). *Metodología de la investigación.* Mexico: McGraw-Hill.

Hérnandez, L. (2014). *ptolomeo.unam.* Obtenido de http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/3735/Tesis.pdf?sequence=1

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodologia de la Investigación.* Mexico.

Herrera, M. (2015). ANALÍSIS Y DISEÑO DE CLOUD COMPUTING PROPIETARIO PARA APLICACIONES DE E-LEARNING BAJO ESTÁNDARES ISO 27001 Y 27002. *(TRABAJO DE GRADUACIÓN).* UNIVERSIDAD CENTRAL DEL ECUADOR, QUITO-ECUADOR.

Hincapié, L. (2016). *Metodología de gestión de mantenimiento desde una perspectiva de Confiabilidad-Disponibilidad-Mantenibilidad (CDM) para apliación en equipos de Tecnología de la Información (TI).* Universidad Nacional de Colombia, Colombia.

Horna, C. (30 de Septiembre de 2015). *americasistemas*. Obtenido de http://www.americasistemas.com.pe/empresas-locales-no-entienden-cual-es-el-rol-de-la-seguridad-de-la-informacion/

Imbaquingo, D., & Pusdá, M. (2015). EVALUACIÓN DE AMENAZAS Y VULNERABILIDADES DEL MODULO DE GESTIÓN ACADEMICA - SISTEMA INFORMATICO INTEGRADO UNIVERSITARIO DE LA UNIVERSIDAD TECNICA DEL NORTE, APLICANDO ISO 27000. *(Tesis Previo a la Obtención del Titulo de Magister).* Universidad de las Fuerzas Armadas, Sangolquí.

ISO. (s.f.). Obtenido de https://www.pmg-ssi.com/2015/10/controlar-acceso-norma-iso-iec-27001/

Kosutic, D. (2016). *Seguro & Simple: Una guia para la pequeña empresa para la implementación de la ISO 27001 con medios propios.* Zagreb: Advisera Expert Solutions Ltd.

Lara, C. (2015). ESTUDIO DE UNA AUDITORÍA EN SEGURIDAD. *(TRABAJO DE TITULACIÓN).* Universidad de Guayaquil, Guayaquil.

Lara, C. (2015). *repositorio.ug.* Obtenido de http://repositorio.ug.edu.ec/bitstream/redug/6978/1/Tesis%20C%C3%A9sar%20Lara.pdf

Lema, G. (2017). DISEÑO DE LAS BUENAS PRÁCTICAS DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN BASADO EN NORMAS ISO 27001 PARA LA DIRECCIÓN GENERAL DE AVIACIÓN CIVIL. *(Trabajo de Titulación).* Universidad de las Americas, Recuperado de: http://dspace.udla.edu.ec/handle/33000/7650.

Lone, C. (29 de Marzo de 2016). *dnvgl*. Obtenido de https://www.dnvgl.es/news/las-empresas-de-todo-el-mundo-aumentan-la-proteccion-de-sus-datos-60517

Magda, M. (2016). DISEÑO DEL PLAN DE GESTIÓN PARA. *(TRABAJO DE TITULACIÓN).* UNIVERSIDAD DE GUAYAQUIL, Guayaquil.

Mariela, I., & Karim, I. (16 de Febrero de 2014). *s3.amazonaws.* Obtenido de https://s3.amazonaws.com/academia.edu.documents/33095415/METODOS_DE_RECOLECCION_DE_DATOS_PARA_UNA_INVESTIGACION.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1524155782&Signature=oeUQ9y98%2FOzLbTH%2Bz4t8MgRl6zU%3D&response-content-disposition=inline%3B%

Martínez, F. (Segundo Trimestre de 2018). *redseguridad*. Obtenido de http://www.redseguridad.com/revistas/red/081/70/index.html

Medina, J. (2015). Análisis del estado actual de la gestión de la seguridad de la información en la sede principal de Corporinoquia. *Trabajo fin de máster.* Universidad Internacional de La Rioja, Yopai.

Moyano, L., & Suaréz, Y. (13 de Septiembre de 2017). *repository.udistrital.* Obtenido de http://repository.udistrital.edu.co/bitstream/11349/6737/1/MoyanoOrjuelaLuzAdriana2017.pdf

Ochoa, A. (2017). *Sistema web de gestión de seguridad de la información asistida por computadora basada en el estándar ISO 27001 en la Universidad nacional José María Arguedas.* Apurimac: Universidad Nacional José María Arguedas.

Ortega, Y., & Cumbe, F. (2016). Análisis y diseño de un sistema de video asistencia y control de acceso basados en normas ISO 27000 para ETAPA EP. *(Trabajo de graduación).* Escuela de Ingeniería Electronica, Cuenca, Ecuador.

Paillacho, S. (2015). *bibdigital.epn.* Obtenido de http://bibdigital.epn.edu.ec/bitstream/15000/10653/1/CD-6286.pdf

Palacios, D. (2015). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN(SGSI) PARA EL ÁREA DE INFORMÁTICA DE LA COOPERATIVA DEL MAGISTERIO DE TÚQUERRES BAJO LA NORMA ISO 27001:2013. *(Tesis de grado).* UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA, Colombia: Recuperado de: http://hdl.handle.net/10596/3817.

Palella, S., & Martins, F. (2012). *Metodología de la Investigación Cuantitativa.* Caracas: Fedupel.

Pallela Stracuzzi, S., & Martins Pestana, F. (2012). *Metodología de la Investigación Cuantitativa.* Maracay: Fedupel.

Pardo, M. (2015). *Modelo de Gestión de Seguridad de la Información para la Universidad Nacional de Loja basado en la norma ISO/IEC 27001.* Loja: Universidad Nacional de Loja.

Pérez, León, & Díaz, R. y. (2013). Funcionalidades de Sistemas de Planificación de Recursos. *INFORMÁTICA EMPRESARIAL*, 155-166.

Perfán, J., & Caicedo, M. (2014). *repository.unad.* Obtenido de http://repository.unad.edu.co:8080/bitstream/10596/2655/3/76327474.pdf

PricewaterhouseCoopers International Limited. (2017). *pwc*. Obtenido de https://www.pwc.es/es/digital/encuesta-mundial-estado-seguridad-informacion-2017.html

Prieto, E. (2016). DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA EMPRESA AGILITY S.A.S. *INGENIERIA EN TELEMATICA.* UNIVERSIDAD DISTRITAL FRANCISCO JOSE DE CALDAS, Bogota.

Públicas, M. d. (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Madrid: Portal de Administración Electrónica (PAe).

Quero, M. (2010). *Confiabilidad y Coeficiente Alfa de Cronbach.* Maracaibo: Telos.

Ramirez, L., Diaz, S., & Gil, G. (2014). *Sistema de Gestión de Seguridad de la Información para una Institución Financiera en el Perú.* Chimbote: Universidad Nacional Del Santa.

Ramos, R., & Gallegos, E. (14 de Diciembre de 2016). *3ciencias.* Obtenido de https://www.3ciencias.com/wp-content/uploads/2016/12/ART-5.pdf

Salcedo, R. (s.f.). *PLAN DE IMPLEMENTACIÓN DEL SGSI BASADO EN LA NORMA ISO 27001:2013.* Universidad de Cataluya de Oberta, España.

Sandoval, C. (abril de 2014). *repositorio.ucsg.* Obtenido de http://repositorio.ucsg.edu.ec/bitstream/3317/1937/1/T-UCSG-POS-MTEL-16.pdf

Sandoval, J. (2017). *DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACION PARA EL CENTRO DE INFORMATICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD NACIONAL DE PIURA, PERIODO 2015-2018.* Universidad Nacional de Piura, Piura.

SGSI. (s.f.). Obtenido de https://www.pmg-ssi.com/2016/08/iso-27001-como-controlar-el-control-de-acceso/

Solarte, F., Enriquez, E., & Del Carmen, M. (2015). *rte.espol.edu.* Obtenido de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

Suarez, S. (01 de Octubre de 2015). *repository.unad.* Obtenido de http://repository.unad.edu.co:8080/bitstream/10596/3777/1/20904541.pdf

Talavera, V. (2015). *tesis.pucp.* Obtenido de http://tesis.pucp.edu.pe/repositorio/bitstream/handle/123456789/6092/TALAVERA_VASCO_DISE%C3%91O_SISTEMA_GESTION.pdf?sequence=1&isAllowed=y

Tech. (s.f.). Obtenido de https://technologyincontrol2.wordpress.com/2017/01/03/usuarios-privilegiados-como-controlar-su-acceso-al-sistema/

Tola, D. (s.f.). *IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA UNA EMPRESA DE CONSULTORÍA Y AUDITORÍA, APLICANDO LA NORMA ISO/IEC 27001.* Escuela Superior Politecnica del Litoral, Guayaquil.

Universidad Continental. (14 de Julio de 2016). *Repositorio Continental.* Obtenido de http://repositorio.continental.edu.pe/bitstream/continental/2186/1/DO_UC_EG_MT_A0313_20162.pdf

Universidad Naval. (08 de Septiembre de 2016). *Gob.* Obtenido de https://www.gob.mx/cms/uploads/attachment/file/133491/METODOLOGIA_DE_INVESTIGACION.pdf

Vidal, D. M. (2012). *Manual ISO 27001.* Chile.

Vilca, E. (2017). *repositorio.udh.* Obtenido de http://repositorio.udh.edu.pe/bitstream/handle/123456789/809/T_047_43087253_T.pdf?sequence=1&isAllowed=y

Vodia, P. (2015). Metodología de Valuación de Riesgos Como Parte del Sistema de Gestión de Seguridad de la Información (SGSI) Aplicado a un Data Center de Alta Gama. *revista politécnica*.

Zeña, V. (11 de Octubre de 2016). *repositorio.unprg.* Obtenido de http://repositorio.unprg.edu.pe/bitstream/handle/UNPRG/166/BC-TES-3899.pdf?sequence=1&isAllowed=y

ANEXO

ANEXO N.° 1. Matriz de Consistencia

PLANTEAMIENTO DEL PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES E INDICADORES	MUESTRA	DISEÑO
Pregunta General ¿En qué medida el uso de la ISO 27001 influye en la seguridad de información en los sistemas ERP de la empresa ICO, año 2021?	**Objetivo General** Determinar en qué medida la ISO 27001 influye en la seguridad de la información, en los sistemas ERP de la empresa ICO, año 2021	**Hipótesis General** El uso de la ISO 27001 permite mejorar la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021.	**Variable 1** ISO 27001	**Población** La población presente en este proyecto de investigación se ve conformado por los 18 módulos que se tiene por cada sistema de recursos empresariales (ERP), de los cuales se seleccionará los 2 únicos sistemas ERP que posee la empresa ICO FOOD SERVICE **Muestra:**	**Método:** Experimental **Nivel Investigación:** Experimental **Diseño:**

Preguntas Específicas ¿En qué medida el uso de la ISO 27001 influye en la confidencialidad de la seguridad de información en los sistemas ERP de la empresa ICO, año 2021? ¿En qué medida el uso de la ISO 27001 influye en la integridad de la seguridad de información en los sistemas ERP de la empresa ICO, año 2021? ¿En qué medida el uso de la ISO 27001 influye en la disponibilidad de la seguridad de información en los sistemas ERP de la empresa ICO, año 2021? ¿En qué medida el uso de la ISO 27001 influye en la prevención de riesgos en la seguridad de información de los sistemas ERP de la empresa ICO, año 2021?	**Objetivo Específicos** Determinar en qué medida la ISO 27001 influye en la confidencialidad de la información, en los sistemas ERP de la empresa ICO, año 2021 Determinar en qué medida la ISO 27001 influye en la Integridad de la información, en los sistemas ERP de la empresa ICO, año 2021 Determinar en qué medida la ISO 27001 influye en la disponibilidad de la información, en los sistemas ERP de la empresa ICO, año 2021 Determinar en qué medida la ISO 27001 influye en la prevención de riesgos en la seguridad de la información, en los sistemas ERP de la empresa ICO, año 2021	**Hipótesis Específicas** La aplicación de la iso 27001 permite mejorar la confidencialidad de la información en los sistemas ERP de la empresa ICO, año 2021 La aplicación de la ISO 27001 permite mejorar la integridad de la información en los sistemas ERP de la empresa ICO, año 2021. La aplicación de la ISO 27001 permite mejorar la disponibilidad de la información en los sistemas ERP de la empresa ICO, año 2021. La aplicación de la ISO 27001 permite mejorar la prevención de los riesgos en la seguridad de la información en los sistemas ERP de la empresa ICO, año 2021.	**Variable 2** Seguridad de la Información	Debido a que en el presente trabajo de investigación se establece que la población será evaluada en su totalidad, ya que se cuenta con solo 18 módulos, 9 módulos por cada sistema de recursos empresariales se usó el método censal donde se estable que la muestra posee la misma cantidad que la población.	Pre - Experimental El diseño se diagrama M_1 Donde: G_1 = Grupo experimen X = Se le aplica el estím O_1 = Observación 1(Po G_2 = Grupo de control − = No se le aplica el O_2 = Observación 2 (P

Figura 24 Matriz de consistencia

Fuente: Elaboración propia

ANEXO N.° 2. Matriz de Operacionalización de variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES
Seguridad de la Información	La seguridad de la información por defecto conlleva métodos cautelosos con el propósito de custodiar y defender la información bajos los parámetros de la Confidencialidad, integridad y disponibilidad. La información se encuentra en diversos medios, en tal caso las empresas u organizaciones deberán tener metodologías las cuales puedan asegurar todos los activos, registros y tener una infraestructura capaz de proteger la información. (Solarte, Enriquez, & Del Carmen, 2015)	**Integridad**	- Nivel a accesos privilegiados - Número de usuarios inactivos - Numero de medidas incluidas en las base de datos y aplicaciones para detectar discrepancias en los datos.
		Confidencialidad	- Nivel de visibilidad de las acciones realizadas - Numero de validaciones del usuario - Nivel de cifrado de la información
		Disponibilidad	- Rango de tiempo disponible de la información - Nivel de fiabilidad de la información
		Riesgos	- Nivel de seguridad de cableado - Nivel de servicio de suministros - Nivel de control de ingreso físico - Nivel de protección contra amenazas externas y ambientales

Figura 25 Matriz de Operacionalización

Fuente: Elaboración propia

ANEXO N.° 3. Instrumentos de recolección de datos

Cuestionario de la aplicación de la iso 27001 para la mejora de la seguridad de la información	5	4	3	2	1
1. ¿Qué cantidad o proporción de usuarios no tienen perfiles asignados en el sistema?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
2. ¿Qué cantidad de usuarios poseen acceso privilegiado a la documentación privada de los sistemas ERP la cual pueda impactar negativamente en la empresa?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
3. ¿Cuál es el grado de Vulnerabilidad que están expuestos los datos, por no dar de baja a los usuarios en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo
4, ¿Cuál es el grado de confianza de la integridad de le información para evitar la discrepancia de datos?	Muy Alta	Alta	Media	Bajo	Muy Bajo
5, ¿Cuál es el grado de visibilidad de las acciones de los usuarios dentro de los módulos en los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo

6. ¿Cuál es el grado de confidencialidad ante la petición de los usuarios, para acceder a la información que pueda generar un impacto negativo en la empresa?	**Muy Alta**	**Alta**	**Media**	**Bajo**	**Muy Bajo**
7. ¿Cuál es la confianza que poseen los módulos de los sistemas erp, para que los usuarios accedan a su cuentas personales	**Muy Alta**	**Alta**	**Media**	**Bajo**	**Muy Bajo**
8. ¿Cuál es el grado de protección de la información, que pueda generar riesgo y perdidas dentro de los sistemas ERP?	**Muy Alta**	**Alta**	**Media**	**Bajo**	**Muy Bajo**
9¿Cuál es el rango de tiempo que la información está disponible para los usuarios?	**7Dx24h**	**7Dx20h**	**7Dx15h**	**7Dx10h**	**7Dx5h**
10. ¿Cuál es el grado de certeza de la información en los módulos de los sistemas ERP?	**Muy Alta**	**Alta**	**Media**	**Bajo**	**Muy Bajo**
11. ¿Cuál es el grado de seguridad con respecto a la conectividad física de los cables de telecomunicación en los sistemas ERP?	**Muy Alta**	**Alta**	**Media**	**Bajo**	**Muy Bajo**

12. ¿Qué impacto tendría el fallo de los suministros de energía sobre los módulos de los sistemas ERP energizados?	**Muy Alta**	**Alta**	**Media**	**Bajo**	**Muy Bajo**
13. ¿Cuál es el grado seguridad que existe sobre los controles de acceso al área de los sistemas ERP?	**Muy Alta**	**Alta**	**Media**	**Bajo**	**Muy Bajo**
14. ¿Cuál es el grado de protección que existe en los módulos de los sistemas ERP ante los ataques externos?	**Muy Alta**	**Alta**	**Media**	**Bajo**	**Muy Bajo**

Figura 26 Instrumento de recolección de datos

Anexo N. °4. Confiabilidad de Instrumento de recolección de datos

Sujeto	ITEM 1	ITEM 2	ITEM 3	ITEM 4	ITEM 5	ITEM 6	ITEM 7	ITEM 8	ITEM 9	ITEM 10	ITEM 11	
	Niveles de acceso privilegiado		Número de usuarios inactivos	Numero de medidas incluidas en las base de datos y aplicaciones para detectar discrepancias en los datos.	Nivel de visibilidad de las acciones realizadas		Numero de validaciones del usuario	Nivel de cifrado de la información	Rango de tiempo disponible de la información	Nivel de fiabilidad de la información	Nivel de seguridad de cableado	N s s
1	3	2	5	3	3	2	3	2	5	3	3	
2	2	1	3	2	2	1	3	1	4	3	3	
3	3	4	5	2	3	3	3	1	5	3	3	
4	3	2	5	3	3	3	2	2	4	4	3	
5	3	4	4	2	3	2	2	2	4	3	3	
6	4	3	4	3	3	4	3	3	5	4	3	
7	4	4	3	2	1	3	3	2	4	3	3	
8	3	2	4	2	3	2	3	3	4	4	3	
9	4	3	5	4	3	3	4	3	5	5	3	
10	2	2	4	2	2	3	4	3	4	3	2	
11	3	2	4	3	2	2	3	3	5	4	2	
12	2	3	3	1	2	1	3	2	4	3	2	
13	3	2	3	2	2	3	3	2	4	3	2	
14	4	3	4	3	3	3	3	3	5	4	2	
15	3	1	4	3	2	2	3	3	4	4	2	
16	2	2	4	2	2	2	2	2	5	3	2	
17	4	4	5	3	3	2	3	4	4	3	2	
18	3	4	5	3	4	4	4	3	5	4	2	

Varianza Poblacional	0,497	1,000	0,543	0,472	0,469	0,694	0,333	0,580	0,247	0,361	0,250
Sumatoria de la Varianza Poblacional	6,364										

k	14	Alfa de Cronbach	0,81
Parte 1	1,08		
Parte 2	0,75		

Figura 27 Confiabilidad del instrumento

Fuente: Elaboración propia

ANEXO N.° 5. Validez del instrumento de recolección de datos

UNIVERSIDAD PRIVADA DEL NORTE

INSTRUMENTO DE OPINION DE EXPERTOS

DATOS GENERALES:

Apellidos y Nombres del Informante	Cargo e Institución donde labora	Nombre del Instrumento	Autor(a) (es) del Instrumento
Flores Masías, Edward José	UPN	Cuestionario	Luis Felipe Herrera Arriola Alexander Henry Ticona Herrera
Título de Estudio:			

ASPECTOS DE VALIDACION:

Coloque el porcentaje, según intervalo. .

INDICADORES	CRITERIOS	DEFICIENTE 00-20%				REGULAR 21-40%				BUENA 41-60%				MUY BUENA 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Está formulado con lenguaje apropiado.															X					
OBJETIVIDAD	Está expresado en conductas o actividades, observables en una organización.															X					
ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.															X					
ORGANIZACIÓN	Existe una organización lógica coherente.															X					
SUFICIENCIA	Comprende los aspectos (indicadores, sub escalas, dimensiones) en cantidad y calidad.															X					
INTENCIONALIDAD	Adecuado para valorar la influencia de la VI en la VD o la relación entre ambas, con determinados sujetos y contexto.															X					
CONSISTENCIA	Basado en aspectos teórico - científico.															X					
COHERENCIA	Entre los índices, indicadores y las dimensiones.															X					
METODOLOGIA	Las estrategias responde al propósito del diagnostico															X					
	PROMEDIO																				

OPINIÒN DE APLICABILIDAD:

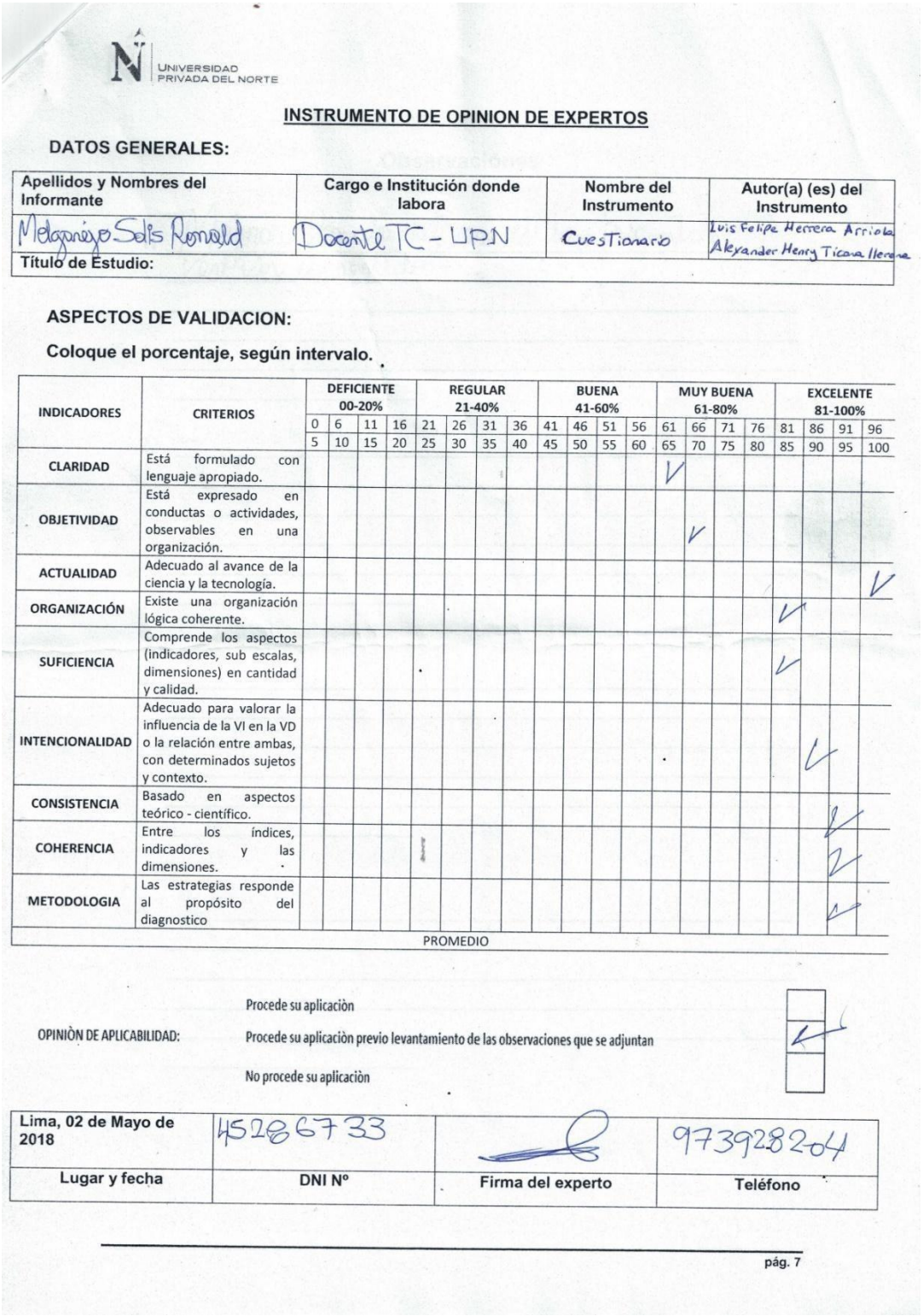
- Procede su aplicaciòn
- Procede su aplicaciòn previo levantamiento de las observaciones que se adjuntan — X
- No procede su aplicaciòn

Lima, 02 de Mayo de 2018	09536323		997922254
Lugar y fecha	DNI N°	Firma del experto	Teléfono

pág. 7

*Figura SEQ Figura * ARABIC 28* Aprobación número 1 del instrumento de

Fuente: Elaboración propia



UNIVERSIDAD PRIVADA DEL NORTE

INSTRUMENTO DE OPINION DE EXPERTOS

DATOS GENERALES:

Apellidos y Nombres del Informante	Cargo e Institución donde labora	Nombre del Instrumento	Autor(a) (es) del Instrumento
Melgarejo Solis Ronald	Docente TC - UPN	Cuestionario	Luis Felipe Herrera Arriola Alexander Henry Ticona Herrera

Título de Estudio:

ASPECTOS DE VALIDACION:

Coloque el porcentaje, según intervalo.

INDICADORES	CRITERIOS	DEFICIENTE 00-20%				REGULAR 21-40%				BUENA 41-60%				MUY BUENA 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Está formulado con lenguaje apropiado.													✓							
OBJETIVIDAD	Está expresado en conductas o actividades, observables en una organización.														✓						
ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.																				✓
ORGANIZACIÓN	Existe una organización lógica coherente.																	✓			
SUFICIENCIA	Comprende los aspectos (indicadores, sub escalas, dimensiones) en cantidad y calidad.																	✓			
INTENCIONALIDAD	Adecuado para valorar la influencia de la VI en la VD o la relación entre ambas, con determinados sujetos y contexto.																		✓		
CONSISTENCIA	Basado en aspectos teórico - científico.																			✓	
COHERENCIA	Entre los índices, indicadores y las dimensiones.																			✓	
METODOLOGIA	Las estrategias responde al propósito del diagnostico																			✓	
PROMEDIO																					

OPINIÒN DE APLICABILIDAD:

- Procede su aplicaciòn
- Procede su aplicaciòn previo levantamiento de las observaciones que se adjuntan ✓
- No procede su aplicaciòn

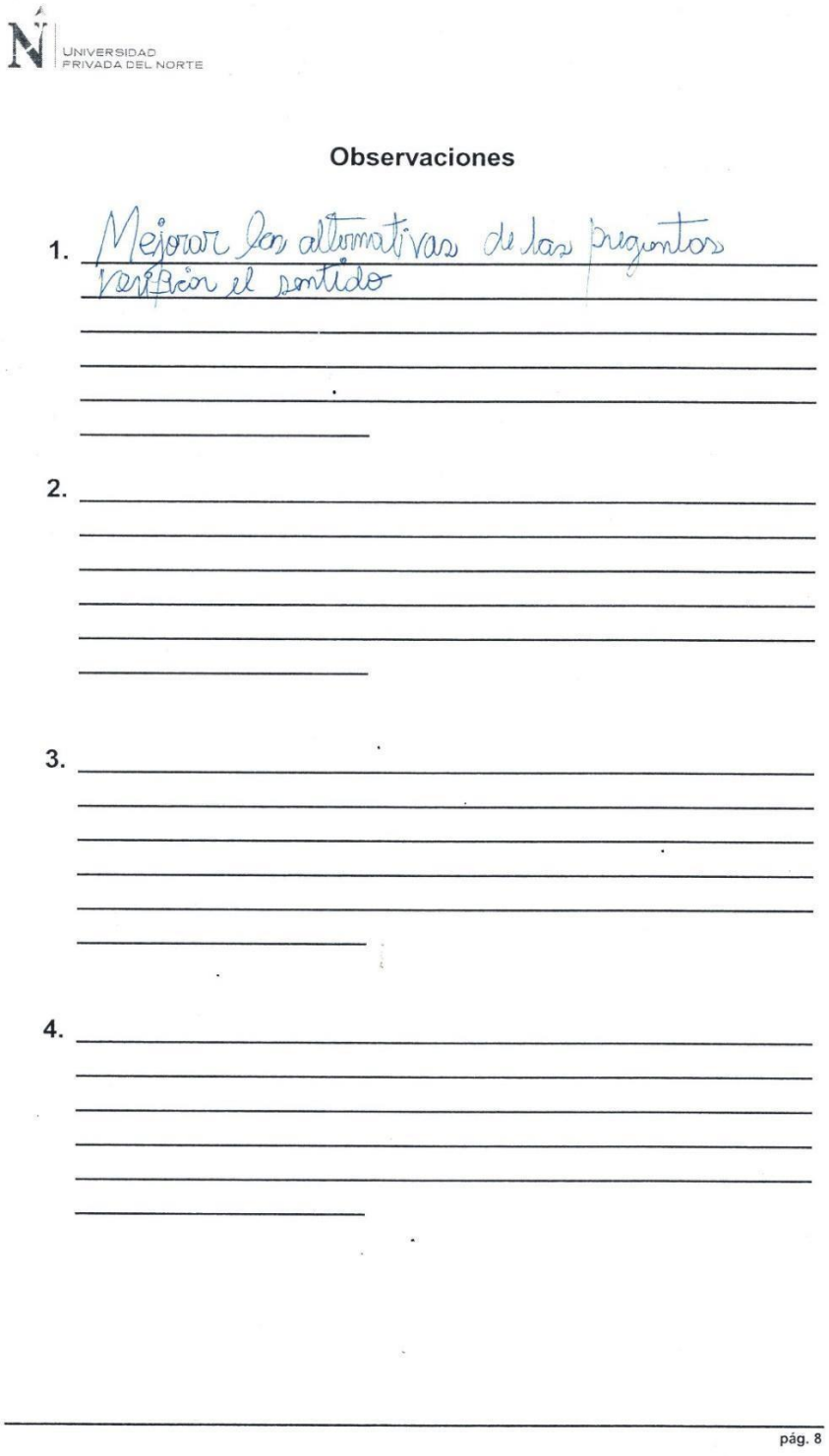
Lima, 02 de Mayo de 2018	45286733		973928204
Lugar y fecha	DNI Nº	Firma del experto	Teléfono

pág. 7

*Figura SEQ Figura * ARABIC 30* Aprobación número 2 del instrumento de validez del datos

Fuente: Elaboración propia

Fuente: Elaboración propia



UNIVERSIDAD PRIVADA DEL NORTE

Observaciones

1. Mejorar las alternativas de las preguntas verificar el sentido

2.

3.

4.

pág. 8

*Figura SEQ Figura * ARABIC 31* Observación número 2 de la validez del instrumento de recolección de datos

Fuente: Elaboración propia

UNIVERSIDAD PRIVADA DEL NORTE

INSTRUMENTO DE OPINION DE EXPERTOS

DATOS GENERALES:

Apellidos y Nombres del Informante	Cargo e institución donde labora	Nombre del Instrumento	Autor(a) (es) del Instrumento
Romero Quiroz Howard Denis	Cliente operativo	Cuestionario	Luis Felipe Herrera Arriola Alexander Henry Tena Herrera
Título de Estudio: Ing. Sistemas			

ASPECTOS DE VALIDACION:

Coloque el porcentaje, según intervalo.

INDICADORES	CRITERIOS	DEFICIENTE 00-20%				REGULAR 21-40%				BUENA 41-60%				MUY BUENA 61-80%				EXCELENTE 81-100%			
		0	6	11	16	21	26	31	36	41	46	51	56	61	66	71	76	81	86	91	96
		5	10	15	20	25	30	35	40	45	50	55	60	65	70	75	80	85	90	95	100
CLARIDAD	Está formulado con lenguaje apropiado.			✓																	
OBJETIVIDAD	Está expresado en conductas o actividades, observables en una organización.										✓										
ACTUALIDAD	Adecuado al avance de la ciencia y la tecnología.										✓										
ORGANIZACIÓN	Existe una organización lógica coherente.										✓										
SUFICIENCIA	Comprende los aspectos (indicadores, sub escalas, dimensiones) en cantidad y calidad.									✓											
INTENCIONALIDAD	Adecuado para valorar la influencia de la VI en la VD o la relación entre ambas, con determinados sujetos y contexto.														✓						
CONSISTENCIA	Basado en aspectos teórico - científico.												✓								
COHERENCIA	Entre los índices, indicadores y las dimensiones.								✓												
METODOLOGIA	Las estrategias responde al propósito del diagnostico														✓						
PROMEDIO																					

OPINIÒN DE APLICABILIDAD:

- Procede su aplicaciòn
- Procede su aplicaciòn previo levantamiento de las observaciones que se adjuntan ✓
- No procede su aplicaciòn

Lima, 02 de Mayo de 2018	42819556		5347432
Lugar y fecha	DNI Nº	Firma del experto	Teléfono

pág. 7

*Figura SEQ Figura * ARABIC 32* Aprobación número 3 del instrumento de

Fuente: Elaboración propia

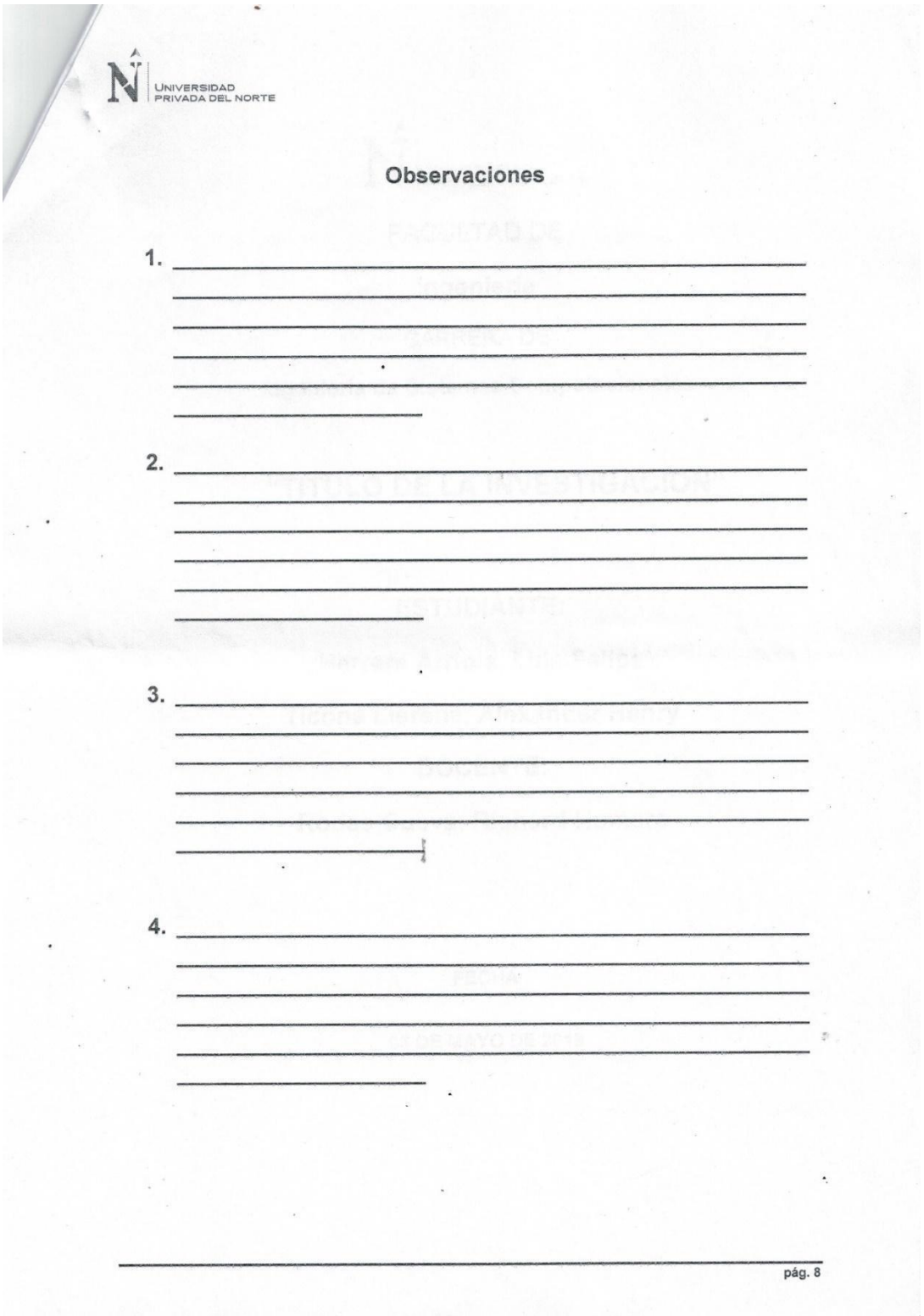


*Figura SEQ Figura * ARABIC 33 Observación número 3 de la validez del instrumento de recolección de datos*

Fuente: Elaboración propia

ANEXO N.° 6. Base de Datos

	Pre01	Pre02	Pre03	Pre04	Pre05	Pre06	Pre07	Pre08	Pre09	Pre10	Pre11	Pre12	Pre13	Pre14
1	3	2	5	3	3	2	3	2	5	3	3	5	2	3
2	2	1	3	2	2	1	3	1	4	3	3	5	2	2
3	3	4	5	2	3	3	3	1	5	3	3	5	2	3
4	3	2	5	3	3	3	2	2	4	4	3	5	2	2
5	3	4	4	2	3	2	2	2	4	3	3	4	2	1
6	4	3	4	3	3	4	3	3	5	4	3	5	2	3
7	4	4	3	2	1	3	3	2	4	3	3	5	2	2
8	3	2	4	2	3	2	3	3	4	4	3	4	2	3
9	4	3	5	4	3	3	4	3	5	5	3	5	2	4
10	2	2	4	2	2	3	4	3	4	3	2	5	3	3
11	3	2	4	3	2	2	3	3	5	4	2	4	3	3
12	2	3	3	1	2	1	3	2	4	3	2	4	3	3
13	3	2	3	2	2	3	3	2	4	3	2	5	3	2
14	4	3	4	3	3	3	3	3	5	4	2	5	3	3
15	3	1	4	3	2	2	3	3	4	4	2	4	3	3
16	2	2	4	2	2	2	2	2	5	3	2	5	3	2
17	4	4	5	3	3	2	3	4	4	3	2	4	3	3
18	3	4	5	3	4	4	4	3	5	4	2	5	3	3

*Figura SEQ Figura * ARABIC 34 Encuesta del Pre-test para las variables de ISO 27001 y Seguridad de*

Fuente: Elaboración propia

	Post01	Post02	Post03	Post04	Post05	Post06	Post07	Post08	Post09	Post10	Post11	Post12	Post13	Post14
1	1	3	3	4	4	3	5	4	3	4	4	2	3	4
2	2	3	2	3	4	3	3	3	3	3	4	2	3	4
3	1	2	2	2	4	3	3	3	3	4	4	2	3	3
4	2	4	3	4	4	4	3	4	5	4	4	3	3	3
5	2	2	3	4	4	3	4	3	4	4	4	3	3	5
6	1	3	3	5	5	5	4	5	4	4	4	2	3	5
7	2	1	2	4	5	3	4	5	5	3	4	2	3	5
8	1	5	2	5	5	4	3	4	5	4	4	3	3	5
9	1	3	2	3	4	3	4	3	3	4	4	2	3	3
10	1	2	2	3	4	3	3	3	5	3	4	2	4	3
11	1	2	2	4	5	4	3	3	3	4	4	3	4	3
12	1	2	2	4	4	4	5	4	4	4	4	3	4	4
13	1	2	3	3	5	4	3	5	3	4	4	2	4	5
14	1	3	3	4	4	4	4	3	3	4	4	3	4	4
15	1	2	2	3	4	3	3	4	3	3	4	2	4	3
16	2	1	2	4	5	4	3	4	5	4	4	3	4	3
17	1	2	2	5	5	5	4	5	4	3	4	2	4	5
18	1	5	3	4	4	5	4	4	5	4	4	2	4	4

*Figura SEQ Figura * ARABIC 35 Encuesta del Post-test para las variables de ISO 27001 y Seguridad de la*

Fuente: ***Elaboración propia***

ANEXO N.° 7. Formato de trabajo de campo

UNIVERSIDAD PRIVADA DEL NORTE

CUESTIONARIO PARA LA VARIABLE "SEGURIDAD DE LA INFORMACIÓN – ICO FOOD SERVICE"

Instrucciones: El cuestionario que le presentamos conlleva una serie de preguntas sobre la seguridad de la información en los sistemas ERP. Para cada pregunta indíquenos de la escala del 1 al 5 marcando con un círculo las alternativas, siendo 1 la representación que usted está totalmente en desacuerdo en que la seguridad de la información en los sistemas erp tenga esta cualidad y 5 la representación de que usted está totalmente de acuerdo. También puede marcar las alternativas alrededor de la opción del medio en caso de que representen la respuesta correcta, la finalidad del cuestionario es que usted pueda indicar con precisión la respuesta correcta.

Cuestionario de la aplicación de la iso 27001 para la mejora de la seguridad de la información	5	4	3	2	1
1. ¿Qué cantidad o proporción de usuarios no tienen perfiles asignados en el sistema?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
2. ¿Qué cantidad de usuarios poseen acceso privilegiado a la documentación privada de los sistemas ERP la cual pueda impactar negativamente en la empresa?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
3. ¿Cuál es el grado de Vulnerabilidad que están expuestos los datos, por no dar de baja a los usuarios en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo
4, ¿Cuál es el grado de confianza de la integridad de le información para evitar la discrepancia de datos?	Muy Alta	Alta	Media	Bajo	Muy Bajo
5, ¿Cuál es el grado de visibilidad de las acciones de los usuarios en los módulos dentro de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
6. ¿Cuál es el grado de confidencialidad ante la petición de los usuarios, para acceder a la información que pueda generar un impacto negativo en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo

pág. 1

*Figura SEQ Figura * ARABIC 36* Primera Evaluación Pre Test parte 1

Fuente: Elaboración propia

UNIVERSIDAD PRIVADA DEL NORTE

7. ¿Cuál es la confianza que poseen los módulos de los sistemas erp, para que los usuarios accedan a su cuentas personales	Muy Alta	Alta	Media	Bajo	Muy Bajo
8. ¿Cuál es el grado de protección de la información, que pueda generar riesgo y perdidas dentro de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
9¿Cuál es el rango de tiempo que la información está disponible para los usuarios?	7Dx24h	7Dx20h	7Dx15h	7Dx10h	7Dx5h
10. ¿Cuál es el grado de certeza de la información en los módulos de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
11. ¿Cuál es el grado de seguridad con respecto a la conectividad física de los cables de telecomunicación en los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
12. ¿Qué impacto tendría el fallo de los suministros de energía sobre los módulos de los sistemas ERP energizados?	Muy Alta	Alta	Media	Bajo	Muy Bajo
13. ¿Cuál es el grado seguridad que existe sobre los controles de acceso al área de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
14. ¿Cuál es el grado de protección que existe en los módulos de los sistemas ERP ante los ataques externos?	Muy Alta	Alta	Media	Bajo	Muy Bajo

pág. 2

*Figura SEQ Figura * ARABIC 37* Primera Evaluación Pre Test parte 2

Fuente: Elaboración propia

UNIVERSIDAD PRIVADA DEL NORTE

CUESTIONARIO PARA LA VARIABLE "SEGURIDAD DE LA INFORMACIÓN – ICO FOOD SERVICE"

Instrucciones: El cuestionario que le presentamos conlleva una serie de preguntas sobre la seguridad de la información en los sistemas ERP. Para cada pregunta indíquenos de la escala del 1 al 5 marcando con un círculo las alternativas, siendo 1 la representación que usted está totalmente en desacuerdo en que la seguridad de la información en los sistemas erp tenga esta cualidad y 5 la representación de que usted está totalmente de acuerdo. También puede marcar las alternativas alrededor de la opción del medio en caso de que representen la respuesta correcta, la finalidad del cuestionario es que usted pueda indicar con precisión la respuesta correcta.

Cuestionario de la aplicación de la iso 27001 para la mejora de la seguridad de la información	5	4	3	2	1
1. ¿Qué cantidad o proporción de usuarios no tienen perfiles asignados en el sistema?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
2. ¿Qué cantidad de usuarios poseen acceso privilegiado a la documentación privada de los sistemas ERP la cual pueda impactar negativamente en la empresa?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
3. ¿Cuál es el grado de Vulnerabilidad que están expuestos los datos, por no dar de baja a los usuarios en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo
4, ¿Cuál es el grado de confianza de la integridad de le información para evitar la discrepancia de datos?	Muy Alta	Alta	Media	Bajo	Muy Bajo
5, ¿Cuál es el grado de visibilidad de las acciones de los usuarios en los módulos dentro de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
6. ¿Cuál es el grado de confidencialidad ante la petición de los usuarios, para acceder a la información que pueda generar un impacto negativo en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo

pág. 1

*Figura SEQ Figura * ARABIC 38* Segunda Evaluación Pre Test
Fuente: Elaboración propia

UNIVERSIDAD PRIVADA DEL NORTE

7. ¿Cuál es la confianza que poseen los módulos de los sistemas erp, para que los usuarios accedan a su cuentas personales	Muy Alta	Alta	Media	Bajo	Muy Bajo
8. ¿Cuál es el grado de protección de la información, que pueda generar riesgo y perdidas dentro de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
9¿Cuál es el rango de tiempo que la información está disponible para los usuarios?	7Dx24h	7Dx20h	7Dx15h	7Dx10h	7Dx5h
10. ¿Cuál es el grado de certeza de la información en los módulos de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
11. ¿Cuál es el grado de seguridad con respecto a la conectividad física de los cables de telecomunicación en los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
12. ¿Qué impacto tendría el fallo de los suministros de energía sobre los módulos de los sistemas ERP energizados?	Muy Alta	Alta	Media	Bajo	Muy Bajo
13. ¿Cuál es el grado seguridad que existe sobre los controles de acceso al área de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
14. ¿Cuál es el grado de protección que existe en los módulos de los sistemas ERP ante los ataques externos?	Muy Alta	Alta	Media	Bajo	Muy Bajo

*Figura SEQ Figura * ARABIC 39* Segunda Evaluación Pre Test

Fuente: Elaboración propia

UNIVERSIDAD PRIVADA DEL NORTE

CUESTIONARIO PARA LA VARIABLE "SEGURIDAD DE LA INFORMACIÓN – ICO FOOD SERVICE"

Instrucciones: El cuestionario que le presentamos conlleva una serie de preguntas sobre la seguridad de la información en los sistemas ERP. Para cada pregunta indíquenos de la escala del 1 al 5 marcando con un círculo las alternativas, siendo 1 la representación que usted está totalmente en desacuerdo en que la seguridad de la información en los sistemas erp tenga esta cualidad y 5 la representación de que usted está totalmente de acuerdo. También puede marcar las alternativas alrededor de la opción del medio en caso de que representen la respuesta correcta, la finalidad del cuestionario es que usted pueda indicar con precisión la respuesta correcta.

Cuestionario de la aplicación de la iso 27001 para la mejora de la seguridad de la información	5	4	3	2	1
1. ¿Qué cantidad o proporción de usuarios no tienen perfiles asignados en el sistema?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
2. ¿Qué cantidad de usuarios poseen acceso privilegiado a la documentación privada de los sistemas ERP la cual pueda impactar negativamente en la empresa?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
3. ¿Cuál es el grado de Vulnerabilidad que están expuestos los datos, por no dar de baja a los usuarios en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo
4, ¿Cuál es el grado de confianza de la integridad de le información para evitar la discrepancia de datos?	Muy Alta	Alta	Media	Bajo	Muy Bajo
5, ¿Cuál es el grado de visibilidad de las acciones de los usuarios en los módulos dentro de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
6. ¿Cuál es el grado de confidencialidad ante la petición de los usuarios, para acceder a la información que pueda generar un impacto negativo en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo

pág. 1

*Figura SEQ Figura * ARABIC 40* Primera Evaluación Post Test parte 1
Fuente: Elaboración propia

UNIVERSIDAD PRIVADA DEL NORTE

7. ¿Cuál es la confianza que poseen los módulos de los sistemas erp, para que los usuarios accedan a su cuentas personales	Muy Alta	Alta	Media	Bajo	Muy Bajo
8. ¿Cuál es el grado de protección de la información, que pueda generar riesgo y perdidas dentro de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
9¿Cuál es el rango de tiempo que la información está disponible para los usuarios?	7Dx24h	7Dx20h	7Dx15h	7Dx10h	7Dx5h
10. ¿Cuál es el grado de certeza de la información en los módulos de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
11. ¿Cuál es el grado de seguridad con respecto a la conectividad física de los cables de telecomunicación en los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
12. ¿Qué impacto tendría el fallo de los suministros de energía sobre los módulos de los sistemas ERP energizados?	Muy Alta	Alta	Media	Bajo	Muy Bajo
13. ¿Cuál es el grado seguridad que existe sobre los controles de acceso al área de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
14. ¿Cuál es el grado de protección que existe en los módulos de los sistemas ERP ante los ataques externos?	Muy Alta	Alta	Media	Bajo	Muy Bajo

pág. 2

*Figura SEQ Figura * ARABIC 41* Primera Evaluación Post Test parte
Fuente: Elaboración propia

UNIVERSIDAD PRIVADA DEL NORTE

CUESTIONARIO PARA LA VARIABLE "SEGURIDAD DE LA INFORMACIÓN – ICO FOOD SERVICE"

Instrucciones: El cuestionario que le presentamos conlleva una serie de preguntas sobre la seguridad de la información en los sistemas ERP. Para cada pregunta indíquenos de la escala del 1 al 5 marcando con un círculo las alternativas, siendo 1 la representación que usted está totalmente en desacuerdo en que la seguridad de la información en los sistemas erp tenga esta cualidad y 5 la representación de que usted está totalmente de acuerdo. También puede marcar las alternativas alrededor de la opción del medio en caso de que representen la respuesta correcta, la finalidad del cuestionario es que usted pueda indicar con precisión la respuesta correcta.

Cuestionario de la aplicación de la iso 27001 para la mejora de la seguridad de la información	5	4	3	2	1
1. ¿Qué cantidad o proporción de usuarios no tienen perfiles asignados en el sistema?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
2. ¿Qué cantidad de usuarios poseen acceso privilegiado a la documentación privada de los sistemas ERP la cual pueda impactar negativamente en la empresa?	50 a 41	31 a 40	21 a 30	11 a 20	1 a 10
3. ¿Cuál es el grado de Vulnerabilidad que están expuestos los datos, por no dar de baja a los usuarios en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo
4, ¿Cuál es el grado de confianza de la integridad de le información para evitar la discrepancia de datos?	Muy Alta	Alta	Media	Bajo	Muy Bajo
5, ¿Cuál es el grado de visibilidad de las acciones de los usuarios en los módulos dentro de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
6. ¿Cuál es el grado de confidencialidad ante la petición de los usuarios, para acceder a la información que pueda generar un impacto negativo en la empresa?	Muy Alta	Alta	Media	Bajo	Muy Bajo

pág. 1

*Figura SEQ Figura * ARABIC 42* Segunda Evaluación Post Test

Fuente: Elaboración propia

UNIVERSIDAD PRIVADA DEL NORTE

7. ¿Cuál es la confianza que poseen los módulos de los sistemas erp, para que los usuarios accedan a su cuentas personales	Muy Alta	Alta	Media	Bajo	Muy Bajo
8. ¿Cuál es el grado de protección de la información, que pueda generar riesgo y perdidas dentro de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
9¿Cuál es el rango de tiempo que la información está disponible para los usuarios?	7Dx24h	7Dx20h	7Dx15h	7Dx10h	7Dx5h
10. ¿Cuál es el grado de certeza de la información en los módulos de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
11. ¿Cuál es el grado de seguridad con respecto a la conectividad física de los cables de telecomunicación en los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
12. ¿Qué impacto tendría el fallo de los suministros de energía sobre los módulos de los sistemas ERP energizados?	Muy Alta	Alta	Media	Bajo	Muy Bajo
13. ¿Cuál es el grado seguridad que existe sobre los controles de acceso al área de los sistemas ERP?	Muy Alta	Alta	Media	Bajo	Muy Bajo
14. ¿Cuál es el grado de protección que existe en los módulos de los sistemas ERP ante los ataques externos?	Muy Alta	Alta	Media	Bajo	Muy Bajo

pág. 2

*Figura SEQ Figura * ARABIC 43* Segunda Evaluación Post Test parte

Fuente: Elaboración propia

Anexo 10 Productos

Documentación Técnica

Se admite mediante la disposición Ministerial N° 246-2007-PCM se autorizó el poder usar la norma técnica peruana o ISO/IEC 17799:2007 EDI, en el cual su uso consiste en una serie de buenas prácticas con el fin de tener una gestión de la seguridad de la información. 2ª. Edición en lo que respecta a todos los organismo del sistema Nacional de Informática; a través de la certeza Ministerial N° 197-2011- PCM, en el que se menciona que solo cierta entidades de Administración públicas están autorizadas para implementar un plan de seguridad de la información que se encuentra especificado en la norma técnica peruana antes mencionada; mediante la siguiente resolución Ministerial N° 129-2012-PCM estipula un nuevo cronograma y la agregación de un nuevo rol oficial el cual contiene procesos para la implementación de la norma técnica peruana "NTP-ISO/IEC 27001:2008", Así mismo la norma técnica peruana ISO/IEC 27001:2008 que conlleva técnicas para la seguridad y un sistema de gestión de seguridad de la información, aceptada por medio de la resolución N° 42-2008/INDECOPI-CNB, por la comisión de Normalización y de fiscalización de Barreras Comerciales No Arancelarias del Instituto Nacional de Defensa de la Competencia y de Protección de la Propiedad Intelectual(INDECOPI) fue reemplazada por una versión llamada ISO/IEC 27001:2014 y a su vez también mejoro sus técnicas de seguridad y su sistema de gestión de la seguridad de la información 2ª Edición aprobada por Resolución N° 129-2014/DNB-INDECOPI; De acuerdo a lo descrito en el número 4.8 articulo 4 y articulo 49 del reglamento de Organización y Funciones de la presidencia del consejo de Ministros, consentido por el Decreto Supremo N° 063-2007-PCM, la Presidencia del Consejo de Ministros se comporta como ente rector del Sistema Nacional de Informática mediante el cual la Oficina Nacional de Gobierno Electrónico e Informático (ONGEI, se encarga de la implementación correcta de la Política Nacional de Gobierno Electrónico e Informático)

CAPÍTULO I PLANIFICACIÓN DE TRABAJO

Para el correcto desarrollo del trabajo se definirá todas las tareas que se deben realizar para llevar a cabo la correcta implementación de la ISO 27001:2013.

Capítulo 2: Contexto Organizacional

DEFINICIÓN DE LA ORGANIZACIÓN

En este punto buscamos con la cooperación de la organización a definir correctamente en que consiste la empresa, la presentación de cómo está estructurada la empresa, así como su infraestructura que se encuentra directamente relacionado con los sistemas de recursos empresariales (ERP).

DEFINICIÓN DE LOS DOMINIOS DE CONTROL DE LA ISO 27001:2013

Usando la ISO 27002:2013 para la definición de los dominios y controles y la creación del cuestionario realizado basado en los controles de la ISO 27001:2013 se pudo analizar los sistemas de recursos empresariales en busca del cumplimiento de la integridad, confidencialidad, disponibilidad y riesgos y poder cuantificar los datos obtenidos.

Capítulo 3 Gestión de Riesgos

DEFINICIÓN DE LA METODOLOGÍA DE RIESGOS

Para poder mejorar el sistema de gestión de la seguridad de la información propuesto, se hará uso de la metodología de magerit, la cual permite establecer conciencia en la organización con los riesgos que trae el uso de la tecnología y permite planificar el tratamiento que se debe implementar para mantener los riesgos bajo control.

INVENTARIO DE ACTIVOS

Para poder definir los riesgos primero se debe establecer los activos que estén relacionados los sistemas de recursos empresariales, que es información que es susceptible a ser atacados ya sea deliberado o accidental y que repercute en la organización causando un efecto negativo siendo uno de estos activos los datos, servicios, aplicaciones equipos, comunicaciones, recursos administrativos, recursos fiscos y recursos humanos

VALORACIÓN DE ACTIVOS

Para la valoración de activos en los sistemas de recursos empresariales, se depende de 3 dimensiones las cuales son confidencialidad, integridad y disponibilidad utilizando la guía del MinTic para, establecer un nivel de valoración en Alto, medio y bajo.

ANÁLISIS DE AMENAZAS

Para el análisis de amenazas se harán uso del tipo de activo identificado con el riesgo identificado con el objetivo de evitar que estos riesgos no controlados generen incidentes en la organización los cuales harán que los activos queden vulnerables ante cualquier amenaza, haremos uso de una tabla para poder ordenar los activos juntos a los riesgos.

VALORACIÓN DE RIESGO

Para la valoración de riesgo se hará uso de la medición del impacto de los riesgos en la organización, ayudara a determinar los riesgos que podemos controlar y que podemos analizar y evaluar, de manera que podamos evitar la materialización de los riesgos, identificando los riesgos con mayor criticidad atravéz de la probabilidad e impacto.

Capítulo 4 Salvaguardas

ESTRATEGIA DE TRATAMIENTO DE RIESGOS

Para la estrategia de tratamiento de riesgo se debe verificar los ataques que se tienen en la organización de modo que se pueda establecer contramedidas que ayude a manejar los riesgos principalmente esto se aplica cuando las pérdidas son demasiadas grandes. Se establecera las medidas que se utilizara dependiendo de la criticidad que este riesgo tendrá definido en probabilidades entre Alta, media y baja

ESTABLECIMIENTO DE TÉCNICAS

Para establecer las técnicas que se utilizaran se debe tener en cuenta las prioridades de la organización y el nivel de los riesgos encontrados. Las técnicas que se usaran son: Aceptar, evitar, controlar, investigar, mitigar y transferir. Con los riesgos identificados se procederá a seleccionar la técnica más conveniente a usar.

ESTABLECIMIENTO DE POLÍTICAS DE SEGURIDAD

Para el establecimiento de políticas de seguridad se hará uso del Sistema Integrado de Gestión de la Presidencia de la República (SIGEPRE) para poder definir las políticas de seguridad acoplándolas a las necesidades de la organización para poder asegurar la confidencialidad, integridad, disponibilidad, riesgos para los sistemas ERP e informar a los trabajadores que trabajan con los sistemas ERP

CONTROLES RECOMENDADOS

Para los controles recomendados se hará uso de los riesgos y priorización de los riesgos los cuales se determinaran los controles basándonos en la ISO 27001:2013 en el cual está especificado los dominios con los controles necesarios para poder tratar los riesgos junto a las técnicas definidas, para poder controlarlos evitando que

se vuelvan una amenaza para los sistemas ERP, ya identificado los controles junto a los riesgos se relacionaran para tener un mayor entendimiento.

MONITOREO

Para el monitoreo se hará seguimiento a los riesgos que se ha identificados, junto al nivel de criticidad que tienen, su tratamiento y el plan de monitoreo que se deben llevar a cabo para poder evitar la manifestación del riesgo a su vez debe estar a cargo un responsable de la empresa que se ocupe de la realización del plan de monitoreo.

ASIGNACIÓN DE RESPONSABILIDADES

Para la asignación de responsabilidades se hará uso de la matriz RASCI la cual ayudara a identificar los roles que los empleados de la organización deben desempeñar para los controles identificados relacionados para los sistemas de recursos empresariales

Capítulo V: Evaluación

METODOLOGÍA

Para la metodología se hara uso del modelo CMM y PHVA que serán de gran ayuda en la auditoria. EL CMM ofrecerá los elementos necesarios para evaluar los puntos que son necesario para verificar el cumplimiento de los controles definidos, permitiendo controlar los procesos y la calidad del SGSI propuesto.

EVALUACIÓN DE MADUREZ

Para la evaluación del nivel de madurez se podra verificar el cumplimiento que tiene cada uno de los controles que hemos establecido de la iso 27001:2013 para el sistema de gestión de la seguridad de la información

RESUMEN DE RESULTADOS

Se evidencia los resultados de la evaluación de madurez de los controles en el Sistema de gestión de la seguridad de la información

Capitulo II: CONTEXTO ORGANIZACIONAL

En el presente capítulo se desarrolla el contexto de la organización, realizando el reconocimiento de esta, así como un análisis para identificar el estado actual de la seguridad de la información en Ico Food Service SAC con respecto a la Norma ISO 27001, donde se evalúa el cumplimiento de cada uno de los dominios y controles descritos en dicha norma.

Reconocimiento Organizacional

En el reconocimiento de la organización se realiza la descripción de la organización, detallando las actividades de la empresa, así como la estructura organizacional, adicional a esto se detalla la infraestructura actual de la organización, teniendo en cuenta la red de datos, los equipos, aplicaciones y sistemas ERP con los que la empresa cuenta en la actualidad.

Descripción

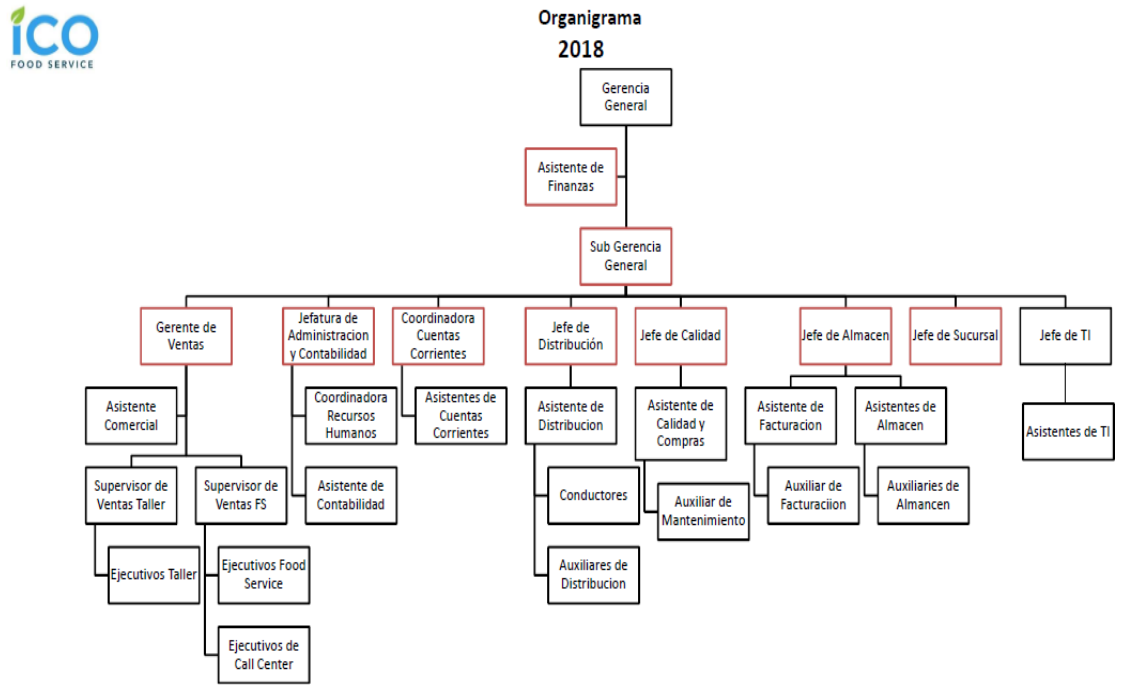
ICO LOGISTICA SAC es una empresa de consumo masivo que se dedica a la distribución de productos Laive, watts, suiza y Bazo Velarde con sede en Lima y Cusco, cuenta con más de 15 años de experiencia en el mercado. Anteriormente se desempeñaron bajo el canal Horizontal, ahora en la actualidad trabaja bajo el canal Food Service mediante una excelente oferta con estrictos controles sanitarios y las herramientas que el cliente necesita.

Las actividades de Ico Food Service comprenden la toma del pedido del cliente, el preparado del pedido y la distribución de su producto, todo ello en base a las compras diarias que realiza Ico a Laive.

Estructura Organizacional

La estructura organizacional de Ico Food Service está dada de forma jerárquica. El rango de mayor autoridad se encuentra a cargo de la gerencia y la sub gerencia general.

Adicionalmente, existe personal asignado a la gerencia de ventas (asesores comerciales, supervisores comerciales y ejecutivos) y las jefaturas de cada áreas, así como lo coordinadores y los asistentes como se puede evidenciar en la siguiente Figura N° 1.



Fuente: (Recursos Humanos, 2021*)*

Infraestructura

Red de Datos

Actualmente la red de datos de Ico es controlada por el proveedor de servicios de internet Óptical Networks SA , con una velocidad de 20 MB punto a punto , adicional a ellos se tiene una L2L que interconecta el local de Puente Piedra y el local de Surco y un servicio de VoIP . Además de ello se tiene también 1 AP en las 3 sedes administradas desde la sede central de Ico.

Las puertas de enlace VoIP de la serie MG 600 XN incluyen puertos FXS de 2/4/8 puertos VoIP con Wi-Fi IEEE 802.1 b/g/n, proporcionando un servicio de datos de voz y ancho de banda flexible, conveniente y abundante.

Esta red de datos funciona de manera integrada entre Surco y Puente piedra, para las sede de Cusco el servicio de datos es de manera independiente con un distinto proveedor de servicios de comunicaciones.

Equipos

A nivel de equipos en las tres sedes, se cuenta con el siguiente número de estaciones de trabajo:

Tabla 25 Estaciones de Trabajo

Área	Lima	Cusco
Gerencia	3	N/A
Ventas	8	3
Distribución	2	1
Administración	6	3
Almacén	4	2
Calidad	2	N/A
TI	3	N/A
Total	28	9

Fuente: (Elaboración Propia, 2021)

Además, se cuenta con dispositivos de telefonía, impresoras y servidores que se listan en la próxima tabla.

Tabla 26 Lista de Equipos

Equipo	*Marca*
Telefonía	Yealink E2 SIP-T21P
AP inalámbrico	TP-LINK TL-WA801ND
Servidor de correos	Gmail empresarial
Impresora - Escáner	Hp-laserjet-pro-m402dn
Portátiles	Notebook HP 14-ac186la - Intel Core i3-5005U 4 Gigas RAM Notebook HP 14-v007la - AMD A10- 5745M APU - 6 Gigas RAM Notebook HP x64-based PC - AMD A10-7300 - 6 Gigas RAM
Servidor de Archivos	WD my Cloud
Servidor de Aplicaciones	Windows Server 2008 R2

Fuente: (Elaboración Propia, 2021)

Aplicaciones

Ico utiliza diferentes herramientas tecnológicas para la gestión de sus operaciones, análisis de información, gestión de servicio, comunicación con los clientes y la gestión de los proyectos laborales internos. En la próxima tabla se listan las aplicaciones que permiten las tareas anteriormente mencionadas.

Tabla 27 Listado de Aplicaciones

Aplicación	Tipo de aplicación	Comentarios
Flex Business ERP	Software ERP	Gestión de procesos y operaciones
Paquete Office	Herramienta de ofimática	
ANT	Software ERP	Gestión de procesos y operaciones
Microsoft Windows	Sistema operativo	
Skype	Comunicaciones	Comunicación interna y con clientes
Power BI	Herramientas de BI	Analisis de información
SQL Server 2008 R2	Bases de datos	Sistema de administración de bases de datos

FreshDesk	Gestor de reclamos	Aplicativo web que permite gestionar las incidencias por parte del cliente

Fuente: (Elaboración Propia, 2021)

Estado Actual con respecto a la norma ISO 27001

En los primeros pasos para poder desarrollar el sistema de gestión de la seguridad de la información de la norma de la organización para la estandarización internacional (ISO) 27001, se efectuara un estudió que posibilita estimar el estado de los sistemas de recursos empresariales en cuanto a la seguridad que presenta la empresa.

En el nexo A se refleja cómo se obtuvo datos de la empresa ICO FOOD SERVICE usando la encuesta como técnica, Jefe del área de las tecnologías de la información Guadalupe Silvestre, Humberto.

Tabla 28: Recopilación de resultados de encuesta

Sigla	Estado de Evaluación	Descripción
NC	No Cumple	No se está cumpliendo
CP	Cumple Parcialmente	Se cumple de manera parcial con lo requerido de la norma 27001, y no es aplicado al 100% por los involucrados
CS	Cumple Satisfactoriamente	Se cumple con lo requerido por la norma 27001 siendo aplicado por los involucrados en el SGSI con un índice de 100%

Fuente (Moyano, 2017)

*Figura Nº SEQ Figura * ARABIC 45* Grafico

Fuente: Elaboración Propia

Una vez analizado la seguridad de la información sobre los sistemas ERP se encontró que:

- Solo 1 de los ítems que evaluamos no cumple.
- Solo 13 de los ítems cumple parcialmente con la evaluación.
- Existe una valoración nula en ítems que cumple satisfactoriamente

Una vez analizados se obtuvo los siguientes resultados

Tabla 29 Producto de la evaluación inicial ICO FOOD SERVICE

Anexo	Control	NC	CP	CS	Punto evaluados
A8	Gestión de Activos	0	1	0	1
A9	Control de Acceso	1	6	0	7
A11	Seguridad Física y Ambiental	0	4	0	4
A12	Seguridad de las operaciones	0	2	0	2
	Suma Total	1	13	0	14

Fuente: (Elaboración Propia, *2021*)

*Figura N° SEQ Figura * ARABIC 46* Producto

Fuente: Elaboración propia

Como se muestra el siguiente grafico vemos que en el análisis inicial en la seguridad de los sistemas ERP los ítems evaluados, la mayoría solo cumplen con la norma parciamente y solo un Ítem no lo cumple dejando con un 0% el cumplimiento satisfactorio.

A.8 Gestión de Activos

Se busca con este control es resguardar que toda la información que posea la empresa debe tener un nivel de seguridad de acuerdo con la importancia en la empresa. La empresa ICO Food Service debe tener claro la importancia de los activos dentro de los sistemas ERP.

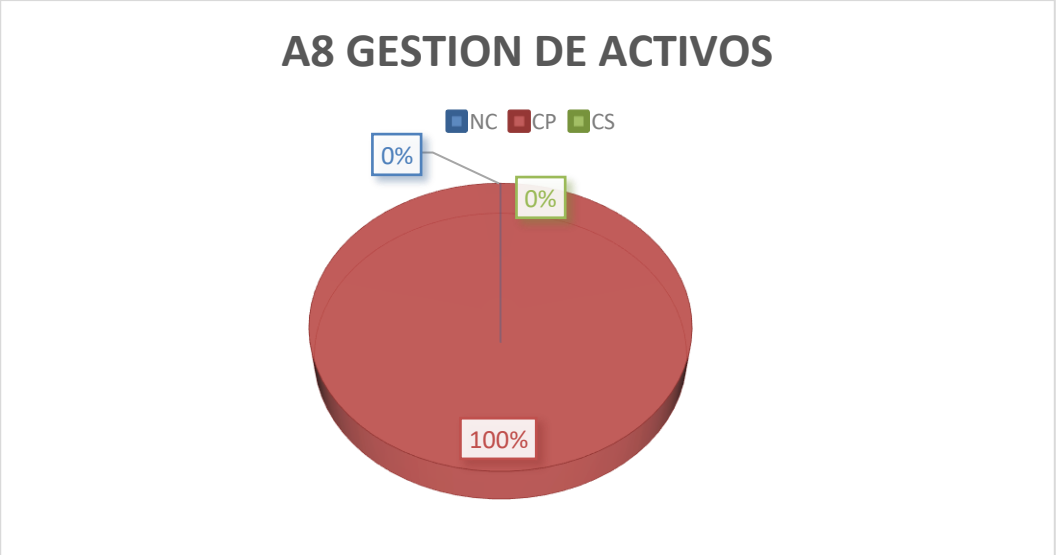


*Figura N° SEQ Figura * ARABIC 47* Gestión de Activos
Fuente: Elaboración propia

A9 Control de Acceso

Se debe estar consciente de la importancia del acceso a los sistemas de información, de manera que los usuarios tengan establecidos sus ya que se debe poner una limitación para poder acceder a la información. En vista de esto la empresa ICO FOOD SERVICE cumple parcialmente con lo establecido en la norma 27001:2013 con el aseguramiento y prevención de los usuarios en los sistemas.

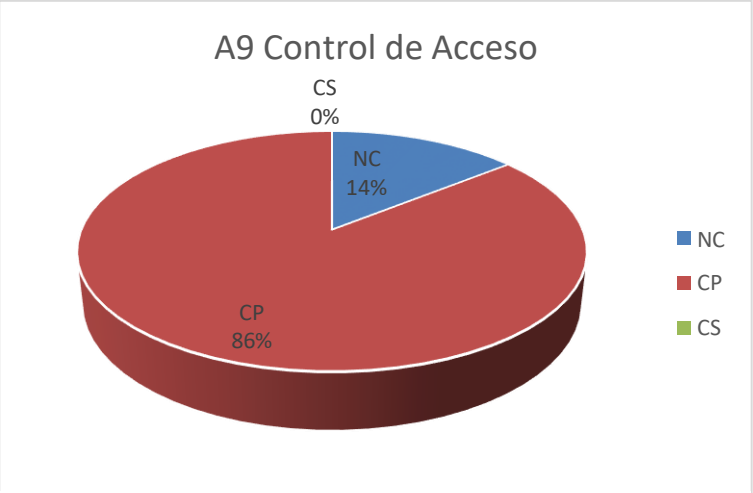


*Figura N° SEQ Figura * ARABIC 48* Control de

Fuente: Elaboración propia

A11 Seguridad Física y Ambiental

Con este control se busca dar conciencia a la empresa ICO FOOD SERVICE sobre prohibir el acceso presencial no autorizado, debido a que se podría causar daños a la información e instalaciones, a su vez prevenir la perdida, compromiso o daños de activos catalogados importantes por la empresa, para ello se deberá crear métodos o controles los cuales impidan cualquier acceso no autorizado, se debe crear medidas de seguridad contra los ataques maliciosos al sistema y accidentes dentro del área, se debe implementar para los equipos un respaldo para mantener su operatividad no se vea interrumpida por medios físicos y sus cables de comunicación deben estar reguardado protegiendo la información que los equipos albergan.

*Figura N° SEQ Figura * ARABIC 49* Seguridad Física y Ambiental
Fuente: Elaboración propia

A12 Seguridad de las Operaciones

Seguridad de la Operaciones

Con el fin de asegurar la información en la empresa ICO FOOD SERVICE se debe reguardar la información y las instalaciones de procesamiento de la información estén seguras contra ataques malintencionados, además se debe tener una amplia visualización de las acciones de los usuarios dentro del sistema, para evidenciar cualquier cambio generado, por lo cual se debe crear controles para la detección, prevención y recuperación de los activos afectados por códigos malicioso con el propósito de crear conciencia a los usuarios y se debe tener un registro global de todas las acciones delos usuarios, debido a que se puede experimentar fallos, excepciones en la seguridad de la información con el fin de visualizar las actividades realizadas y estar verificándolo periódicamente.

*Figura N° SEQ Figura * ARABIC 50* Seguridad de las

Fuente: Elaboración propia

CAPITULO III: GESTIÓN DE RIESGOS

Este capítulo describe la metodología que se va a emplear en la gestión de riesgos con la finalidad de que los órganos de gobierno tomen decisiones eficientes según los riesgos derivados de las tecnologías de la información , asimismo con el inventario de activos de la compañía y la valoración de estos , teniendo en cuenta la disponibilidad , integridad y confidencialidad de la información , de esta forma se realizará el análisis de amenazas y la valoración de los riesgos , estimando de esta manera los riesgos a los que se encuentra expuesta los sistemas ERP en cuanto a seguridad de la información de la empresa.

Además de ello, la parte más importante para la implementación del SGSI es el análisis y la gestión de riesgos de los activos de información que se encuentren involucrados dentro de los procesos que abarca el SGSI proporcionado

Metodología

Como metodología para la gestión de riesgos en el plan de implementación de la norma ISO 27001 se acuerda trabajar con MAGERIT, la cual implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información8. MAGERIT presenta los siguientes objetivos directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Objetivos Indirectos:

Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

INVENTARIO DE ACTIVOS

Para empezar con la gestión de riesgos se requiere un inventario de activos. Los activos son componentes o funcionalidades de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.

Tabla 30 Lista de Activos de la empresa ICO LOGÍSTICA S.A.C

ID	Tipo	Activo	Descripción
ACT_0002	Comunicaciones	Intranet	cableado categoría 5E Router suministrado por Óptical Networks.
ACT_0004	Datos	Backups	Se realizan Backups automáticos de: - BD del Sistema ANT - BD del sistema Uniflex - Backups de los archivos de usuarios en Google Drive
ACT_0005	Datos	Código fuente aplicaciones de las áreas operacionales y administrativas	Código en Visual Basic .NET y Fox Pro de: - Script estructura ANT - Script datos Uniflex - Ejecutables y archivos config de los aplicativos
ACT_0006	Datos	Bases de datos corporativas	Bases con información de: - Usuarios de los dos ERP - Documentos configurados - Información contable - Clientes - Cotizaciones - Consultorías y Capacitaciones - Modelo entidad relación Uniflex - Programas - Formatos documentos (manuales, accesos)
ACT_0009	Hardware	Servidor De los Sistemas	Trabaja con Windows Server 2008 R2
ACT_0013	Hardware	Discos duros de servidores y estaciones de trabajo	

ACT_0015	Hardware	UPS	8 tomas. Con autonomía de 5 a 20 min Da soporte a 5 equipos.
ACT_0017	Instalaciones	Sala eléctrica	Cuarto de suministro eléctrico del edificio
ACT_0020	Software	Sistema ERP	- Sistema ERP Uniflex que soporta todos los procesos de la Empresa - Sistema ERP ANT que soporta los procesos de la empresa
ACT_0025	Software	Bases de datos: SQL server 2008 R2 Express Edition	

Fuente: Elaboración Propia

VALORACIÓN DE ACTIVOS

A continuación se va a definir una tabla de valoraciones de activos, este depende de tres dimensiones fundamentales y de gran impacto en la seguridad de la información los cuales son la confidencialidad, integridad y disponibilidad.

Confidencialidad

La definición de confidencialidad apunta a una meta, la cual impida que la información este indispuesta para las personas, corporación o procesos no permitidos. La confidencialidad debe ser definida por los activos que utiliza la empresa, se usara los valores dados por Magerit 3.0 para la clasificación de los activos.

Tabla 31 Criterios de evaluación de Confidencialidad

Escala de Valoración	*Valor*	*Confidencialidad*	
3	Alto	Un activo es capaz de poder controlar la información reservada, su mal manejo puede perjudicar a la empresa trayendo resultados gran impacto.	La información que esté disponible para solamente uno de los procesas de la empresa y si es conocida por terceras personas sin tener una autorización de la gerencia, causaría un impacto negativo de disposición legal, operativa, imagen empresarial y económica.

2	Medio	Un activo es capaz de poder controlar la información clasificada, su mal manejo puede traer un impacto mediano a la empresa.	Información disponible para todos los procesos de la entidad y que en caso de ser conocida por terceros sin autorización puede conllevar un impacto negativo para los procesos de la misma. Esta información es propia de la entidad o de terceros y puede ser utilizada por todos los funcionarios de la entidad para realizar labores propias de los procesos, pero no puede ser conocida por terceros sin autorización del propietario.
1	Bajo	Un activo es capaz de poder controlar la información pública, su mal manejo no genera un impacto en la empresa.	Información que puede ser entregada o publicada sin restricciones a cualquier persona dentro y fuera de la entidad, sin que esto implique daños a terceros ni a las actividades y procesos de la entidad.

Fuente: (Elaboración Propia basado en Guía para la gestión y clasificación de activos MinTic, 2016)

Integridad

La integridad es una peculiaridad de la información que nos garantiza que la información no ha sido modificada o alterada por terceros. La valoración de los activos de la empresa ICO FOOD SERVICE se menciona a continuación

Tabla 32 Criterios de Evaluación de la Integridad

Escala de Valoración	Valoración	Integridad
3	Alto	Los errores deben ser solucionados de inmediato. Un activo es capaz de poder controlar la información en caso de existir una pérdida reservada, su mal manejo puede perjudicar a la empresa trayendo resultados gran impacto.
2	Medio	Los activos son capaces de controlar la información, en caso de que llegue a presentar perdidas de exactitud o completitud generaría un impacto negativo de disposición legal, retrasos de funciones o causar una pérdida de imagen moderado a los empleados públicos de la empresa.

1	Bajo	Los activos son capaces de controlar la información, en caso de presentar inexactitud y completitud, no originaría un impacto influyente para la empresa o proveedores externos
0	No Clasificada	En caso de no tener inventariado un activo, este de ser considerado por la organización como una información de integridad alta.

Fuente: (Elaboración Propia basado en Guía para la gestión y clasificación de activos MinTic, 2016)

Disponibilidad

La disponibilidad es la cualidad por la cual la información a la que se refiere debe ser accesible y utilizable por la petición de una entidad o proceso que tenga permitido su uso en cualquier momento y forma en que lo necesiten, del mismo modo con los recursos necesarios para que este funcione.

En el siguiente esquema veremos la valoración de la disponibilidad para los activos de la empresa ICO FOOD SERVICE, en una clasificación de 3 niveles.

Tabla 33 Criterios de valoración de la Disponibilidad

Escala de Valoración	*Valoración*	*Integridad*
3	Alto	Si no hay disponibilidad de la información, puede originar un gran impacto perjudicial de índole legal o económica, demora de funciones o producir una desconfianza hacia los entes externos.
2	Medio	Si no hay disponibilidad de la información, puede originar un gran impacto perjudicial de índole legal o económica, demora de funciones o producir una desconfianza moderado hacia los entes externos
1	Bajo	Si no hay disponibilidad de la información, puede originar una afectación a las operaciones normales de la entidad o entes externos, pero esta no conlleva implicaciones legales, económicas o desconfianza a la imagen de la empresa.

0	No Clasificada	En caso de no tener inventariado un activo de información y no haberlo clasificado, este debe ser considerado por la organización como activos de información de disponibilidad alta.

Fuente: (*Elaboración Propia basado en Guía para la gestión y clasificación de activos MinTic, 2016*)

ANÁLISIS DE AMENAZAS

Las amenazas son eventos que provocan un percance en la organización generando daños materiales o perdidas inmateriales de sus activos.

La materialización de estas puede generar un incidente que modifica el estado de seguridad de los activos ya que estos están siempre expuestos a muchos riesgos.

Las amenazas suelen ser las causantes de los incidentes potenciales que generan daños al sistema de información o a la organización. Tras el análisis de los activos en Ico Logística se detectaron las amenazas listadas en la siguiente tabla.

Recordatorio (Todos los ítems son válidos ya que son los que utilizan los erp)

Tabla 34 Resumen de Amenazas

C = Comunicaciones; D = Datos; H = Hardware; S = Software;
I = Instalaciones; R = RRHH;

			Nro Activos Afectados por Tipo						
ID Riesgo	***Riesgo***	***Vector Amenaza***	***C***	***D***	***H***	***I***	***R***	***S***	***Total***
R_001	Abuso de privilegios de acceso	Abuso de información privilegiada y actos no autorizados						4	4
R_002	Acceso no autorizado	Abuso de información privilegiada y actos no autorizados		3				2	7
R_003	Alteración de la información	Ataque interno y/o externo	1	2	2			2	7
R_004	Corrupción de la información	Ataque interno y/o externo		3				2	5

C = Comunicaciones; D = Datos; H = Hardware; S = Software; I = Instalaciones; R = RRHH; S = Software

			Nro Activos Afectados por Tipo						
ID Riesgo	***Riesgo***	***Vector Amenaza***	***C***	***D***	***H***	***I***	***R***	***S***	***Total***
R_005	Corte de suministro eléctrico	Fallos de la dependencia			1	1			1
R_006	Afectaciones de los soportes de almacenamiento de la información	Errores y Omisiones						3	3
R_007	Denegación de servicios	Sistemas Automatizado y código malicioso		1				3	4
R_008	Errores de configuración	Fallos en el sistema y en el medio ambiente						6	6
R_009	Errores de usuarios	Errores y omisiones						2	2
R_010	Errores de mantenimiento/ actualizaciones de programas(software)	Errores y omisiones						6	6
R_011	Errores de mantenimiento/ actualizaciones de equipos(hardware)	Errores y omisiones			10				10
R_012	Introducción de falsa información	Ataques internos y/o externo		3					3
R_013	Difusión de software dañino	Sistemas Automatizados y Código Malicioso	2	1				3	6
R_014	Errores de configuración	Fallos en el sistema y en el medio ambiente						9	9
R_015	Errores de los usuarios	Errores y Omisiones						3	3
R_016	Errores del administrador	Errores y Omisiones						6	6

Fuente: (Elaboración Propia, *2021*)

VALORACION DEL RIESGO

La valoración del riesgo permite estimar la magnitud de los riesgos a los que está expuesta la organización, además de ello se va a determinar los riesgos que van a ser controlados por medio de su identificación, análisis y evaluación. La materialización de una amenaza consta de dos elementos: probabilidad e impacto, estos determinan el nivel del riesgo.

De acuerdo a la probabilidad se determinan los siguientes criterios de valoración:

Tabla 35 Criterios de Valoración según la probabilidad

Escala de Valoración	Valoración	Descripción
3	Alto	La amenaza se puede materializar mínimo una vez al mes
2	Medio	La amenaza se puede materializar a lo sumo una vez en el semestre
1	Bajo	La amenaza se puede materializar a lo sumo una vez al año

Fuente: Elaboración Propia

Según el impacto se determinan los siguientes criterios de valoración:

Tabla 36 Criterios de valoración según Impacto

Escala de Valoración	Valoración	Descripción
3	Alto	La ocurrencia del evento tiene impacto a nivel de confidencialidad, integridad y/o disponibilidad de la información poniendo en riesgo la reputación de la empresa y/o inconvenientes legales.
2	Medio	La ocurrencia del evento tiene impacto a nivel de confidencialidad, integridad y/o disponibilidad de la información sin poner en riesgo la reputación de la empresa o necesidad de medidas legales.
1	Bajo	La ocurrencia del evento no tiene consecuencias relevantes para la organización.

Fuente: Elaboración Propia

Por la combinación probabilidad - impacto se define el mapa de riesgo que se presenta a continuación, los números en el interior de las celdas son calculados por la multiplicación de la probabilidad por el impacto. Indican junto con los tonos de colores la criticidad del riesgo.

Tabla 37 Mapa de Riesgo

MAPA DE RIESGO				
Probabilidad	*3 - Alta*	3	6	9
	2 - Media	2	4	6
	1- Baja	1	2	3
		1 - Bajo	*2 - Medio*	*3 -Alto*
	Impacto			

Fuente: Elaboración Propia

A continuación se presenta un resumen de los resultados obtenidos:

Tabla 38 Resumen Valoración del riesgo

		Promedio Probabilidad = PP Promedio Impacto = PI Estimado = E Valoración Riesgo = VR			
ID Vector	***V. Amenaza***	***PP***	***PI***	***E***	***VR***
VA_001	Abuso de información privilegiada y actos no autorizados	3	2	6	**RC**
VA_002	Ataque interno y/o Ataque externo	3	2	6	**RC**
VA_003	Errores y Omisiones	3	2	6	**RC**
VA_004	Fallos de dependencia	2	1	2	**RM**
VA_005	Fallos en el sistema y en el medio ambiente	2	2	4	**RC**
VA_006	Sistemas Automatizados y Código Malicioso	2	3	6	**RM**

Fuente: Elaboración Propia

CAPITULO IV. SELECCIÒN DE SALVAGUARDAS

En este capítulo se busca implantar medidas de resguardar o proteger, conocido como salvaguarda o tratamiento que permite prevenir, reducir, impedir o poder controlar los riesgos que se tienen identificados, para este capítulo se definirán el plan para poder tratar los riesgos que están presente en la organización, a su vez estudiar y entender las técnicas que serán parte del tratamiento y tener en cuenta las prioridades de la organización.

Se pondrán normas de seguridad con el objetivo de garantizar las dimensiones definidas como son las disponibilidades, integridad, confidencialidad y riesgos de la información, además de los controles recomendados, seguimiento y asignamiento de responsabilidades, con ayuda de la matriz de RASCI

ESTRATEGÍA PARA TRATAMIENTO DE RIEGOS

Una de los principales planes para poder tratar los riesgos es el estudio de la situación y definir en cuál de los casos se encuentran el riesgo, con el fin de poder centrarse en el verdadero objetivo.

Cuando exista una debilidad o vulnerabilidad, se debe implementar técnicas que puedan ayudarnos a disminuir las probabilidades de una vulnerabilidad.

Cuando exista la manera de explotar una debilidad o vulnerabilidad se debe aplicar una protección en capas, diseños arquitectónicos y una serie de controles administrativos de modo que se pueda prevenir que ocurran incidentes.

Cuando existe un ataque un costo menor que la ganancia que recibe el atacante por realizarlo, es implícito poner en marcha una contramedida para poder reducir los motivos de realiza daños por parte del atacante.

Cuando exista una perdida muy grande, se debe aplicar principios de diseño, procedimientos y técnicas para reducir el rango que abracara el ataque lanzado, rebajando las pérdidas que pueden surgir.

Siguiendo con lo definido anteriormente y la valoración de riesgos se especificara lo siguientes planes para tratar riesgos.

Tabla 39 Estrategias de tratamiento de riesgos

ESTRATEGIAS PARA TRATAMIENTO DE RIESGOS				
Probabilidades	3 – Alta	3 Zona de riesgo moderado tratamiento: Reducir la posibilidad de ocurrencia Evitar riesgo	6 Zona de riesgo moderado tratamiento: Reducir la posibilidad de ocurrencia Evitar riesgo Compartir o transferir	9 Zona de riesgo moderado tratamiento: Reducir la posibilidad de ocurrencia Evitar riesgo Compartir o transferir
	2 – Media	2 Zona de riesgo Bajo Tratamiento: Reducir la posibilidad de ocurrencia	4 Zona de riesgo moderado tratamiento: Reducir la posibilidad de ocurrencia Evitar riesgo	6 Zona de riesgo moderado tratamiento: Reducir la posibilidad de ocurrencia Evitar riesgo Compartir o transferir
	1 – Baja	1 Zona de riesgo moderado tratamiento: Asumir el riesgo	2 Zona de riesgo moderado tratamiento: Reducir riesgo Evitar el riesgo	3 Zona de riesgo moderado tratamiento: Reducir riesgo Evitar el riesgo
		1 – Baja	2- Media	3 – Alta
	Impacto			

Fuente: Elaboración Propia

TECNICAS PARA EL TRATAMIENTO DEL RIESGO

Teniendo en cuenta las preferencias o prioridades en la organización y el nivel de riesgo identificado se precisa distintas técnicas como tratamiento de riesgos:

Aceptar (A): Nos muestra la aceptación de la amenaza, después de decidir tomar el riesgo que tenga el mínimo de probabilidad de suceder. El uso de esta técnica es la aceptación del peligro o riesgo, enfocándose en que el riesgo ocurra, pero no realiza ninguna acción para evitarlo, esta técnica se utiliza siempre y cuando los riesgos sean bajos o muy bajos.

Evitar (E): Se trata de evitar que suceda el mismo riesgo, debido a que podría significar una probabilidad media o alta, de manera que pueda perjudicar a la empresa o Institución. En esta técnica se encuentra las opciones para un defensa o salvaguardas preventivo que determina normas, políticas, controles, y acciones que tratan de eludir cualquier eventualidad que lo ocasiona y minimizar que el

acontecimiento vuelva a pasar. Los ideales evitan que se concrete el riesgo o amenaza

Controlar (C): Son técnicas que se encargan de reducir la probabilidad de la amenaza o impacto. Frecuentemente se verifica las acciones o productos que pasan a formar parte del plan de trabajo que son vigilados y notificados como parte de la examinación del cumplimiento regular y el informe de progreso de programa.

Investigar (I): Esta técnica es diferente de las otras que se hayan usado debido que para su utilización se requiere una investigación, así mismo esta técnica no establece una mitigación de los riesgos individuales, la utilización de esta es debido a que no se ha podido reconocer una respuesta claro a los riesgos, por los cuales necesitan realizar más estudios.

Mitigar (M): Se definen salvaguardas que nos ayudan a la detección de amenazas que se manifiestan. Así pues esta técnica ayuda en lo máximo posible en evitar el deterioro de un activo o nos ayuda a frenar el ataque que se pueda originar, de vez en cuando las medidas que utilizan solo se enfocan en la pronta recuperación del sistema cuando una amenaza lo inutilizar.

Transferir (T): Esta técnica transfiere completamente o parcialmente los riesgo que tenga una compañía a otra, ya fuera por una póliza de seguro o un contrato outsourcing. Es un medio de compartir los riesgos. Existen 2 formas de compartir el riesgo:

- Riesgo cualitativo: Comparte los riesgos por un medio externalización de componentes del sistema, de forma que se reparten responsabilidades.
- Riesgo Cuantitativo: Por medio de la contratación de seguros, a cambio de una prima, el tomador se encarga de la reducción del impacto de los posibles riesgos y el asegurador toma la responsabilidad de las consecuencias.

A través del análisis realizado se determinan las técnicas que se usaran para los riesgos encontrados en la organización. Para un mejor entendimiento dirigirse a la sección de tratamiento en el anexo C – "Evaluación y Tratamiento de Riesgos"

		Nro. De Riesgo x Técnicas de tratamiento						
ID V. Amenaza	Vector Amenaza	A	C	E	I	M	T	Total
VA_001	Abuso de información privilegiada y actos no autorizados		2	2	1			2
VA_002	Ataque interno y/o Ataque externo		3	3		3		3
VA_003	Errores y Omisiones		6	6		6		6
VA_004	Fallos de dependencia		1	1	1	1		1
VA_005	Fallos en el sistema y en el medio ambiente			2	2			2
VA_006	Sistemas Automatizados y Código Malicioso		2	2		2		2
	Suma total		14	15	4	12		16

Tabla 40

Riesgos por técnicas

Fuente: Elaboración Propia

PLAN DE TRATAMIENTO DE RIESGOS

Habiendo definido las estrategias y las técnicas que se utilizaran, se pasara a definir el plan de tratamiento de los riesgos encontrados en el cual se pasara a optar por el salvaguardamiento, políticas, controles, monitoreo y el asignamiento de responsabilidades.

POLITICAS DE SEGURIDAD SGSI

La planeación de un Sistema de gestión de la seguridad de la información (SGSI) conlleva a la creación de políticas de seguridad en la cuales se definirán las medidas necesarias para garantizar la disponibilidad, riesgos, integridad y confidencialidad de la información en los sistemas ERP de la empresa ICO FOOD SERVICE. Debido

a ello debe ser establecida, asignada e informada a todos los trabajadores de la empresa (duda)

OBJETIVO

El objetivo primordial de las políticas del Sistema de Gestión de la Seguridad de la Información es el establecimiento de normas que puedan asegurar la disponibilidad, riesgos, integridad y confidencialidad de la información en los sistemas de recursos empresariales (ERP) en ICO FOOD SERVICE.

ALCANCE

Estas políticas deben ser empleadas por administradores del Sistema ERP en la empresa ICO FOOD SERVICE, debido a que ellos son los encargados del bienestar de los sistemas erp para que los usuarios de la empresa que cuenten un acceso al sistema puedan utilizarlo sin problemas.

RESPONSABLE

Todos los trabajadores a cargos del bienestar de los sistemas de recursos empresariales de la empresa ICO FOOD SERVICE.

DEFINICIÓN

La empresa ICO FOOD SERVICE sabe la importancia de la información que maneja es imprescindible para lograr sus objetivos, por ello es de vital importancia asegurar las confidencialidad, Integridad, Disponibilidad y riesgos de la organización. Así mismo la empresa se responsabiliza de:

- Proteger la información y los activos de tecnología de la información
- Definir los controles de seguridad una vez puesto en funcionamiento las políticas, estándares, guías y procedimientos, apoyados con mecanismos y servicios automatizados que nos permitan ayudar a resguardar la información de la organización

- Gestionar los riesgos a los cuales la organización se encuentra expuesto, para la protección de su información
- Examinar periódicamente el cumplimiento de las políticas de la seguridad de la información.

Ico Logística SAC basada en las directrices de seguridad de la información nacional y adaptándolas al caso de la organización establece que:

- Antes de asignar el equipo de cómputo a un nuevo usuario, el Área de desarrollo y gerencia debe asegurarse que no existe información confidencial en dicho equipo, en caso contrario, debe proceder a respaldar completamente la información y posteriormente deberá borrarla del equipo.
- El área de gerencia y administración debe establecer las medidas y mecanismos de control, monitoreo y seguridad, para el correo electrónico y los accesos a páginas o sitios de Internet con contenidos u orígenes sospechosos.
- El área de soporte debe realizar pruebas (mínimo una vez al año) de penetración, así como un análisis de vulnerabilidades de la red para la medición de la seguridad perimetral de la red interna ante un ataque desde el exterior.
- El administrador de la seguridad es el autorizado para habilitar páginas bloqueadas siempre y cuando el acceso a estas se encuentre previamente autorizado por el director respectivo existiendo una justificación para ello.
- El área de gerencia y desarrollo debe llevar registro de todas las personas a las que se les ha otorgado algún privilegio de acceso.
- El área de gerencia y desarrollo debe revisar los derechos de acceso de forma bimestral.
- El área de gerencia y administración debe garantizar que los empleados retirados de la entidad devuelvan la información confidencial y reservada que tiene bajo su resguardo.

- El personal de Ico Logística SAC debe utilizar el correo electrónico únicamente con fines laborales.
- El uso de internet debe de estar controlado por un dispositivo de seguridad como un proxy, permitiendo solamente a los usuarios autorizados el utilizar el servicio.
- El uso de internet debe de ser sólo para fines laborales y no para realizar actividades personales o con fines de lucro.
- En caso de sospecha de revelación de contraseñas a personas no autorizadas, estas contraseñas deben ser cambiadas inmediatamente.
- Es responsabilidad de los usuarios revisar los archivos adjuntos con el antivirus antes de descargarlos a cualquier equipo de cómputo.
- Está estrictamente prohibido el uso inapropiado de Internet para desarrollar actividades ilegales, acceder y/o descargar contenido pornográfico, descargar cualquier tipo de software sin autorización del área de gerencia, cargar o descargar software comercial violando las leyes de derecho de autor.
- Está prohibido ingresar a las áreas de trabajo o extraer de las instalaciones de Ico Logística SAC medios removibles (CD, DVD, USB, Discos Duros, ZIP, entre otros), sin la debida autorización.
- La clave de usuario debe ser única para cada usuario que solicite acceso.
- La información debe clasificarse en términos de su valor y criticidad como: Pública, Clasificada o Reservada, y es responsabilidad del propietario que se haya designado.
- Las contraseñas deben ser otorgadas a los usuarios de forma segura. Se debe evitar enviar las contraseñas por correo.
- Las contraseñas deben tener una longitud mínima de 8 caracteres, combinar caracteres alfanuméricos y ser cambiadas máximo cada 90 días.

- Las contraseñas referentes a las cuentas "predefinidas" incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

SANCIONES

A los trabajadores que se les encuentre infringiendo las políticas establecidas será sujetos a medidas disciplinarias, las cuales pueden implicar el despido del trabajador. Al infringir una de estas políticas como medida cautelar se procederá hacerle presente al superior del trabajador mediante un correo, con copia a Recursos Humanos.

En cuyo caso caiga en terceros la infracción de las políticas, se les hará llegar un correo una solicitud de motivo de infracción al represéntate legal de la firma.

Además, en caso de una utilización incorrecta de la información de la empresa implicaría efectos penales y se notificara a los implicados en el tema.

CONTROLES RECOMENDADOS

Una vez identificados las estimación identificación y priorización de los riesgos se fomentara la investigación y establecimiento de los controles adecuados para utiliza en el tratamiento.

La fomentación de los controles se encuentra basados en los dominios del anexo A de la norma ISO 27001:2013

- Documentación de Políticas

La gran mayoría de los incidentes surgidos en la empresa surgen debido a la falta de establecimiento de políticas y documentación acerca de la seguridad de la información, se desarrolló una serie de políticas que guardan relación con los dominios de la norma con los que se procura reducir la ocurrencia de que una amenaza surja.

Tabla 41 Lista de Políticas de Desarrolladas

				Nivel de Riesgo		
ID	Política	Dominio	V. Amenaza	RB	RC	RM
P_0001	Política de Seguridad de la información	A5,A8	Abuso de la información privilegiada y actos no autorizados		X	
			Ataques internos y/o externos		X	
			Errores y Omisiones		X	
P_002	Política de control de Acceso	A5,A9	Abuso de información privilegiada y actos no autorizados		X	
P_003	Política de seguridad física y ambiental	A5,A11	Fallos de la dependencia			X
			Fallos en el sistema y en el medio ambiente		X	
			Ataques internos y/o externos		X	
P_004	Política de protección contra código malicioso	A5,A12	Sistemas automatizados y códigos maliciosos			X

- Aplicación de los controles de los Dominios

En lo mencionado anteriormente los controles que seleccionamos está directamente asociado con los 14 dominios establecidos por la norma ISO/IE 27001:2013.

El dominio A5 – Políticas de seguridad, se encuentra ya mencionado en la lista de políticas desarrolladas, abarca todo un anexo donde define las técnicas y reglas para poder impedir el aprovechamiento de las debilidades que existen.

Aquí se muestra los controles recomendados para las amenazas encontradas.

ID Riesgo	Riesgo	V. Amenaza	N. Riesgo	A5	A6	A7	A8	A9	A10	A11	A12	A13	A14	A15	A16
R_001	Abuso de privilegios de acceso	Abuso de información privilegiada y actos no autorizados	RC	x			x			x	x	x			
R_002	Acceso no Autorizado	Abuso de información privilegiada y actos no autorizados	RC	x				x	x						
R_003	Alteración accidental de la información	Ataque interno y/o externo	RC	x				x			x		x		
R_004	Corrupción de la información	Ataque interno y/o externo	RC	x					x		x				
R_005	corte de suministros eléctrico	Fallos de la dependencia	RM	x											x
R_006	Afecciones de los soportes de almacenamiento de la información	Errores y omisiones	RC	x			x				x				
R_007	Denegación de servicios	Sistema Automatizado y código malicioso	RM	x				x			x				x
R_008	Errores de Configuración	Fallos en el sistema y en el medio ambiente	RC	x									x		
R_009	Errores de usuario	Errores y omisiones	RC	x		X		x							

R_010	Errores de mantenimiento/ Actualización de programas (software)	Errores y omisiones	RC	x							x		x		
R_011	Errores de mantenimiento/ Actualización de programas (hardware)	Errores y omisiones	RC	x						x				x	
R_012	Introducción de falsa información	Ataques internos y/o externos	RC		x				x		x	x			
R_013	Difusión de software dañino	Sistemas automatizados y código malicioso	RM						x		x	x			
R_014	Errores de configuración	Fallos en el sistema y en el medio ambiente	RC					x		x			x		x
R_015	Errores de los usuarios	Errores y omisiones	RC	x	x			x			x				
R_016	Errores del administrador	Errores y omisiones	RC	x	x						x				

Figura 51Vinculación de riesgos con los controles de la ISO 27001:2013

En el siguiente "**Evaluación y Tratamiento de Riesgos**" una vez asociados los dominios, se encontrará los controles adecuados para salvaguardar lo que nos permite es evitar que se origine el riesgo y saber determine el tipo de técnica que se puede emplear según sea el riesgo que se va tratar. Se muestra un resumen en la siguiente tabla 49:

Tabla 42 Lista de Controles

Dominio	Control	A	C	E	I	M
A6	6.1.2 Separación de funciones de trabajo y áreas de negocio			x		
	6.2.2 Asignación de roles de trabajo y responsabilidades		x	x		
A7	Capacitación del personal en seguridad de la información			x		
A8	8.2.1 , 8.2.2 clasificar y etiquetar la información en los sistemas ERP		x	x		
	Inventario de activos			x		
A9	9.1.1, 9.2.1, 9.2.3 Políticas de control de acceso Registro y baja de usuarios Gestión de derechos de acceso privilegiados			x		
	Registro y baja de usuario (Gestión del mantenimiento de usuarios) Restricción de acceso a la información(Reglas de acceso) Control			x		
	9.1.2 Acceso a los servicios en red() Firewall e IPS			x		
A10	10.1.2 Gestión de claves(Criptografía de clave privada)			x		
	10.1.1 Políticas de sobre el uso de controles criptográficos			x		
A11	11.1.2 Controles de acceso físico(registro de ingresos)			x		
	11.2.4 mantenimiento de equipos			x		
A12	12.2.1 controles contra código malicioso 12.3.1 Respaldo 12.4.1 Registro de eventos 12.5.1 Restricción sobre la instalación de software		x	x		
	12.2.1 controles contra código malicioso 12.4.2 protección de los registros 12.5.1 Restricción de la instalación de software 12.3.1 Respaldo			x		x

	12.4.1 Registro de eventos			x	x	
	12.5.1 Instalación de software en sistemas operacionales			x		
	12.6.2 Restricción sobre la instalación de software 12.2.1 Controles contra código malicioso			x		
A13	13,1,1 Controles de red 13,2,3 Mensajes electrónicos 13,2,2 Acuerdo de transferencia de información (implementación de servicios FTP/SSL y software de monitoreo de la red)			x		
A14	14,2,3 -revisión de técnicas de aplicaciones después de los cambios a la plataforma operativa 14,2,1 Políticas de desarrollo seguro 14,2,9 Pruebas de aceptación del sistema			x		
	14,2,5 Principio de ingeniería segura			x		
	14,2,7 Desarrollo contratado externamente			x		
A15	15,2,2 Gestión de cambios a los servicios de los proveedores 15,1,2 Abordar la seguridad dentro de los acuerdos del proveedor			x		
A16	16,1,2 Reporte de eventos de seguridad 16,1,5 Respuesta a los incidentes de seguridad 16,1,6 Aprendizaje de los incidentes de la seguridad de la información		x	x	x	
	16,,1,3 Reporte de debilidades de seguridad de la información 16,1,5 Respuesta a los incidentes de seguridad			x	x	x
A17	17,1,2 Implementación de la continuidad de seguridad de la información 17,1,3 Verificación , revisión y evaluación de la continuidad de la seguridad de la información			x		
	17,1,1 Planificación de continuidad de la seguridad de la información		x	x		x
	17,1,1 Planificación de continuidad de la seguridad de la información 17,2,1 Instalación de procesamiento de la información			x		
	17,2,1 Instalación de procesamiento de la información		x	x		x

A18	18,1,3 Protección de registros 18,2,3 Revisión del cumplimiento técnico			x				

Fuente: Elaboración propia

En un trabajo en conjunto entre el plan de monitoreo y plan de tratamiento nos da un mayor entendimiento de que tan adecuado son las estrategia que se han realizado, de manera que se puedan tomar acciones las cuales nos permitan adelantarnos a los problemas, A continuación se mostrará el monitoreo para los riesgos encontrados y los responsables que estarán a cargo.

RIESGO	NIVEL	TRATAMIENTO				PLAN DE MONITOREO	RESPONSABL
		A	E	M	T		
Abuso de privilegios de acceso	RC		x	x		Auditoría interna de las funciones de los empleados	Sub-Gerente General / Geren General
Acceso no autorizado	RC		x			Registro y evaluación periódica de logs de aplicaciones críticas	Jefe TI / Asisten TI
Alteración de la información	RC		x			Evaluación periódica de la información registrada	Jefe TI / Asisten TI
Corrupción de la información	RC			x		Evaluación periódica de la información registrada	Sub-Gerente General / Jefe T
Corte de suministro eléctrico	RM	X	x			Evaluación periódica de los suministros eléctricos Evaluación al proceso de respaldo externo	Jefe Calidad Auxiliar Mantenimiento
Afectaciones de los soportes de almacenamiento de la información	RC		x			Evaluación y actualización de activos de almacenamiento Evaluación de activos de respaldo	Jefe TI / Asisten TI
Denegación de servicios	RM		x	x		Informes de errores y excepciones	Jefe TI / Asisten TI
Errores de configuración	RC		X			Informes de errores	Asistente TI
Errores de usuarios	RC		X			Informes de errores	Jefe TI
Errores de mantenimiento/ actualizaciones de programas(software)	RC		X	x		Informes de errores	Jefe TI / Asisten TI
Errores de mantenimiento/ actualizaciones de equipos(hardware)	RC		x	x		Informes de errores	Sub-Gerente General / Jefe T
Introducción de falsa información	RC		X			Seguimiento a capacitaciones sobre responsabilidad en el manejo de información	Sub-Gerente General / Jefe T
Difusión de software dañino	RM		X			Informes de errores y seguimiento a resultados de antivirus Reporte vía correo de amenazas recientes y logs de acciones tomadas	Sub-Gerente General / Jefe T

Fuente: Elaboración propia

Errores de configuración	RC			x		Informes de errores	Asistente TI
Errores de los usuarios	RC		x			Informes de errores	Jefe TI
Errores del administrador	RC		x			Informes de errores	Jefe TI / Asisten TI

Figura 52 Plan de Monitoreo

Asignación de Responsabilidades

Usando los controles facilitados por la norma ISO 27001:2013 y el modelo de una matriz RASCI se trata de lograr que los empleados puedan entender sus roles y deberes asignados en la seguridad de la información. El modelo de la matriz RASCI está conformado por los siguientes roles:

- **Responsible (R)**
  Es quien está a cargo de realizar una tarea. Usualmente debe de haber un encargado por tarea.
- **Accountable (A)**
  Es quien se hace responsable del cumplimiento de una tarea y es quien debe rendir cuentas
- **Apoyo – (S)**
  Son recursos están designado al Responsible (R), para cumplir con sus tareas, así mismo trabajan en ella.
- **Consulted (C)**
  Provee de información necesaria, para el cumplimiento de una tarea.
- **Informed (I)**
  Este rol se designa a quien se debe ser informado sobre todos los avances y resultados de las tareas.

Con el objetivo de implementar el sistema de gestión de la seguridad de la información se deben definir los roles y responsabilidades en el área en el cual están alejados los sistemas ERP, para ello se definirá los roles de los involucrados que deben encargarse de cada uno de los controles. Los roles identificados de los involucrados son:

- **Gerente General**
  Encargado de monitorear las actividades relacionadas con el SGSI así como todas las actividades administrativas y financieras, asumido por el señor Arturo Castillo Orbegoso

- **Sub-Gerente General**

Encargado de la coordinación y verificación de las actividades del SGSI , asi como la correcta administración de los recursos de la empresa , asumido por la Sub Gerente Maria Alejandra Pinto Rivera

- **Jefe de TI**
  Encargado de la correcta administración y funcionamiento de los recursos informáticos de la organización asi como el correcto uso de los mismos, en el momento asumido por el jefe de TI Humberto Guadalupe

- **Asistente de TI**
  Encargado del soporte y mantenimiento a los sistemas ERP, realiza las coordinaciones con proveedores, velar y monitorear por el correcto funcionamiento del sistema SGSI, asumido por

- **Líder de SI**
  Encargado de la implementación de técnicas y/o procedimientos para la gestión de incidentes de seguridad de la información, así como para la mejora de los procesos dentro de la organización, en el momento asumido por el Jefe de TI

Tabla 43 Matriz RASCI

	Gerente General	Sub Gerente General	Asistente de TI	Jefe de TI	Líder de SI
A5 Políticas de la seguridad de la Información					
5.1.1 Políticas de la seguridad **de la información	I	A	S	R	C
5.1.2 Revisión de las políticas para la seguridad de la información	I	I	S	R	A
A6 Organización de la seguridad de la información					
6.1.2 Separación de funciones de trabajo y áreas de negocio	A	R	I	I	C

6.2.2 Asignación de roles de trabajo y responsabilidades	A	R	I	I	C
A7 Seguridad de los Recursos Humanos					
7.2.2 Capacitación del personal en la seguridad de la información	I	A	S	S	R
A8 Gestión de Activos					
8.2.1 Clasificar y etiquetar la información en los sistemas ERP	I	A	S	R	C
8.2.2 Inventario de activos					
A9 Control de Acceso	I	R	S	R	C
9.1.1 Políticas de Control de acceso	I	R	S	R	C
9.2.1 Registro y baja de usuarios	I	I	R	A	C
9.2.3 Gestión de derechos de acceso privilegiados	I	I	R	A	C
9.4.1 Restricción de acceso a la información	I	I	S	R	A
9.1.2 Acceso a los servicios en red	I	I	R	A	S
A10 Criptografía					
10.1.2 Gestión de claves	I	I	R	A	S
10.1.1 Políticas sobre el uso de controles criptográficos	I	A	I	R	S
A11 Seguridad Física y del Entorno	I	S	I	R	A
11.1.2 Controles de acceso Físico	I	A	S	S	R
11.2.4 Mantenimiento de equipos	I	S	R	A	C
A12 Seguridad de las operaciones					
12.2.1 controles contra código malicioso	I	I	S	R	A
12.3.1 Respaldo	I	I	R	A	C
12.4.1 Registro de Eventos	I		R	A	S

12.5.1 Restricción sobre la instalación de software	I		S	R	A
12.4.2 Protección de los registros	C	I	R	A	S
12.6.2 Restricción sobre la instalación de software	I	C	R	A	C
A13 Seguridad de las comunicaciones					
13.1.1 Controles de red	I	I	S	R	C
13.2.2 Mensajes electrónicos	I	I	R	A	S
13.2.3 Acuerdo de transferencia de información	I	C	R	A	S
A14 Adquisición, desarrollos y mantenimiento de sistemas					
14.2.5 Principio de ingeniería segura	I	A	S	R	C
A15 Relación con los proveedores					
15.2.2 Gestión de cambios a los servicios de los proveedores	I	C	R	A	S
15.1.2 abordar la seguridad dentro de los acuerdos del proveedor	I	C	R	A	S
A16 Gestión de incidente de seguridad de la información					
16.1.2 Reporte de eventos de seguridad	I	C	R	A	S
16.1.5 Respuesta a los incidentes de seguridad	I	I	S	R	A
16.1.6 Aprendizaje de los incidentes de la seguridad de la información	I	I	S	R	C
16.1.3 Reporte de debilidades de seguridad de la información	I	I	R	A	S

A17 Gestión de la continuidad del negocio	A	R	I	I	C
17.1.2 Implementación de la continuidad de seguridad de la información	I	I	S	R	A
17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	I	C	S	R	A
17.1.1 Planificación de continuidad de la seguridad de la información	I	A	S	R	C
17.2.1 Instalación de procesamiento de la información	R	A	S	S	C
A18 Cumplimiento					
18.1.3 Protección de registros	I	A	S	R	C
18.2.3 Revisión del cumplimiento técnico	I	A	I	R	S

Fuente: Elaboración propia

CAPITULO V: EVALUACIÓN- AUDITORIA CUMPLIMIENTO

En este capítulo de evaluación se mostrará los resultados del análisis y los resultados que se obtuvieron a partir de la evaluación que se realizado para la mejora de la seguridad de la información usando la norma ISO 27001:2013, de acuerdo a los resultados en el plan de implementación del sistema de gestión de la seguridad de la información que se realizó en la empresa ICO FOOD SERVICE. El llevar a cabo una auditoria tiene como objetivo observar la madurez del SGSI definido por los controles expuesto en la norma y los niveles de madurez establecido para la organización.

METODOLOGIA

Haciendo uso del modelo de capacidad de madurez (CMM) y la metodología PHVA bajo esos estándares se hará uso de la auditoría. El uso del modelo CMM proporciona un mejor control sobre los procesos y la calidad del sistema de gestión de la seguridad de la información.

El modelo CMM está orientado en la mejora continua de los procesos, trata de reconocer todos aquellos elementos deseables en la organización que ayuden a estimar el cumplimiento de los controles establecidos para llevar a cabo el sistema de gestión de la seguridad de la información. Los elementos identificados que nos ayudaran en la evaluación, para su cumplimiento son:

- Documentos Formales (DF)
- Procedimientos Empíricos (PEmp)
- Procedimientos Estandarizados (PEst)

- Mejora continua (MC)
- Capacitaciones (C)
- Monitorea (M)
- Herramientas Automatizadas(HA)

Comenzando con la cantidad de elementos, esfuerzos y la responsabilidad de la alta gerencia como la de los trabajadores involucrados en el sistema de gestión de la seguridad de la información de la organización ICO FOOD SERVICE buscando establecer los niveles y criterios de madurez.

Ahora bien los niveles de madurez son organizados y progresivos en concordancia con su importancia y preferencia, para este caso los niveles de madurez establecidos para ICO FOOD SERVICE está desde el 0 a 5 los cuales nos ayudaran para que el sistema de gestión de la seguridad de la información propuesto sea de calidad.

	Procedimientos Empíricos	Documentos Formales	Procedimientos Estandarizados	Capacitaciones	Mejora continua	Monitoreo	Herramientas Automatizadas
0							
1	X						
2	x	x	X				
3		x	X	x			
4		x	X	x	x	x	
5					x	x	X

Tabla 44 Elementos de evaluación

Fuente: Elaboración propia
http://biblioteca.usac.edu.gt/tesis/08/08_0213_CS.pdf

Evaluación de Madurez

Como se ha descrito en todo el documento, para poder realizar una implementación de un sistema de gestión de la seguridad no hemos basado en la guía de la ISO

27001:2013, la cual brinda 14 dominios los cuales contienen 35 objetivos y 114 controles en su totalidad.

El motivo principal de la evaluación de madurez es verificar el nivel de implementación de cada uno de los controles en ICO FOOD SERVICE.

Tabla 45 Niveles de Madurez

ID	Nivel de Madurez	Criterios
0	0 - Inexistente	
1	1 - Inicial	En este nivel se encuentran procesos de los cuales no se encuentran documentados, planificados ni medidos. Por lo general no se llega a cumplir la metas planteadas, el tiempo, costo ni los recursos que se han establecidos.
2	2 - Repetible	En este nivel se deberá empezar a crear documentación para los procesos que tengan establecidos. Se deben tener un nivel de compromiso en cuanto a tiempo, costo, recursos y la creación de políticas es necesario para una mejor administración dentro de la organización.
3	3 - Definido	En este nivel se encuentra lo que son las implementaciones y actualizaciones de los procesos para la mejora del desempeño dentro de la organización, en este nivel se encuentran las capacitaciones de los empleados de la organización y una ligera reducción del tiempo, coste y recursos . El propósito del nivel es acerca de la planeación y la mejora continua.
4	4 - Administrado	En este nivel se encuentra una medición cuantificable de los procesos junto al producto y servicios, se aseguran del cumplimiento de los planes y programas de mejora.
5	5 - Optimizado	En este nivel se encontró que la organización trata de mejorar los procesos implementados de un modo controlable. Con el fin de lograr esta meta se deben identificar las fortalezas y debilidades .

Fuente: Elaboración propia

Los criterios de madurez plasmados anteriormente permiten medir la situación de la empresa en función a los controles que se han propuesto.

En la siguiente tabla se presenta la evaluación de madurez aplicada a Ico Logística SAC tras ultimar tareas del Plan de Implementación del SGSI.

CONTROLES ISO/IEC 27001:2013			ID EST	ESTADO	EVIDENCIA
A5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACION**				
A5.1	Dirección de la gerencia para la seguridad de la información				
Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes					
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	1	INICIAL	Documento de PS-ISO27001-01
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	1	INICIAL	Documento de PS-ISO27001-01
A6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACION**				
A6.1	Organización interna				
Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.					

A6.1.2	Segregación de funciones	Control: Las funciones y áreas de responsabilidad en conflicto deben ser segregadas para reducir oportunidades de modificación no autorizada o no intencional o mal uso de los activos de la Organización.	1	INICIAL	Matriz RASCI ICO
A6.2.2	Teletrabajo	*Control* Una política y medidas de seguridad de apoyo deben ser implementadas para proteger Información a la que se accede, se procesa o almacena en sitios de teletrabajo.	*2*	*REPETIBLE*	Documento de PS-ISO27001-01

A7	**SEGURIDAD DE LOS RECURSOS HUMANOS**				
A7.1	Durante el empleo				
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.					
A7.2.2	Conciencia, educación y capacitación sobre la seguridad de la información	*Control* Todos los empleados de la organización y, cuando fuera relevante, los contratistas deben recibir educación y capacitación sobre la conciencia de la seguridad de la información, así como actualizaciones regulares sobre políticas y procedimientos de la organización, según sea relevante para la función del trabajo que Cumplen.	*1*	INICIAL	-Documento KirkPatrick SGSI-01 -Capacitación mensual de SI
A8	**GESTION DE ACTIVOS**				
A8.2	Clasificación de la información				
Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.					
A8.2.1	Clasificación de la información	*Control* La información debe ser clasificada en términos de los requisitos legales, valor, criticidad y sensibilidad respecto a una divulgación o modificación no autorizada.	*1*	INICIAL	Software Data Clasisification Toolkit

A8.2.2	Etiquetado de la información	*Control* Un conjunto apropiado de procedimientos para el etiquetado de la información debe ser desarrollado e implementado en concordancia con el esquema de clasificación de la información adoptado por la organización.	*1*	INICIAL	Software Data Clasisification Toolkit
A9	**CONTROL DE ACCESO**				
A9.1	Requisitos de la empresa para el control de accesos				
Objetivo: Limitar el acceso a la información y a las instalaciones de procesamiento de la Información.					
A9.1.1	Política de control de acceso	*Control* Una política de control de acceso debe ser establecida, documentada y revisada basada en requisitos del negocio y de seguridad de la Información.	*2*	REPETIBLE	Hullero para el área de Servidores y redes
A9.1.2	Accesos a redes y servicios de red	*Control* Los usuarios deben tener acceso solamente a la red y a servicios de red que hayan sido específicamente autorizados a usar.	*2*	REPETIBLE	Documento De permisos DP-SGSI 01
A9.2	Gestión de acceso de usuario				
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.					
A9.2.1	Registro y baja de usuarios	*Control* Un proceso formal de registro y baja de usuarios debe ser implementado para permitir la asignación de derechos de acceso.	*2*	REPETIBLE	Módulo de Gestión de Usuario ERP

A9.2.3	Gestión de derechos de acceso privilegiados	*Control* La asignación y uso de derechos de acceso privilegiado debe ser restringida y controlada.	*2*	REPETIBLE	Módulo de Gestión de Usuario ERP
A9.4	Control de acceso a sistema y aplicación				
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.					
A9.4.1	Restricción de acceso a la información	*Control* El acceso a la información y a las funciones del sistema de aplicación debe ser restringido en concordancia con la política de control de acceso.	*1*	INICIAL	Documento de Gestión de perfiles DGP-01
A10	**CRIPTOGRAFIA**				
A10.1	Controles Criptográficos				
Objetivo: Asegurar el uso apropiado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información.					
A10.1.1	Política sobre el uso de controles criptográficos	Control Una política sobre el uso de controles criptográficos para la protección de la información debe ser desarrollada e implementada	2	REPETIBLE	*Documento GC-01*
A10.1.2	Gestión de Claves	*Control* Una política sobre el uso, protección y tiempo de vida de las claves criptográficas debe ser desarrollada e implementada a través de todo su ciclo de vida.	*2*	*REPETIBLE*	*Documento GC-01*
A11	**SEGURIDAD FISICA Y AMBIENTAL**				
A11.1	Áreas Seguras				
Objetivo: Impedir acceso físico no autorizado, daño e interferencia a la información y a las Instalaciones de procesamiento de la información de la organización.					

A11.1.2	Controles de ingreso físico	Control Las áreas seguras deben ser protegidas por medio de controles apropiados de ingreso para asegurar que se le permite el acceso sólo al personal autorizado.	1	INICIAL	Hullero para el área de Servidores y redes
A11.2	Equipos				
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.					
A11.2.4	Mantenimiento de equipos	*Control* Los equipos deben mantenerse de manera correcta para asegurar su continua disponibilidad e integridad.	*1*	INICIAL	Documento de Programación de mantenimiento mensual ME-SGSI-01

A12	**Seguridad de las Operaciones**				
A12.2	Protección contra código malicioso				
Objetivo: Asegurar que la información y las instalaciones de procesamiento de la información Estén protegidas contra códigos maliciosos.					
A12.2.1	Controles contra códigos maliciosos	*Control* Controles de detección, prevención y recuperación para proteger contra códigos maliciosos deben ser implementados, en combinación con una concientización apropiada de los usuarios.	*1*	INICIAL	- Antivirus ESET Endpoint
A12.3	Respaldo				
Objetivo: Proteger contra la pérdida de datos					

A12.3.1	Respaldo de la información	*Control* Copias de respaldo de la información, del software y de las imágenes del sistema deben ser tomadas y probadas regularmente en concordancia con una Política de respaldo acordada.	*1*	INICIAL	Documento para la Gestión del Respaldo GP-SGSI-01
A12.4	Registros y Monitoreo				
Objetivo: Registrar eventos y generar evidencia					
A12.4.1	Registro de Eventos	*Control* Registros (logs) de eventos de actividades de usuarios, excepciones, fallas y eventos de seguridad de la información deben ser producidos, Mantenidos y regularmente revisados.	*2*	REPETIBLE	Documento de logs generados del servidor LDOC-01
A12.4.2	Protección de los registros	*Control* Las instalaciones para registros (logs) y la información de los registros (logs) deben ser Protegidas contra la adulteración y el acceso no autorizado.	*2*	REPETIBLE	Documento de protección de registros PR-SGSI-01

A12.6	Gestión de vulnerabilidad técnicas				
Objetivo: Prevenir la explotación de vulnerabilidades técnicas					
A12.6.2	Restricción sobre la instalación de software	*Control* Reglas que gobiernen la instalación de software por parte de los usuarios deben ser establecidas e implementadas.	*1*	INCIAL	Documentos de restricciones en función a las instalaciones DI-SGSI-01
A13	**Seguridad de las Comunicaciones**				
A13.1	Gestión y seguridad de la red				
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de la información de apoyo.					

A13.1.1	Controles de red	*Control* Las redes deben ser gestionadas y controladas para proteger la información en los sistemas y las aplicaciones.	*1*	INICIAL	-Firewall Fortinet e IPS
A13.2	Transferencia de la información				
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.					
A13.2.2	Acuerdo sobre transferencia de información	*Control* Los acuerdos deben dirigir la transferencia segura de información del negocio entre la organización y partes externas.	*1*	INICIAL	Documento de acuerdo con proveedores DTRA-SGSI-01
A13.2.3	Mensajes electrónicos	*Control* La información involucrada en mensajería electrónica debe ser protegida apropiadamente.	*1*	INICIAL	Implementación de Secure Gmail

A14	**Adquisición, desarrollo y mantenimiento de sistemas**				
A14.2	**Seguridad en los procesos de desarrollo y soporte**				
Objetivo: Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.					
A14.2.5	Principios de ingeniería de sistemas seguros	*Control* Principios para la ingeniería de sistemas seguros deben ser establecidos, documentados, mantenidos y aplicados a cualquier esfuerzo de implementación de sistemas de información.	*0*	INEXISTENTE	
A15	**Relaciones con los proveedores**				

A15.1	**Seguridad de la información en las relaciones con los proveedores**				
Objetivo: Asegurar protección a los activos de la organización que son accesibles por los proveedores					
A15.1.2	Abordar la seguridad dentro de los acuerdos con proveedores	*Control* Todos los requisitos relevantes de seguridad de la información deben ser establecidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar, o proveer componentes de infraestructura de TI para la información de la organización.	*1*	INICIAL	Implementación de SLA con proveedores
A15.2	Transferencia de la información				
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.					
A15.2.2	Gestión de cambios a los servicios del proveedor	*Control* Los cambios a la provisión de servicios por parte de proveedores, incluyendo el mantenimiento y mejoramiento de políticas, procedimientos y controles existentes de seguridad de la información deben ser gestionados tomando en cuenta la criticidad de la información del negocio, sistemas y procesos involucrados y una reevaluación de riesgos.	*1*	INICIAL	Documento de gestión de cambio SGSI-GC-01

A16	**Gestión de incidentes de seguridad de la información**				
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**				
Objetivo: Asegurar un enfoque consistente y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.					

A16.1.2	Reporte de eventos de seguridad de la información	*Control* Los eventos de seguridad de la información deben ser reportados a través de canales de gestión apropiados tan rápido como sea posible.	*1*	INICIAL	Documento de alertas programadas frente a accesos no autorizados AP-SGSI-01
A16.1.3	Reporte de debilidades de seguridad de la información	*Control* Empleados y contratistas que usan los sistemas y servicios de información de la organización deben ser exigidos a advertir y reportar cualquier debilidad observada o de la que se sospecha en cuanto a seguridad de la información en los sistemas o servicios.	*1*	INICIAL	Comité mensual con proveedores
A16.1.5	Respuesta a incidentes de seguridad de la información	*Control* Los incidentes de seguridad de la información deben ser respondidos de acuerdo con los procedimientos documentados.	*1*	INICIAL	Documento de alertas programadas frente a accesos no autorizados AP-SGSI-01
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	*Control* El conocimiento adquirido a partir de analizar y resolver los incidentes de seguridad de la información debe ser utilizado para reducir la probabilidad o el impacto de incidentes futuros.	*0*	INEXISTENTE	

A17	**Aspectos de seguridad de la información en la gestión de continuidad del negocio**
A17.1	**Continuidad de seguridad de la información**

Objetivo: La continuidad de seguridad de la información debe estar embebida en los sistemas de gestión de continuidad del negocio de la organización					
A17.1.1	Planificación de continuidad de seguridad de la información	*Control* La organización debe determinar sus requisitos de seguridad de la información y continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo durante una crisis o desastre.	*1*	INICIAL	Documento de análisis de impacto del negocio DAI-SGSI-01
A17.1.2	Implementación de continuidad de seguridad de la información	*Control* La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel requerido de continuidad de seguridad de la información durante una situación adversa.	*1*	INICIAL	Documento de análisis de impacto del negocio DAI-SGSI-01
A17.1.3	Verificación , revisión y evaluación de continuidad de seguridad de la información	*Control* La organización debe verificar los controles de continuidad de seguridad de la información que han establecido e implementado a intervalos regulares para asegurarse que son válidos y efectivos durante situaciones adversas.	*1*	INICIAL	Documento de análisis de impacto del negocio DAI-SGSI-01
A17.2		Redundancias			
Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información					
A17.2.1	Instalaciones de procesamiento de la información	*Control* Las instalaciones de procesamiento de la información deben ser implementadas con redundancia suficiente para cumplir con los requisitos de disponibilidad.	*0*	INEXISTENTE	

A18	**Cumplimiento**
A18.1	**Cumplimiento con requisitos legales y contractuales**

Objetivo: Evitar infracciones de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas a la seguridad de la información y a cualquier requisito de seguridad.					
A18.1.3	Protección de registros	*Control* Los registros deben ser protegidos de cualquier pérdida, destrucción, falsificación, acceso no autorizado y divulgación no autorizada, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.	*1*	INICIAL	
A18.2		Redundancias			
Objetivo: Asegurar la disponibilidad de las instalaciones y procesamiento de la información					
A18.2.3	Revisión del cumplimiento técnico	Los sistemas de información deben ser revisados regularmente respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización	*1*	INICIAL	Documento de revisión de sistemas ERP DR-SGSI-01

Figura 53 Evaluación de la madurez de los controles de la ISO 27001:2013

Fuente: Elaboración propia

En la Figura 53 se puede evidenciar la evaluación de los controles implementados proporcionado por la ISO 27001:2013 en estado se encuentran así como la evidencia que se está realizando en cada uno de ellos.

Resumen de Resultados

En este capítulo se muestra los resultados, además de ello también la revisión del estado de los controles brindados por la ISO 27001 en la empresa Ico Logística SAC

Se puede visualizar también que la organización se encuentra en un nivel de madures**,** la clasificación de los controles aplicados se muestra en la siguiente tabla

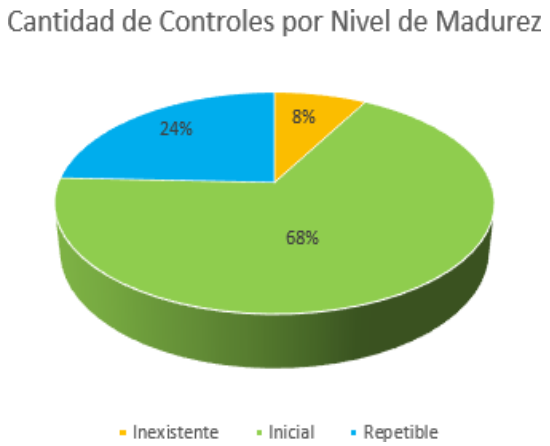


Figura 54 Resultado de la madurez en los controles implementados

Fuente: Elaboración propia

En la Figura 54 se observa el resultado de la madurez en los controles implementados en qué estado esos se encuentran.

3 en estado Inexistente (8%)
25 en estado Inicial (68%)
9 en estado Repetible (24%)

La siguiente tabla nos muestra los resultados de madurez por cada dominio estimado de la norma ISO 27001

Tabla 46
Resultado de la madurez de los controles de la iso 27001:2013

Dominio	Controles Aplicados	0	1	2	3	4	5
A5-Política de seguridad	2		2				
A6-Organización de la SI	2		1	1			
A7-Seguridad de los RRHH	1		1				
A8-Gestión de activos	2		2				
A9-Control de accesos	5		1	4			
A10-Criptografía	2			2			
A11-Seguridad física y ambiental	2		2				

A12-Seguridad en las operaciones	5		3	2			
A13-Seguridad en las comunicaciones	3		3				
A14-Adquisición de sistemas, desarrollo y mantenimiento	1	1					
A15-Relación con proveedores	2		2				
A16-Gestión de los incidentes de seguridad	4	1	3				
A17-Continuidad del negocio	4	1	3				
A18-Cumplimiento con requerimientos legales y contractuales	2		2				
TOTAL	37	3	25	9			

Fuente: Elaboración propia

En los resultados de la evaluación de madurez del SGSI en la empresa Ico Logística SAC se resalta que:

- La empresa no le ah tomado mucha importancia a 3 controles de los 37 de la norma ISO 27001 ya que la organización estima una probabilidad baja para que se materialicen las amenazas relacionadas a la carencia de los mismos , los controles que pertenecen a esta categoría son:

  A14.2.5: Principios de ingeniería de sistemas seguros
  A16.1.6: Aprendizaje de los incidentes de seguridad de la información
  A17.2.1: Instalaciones de procesamiento de la información

- La implementación de los controles de la norma ISO 27001 ha permitido a la empresa fortalecer la seguridad de la información con los procedimientos que se han establecido y con la documentación estandarizada con el 24% de los controles

- De la totalidad de controles aplicados, ninguno tiene un nivel de madures más alto esto nos muestra que es escaso la cantidad de herramientas que permitan automatizar los controles para el SGSI.

- El 68% de los controles aplicados se encuentra en un estado inicial, esto quiere decir que la empresa recién ha empezado a tomar conciencia en cuanto al SGSI

Como se puede observar el nivel de madurez de la empresa aún se encuentra

bajo, sin embargo se puede apreciar un gran avance con los controles implementados, además lo beneficioso es que se encuentran ya iniciados, muy diferente antes de iniciar con la implementación

La implementación del SGSI es un proceso que requiere bastante tiempo, trabajo y algunos costos económicos, Sin embargo, beneficia el crecimiento y alcance de los objetivos de la organización si se gestiona de forma adecuada bajo el ciclo de mejora continua. Por consiguiente, se sugiere establecer capacitaciones, monitoreo, automatización de los controles y auditorías internas que permitan incrementar los niveles de madurez del SGSI.

Anexo 11

Evidencia de la frecuencia y los tipos de ataques en la organización

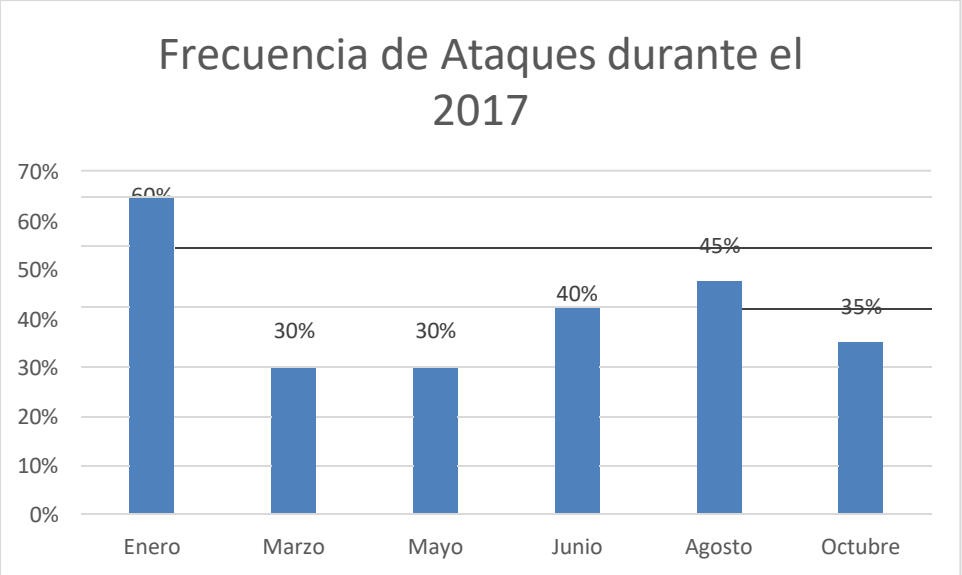


*Figura SEQ Figura * ARABIC 55* Porcentaje de ataques en el año

Fuente: RRHH, *2021*

Como vemos en la figura 55 nos muestra un estadístico de los meses en los cuales la empresa ha sido atacada comprometiendo información

*Figura SEQ Figura * ARABIC 56 El Porcentaje y los tipos de ataques*

Fuente: Tecnologías de la información, 2017

Anexo 12

CARTA DE AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

UNIVERSIDAD PRIVADA DEL NORTE

Yo Arturo Castillo Orbegoso
(Nombre del representante legal o persona facultada en permitir el uso de datos)

identificado con DNI 07885245 en mi calidad de Gerente General
(Nombre del puesto del representante legal o persona facultada en permitir el uso de datos)

del área de la gerencia general
(Nombre del área de la empresa)

de la empresa/institución Ico Logistica SAC
(Nombre de la empresa)

con R.U.C N° 20509422444, ubicada en la ciudad de Lima

OTORGO LA AUTORIZACIÓN,

Al señor Henry Alexander Tiona Llerena
(Nombre completo del Egresado/Bachiller)

identificado con DNI N° 47541198, egresado de la ( )Carrera profesional o ( )Programa de Postgrado de Ingeniería de Sistemas Computacionales para
(Nombre de la carrera o programa)

que utilice la siguiente información de la empresa:

Activos tecnologicos de la empresa, informe detallado de los sistemas de información seguridad de la información.
(Detallar la información a entregar)

con la finalidad de que pueda desarrollar su ( )Trabajo de Investigación, (X)Tesis o ( )Trabajo de suficiencia profesional para optar al grado de ( )Bachiller, ( )Maestro, ( )Doctor o (X)Título Profesional.

Adjunto a esta carta, está la siguiente documentación:
( ) Ficha RUC
( ) *Vigencia de Poder (Para informes de suficiencia profesional)
( ) Otro (ROF, MOF, Resolución, etc. para el caso de empresas públicas válido tanto para Tesis, Trabajo de Investigación o Trabajo de Suficiencia Profesional).

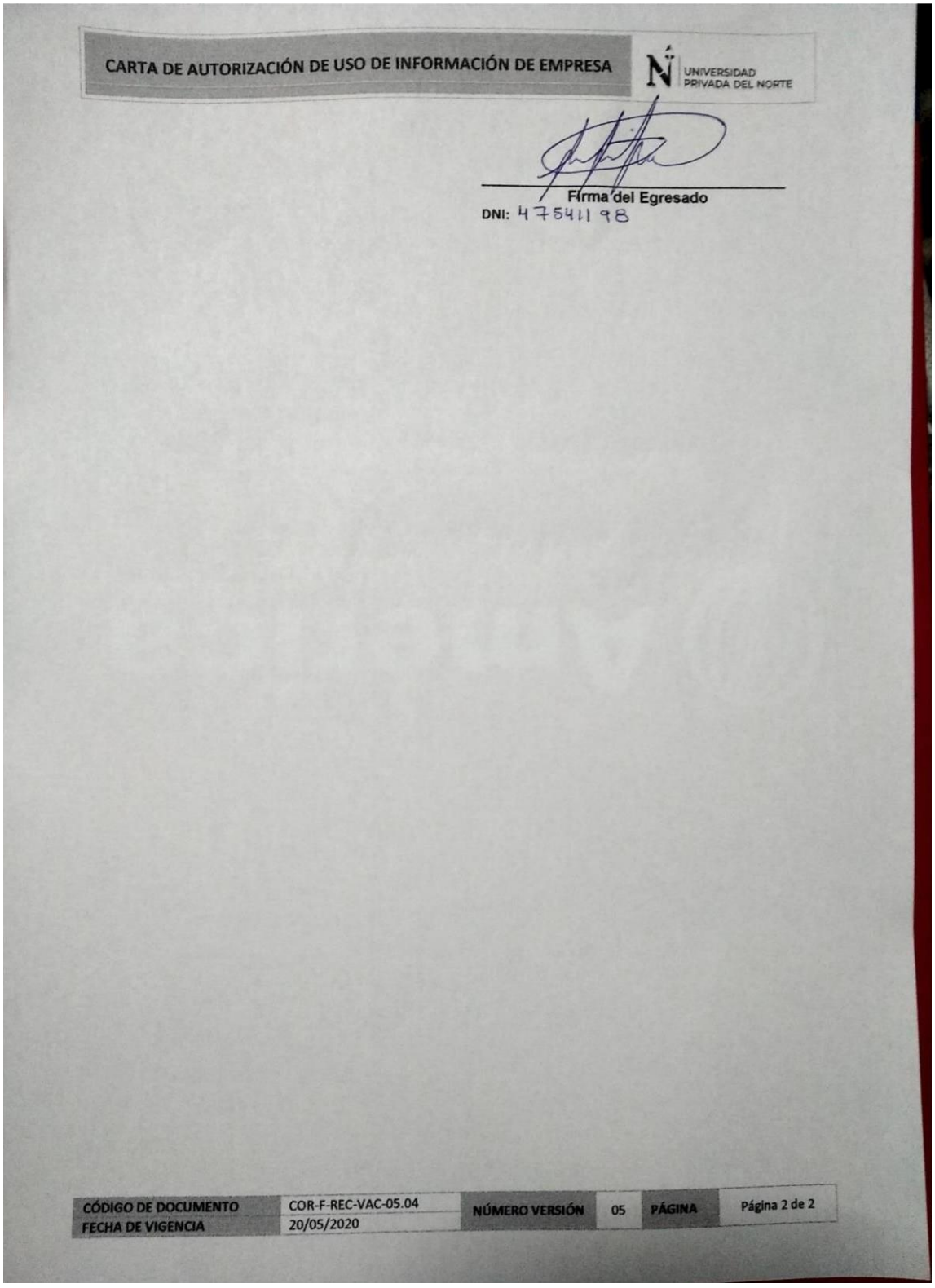
*** Nota: En el caso este formato se use como regularización o continuidad del trámite durante la coyuntura de emergencia – Covit19, se debe de omitir la "Vigencia de Poder" requerido para los informes de Suficiencia Profesional.**

Indicar si el Representante que autoriza la información de la empresa, solicita mantener el nombre o cualquier distintivo de la empresa en reserva, marcando con una "X" la opción seleccionada.
( ) Mantener en Reserva el nombre o cualquier distintivo de la empresa; o
( ) Mencionar el nombre de la empresa.

ICO LOGISTICA S.A.C.
ARTURO CASTILLO ORBEGOSO
GERENTE GENERAL
07885245

Firma y sello del Representante Legal
DNI: 07885245

El Egresado/Bachiller declara que los datos emitidos en esta carta y en el Trabajo de Investigación, en la Tesis son auténticos. En caso de comprobarse la falsedad de datos, el Egresado será sometido al inicio del procedimiento disciplinario correspondiente; asimismo, asumirá toda la responsabilidad ante posibles acciones legales que la empresa, otorgante de información, pueda ejecutar.



CARTA DE AUTORIZACIÓN DE USO DE INFORMACIÓN DE EMPRESA

UNIVERSIDAD PRIVADA DEL NORTE

Firma del Egresado

DNI: 47541198

CÓDIGO DE DOCUMENTO	COR-F-REC-VAC-05.04	NÚMERO VERSIÓN	05	PÁGINA	Página 2 de 2
FECHA DE VIGENCIA	20/05/2020				