UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA

ESCUELA ACADÉMICO PROFESIONAL DE SISTEMAS

Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001

TESIS PARA OBTENER EL TITULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

Manuel Armando Agurto Castillo

ASESOR:

Mg. Carmen Zulema Quito Rodríguez

LÍNEA DE INVESTIGACIÓN:

Auditoria de Sistemas y Seguridad de la Información

PIURA – PERÚ

2017

PÁGINA DEL JURADO

Ing. Jaime Leandro Madrid Casariego

Presidente

Ing. Adín Saúl Velasco Campoverde

Secretario

Ing. Elmer Alfredo Chunga Zapata

Vocal

DEDICATORIA

A mis padres por su incondicional apoyo y confianza a lo largo de mi vida personal y profesional, por la motivación constante que me permitió hacer frente a cualquier obstáculo que me hicieron crecer como persona y profesionalmente;

Al personal de trabajo del área QHSE de la empresa PISER S.A.C y a mis maestros por su asesoría y su apoyo constante en la investigación.

AGRADECIMIENTO

En primer lugar, agradecerle a Dios por haberme colmado de bendiciones,

A la vez el agradecimiento sincero de mis asesores Ing. Carmen Quito Rodríguez y al Ing. Rubén More Valencia, al Ing. Carlos Correa García asesor experto en el tema de investigación, por haberme brindado su tiempo, apoyo y guía permanente. Finalmente agradecer a mi familia por el constante apoyo a lo largo de mi formación profesional.

DECLARATORIA DE AUTORÍA

Yo, **Manuel Armando Agurto Castillo**, estudiante de la escuela profesional de Ingeniería de Sistemas, de la universidad César Vallejo filial Piura; declaro que el trabajo académico titulado **"Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"** presentada, en 147 folios para la obtención del título profesional de Ingeniero de Sistemas es de mi autoría.

Por lo tanto, declaro lo siguiente:

- He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo establecido por las normas de elaboración de trabajos académicos.
- No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.
- Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.
- Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.
- De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Piura, 01 Diciembre del 2017

_____

Manuel Armando Agurto Castillo

DNI: 46158659

PRESENTACIÓN

La norma ISO 27001 es la que concede los tres pilares fundamentales, la confidencialidad, integridad y disponibilidad de los activos de la información. En la empresa PISER S.A.C los procesos implementados del estándar ISO 9001 son importantes y deben tratarse siempre como un proceso más de la empresa dado que al relacionar, estandarizar y finalmente ejecutar todos los procedimientos del estándar hace que genere gran cantidad de información, proponiéndose esta tesis titulada Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001, a continuación se describe en siete capítulos:

Capítulo I – Introducción, es donde se plasmó las bases teóricas conceptuales en la que está basada la presente investigación, así como el planteamiento del problema.

Capítulo II – Método, muestra la variable y sus indicadores de seguridad por parte de las dimensiones dadas por la ISO 27001 para el proceso del diagnóstico de los activos de información, lo que implicó identificar los activos a resguardar.

Capítulo III – Resultados, se definió las interpretaciones de tablas y figuras estadísticas de cada resultado y cada indicador considerado en este estudio.

Capítulo IV – Discusión, se relacionaron los resultados obtenidos, comparándolos con los antecedentes y las teorías nombradas en el marco teórico.

Capítulo V – Conclusiones, se presentó los principales hallazgos de la investigación.

Capítulo VI – Recomendaciones, se planteó nuevos temas y problemas de investigación a seguir.

Capítulo VII – Propuesta, se presentó con la finalidad de proponer controles de seguridad de la información acorde con la norma ISO 27001.

Señores miembros del jurado espero cumplir con los requisitos de aprobación de la presente tesis.

ÍNDICE

RESUMEN

DIAGNÓSTICO DE LOS ACTIVOS DE INFORMACIÓN DE LOS PROCESOS IMPLEMENTADOS POR EL ESTÁNDAR ISO 9001 EN EL ÁREA QHSE DE LA EMPRESA PISER S.A.C TALARA, BASADO EN LA NORMA ISO 27001.

Autor: Manuel Armando Agurto Castillo.

Esta investigación tuvo como objetivo elaborar un diagnóstico de los activos de información, donde se planteó como tema de investigación debido que el área QHSE es la encargada de la estandarización y ejecución de procedimientos del estándar ISO 9001, generando gran cantidad de información la cual está expuesta a deteriorarse, perderse, ser modificada o llegar a manos de la competencia, ya que para la ISO 27001, en toda empresa, el activo fundamental es su información. Se realizaron constantes reuniones con los colaboradores del área de logística e informática y el área QHSE para identificar y valorar los activos de información de los procesos implementados bajo la norma ISO 27001, se utilizaron cuestionarios y listas de cotejo para cada dimensión según la norma ISO 27001, obteniendo resultados que el 58% de fuga de documentación especializada es de manuales, procedimientos, documentación técnica, por debajo con el 33% otra de la fuga de documentación es por las incidencias en información de carácter personal. En conclusión, luego de realizar dicha investigación se propuso elaborar la propuesta técnica, en la que incluyen los controles de seguridad basada en la norma ISO 27001, acorde con los procesos implementados por el estándar ISO 9001.

Palabras claves: Seguridad de la Información, ISO 27001, Activos de información.

ABSTRACT

DIAGNOSIS OF INFORMATION ASSETS OF THE PROCESS IMPLEMENTED BY THE ISO 9001 STANDARD IN THE QHSE AREA OF THE PISER S.A.C COMPANY - TALARA, BASED ON THE ISO 27001 STANDARD.

Author: Manuel Armando Agurto Castillo.

This research aimed to develop a diagnosis of the information assets, which it was raised as a research topic because the QHSE area is in charge of the standardization and execution of ISO 9001 procedures, generating a large amount of information which is exposed to deteriorate, to lose itself, to be modified or to fall into the rival company hands, since for ISO 27001, in every company, the fundamental asset is its information. Constant meetings were held with logistics and IT staff and the QHSE area to identify and value the information assets of processes implemented under the ISO 27001 standard, questionnaires and checklists were used for each dimension according to ISO 27001, obtaining results that 58% of specialized documentation leakage is about manuals, procedures, technical documentation, below with 33% another documentation leak is due to incidents in personal information. In conclusion after this investigation was made, it was proposed to elaborate the technical proposal, which includes the security controls based on the ISO 27001 standard, in accordance with the processes implemented by the ISO 9001 standard.

Keywords: Information Security, ISO 27001, Information Assets.

I. INTRODUCCIÓN

1.1 Realidad Problemática

"El estándar ISO 27001 es una norma internacional que proporciona el aseguramiento, la confidencialidad, integridad y disponibilidad de los datos de la información, concede a las empresas la estimación del peligro y la aplicación de los registros necesarios para mitigarlos". (ISO Tools - Excellenge, 2013)

Actualmente las empresas están implementando el estándar ISO 27001 que dispone todos sus requerimientos obligatorios al momento de aplicar un Sistema de Gestión de Seguridad de la información (SGSI), todo eso a crecido con la finalidad de ayudar como ideal para la empresa, para la implementación de dicho sistema de seguridad, procedimiento, seguimiento y progreso del (SGSI), generando una confianza por el adecuado proceso de seguridad a la información obteniendo mejoras continuas teniendo la facilidad frente a cualquier cambio inesperado que se pueda presentar en la empresa tanto como procesos del negocio y la tecnología ya que día a día avanza a gran velocidad haciendo que las empresas tomen conciencia a lo que están expuestos sus negocios. (Cañizares, y otros, 2011)

Los activos de información tanto digitales como escritos en papel es el activo fundamental en cualquier empresa y hasta la actualidad es desafiada por diferentes problemas que se presentan diariamente en el negocio; es importante la seguridad de los activos de información ya que se debe aplicar en los procesos del negocio para una mejora en los procedimientos manuales como digitales como parte esencial en la continuidad del negocio, teniendo en cuenta a los procedimientos que involucran a las personas, tecnología y a terceros. (Cañizares, y otros, 2011)

"Peruana de Inspección y Servicios S.A.C (PISER S.A.C) es una empresa ubicada Lote A-224 Parque Industrial Talara - Alta, dedicada a prestar diversos servicios en actividades industriales, petroleras y otras, desarrollando sus actividades desde el año 2007 en el rubro petrolero". (PISER S.A.C, 2014). Actualmente la información en la empresa Peruana de Inspección y Servicios S.A.C es el activo más valioso, cada vez aparecen

más riesgos a los que están comprometidos los activos de información de los procesos implementados del estándar ISO 9001 la cual se debe preservar el aspecto más seguro y eficiente posible. Las dimensiones de seguridad no solo implica tecnología, también se debe tener en cuenta todos los aspectos organizativos y relativos al personal de trabajo de dicha empresa, el área seguridad en el rubro petrolero es conocida por las siglas en inglés de “Quality, Health, Safety & Environment (QHSE), en español Calidad, Salud, Seguridad y Ambiente las cuales representan las principales funciones dentro del área de seguridad”. (Manual de Organización y Funciones, 2016), QHSE es una de las principales áreas por lo que está inmersa a la cantidad de información tanto de personal, transporte, operaciones e implementación del estándar de calidad, siendo estos últimos uno de los más importantes por su ejecución de sus procedimientos implementados la cual genera información. Según (MAGERIT – versión 3.0, 2012) los activos de Información incluyen: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. Para la empresa Peruana de Inspección y Servicios S.A.C los activos de información son fundamentales y deben tratarse siempre como un proceso más de la empresa, la cual se realizó un diagnóstico a los activos de información que implica comprender los activos y operaciones a resguardar, localizar los puntos débiles de cada procedimiento ejecutado y sobre todo el reconocimiento de las amenazas posibles presentadas, se identificó la frecuencia, porcentaje del riesgo de incidencia de cada indicador para las dimensiones según la ISO 27001 que son la confidencialidad, integridad y disponibilidad para que así la empresa tenga referencia de la seguridad de sus activos de los procesos implementados por el estándar ISO 9001.

1.2 Trabajos Previos

Para Gonzales Sánchez (2013), en su investigación para optar título profesional de ingeniero de sistemas en la universidad católica de Colombia, con nombre de tesis “Diagnóstico y actualización del sistema de gestión de seguridad de la información (SGSI) para ventas y servicios S.A.C”. Es

aplicada a una compañía prestadora de servicios de tercerización en Marketing Inbound como su propio nombre lo dice es la encargada de la atracción de los clientes y Marketing Outbound es la tradicional que se encarga de perseguir a los clientes, correspondiente al grupo Aval. En esta investigación se midió la seguridad de la información por ser el activo fundamental de mayor importancia dentro la compañía, la seguridad de la información a medida que va desarrollándose es indispensable aplicar nuevas medidas para el desarrollo de la información en la empresa, el autor identificó que los típicos peligros que se encontraron para los activos de información eran los desastres naturales y pillaje, al tener toda información en documentos tanto físicos como almacenada digitalmente, esto era muy difícil por lo que la información saliera de la empresa sin que nadie se fijara de su desaparición o del lugar que ha sido extraída por personal no autorizado. Para eso analizó poder neutralizar el hecho de que la información era más indefensa, se inició a ejecutar procesos y normas para el uso apropiado de la información, ofreciéndola de probables inseguridades y advertencias para sostener la continuidad del negocio y conservar la información supervisada. En el diagnóstico previo se necesita garantizar que la seguridad y la observación a los activos de información se mantienen y que se haya desarrollado en los distintos procedimientos para el uso y seguimiento de los activos de información y como instrumentos utilizar distintas herramientas tecnológicas para velar por la seguridad de la información, Net scan, Excel, Word, Power point. Finalmente, el autor como resultados obtuvo que el diagnóstico de activos de la información midió la eficacia de los procedimientos evaluados para sostener los activos de información del área servicio al cliente en este caso la in y out bound bajo un riesgo aceptable. El manejo de identificación de información mostró los activos críticos para la empresa, con el fin de constatar la ejecución de las políticas, normas y procesos definidos. Los procedimientos de implementación y ejecución de registro para manipular los riesgos de seguridad de la información fueron ordenados a sostener la confidencialidad integridad y disponibilidad de los activos de información. La implementación del plan para el manejo de la seguridad de la información en las empresas

ofrece una seguridad segura y verdadera en los sistemas de información, mejoras continuas en los distintos desarrollos, así como también aumento de la tranquilidad y confianza del usuario en la empresa. (Gonzales Sanchez, 2013)

Para Vásquez Montenegro y otros (2008), en su investigación para optar título profesional de ingeniero de sistemas en la universidad Católica Santo Toribio De Mogrovejo Chiclayo, con nombre de tesis “Elaboración y Aplicación de un sistema de Gestión de la Seguridad de la Información (SGSI) para la realidad Tecnológica de la USAT”. En esta investigación se identificó los casos que en particular se presenta en muchas empresas por el riesgo que enfrenta en su amplia variedad de fuentes, relacionando los problemas sociales como espionaje, sabotaje, vandalismo como también problemas naturales tales como incendios o inundaciones y también no dejando escapar ciertas fuentes como los daños con virus informáticos y ataques de intrusión la cual se está volviendo cada vez más comunes en las empresas, se analizó inmediatamente la solución con la elaboración y aplicación del SGSI para la aplicación de métricas según la normativa ISO 27001, esta tesis servirá de apoyo para el diagnóstico de la investigación en la que identificaron los puntos vulnerables de cada proceso y cada amenaza asociada dentro de los activos de información de la empresa ya estén relacionados con los problemas sociales, naturales e informáticos, el autor obtuvo como resumen de los resultados, posteriormente demostró haber estudiado los instrumentos para la recolección de información y herramientas en el procesamiento de la misma, el autor usó como método la entrevista, observación y encuestas, las herramientas utilizadas fueron Excel y el software SPSS quienes ofrecen muy buenas facilidades para el uso considerable de volúmenes de información y ejecutar con exactitud los análisis estadísticos confiables que ayudaron en el desarrollo, Y finalmente el autor observó por medio de los resultados la realidad que vive USAT en cuanto refiere al tema de seguridad de la información. Es estimable orientar a los estudiantes como a profesores y/o administrativos de manera que se domine un poco más vincular el tema de seguridad de la información, con el

propósito de disminuir los desfavorables que se presentan, pero no solo son los usuarios quienes deben recibir dicha preparación, debe ser publicado desde las áreas que se encuentran directamente relacionadas con el tema, ya que, el tema de seguridad es muy amplio y complejo. (Vásquez Montenegro, y otros, 2008)

Para Perafán Ruiz y otros (2014), en su investigación para optar título: Especialista en Seguridad Informática de sistemas en la universidad nacional Abierta y a Distancia situada en Popayán – Colombia, con nombre de tesis "Análisis de Riesgos de la Seguridad de la información para la Institución Universitaria Colegio Mayor del Cauca". Los autores identificaron los riesgos, amenazas y la gestión de vulnerabilidades, a partir del análisis presentando en la investigación se procede a la preparación y definición del plan de vulnerabilidades, Pentest o Ethical Hacking, El análisis de riesgo permite realizar un diagnóstico para conocer las debilidades y fortalezas internas encaminadas en la generación de los controles adecuados y normalizados dentro de las políticas de seguridad informática que hacen parte de un Sistema de Gestión de Seguridad de la Información (SGSI), además de facilitar su continuo monitoreo a través de procesos de auditorías y mejoras continuas. Posteriormente los autores se apoyaron en la metodología Magerit se desarrollaron tres procesos para el logro del proyecto "Análisis de riesgos de la seguridad de la información para la institución universitaria colegio mayor del cauca. En la valoración de los Activos lo realizaron el proceso de acuerdo a la metodología Magerit Versión 3 donde usaron las siguientes dimensiones: Disponibilidad, Integridad de los datos, Confidencialidad de la información, las utilizaron para evaluar los resultados de la materialización de una amenaza. Finalmente, los autores lograron obtener todos los propósitos programados; los registros creados que proporcionan renovar y ordenar los procedimientos de la IUCMC aplicando la noción de seguridad de la información. Aplicar la metodología MAGERIT para el análisis de riesgo es el primer paso para proteger la seguridad de los activos de información y el normal funcionamiento interno de la IUCMC. Este estudio de riesgos puede ser determinado como apoyo para la

implementación del SGSI; encaminado a: Disminuir el entorno de riesgo actual. Organizar las dimensiones de control interno obligatorias. Reducir el nivel de presentación de los sistemas que se procesan. Reforzar la confiabilidad, integridad y disponibilidad de los activos de información. Lograr reducir la inseguridad actual a su nivel mínimo. (Perafán Ruiz, y otros, 2014)

Para Adrianzén Masías (2012), en su investigación para optar título de ingeniero de sistemas en la universidad César Vallejo Piura, con nombre de tesis “Evaluación de la estructura de control interno de gestión de seguridad de la información aplicando la norma ISO 27001 a la unidad de dirección regional de transporte y comunicaciones Piura”. Este antecedente local demostró cómo se define la norma para su aplicación de tecnologías de la información y las comunicaciones la estructura de control interno aplicando una evaluación necesaria que exista garantía del adecuado funcionamiento de todos los sistemas, para eso el autor analizó y diagnosticó aplicando el estándar ISO 27001 para el procedimiento y aplicación de la normativa vigente, la población de la presente investigación lo conformaron los 20 trabajadores de la unidad de dirección regional de transporte y comunicaciones Piura, debido a que la población es muy pequeña (n<=20) se tomó a los 20 trabajadores de la Entidad mencionada. La selección de la muestra fue en base a un muestreo no probabilístico, de tipo intencional o por conveniencia; que para el caso la muestra fue el total de la población, los instrumentos que se utilizaron en la investigación fueron una ficha de observación, entrevista y una guía de reportes. En los resultados de la Tesis, el autor da a conocer los distintos entregables asociados a la norma ISO/IEC 27001, que se consideraron para el desarrollo realizado en la unidad de dirección regional de transporte y comunicaciones Piura. El autor mencionó las listas de los distintos entregables: Procedimientos para el control de documentos y registros, políticas de seguridad, plan del proyecto, documento del alcance del SGSI y plan de tratamiento de riesgos. (Adrianzén Masías , 2012)

1.3 Teorías Relacionadas al Tema

1.3.1 La norma ISO 27001

ISO 27001 se ha desarrollado con el propósito de ocuparse como molde para la organización; La implementación, operación, monitorización y mejoramiento de un Sistema de Gestión de Seguridad de la Información (SGSI) para la ejecución de cualquier empresa; Al respecto, (Cañizares, y otros, 2011) señala que, “Cada empresa tiene que proteger con tres de las características incorporadas a la información, las cuales son de mucha utilidad”. Es decir, la proposición de esta norma está enfocada a gestionar la seguridad de la información. Según (Cañizares, y otros, 2011) señala que, “La confidencialidad nos garantiza que la información es abordable solo para los usuarios que son permitidos a tener acercamiento a los activos de información”. Es decir, el respaldo de disposición a la información de los beneficiarios que se encuentran acreditados para tal exigencia. Para (Cañizares, y otros, 2011) señala que, “La integridad es el aval que la información y los procedimientos de su desarrollo no sean cambiados ni modificados de forma ilegal, además brinda localizar cómodamente las probables correcciones que se haya presentado”. Es decir, es la protección de la información completa y precisa. Finalmente, para (Cañizares, y otros, 2011) señala que, “La disponibilidad es la afirmación que los beneficiarios autorizados tienen para entrar a los activos de información cuando la necesiten”. Es decir que es el aval de que los usuarios tienen contacto a la información en el momento que se requiere.

1.3.2 La Seguridad de la Información

Es la agrupación de dimensiones advertidas y reactivas de las entidades y de los procedimientos científicos que autorizan a las empresas conceder, defender y preservar la información buscando conservar la confidencialidad, la disponibilidad e integridad de la misma. El pensamiento de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último solo se encarga de la seguridad en el entorno informático. Pero la información puede hallarse en distintos métodos o aspectos, y no solo en modos informáticos. Según (Godoy Lemus, 2014) señala que, “para

la persona como individuo, la seguridad de la información es un producto característico con relación a su privacidad, la que puede recolectar diferentes dimensiones dependiendo de la cultura del mismo". La propiedad de la seguridad de la información ha desarrollado y progresado ampliamente a partir de la segunda guerra mundial, transformándose en una carrera acreditada a nivel mundial. (Godoy Lemus, 2014)

¿Por qué es necesaria la seguridad de la información?

La información y los procedimientos que la respaldan, los sistemas y redes son fundamentales activos de la empresa. Determinar, elaborar, sostener y renovar la seguridad de la información, pueden ser importante para sostener la competitividad, flujo de liquidez, rentabilidad, cumplimiento de la legalidad e imagen comercial. (NTP ISO/IEC 17799, 2007)

1.3.3 Planificación de la Seguridad

Hoy en día el ágil progreso del ambiente técnico solicita que las empresas adopten un grupo minúsculo de registros de confianza para resguardar su información. El objetivo del plan de seguridad del sistema es otorgar una vista amplia de los requerimientos de seguridad del sistema y se detallan los controles en el lugar o los previstos para ejecutar esos requerimientos. (Galindo López, 2014)

1.3.4 Tipos de Seguridad

Es probable clasificar la seguridad en las redes en 2 tipos: Física y Lógica.

La seguridad Física: Se describe a los registros y dispositivos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto del mismo; implementados para preservar el hardware y medios de acumulación de datos. Por ejemplo: Desastres, incendios, equipamiento e inundaciones. (Arreola Illescas, 2014)

Seguridad Lógica: Consiste en la práctica de obstáculos y métodos que protegen el acercamiento a los datos y sólo se conceda permitir a ellos a las personas acreditadas para hacerlo. Por ejemplo: Controles de acceso, identificación, roles y permisos y transacciones. (Arreola Illescas, 2014)

1.3.5 Diagnóstico de la Información

"El diagnóstico de la seguridad de la información es la acción de inspeccionar y comparar los riesgos afiliados a los procedimientos del referido establecimiento y su entorno". (ISO Tools - Excellenge, 2013); Es decir que el diagnóstico de la información en la empresa es eficaz que va a permitir:

- Conocer los puntos indefensos de cada procedimiento, comprender los activos y recursos a resguardar y las amenazas asociadas sobre el diagnóstico.
- Evaluar la facilidad y existencia de los registros a la exposición de amenazas que se están desarrollando.
- Analizar la frecuencia y la seguridad de confidencialidad, integridad y disponibilidad aprobable para que la empresa pueda existir.
- Evaluar la situación actual operativa y tecnológica.
- Evaluar la capacidad de restauración frente a incidentes y la posibilidad de continuidad de los procesos de negocio por la disponibilidad en su arquitectura Tecnológica. (ISO Tools - Excellenge, 2013)

1.3.6 ¿Qué se debe Diagnosticar?

Las empresas se estructuran en sistemas con el fin de alcanzar algunos propósitos a través de la utilización de procedimientos. Al respecto, (ISO Tools - Excellenge, 2013) señala que, "Para el diagnóstico eficaz de seguridad de la información se sugiere el análisis funcional de la empresa". Para eso se considera las siguientes áreas según (ISO Tools - Excellenge, 2013)

- Sistema de gestión, planes de seguridad, políticas y base reglamentaria.
- Inventario de software, hardware y la evaluación de su valor real.
- Acceso a aplicaciones de la empresa y accesos remotos y utilización de servicios.
- Arquitectura Operativa y tecnológica.

- Seguridad física y ambiental de la edificación. (ISO Tools - Excellenge, 2013)

La eficacia del control trabajado, el importe económico, la empleabilidad y el adiestramiento del personal encargado. Para eso, (ISO Tools - Excellenge, 2013) señala que, “Todas ellas deben estar reconocidas y registradas. Así mismo, de cada una de ellas deben comprobarse distintos aspectos fundamentales vinculados con la normativa actual, la aplicabilidad al proceso verdadero de la empresa”.

1.3.7 ¿Cómo se debe realizar el diagnóstico?

El diagnóstico de la seguridad de la información sugiere un planteamiento sistematizado y por objetivos, aplicado a los principios esenciales de seguridad, análisis y de inspección. El procedimiento para arremeter el diagnóstico se puede resumir en las siguientes fases según (ISO Tools - Excellenge, 2013)

- Mostrar el programa de diagnóstico con la descripción de los objetivos, reconocimientos de activos y requerimientos, métodos a aplicar, procesos utilizables y temporalización.
- Contar con trabajadores bien preparados y competentes que sean capaces de comprobar e inspeccionar los equipos y aplicaciones informáticas, la red y el personal a cargo.
- Establecer un documento que registre evidencias, disponer el expediente solicitado, seleccionar actas y material enlazados con las pruebas realizadas.
- Mostrar un informe con los resultados del diagnóstico que reúna la identificación del sistema, el equipo encargado, las fechas de realización, los principios de evaluación y objetivos demostrados, los resultados finales, los componentes no conformes, una conclusión final y una serie de advertencias de mejora. (ISO Tools - Excellenge, 2013)

1.3.8 Los activos de información

Según (MAGERIT – versión 3.0, 2012) es el componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. No todos los activos son de la misma clase, dependiendo de la especie de activo, las amenazas y las salvaguardas, aunque en cada caso hay que adaptarse a la organización objeto del análisis según (MAGERIT – versión 3.0, 2012):

- **Datos** que materializan la información.
- **Servicios** auxiliares que se necesitan para poder organizar el sistema.
- Las **aplicaciones informáticas** (software) que permiten manejar los datos.
- Los **equipos informáticos** (hardware) y que permiten hospedar datos, aplicaciones y servicios.
- Los **soportes de información** que son dispositivos de almacenamiento de datos.
- El **equipamiento auxiliar** que complementa el material informático.
- Las **redes de comunicaciones** que permiten intercambiar datos.
- Las **personas** que explotan u operan todos los elementos anteriormente citados según (MAGERIT – versión 3.0, 2012).

1.3.9 Estándar ISO 9001

La organización internacional de estandarización ISO 9001, se adapta a los procedimientos de gestión de calidad (SGC) y que abarca en todos los componentes de administración de calidad con los que la empresa debe detallar para poseer un método objetivo que le conceda desarrollar y renovar la calidad de sus productos o servicios. (Gitek | Consultoria Empresarial, 2016)

1.3.10 Procesos Implementados en el Área QHSE

Esta certificación requiere un alto nivel de concientización y compromiso por parte de los trabajadores y empleados de la organización, es por ello que el equipo consultor realiza un seguimiento constante de la difusión, implementación de la documentación generada (políticas, objetivos, procedimientos, entre otros) e implementación de los controles de calidad y en todo el ámbito del alcance de la certificación. (Gitek | Consultoria Empresarial, 2016). En la empresa Peruana de Inspección y Servicios S.A.C (PISER S.A.C) es amplia teniendo en cuenta las operaciones de los colaboradores de campo, operaciones e indicadores diarias en el área QHSE y los procesos implementados por el estándar ISO 9001, de tal manera que se debe formar parte de todos los procesos del negocio, tanto si los procesos son manuales como automatizados, según (Cañizares, y otros, 2011) señala que, “Para proteger adecuadamente el activo información hay que dar respuesta a cuatro preguntas: QUÉ, DÓNDE, CÓMO y CUÁNDO”. Ya que esto facilita en la protección de los activos de información.

1.4 Formulación del Problema

1.4.1 Pregunta General

- ¿Cuál es el Diagnóstico de los activos de información de los procesos implementados por estándar ISO 9001 en el área QHSE basado en la norma ISO 27001?

1.4.2 Sub Preguntas

- ¿Cuáles son los activos de información asociados a los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001?
- ¿Cuáles son los indicadores de seguridad de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001?
- ¿Cómo mejorar los indicadores basados en una propuesta de controles de seguridad para los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001?

1.5 Justificación del Estudio

El diagnóstico de los activos de la información basado en la norma ISO 27001 permitió a la empresa, tener una evaluación y alcance en la frecuencia de los riesgos e incidentes de la documentación a todos los niveles dentro del área QHSE con el fin de lograr una positiva dirección y controles, de tal modo ampliar sus beneficios, acumular sus conformidades y ganar superioridad competitiva en cuanto a sus activos de información ya que es el activo fundamental en el área QHSE por sus procesos implementados.

Se desarrolló un diagnóstico para evaluar y conseguir identificar los activos de información de los procesos en el área QHSE para determinar los indicadores de seguridad según los tres pilares fundamentales de la ISO 27001 que son la confidencialidad, Integridad y disponibilidad.

Por ello el diagnóstico es eficiente en la seguridad de activos de información, es recomendable el análisis funcional de la empresa, para eso presenta el programa de "diagnóstico con la identificación de activos y recursos, definición de los objetivos, técnicas aplicar, recursos disponibles y temporalización", se presenta un informe con las conclusiones del diagnóstico que reúne "el reconocimiento de los activos de información, la determinación de sus indicadores según sus dimensiones por la norma ISO 27001, los criterios de medición y objetivos comprobados, los resultados finales y la elaboración de una propuesta de controles de seguridad para los activos de información de los procesos implementados por el estándar ISO 9001 como una conclusión final para la empresa".

En la actualidad las empresas están ligadas a trabajar con excesiva información y exigen adaptar nuevos procesos obligatorios que van de la mano con las tecnologías y que permitan conservar una información segura y muy bien protegida, es necesario tener un elevado entendimiento de la importancia e implicancia de proteger a la información en la empresa Peruana de Inspección y Servicios S.A.C.

Se procura obtener nuevos conocimientos ante las posibilidades de conocer sobre el diagnóstico a los activos de información, para formalizar con los distintos lineamientos impuestos para apropiado uso de la seguridad de los activos de información en el área QHSE. La realización de un correcto

diagnóstico en el área QHSE de la empresa PISER S.A.C es clave para una adecuada gestión, ya que proporcionará a la empresa atender correctamente a sus compromisos, además condicionalmente minimiza el descontento de terceras partes en caso de fallos de seguridad de la información, el diagnóstico permitió menos coste en la gestión de incidencias, sobre todo menos coste en la implantación global del SGSI a futuro.

1.6 Objetivos

1.6.1 Objetivo General

- Elaborar un Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.

1.6.2 Objetivos Específicos

- Identificar los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.
- Determinar los indicadores de seguridad de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.
- Elaborar una propuesta de controles de seguridad para los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.

II. MÉTODO

2.1 Diseño de Investigación

2.1.1 No Experimental:

Porque sólo se busca describir las características de la variable del estudio tal como se muestra en la realidad, que se detalla una condición o situación del mundo real que puede afectar a un activo de información en la organización.

2.1.2 Tipo de Estudio

Investigación Descriptiva:

Es descriptiva porque se busca determinar las características de la seguridad que poseen los activos de información, describiendo su frecuencia y porcentaje en incidentes, amenazas y vulnerabilidades que se han dispuesto.

2.2 Cuadro de Operacionalización:

VAR.	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	DATOS	INST.	FUENTE DE INFORMACIÓN
Variable: Activos de Información del Área QHSE	"La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Esto es muy importante en el creciente del ambiente interconectado de negocios. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades". (NTP ISO/IEC 17799, 2007)	Esta variable será medida a través de cuestionarios y listas de cotejo para determinar los indicadores de seguridad según los tres pilares fundamentales de la norma ISO 27001 que son Confidencialidad, integridad y disponibilidad.	Confidencialidad	Nivel de frecuencia de incidentes de acceso indebido a los documentos del SGC.	Incidentes de acceso indebido.	Cuestionario Lista de Cotejo	Supervisor QHSE, Asistente QHSE, Supervisor de Logística e Informática, Gerencia -RR.HH
				Incidentes de accesos indebidos a la información más comunes del SGC.	Accesos indebidos más comunes.		
				Nivel de distribución de copias controladas del SGC.	Distribuciones controladas		
				Nivel de distribución de copias no controladas del SGC.	Distribuciones no controladas.		
				Medios de fuga de información del SGC en el área QHSE.	Equipos portátiles.		
				Porcentaje de soportes de información que más se utiliza en el SGC.	Soportes de información.		
			Integridad	Incidentes de impacto en la integridad de los documentos más comunes del SGC.	Incidentes de impacto a la integridad más comunes	Cuestionario Lista de Cotejo	
				Nivel de frecuencia de incidentes de impacto en la integridad de los documentos del SGC.	Incidentes de impacto en la integridad.		
				Nivel de la integridad en la elaboración de documentos y control de versiones.	Documentos y control de versiones.		
			Disponibilidad	Respaldos electrónicos del SGC disponibles en el área QHSE.	Respaldos electrónicos	Cuestionario Lista de Cotejo	
				Incidentes de impacto en la disponibilidad de los documentos más comunes del SGC.	Disponibilidad de documentos comunes del SGC.		
				Vectores de pérdida de la disponibilidad de la información del SGC.	Vectores de pérdida de disponibilidad de información.		

Elaboración: Propia

2.3 Población y Muestra

Indicadores	Unidad de Análisis	Población/Muestra	Fuente de Información
Nivel de frecuencia de incidentes de acceso indebido a los documentos del SGC.	-Accesos a documentos. -Accesos a computadoras. -Fuga de información.	**Población** -Periodo Setiembre.	-Supervisor QHSE. -Gerencia. -RRHH. -Supervisor de Logística e informática.
Incidentes de accesos indebidos a la información más comunes del SGC.	- Fuga de información comercial y administrativa. - Accesos a manuales, procedimientos, documentación técnica, etc.	**Población** -Todas personas autorizadas.	-RRHH -Supervisor QHSE.
Nivel de distribución de copias controladas del SGC.	- Copias controladas distribuidas a personal interno y externo a la empresa.	**Población** -Todas distribuciones controladas de la documentación.	-Supervisor QHSE.
Nivel de distribución de copias no controladas del SGC.	- Copias no controladas distribuidas a personal interno y externo a la empresa.	**Población** -Todas distribuciones no controladas de la documentación.	-Supervisor QHSE.
Medios de fuga de información del SGC en el área QHSE.	- Laptops. - Notebooks. - Tablets.	**Población** -Todos los equipos portátiles en el área QHSE.	-Supervisor QHSE. -Gerencia. -Supervisor de Logística e informática.
Porcentaje de soportes de información que más se usa en el área QHSE.	- Discos duros externos. - Memorias USB. - Equipo de escritorio.	**Población** -Todos los medios removibles en el área QHSE.	-Supervisor QHSE. -Supervisor de Logística e informática.

Elaboración: Propia

Indicadores	Unidad de Análisis	Población/Muestra	Fuente de Información
Incidentes de impacto en la integridad de los documentos más comunes del SGC.	- Correcciones. - Cambios de versión. - Nuevos documentos.	**Población** -Todos los cambios en los documentos en el área QHSE.	-Supervisor QHSE.
Nivel de frecuencia de incidentes de impacto en la integridad de los documentos del SGC.	- Destrucción de documentos. - Corrupción de información. - Daños físicos.	**Población** -Periodo Setiembre.	-Supervisor QHSE. -Gerencia. -RRHH. -Supervisor de Logística e informática.
Nivel de la integridad en la elaboración de documentos y control de versiones.	- Equipos informáticos. - Discos duros externos. - Soportes físicos. - Equipamiento auxiliar.	**Población** -Todos los medios de soporte de los documentos.	-Supervisor QHSE. -Asistente QHSE. -Gerencia. -Supervisor de Logística e informática.
Respaldos electrónicos del SGC disponibles en el área QHSE.	-Copias de respaldo en el área QHSE.	**Población** -Todos los respaldos en el área QHSE.	-Supervisor QHSE. -Asistente QHSE. -Supervisor de Log. e Informática.
Incidentes de impacto en la disponibilidad de los documentos más comunes del SGC.	- Pérdida de documentos físicos. - Indisponibilidad de documentos por caída de servicios. - Indisponibilidad de soportes de información.	**Población** -Todos los incidentes de impacto en la disponibilidad de los documentos.	-Supervisor QHSE. -Asistente QHSE. -Gerencia. -Supervisor de Logística e informática.
Vectores de pérdida de la disponibilidad de la información del SGC.	- Procedimientos y controles del SGC. - Limitaciones de tecnología. - Exceso de confianza.	**Población** -Todos los incidentes de pérdida de documentación en equipos informáticos en el área QHSE.	-Supervisor QHSE. -Asistente QHSE. -Supervisor de Logística e informática.

Elaboración: Propia

2.4. Técnicas e Instrumentos de Recolección de datos, validez y confiabilidad

Técnicas	Instrumentos
Encuestas	Cuestionarios
Observación	Lista de cotejo

2.5 Métodos de Análisis de Datos

2.5.1 Análisis Descriptivos

De acuerdo a la proporción de la variable de análisis, se hizo la evaluación a los resultados en gráficos de barras o tablas de frecuencia según sea la condición de la variable.

2.6 Aspectos Éticos

El autor de dicho proyecto se compromete lealmente a respetar y obedecer la formalidad de los resultados obtenidos, la confiabilidad de la información proporcionada por el área QHSE de la empresa PISER SAC. Y la identificación de las personas que participan en la investigación.

III. RESULTADOS
3.1 Análisis Descriptivo de Datos

En esta parte se presentan los resultados obtenidos de los instrumentos de evaluación a los activos de información, realizada al Supervisor QHSE, Asistente QHSE, Supervisor De logística e Informática, Gerencia y Recursos Humanos de la empresa PISER S.A.C. Los modelos de instrumentos y los gráficos de análisis se pueden apreciar en el Anexo N° 01 y Anexo N°02.

3.1.1 Resultados de análisis de Indicadores de Confidencialidad

En la pregunta 01 de la encuesta, se obtuvo que el nivel de compromiso de los colaboradores por preservar la confidencialidad de los activos de información, es bajo con un porcentaje de 57% demostrándose poco compromiso con la confidencialidad de la información, seguidamente con el 29% afirmó que existe un compromiso relativamente medio y finalmente se detectó que el 14% del personal indica que no aplica o no asume un nivel de compromiso de confidencialidad, es decir, este es nulo.

En la pregunta 02 de la encuesta, se mostró que el 55% estimó que el área de logística e informática es la que establece los controles de seguridad de la información, seguidamente el 27% estimó que es gerencia y/o alta dirección la que establece los controles de seguridad y por último con el 18% reveló que el área QHSE es la que establece los controles de seguridad de la información.

En la pregunta 03 del indicador: **Incidentes de accesos indebidos a la información más comunes del SGC**, se identificó tres incidentes más comunes de accesos indebidos de la información donde también se indicó su porcentaje, el primer incidente de acceso más común y con un porcentaje de 58% es la fuga de documentación especializada: manuales, procedimientos, documentación técnica, etc. El segundo acceso indebido es por las incidencias en información de carácter personal la cual su porcentaje que evidenció es de 33% y finalmente como último incidente de acceso indebido más común del SGC es por la fuga de información comercial y administrativa la cual reveló un porcentaje de 8% por los colaboradores.

En la pregunta 04 del indicador: **Medios de fuga de información del SGC en el área QHSE,** se reveló que el 30% de los colaboradores estimó que uno de los

medios de fuga del SGC es la computadora portátil por ser un soporte de información confidencial de amplio almacenamiento, con el 25% de medio de fuga se identificó los dispositivos USB, posteriormente tal como se mostró en la figura el 20% de medios de fuga es el correo electrónico institucional, por debajo con el 15% según los colaboradores indicaron que son los medios removibles y con el 5% se contempló como medio de fuga el correo electrónico personal y finalmente otro con 5% indicaron que son otros los medios de fuga.

En la pregunta 05 de la encuesta, se afirmó que el 64% de los colaboradores el principal vector de fuga de información del SGC es por el exceso de confianza, seguidamente se notó que el 18% es por la deshonestidad / intereses económicos, por debajo con el 9% se mostró que es por las motivaciones personales y/o laborales y finalmente al igual con un 9% se estimó que los vectores de fuga son otros.

En la pregunta 06 del indicador: **Nivel de frecuencia de incidentes de acceso indebido a los documentos del SGC**, se observó que el nivel de frecuencia de incidentes es entre media y alta ya que la suma de los dos niveles es de 72%, la cual la frecuencia en número es más de 6 veces y mayor de 10 en el mes de Septiembre y por debajo con el 14% se evidenció que la frecuencia de incidentes sea no mayor a 5, la cual hace que el nivel sea considerada como baja y por último se mostró que el 14% desconoce completamente esa información.

En la pregunta 07 de la encuesta, se obtuvo que el 71% estimó que las personas autorizadas a la información confidencial del SGC son del área QHSE y otras áreas estratégicas y operativas, la cual hace que el nivel de confidencialidad sea media, se mostró también que el 14% estimó que las personas autorizadas con acceso a la documentación es solo el área de QHSE, la cual se estimó que el nivel de confidencialidad es controlada y por último se identificó al igual con el 14% se reveló que los accesos a la información del SGC es de toda la institución, la cual hace que el nivel de confidencialidad a la información sea alta.

En la pregunta 08 del indicador: **Nivel de distribución de copias controladas del SGC**, se obtuvo que el 57% de los colaboradores estimó que se distribuyen solo copias controladas del SGC teniendo como respaldo de seguridad un formato de

control de entrega de documentos, la cual hace que el nivel de distribución de copias sea controlado.

En el indicador: **Nivel de distribución de copias no controladas del SGC**, se identificó que el 43% de los colaboradores estimó que actualmente no existe control de distribución de copias no controladas del SGC ni cuentan con algún formato que respalde la entrega de copias no controladas, la cual hace que el nivel de distribución de copias sea no controlado.

En la pregunta 09 del indicador: **Porcentaje de soportes de información que más se utiliza en el SGC**, se observó que los soportes de información son fijos y movibles, donde el 20% estimó que son los equipos de escritorio y en la suma del porcentaje de los soportes de información movibles se demostró que son los que más se utilizan en el SGC donde se obtuvo que el 72% es por los equipos portátiles, memorias USB y posteriormente los discos duros y otros medios removibles, finalmente con el 8% se detectó que son otros los recursos de soporte de información que más se utiliza.

3.1.2 Resultados de Indicadores de Integridad

En la pregunta 01 de la encuesta, se destacó que el 57% de los colaboradores reveló que se demuestra poco compromiso con la integridad de la información, la cual hace que el nivel de compromiso de la integridad sea baja, se mostró también que el 29% estimó que no se aplica ni es asumido por los colaboradores, la cual hace que su nivel de compromiso de integridad no exista y sea considerado como nulo y por debajo con el 14% se confirmó que existe un compromiso relativamente, la cual hace que su nivel de compromiso por preservar la integridad sea media.

En la pregunta 02 del indicador: **Incidentes de impacto en la integridad de los documentos más comunes del SGC**, se identificó cuatro incidentes más comunes de accesos indebidos a los documentos, donde también se ratificó su porcentaje, el primer incidente de acceso más común y con un porcentaje de 35% es por los errores en el control de versiones, se reveló también dos incidentes de impacto en la integridad ambas con un mismo porcentaje de 29% donde el segundo incidente es por el deterioro de documentos físicos y el tercer incidente con el mismo porcentaje es por la manipulación / adulteración de los registros de información y

por último y cuarto incidente es por el deterioro de documentos electrónicos con un porcentaje de 6% que reveló los colaboradores.

En la pregunta 03 de la encuesta, se confirmó que el 45% estimó que el principal vector de pérdida de integridad de la información es por las limitaciones en la tecnología, seguidamente con 27% estimó que es por exceso de confianza, por debajo se mostró con 18% se estimó que es por la debilidad de procedimientos y controles, por último, con el 9% se obtuvo que son otros los vectores de pérdida de integridad de la información del SGC.

En la pregunta 04 del indicador: **Nivel de frecuencia de incidentes de impacto en la integridad de los documentos del SGC**, se observó que el nivel de incidentes de impacto en la integridad es entre baja y media ya que la suma es el 85% de los colaboradores, la cual la frecuencia en número es más de 1 y no mayor de 10 veces en el mes de Setiembre y por debajo con el 14% desconoce completamente sobre el impacto de la integridad de los documentos.

En la pregunta 05 del indicador: **Nivel de la integridad en la elaboración de documentos y control de versiones,** se detectó que el 57% estimó que algunas veces se presentan inconvenientes de control de versiones, la cual hace que el nivel de la integridad en el control de versiones sea media, seguidamente con el 29% estimó que existen procedimientos para la elaboración de documentos y control de versiones, eso reveló que el nivel de integridad es controlada y finalmente por debajo con el 14% estimó que frecuentemente hay inconvenientes en el control de versiones, la cual demostró que el nivel de integridad es baja.

En la pregunta 06 de la encuesta, se constató que el soporte físico impreso y los soportes de backup en medios externos, ambos soportes de integridad de información tienen un igual porcentaje de 25% de los colaboradores y con el 17% se estimó que están los soportes electrónicos de PC´s, Soporte en servidor de activos y discos duros y otros medios removibles.

3.1.3 Resultados de Indicadores de Disponibilidad

En la pregunta 01 de la encuesta, se obtuvo que el 57% estimó que existe un compromiso relativamente, la cual se mostró que el nivel de compromiso por preservar la disponibilidad de la información es medio, seguidamente con el 29%

indicó poco compromiso con la disponibilidad de la información, la cual hace que el nivel de compromiso sea bajo y finalmente por debajo con el 14% se destacó que existe un alto compromiso por preservar la disponibilidad.

En la pregunta 02 del indicador: **Incidentes de impacto en la disponibilidad de los documentos más comunes del SGC**, se identificó dos incidentes más comunes en la disponibilidad a los documentos, donde también se obtuvo su porcentaje, el primer incidente de impacto en la disponibilidad más común y con un porcentaje de 50% es por la indisponibilidad de servidores en la empresa, se reveló también que el segundo incidente de impacto en la disponibilidad es por la pérdida de documentos físicos con un porcentaje de 30%, seguidamente con el 10% se afirmó que desconoce este proceso y por último también con el 10% otros son los incidentes de impacto en la disponibilidad.

En la pregunta 03 del indicador: **Vectores de pérdida de la disponibilidad de la información del SGC**, se obtuvo que el 38% estimó que los vectores de pérdida de la disponibilidad son las limitaciones en la tecnología, seguidamente con el 31% es por la debilidad de procedimientos y controles, también se notó que el 25% es por el exceso de confianza que existe en la empresa y finalmente con el 6% reveló que es por la deshonestidad / rivalidades personales / cultura organizacional.

En la pregunta 04 de la encuesta, se obtuvo que el 71% de los colaboradores el nivel de incidentes de impacto de la disponibilidad, la cual se mostró la frecuencia en número ser más de 6 veces y no mayor de 10 y por debajo con el 14% se evidenció que la frecuencia en número de incidentes sea mayor de 1 y menor de 5 veces, la cual hace que el nivel sea considerado como baja y por último se obtuvo que el 14% desconoce completamente esa información.

En la pregunta 05 del indicador: **Respaldos electrónicos del SGC disponibles en el área QHSE**, se obtuvo que el 70% de los colaboradores estimó que los respaldos electrónicos en el área QHSE es por el uso de discos duros y otros medios removibles, también se observó que el 20% es por copias de respaldo en CD / DVD, finalmente con el 10% otros son los tipos de copias de respaldo lo que hace que sean disponibles en el área QHSE.

IV. DISCUSIÓN

Según lo mencionado por Gonzales Sánchez (2013), este autor obtuvo como resultados los procesos de identificación de información lo cual evidenció los activos críticos para la organización, con el fin de controlar el cumplimiento de las políticas, normas y procedimientos definidos de los procesos de implementación y operación de controles para manejar los riesgos de seguridad de la información fueron orientados a mantener la confidencialidad integridad y disponibilidad de los activos de información. Todos esos resultados fueron identificados por el SGSI, dado que sirvió en la investigación como aporte para el manejo de la seguridad que pueda existir en el área QHSE, obteniendo como resultado en la investigación que la documentación del SGC podría ser usada por otras personas ajenas a el área de QHSE y áreas estratégicas, la documentación del SGC está soportada principalmente en medios físicos (documentación impresa) y en medios externos. Según (ISO Tools - Excellenge, 2013) “El diagnóstico de la seguridad de la información es la acción de inspeccionar los riesgos afiliados a los procedimientos del referido establecimiento y su entorno” dado que fuese el caso que no se inspeccionen como en el área QHSE es válido el resultado por la investigación dado que se identificó una lista de debilidades en la seguridad de la información, es por eso que dentro de los objetivos de la investigación se ha propuesto elaborar un plan de controles de seguridad a fin de superarlas y desarrollar una cultura de seguridad de información que contribuya a proteger los activos de información del SGC en el área QHSE.

Según lo indicado por Vásquez Montenegro y otros (2008), obtuvieron resultados que en particular se presenta en muchas empresas por el riesgo que enfrenta en su amplia variedad de fuentes, relacionando los problemas sociales como espionaje, sabotaje, vandalismo como también no dejando escapar ciertas fuentes como los daños con virus informáticos y ataques de intrusión a los soportes de información, la cual se está volviendo cada vez más comunes en las empresas, según (Galindo López, 2014) señala que hoy en día el ágil progreso del ambiente técnico solicita que las empresas adopten un grupo minúsculo de registros de confianza para resguardar su información. El objetivo del plan de seguridad del sistema es otorgar una vista amplia de los requerimientos de seguridad del sistema

y se detallan los controles en el lugar o los previstos para ejecutar esos requerimientos. Por otro lado basado en el diagnóstico se ha obtenido como resultado que los principales vectores de fuga de la información existe el exceso de confianza por los colaboradores, lo cual demostró que es el que mayor incidencia tiene, relacionándolo como uno de los problemas sociales del antecedente anteriormente nombrado, también se mostró que existen inconvenientes relacionados con la indisponibilidad de servidores y sistemas de información la cual hace que genere espionaje, sabotaje en los procesos implementados del SGC, aplicando según la teoría nombrada que las empresas tienen que adoptar un grupo minúsculo de registros de confianza para resguardar su información, identificando en el área QHSE que solo cuenta con un registro de control de documentos de copia controlada por parte del estándar ISO 9001, es por eso que dentro de los controles de seguridad como alternativa se realizaron registros propuestos para cada dimensión según los tres pilares de la norma ISO 27001 ya que el objetivo del plan de seguridad del sistema es otorgar una vista amplia de los requerimientos de seguridad en el SGC.

Según lo nombrado por Perafán Ruiz y otros (2014), obtuvieron resultados a través del diagnóstico donde identificó las debilidades de los riesgos y amenazas y la gestión de vulnerabilidades, a partir del análisis presentando en la investigación se procede a la preparación y definición del plan de vulnerabilidades, dado el antecedente en este caso se procedió hacer el diagnóstico en los procesos implementados del estándar ISO 9001 ya que la documentación del SGC está soportada principalmente en medio físicos (documentación impresa) y en medios externos, constatando que es una de las principales debilidades en cuanto a la seguridad de la información, según (Godoy Lemus, 2014) señala que, “para la persona como individuo, la seguridad de la información es un producto característico con relación a su privacidad, la que puede recolectar diferentes dimensiones dependiendo de la cultura del mismo”, es por eso que parte de la propuesta como beneficio en la investigación dentro de los controles de seguridad según la norma ISO 27001, está recomendado el respaldo de la información del SGC para mitigar riesgos de pérdida de integridad y disponibilidad de la información en el SGC, dando mérito a la teoría una de las alternativas dentro de los controles

de seguridad es desarrollar programas de sensibilización difusión de la política y lineamientos de seguridad de la información, ya que todo parte de una cultura de concientización de cada colaborador para un mejor manejo en la seguridad de la información.

En la investigación de la dimensión de confidencialidad se obtuvo un nivel de compromiso bajo por preservar dicha dimensión demostrándose poco compromiso por parte de los colaboradores. Según (Cañizares, y otros, 2011) señala que, “La confidencialidad nos garantiza que la información es abordable solo para los usuarios que son permitidos a tener acercamiento a los activos de información”. Eso quiere decir que el apoyo de distribución a la información es solo para los usuarios que se encuentran favorecidos para tal requerimiento. Demostrándose con otro de los resultados es que las personas autorizadas a la información confidencial del SGC son del área QHSE y otras áreas estratégicas y operativas, lo cual hace que el nivel de confidencialidad sea medio. Al respecto, (Cañizares, y otros, 2011) señala que, “Cada empresa tiene que proteger con tres de las características incorporadas a la información, las cuales son de mucha utilidad”. Es decir, la proposición de esta norma está enfocada a gestionar la seguridad de la información. La norma ISO 27001 brinda la referencia de los controles de seguridad tales que se adecuan a la empresa, dentro de ellos para la dimensión de confidencialidad no significaría implementarse un control de reconocimiento biométrico para el ingreso a las instalaciones del área QHSE si solo son pocos los involucrados, pero tampoco significa que deba estar insegura para eso al menos se debe tener un control en la entrada que impida el ingreso de personal extraño a instalaciones del SGC o que firme el formato de acuerdo de la confidencialidad.

V. CONCLUSIONES

1. Con la culminación de la presente investigación se elaboró el diagnóstico de los activos de información de los procesos implementados, revelando que existe la percepción de un alto número de incidentes de fuga y acceso indebido a la información, y también existe una cantidad relativamente alta de equipos portátiles usándose en el área QHSE sin ningún control alguno por parte del personal autorizado.
2. Dadas las reuniones con el responsable de la certificación del estándar ISO 9001, se puedo identificar los activos de información, actualizando y verificando a través de las listas maestras de documentos internos y externos, listas maestras de registros del SGC y finalmente se obtuvo un único formato de control de entrega de documentos, todo eso por parte del estándar ISO 9001, constatando cada documento con firma y sello del supervisor QHSE para su respectiva validez y aprovechamiento en el diagnóstico.
3. Mediante la investigación se pudo determinar los indicadores de seguridad que presentan inconvenientes en el área QHSE, enlazados con la indisponibilidad de servidores y sistemas de información, por lo que es necesario mejorar los mecanismos preventivos y correctivos de soporte, así como los mecanismos de contingencia de seguridad de la información.
4. Por último el diagnóstico de los activos de información es fundamental ya que nos hace dominar las principales debilidades obtenidas en la investigación donde se mostró que existe un bajo compromiso con la seguridad de la información, otra debilidad es que la documentación del SGC podría ser usada por otras personas ajenas a el área QHSE y áreas estratégicas, finalmente los controles de seguridad son a fin de superarlas y proponer una cultura de seguridad de información que contribuya a proteger los activos de información del SGC.

VI. RECOMENDACIONES

1. Se realizó el Diagnóstico de los activos de información a los procesos implementados por el estándar ISO 9001, dado como investigación adicional es realizar una evaluación más exhaustiva, donde se podría utilizar los enfoques como la norma ISO 27005, Magerit o algún otro enfoque metodológico orientado específicamente a la gestión y tratamiento de riesgos.
2. Por la limitación de tiempo, solo se diagnosticaron los procesos implementados en el área QHSE, por lo que se sugiere que, basado en la metodología utilizada en esta tesis, se puede hacer un diagnóstico y tratamientos de riesgos a todas las áreas de la empresa PISER S.A.C, la cual estaría a favor de su desarrollo y crecimiento en cuanto a la seguridad de su información, ya que daría un golpe a todas las posibles amenazas que se puedan presentar.
3. Después de realizarse el diagnóstico, es aconsejable como una investigación complementaria seguir apropiadamente con la implementación del SGSI, ya que toda implementación como primordial requisito se requiere de un diagnóstico como base actual de situación de la empresa a la que se requiere dicho estándar, en el cual se empleen estándares y sean aprobadas, actualmente existen varias herramientas de buenas prácticas como ITIL para la implementación de un SGSI.
4. Es recomendable y fundamental aplicar estándares y buenas prácticas de guía, la implementación va a obedecer de las exigencias de la empresa. Destacando que estos estándares y procedimientos indican que es aquello que se debe controlar, pero no indica el cómo.

VII. PROPUESTA

CONTROLES DE SEGURIDAD BASADO A LA NORMA ISO 27001

Objeto y campo de aplicación

“Esta Norma Técnica Peruana especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la información”. (NTP-ISO/IEC 27001, 2014)

Referencias Normativas

Los siguientes documentos, en parte o en su totalidad, se referencian normativamente en este documento y son indispensables para su aplicación. (NTP-ISO/IEC 27001, 2014)

Controles de seguridad

Los controles de seguridad son políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos. (NTP-ISO/IEC 27001, 2014)

Anexo A (Normativo)

“Los objetivos de control y controles listados en la tabla A.1 son directamente derivados y alineados con los listados en ISO/IEC 27001 – 27002:2013”. (Vásquez Montenegro, y otros, 2008)

Objetivos de control y controles de seguridad:

Según (NTP-ISO/IEC 27001, 2014) **los controles de referencia son definidos:**

A.5 Política de seguridad de la información

A.5.1 Dirección de la gerencia para la seguridad de la información.

A.5.1.2 Revisión de las políticas para la seguridad de la información.

A.6 Organización de la seguridad de la información

A.6.1 Dispositivos móviles y teletrabajo.

A.6.1.1 Política de dispositivos móviles.

A.7 Seguridad de los recursos humanos

A.7.1 Antes del empleo

A.7.1.1 Selección.

A.7.2 Durante el empleo

A.7.2.1 Conciencia, educación y capacitación sobre la seguridad de la información.

A.7.2.2 Proceso disciplinario

A.7.3 Terminación y cambio de empleo

A.7.3.1 Terminación o cambio de responsabilidades del empleo.

A.8 Gestión de activos

A.8.1 Responsabilidad por los activos

A.8.1.1 Inventario de activos.

A.8.2.1 Clasificación de la información.

A.8.3 Manejo de los medios

A.8.3.1 Gestión de medios removibles.

A.9 Control de acceso

A.9.1 Requisitos de la empresa para el control de acceso

A.9.1.1 Política de control de acceso.

A.9.2 Gestión de acceso de usuario

A.9.2.1 Registro y baja de usuarios.

A.9.3 Control de acceso a sistemas y aplicación

A.9.3.1 Restricción de acceso a la información.

A.10 Seguridad física y ambiental

A.10.1 Áreas seguras

A.10.1.1 Controles de ingreso físico.

A.10.1.2 Protección contra amenazas externas y ambientales.

A.10.1.3 Trabajo en áreas seguras.

A.11 Equipos

A.11.1 Emplazamiento y protección de los equipos

A.11.1.2 Servicios de suministro.

A.11.1.3 Mantenimiento de equipo.

A.12 Seguridad de las operaciones

A.12.1 Procedimientos y responsabilidades operativas

A.12.1.1 Procedimientos operativos documentales.

A.12.2 Respaldo

A.12.2.1 Respaldo de la información.

A.14. Gestión de incidentes de seguridad de la información

A.14.1 Gestión de incidentes de seguridad de la información y mejoras

A.14.1.2 Reporte de las debilidades de seguridad de la información.

A.15 Cumplimiento

A.15.1 Cumplimiento de requisitos legales y contractuales

A.15.1.2 Protección de los registros.

A.15.2 Revisiones de seguridad de la información

A.15.1.3 Cumplimiento de políticas y normas de seguridad. (NTP-ISO/IEC 27001, 2014)

VIII. REFERENCIAS

Adrianzén Masías , Miguel. 2012. *Evaluación de la estructura de control interno de gestión de seguridad de la información aplicando la norma ISO 27001 a la unidad de dirección regional de transporte y comunicaciones Piura.* Piura : s.n., 2012.

Alonzo Mendoza, Sara E. 2014. Segunda Cohorte del Doctorado en Seguridad Estratégica. Primera. s.l. : Consejo Editorial Guatemala, 2014.

Arreola Illescas, Saúl D. 2014. Segunda Cohorte del Doctorado en Seguridad Estratégico. Guatemala : Carolina Villatoro, 2014.

Brochure PISER. 2016. 2016.

BSI - Guia de Transicion - ISO 27001:2013 . BSI. Group Mexico S de RL de CV. [En línea] http://www.bsigroup.com/LocalFiles/es-MX/ISO%20IEC%2027001/Gu%C3%ADa%20de%20Transici%C3%B3n_ISO27001.pdf.

Cañizares, Ricardo y Merino, Cristina. 2011. *Implantacion de un Sistema de Gestion de Seguridad de la Informacion segun ISO 27001.* España : FC EDITORIAL, 2011. pág. 292. ISBN/978-84-92735-87-7.

Galindo López, Celvin Manolo. 2014. Segunda Cohorte del Doctorado en Seguridad Estratégica. Guatemala : Carolina Villatoro, 2014, Vol. I.

Gitek | Consultoria Empresarial. 2016. *Avance de consulturia de implementacion de un sistema de gestion de calidad basado en la norma ISO 9001 : 2008.* 2016.

Godoy Lemus, Rodolfo. 2014. Segunda Cohorte del Doctorado en Seguridad Estratégica. Guatemala : Carolina Villatoro, 2014, Vol. I.

Gonzales Sanchez, Frank Jonathan. 2013. http://repository.ucatolica.edu.co/jspui/bitstream/10983/866/2/Manten. [En línea] 2013. http://cip.org.pe/imagenes/temp/tesis/42464064.doc?.

ISO Tools - Excellenge. 2013. [En línea] 2013. http://www.isotools.org/normas/riesgos-y-seguridad/iso-27001.

MAGERIT – versión 3.0. 2012. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. [En línea] 2012. http://docslide.us/documents/libroimetodopdf.html?. NIPO: 630-12-171-8.

Manual de Organización y Funciones. 2016. *Manual de Organización y Funciones .* 2016.

NTP ISO/IEC 17799. 2007. [En línea] 2da Edición, 16 de 01 de 2007. http://www.ongei.gob.pe/normas/0/NORMA_0_RESOLUCI%C3%93N%20MINISTERIAL%20N%C2%BA%20246-2007-PCM.pdf.

NTP-ISO/IEC 27001. 2014. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. [En línea] 20 de Noviembre de 2014. http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf. I.C.S: 35.040.

Perafán Ruiz, John Jairo y Caicedo, Cuchimba Mildred. 2014. [En línea] 2014. http://repository.unad.edu.co/bitstream/10596/2655/3/76327474.pdf.

PISER S.A.C. 2014. [En línea] 2014. http://www.piser.com.pe/nosotros.html.

TECNETCOM. 2005. TECNOLOGÍAS INFORMÁTICAS DE COSTA RICA. [En línea] 2005. http://www.tecnetcom.com/index.php?option=com_content&task=view&id=22&Itemid=45.

Vásquez Montenegro, Juan Carlos y De La Cruz Guerrero, César Wenceslao. 2008. [En línea] 2008. cip.org.pe/imagenes/temp/tesis/42464064.doc.

ANEXOS

Anexo N°01: Técnicas e instrumentos de recolección de Datos.

PISER S.A.C.

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

CUESTIONARIO DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Nombre:
Cargo:
Área:

FORMULARIO N° 01: CONFIDENCIALIDAD DE LOS ACTIVOS DE INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa a escoger
Objetivo: Determinar los indicadores de seguridad de Confidencialidad
Elaboración: Propia

01) ¿Existe compromiso por preservar la confidencialidad de la información del SGC?

- **a)** ☐ Alto: Existe un alto compromiso
- **b)** ☐ Medio: Existe un compromiso relativamente medio
- **c)** ☐ Bajo: Se demuestra poco compromiso con la confidencialidad de la información
- **d)** ☐ Nulo: No se aplica ni es asumido por los colaboradores
- **e)** ☐ Adverso: La confidencialidad de la información se percibe como una limitación al trabajo

Comente si considera necesario

02) ¿Qué área establece los controles de seguridad de la información del SGC?

- **a)** ☐ Gerencia y/o Alta Dirección
- **b)** ☐ Logística e Informática
- **c)** ☐ QHSE
- **d)** ☐ Otros:

Comente si considera necesario

03) Señale los incidentes de accesos indebidos a la información que son más comunes del SGC
Si es necesario marque más de una alternativa

- **a)** ☐ Fuga de documentación especializada: manuales, procedimientos, documentación técnica, etc.
- **b)** ☐ Fuga de información comercial y administrativa
- **c)** ☐ Espionaje industrial de la competencia
- **d)** ☐ Incidencias en información de carácter personal
- **e)** ☐ Otros
- **f)** ☐ Desconozco este proceso

Comente si considera necesario

Formulario N° 01: Confidencialidad de los Activos de Información
Elaboración: Propia

PISER

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

CUESTIONARIO DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

04) Señale los principales medios de fuga de información del SGC en el área QHSE

Si es necesario marque más de una alternativa

- **a)** ☐ Correo electrónico institucional
- **b)** ☐ Correo electrónico personal
- **c)** ☐ Dispositivos USB
- **d)** ☐ Computadora portátil
- **e)** ☐ Medios removibles
- **f)** ☐ Otros

Comente si considera necesario

05) Señale los principales vectores de fuga de información del SGC

Si es necesario marque más de una alternativa

- **a)** ☐ Motivaciones personales, profesionales y/o laborales
- **b)** ☐ Deshonestidad / Intereses económicos
- **c)** ☐ Desconocimiento / Falta de conciencia
- **d)** ☐ Exceso de confianza
- **e)** ☐ Otros

Comente si considera necesario

06) Estime la frecuencia de incidentes de acceso indebido a los documentos del SGC del periodo de Septiembre

- **a)** ☐ Baja: Entre 1 y 5
- **b)** ☐ Media: Entre 6 y 10
- **c)** ☐ Alta: Más de 10
- **d)** ☐ Desconozco completamente esta información

Señale un número estimado:

Comente si considera necesario:

07) Señale el nivel de confidencialidad de las personas con acceso a la información del SGC

- **a)** ☐ Controlada: Solo el área de QHSE
- **b)** ☐ Media: Area de QHSE y otras áreas estratégicas y operativas
- **c)** ☐ Alta: Toda la institución
- **d)** ☐ Extrema: Es información de dominio público

Señale un número estimado de personas:

Comente si considera necesario:

Formulario N° 01: Confidencialidad de los Activos de Información
Elaboración: Propia

PISER S.A.C.

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

CUESTIONARIO DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

08) Evalúe el nivel de distribución de documentos de copias controladas y no controladas del SGC

Si no se cuenta con formato para el control de copia no controlada marque la alternativa

a)		Controlada: Se distribuyen solo copias controladas
b)		Media: Algunas veces se distribuyen copias no controladas
c)		Baja: Se distribuyen solo copias no controladas
d)		No controlada: Actualmente no existe control de distribución

Estime un número de distribución de copias controladas:

Estime un número de distribución de copias no controladas:

Comente si considera necesario:

09) Señale los principales soportes de información que más se utiliza en el SGC

a)		Equipos de Escritorio.	N°	
b)		Equipos Portátiles	N°	
c)		Memorias USB	N°	
d)		Discos duros y otros medios removibles	N°	
e)		Otros:	N°	

Comente si considera necesario:

10) Señale los principales riesgos asociados a la confidencialidad de la documentación del SGC:

N°	Riesgo	Proceso

Formulario N° 01: Confidencialidad de los Activos de Información
Elaboración: Propia

PISER

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

CUESTIONARIO DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Nombre:

PISER

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

04) Estime el nivel de frecuencia de incidentes de impacto en la integridad de los documentos del SGC en el periodo de Sep

- **a)** ☐ Baja: Entre 1 y 5
- **b)** ☐ Media: Entre 6 y 10
- **c)** ☐ Alta: Más de 10
- **d)** ☐ Desconozco completamente esta información

Señale un número estimado: ☐

Comente si considera necesario:

05) Evalúe el nivel de la integridad entre elaboración de documentos y control de versiones del SGC

- **a)** ☐ Controlada: Existen procedimientos para la elaboración de documentos y control de versiones
- **b)** ☐ Media: Algunas veces se presentan inconvenientes de control de versiones
- **c)** ☐ Baja: Frecuentemente hay inconvenientes en el control de versiones

Estime un número de cambios en el ultimo año: ☐

Comente si considera necesario:

06) Señale los principales medios de soportes de integridad de la información del SGC:

- **a)** ☐ Soporte físico impreso
- **b)** ☐ Soporte electrónico en PC's
- **c)** ☐ Soporte en servidor de archivos
- **d)** ☐ Soporte backup en medios externos — N° ☐
- **e)** ☐ Discos duros y otros medios removibles — N° ☐
- **f)** ☐ Otros: ☐ — N° ☐

Comente si considera necesario:

07) Señale los principales riesgos asociados a la integridad de la documentación de SGC:

N°	Riesgo	Proceso

Formulario N° 02: Integridad de los Activos de Información
Elaboración: Propia

PISER

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

CUESTIONARIO DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Nombre:
Cargo:
Área:

FORMULARIO N° 03: DISPONIBILIDAD DE LOS ACTIVOS DE INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa a escoger
Objetivo: Determinar los indicadores de seguridad de Disponibilidad
Elaboración: Propia

01) ¿Existe compromiso por preservar la disponibilidad de la información del SGC?

- **a)** ☐ Alto: Existe un alto compromiso
- **b)** ☐ Medio: Existe un compromiso relativamente medio
- **c)** ☐ Bajo: Se demuestra poco compromiso con la disponibilidad de la información
- **d)** ☐ Nulo: No se aplica ni es asumido por los colaboradores

Comente si considera necesario

02) ¿Cuáles son los principales incidentes de impacto a la disponibilidad de los documentos más comunes del SGC?

Si es necesario marque más de una alternativa

- **a)** ☐ Pérdida de documentos físicos
- **b)** ☐ Indisponibilidad de servidores
- **c)** ☐ Destrucción de los registros de información
- **d)** ☐ Otros
- **e)** ☐ Desconozco este proceso

Comente si considera necesario

03) Señale los principales vectores de pérdida de la disponibilidad de la información del SGC

Si es necesario marque más de una alternativa

- **a)** ☐ Debilidad de procedimientos y controles
- **b)** ☐ Deshonestidad / Rivalidades personales / Cultura organizacional
- **c)** ☐ Limitaciones en la tecnología
- **d)** ☐ Exceso de confianza
- **e)** ☐ Otros

Comente si considera necesario

Formulario N° 03: Disponibilidad de los Activos de Información
Elaboración: Propia

PISER S.A.C.

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

04) Estime el nivel de frecuencia de incidentes de impacto de la disponibilidad de los documentos del SGC en el perio

- **a)** ☐ Baja: Entre 1 y 5
- **b)** ☐ Media: Entre 6 y 10
- **c)** ☐ Alta: Más de 10
- **d)** ☐ Desconosco completamente esta información

Señale un número estimado: ☐

Comente si considera necesario:

05) Señale los principales respaldos electrónicos del SGC disponibles en el área QHSE

a)	☐ Respaldo en CD/DVD	Frecuencia	☐
b)	☐ Respaldo en cintas tape backup	Frecuencia	☐
c)	☐ Discos duros y otros medios removibles	Frecuencia	☐
d)	☐ Otros: ☐	Frecuencia	☐

Comente si considera necesario:

06) Señale los principales riesgos asociados a la disponibilidad de la documentación del SGC:

N°	Riesgo	Proceso

Formulario N° 03: Disponibilidad de los Activos de Información
Elaboración: Propia

PISER S.A.C.

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

ENCUESTA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Nombre:
Cargo:
Área:

FORMULARIO N° 04: SEGURIDAD DE LA INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa a escoger
Objetivo: Determinar la situación actual de la seguridad de la información
Fuente: Elaboración Propia

1) ¿Existe compromiso gerencial por la seguridad de la información?

- **a)** ☐ Alto. Existe un alto compromiso
- **b)** ☐ Medio. Existe un compromiso medio
- **c)** ☐ Bajo. Se demuestra poco compromiso con la seguridad de la información
- **d)** ☐ Nulo. No se aplica ni es asumido por los colaboradores
- **e)** ☐ Adverso. La seguridad de la información se percibe como una limitación al trabajo

Comente si considera necesario

2) Si existe compromiso gerencial explique como se demuestra:
Si es necesario marque más de una alternativa

- **a)** ☐ Políticas de seguridad de la información
- **b)** ☐ Charlas de sensibilización y concientización
- **c)** ☐ Difusión de boletines o recomendaciones de seguridad de la información
- **d)** ☐ Normatividad de seguridad de la información
- **e)** ☐ Otros:

Comente si considera necesario

3) Percibe que existe conciencia en la seguridad de la información en los trabajadores.

- **a)** ☐ Alta. En general existe conciencia en la seguridad de la información
- **b)** ☐ Media. Hay conciencia pero no está generalizada en todos los colaboradores
- **c)** ☐ Baja. Por lo general no existe conciencia en la seguridad de la información
- **d)** ☐ Nula. En general no existe conciencia en la seguridad de la información

Comente si considera necesario

Formulario N° 04: Evaluación de la Seguridad de la Información
Elaboración: Propia

PISER S.A.C.

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

ENCUESTA DE EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

4) ¿Quién establece los controles de seguridad de la información?

a) ☐ Gerencia y/o Alta Dirección
b) ☐ Logistica e Informática
c) ☐ QHSE
d) ☐ Otros: ____

Comente si considera necesario

____

5) ¿Cómo participa QHSE y Logistica e Informática en la seguridad de la información?

Si es necesario marque más de una alternativa

a) ☐ Demuestra su compromiso con la seguridad de la información
b) ☐ Aplica políticas de seguridad de la información
c) ☐ Realiza charlas de concientización y sensibilización
d) ☐ Difusión de boletines y/o recomendaciones de seguridad de la información
e) ☐ Se limita a realizar su trabajo técnico. No aborda el tema de seguridad de la información
f) ☐ Otro: ____

Comente si considera necesario

____

6) Como percibe la aplicación de controles de seguridad de la información

a) ☐ Se aplican controles en base a una adecuada evaluación de riesgos
b) ☐ Se aplican controles sin una adecuada evaluación de riesgos
c) ☐ Se muy pocos controles y sin una adecuada evaluación de riesgos
d) ☐ Desconozco este proceso

Comente si considera necesario

____

Formulario N° 04: Evaluación de la Seguridad de la Información
Elaboración: Propia

PISER S.A.C.

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

Área: _____ **Fecha:** _____

LISTA DE COTEJO N° 01: CONFIDENCIALIDAD DE LOS ACTIVOS DE INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa correcta

Objetivo: Determinar los indicadores de seguridad de Confidencialidad

Elaboración: Propia

SITUACIÓN A EVALUAR	SI	NO	OBSERVACIONES
CONFIDENCIALIDAD			
Los documentos se encuentran archivados en sus debidos portafolios.			
Existe acumulaciones de documentos del SGC en el área.			
Existe solicitud o formato de confidencialidad.			
Existe incidentes de acceso indebido a los documentos.			
Existe formato de control de distribución de copias controladas.			
Aplican el formato de control de distribución de copias controladas.			
Existe formato de control de distribución de copias no controladas.			
Existe medios de fuga de información en el área.			
Existe autorización de ingreso de personas al área QHSE.			
Existe políticas de Confidencialidad en el área.			
Existe compromiso por preservar la confidencialidad en el área.			
Existe soportes de información en el área.			
Los controles de seguridad de la información los brinda QHSE.			
Existe inventario de los procesos implementados por el SGC.			
Existe estadística de incidentes de seguridad de la información que tenga impacto sobre la confidencialidad.			

Lista de Cotejo N° 01: Evaluación de la Seguridad de la Información
Elaboración: Propia

PISER

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

Área: _____ **Fecha:** _____

LISTA DE COTEJO N° 02: INTEGRIDAD DE LOS ACTIVOS DE INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa correcta
Objetivo: Determinar los indicadores de seguridad de Integridad
Elaboración: Propia

SITUACIÓN A EVALUAR	SI	NO	OBSERVACIONES
INTEGRIDAD			
Existe compromiso por preservar la integridad.			
Existe incidentes de impacto a la integridad en documentos.			
Se presentan incidentes en el control de versiones de la documentación del SGC.			
Existe incidentes por los colaboradores en el SGC.			
Existe modificaciones de documentos en el área QHSE.			
Existe procedimientos para la elaboración de documentos.			
Existe algún formato o registro para las incidencias de integridad de información.			
Existe autorización para la actulización de documentos del SGC.			
Existe control incidencias de modificaciones de información del servidor.			
Existe pérdida o eliminación de información en el servidor.			
Existe control incidencias de modificaciones de información del servidor.			
Existe estadística de impacto sobre la integridad de la información.			
Existe normas o políticas en el área QHSE para la integridad de la información.			

Lista de Cotejo N° 02: Evaluación de la Seguridad de la Información
Elaboración: Propia

PISER

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

Área: **Fecha:**

LISTA DE COTEJO N° 03: DISPONIBILIDAD DE LOS ACTIVOS DE INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa correcta
Objetivo: Determinar los indicadores de seguridad de Disponibilidad
Elaboración: Propia

SITUACIÓN A EVALUAR	SI	NO	OBSERVACIONES
DISPONIBILIDAD			
Los documentos se encuentran a disponibilidad en el área QHSE.			
Las laptops cuentan con contraseña de seguridad.			
Existe formatos de impacto a la disponibilidad de los documentos.			
Los respaldos electronicos del SGC están disponibles en el área QHSE.			
Existe inconvenientes relacionados con la indisponibilidad de servidores			
Existe estadística de impacto sobre la disponibilidad de la información.			
El personal administrativo puede acceder a la base de datos del SGC.			
Existe control de disponibilidad de los equipos informáticos para salida del área.			
Existe disponibilidad de equipos informáticos a colaboradores.			
Existe disponibilidad de acceso al servidor de la empresa a practicantes.			
Existe backup para un rápido respaldo de información en el área QHSE.			
Existe formatos o registros de seguimiento de copias de respaldo del SGC.			

Lista de Cotejo N° 03: Evaluación de la Seguridad de la Información
Elaboración: Propia

Anexo N°02: Validación de Técnicas e Instrumentos

Validación de Encuesta de Confidencialidad de los Activos de Información

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Carlos Augusto Correa García
ESPECIALIDAD: Tecnología y Seguridad de la Información
DNI: 02873553

Por medio de la presente hago constar que re*alicé la revisión, con fines de validación* del instrumento denominado Cuestionario 01: Confidencialidad de Activos elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad				✓	
3.Actualidad				✓	
4.Organización				✓	
5.Suficiencia			✓		
6.Intencionalidad				✓	
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Piura el dia 30 del mes de Setiembre del 2016

CARLOS AUGUSTO CORREA GARCIA
INGENIERO INFORMATICO
Reg. CIP N° 129301

Encuesta de Confidencialidad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Karla Castillo Vega
ESPECIALIDAD: Ingeniero de Sistemas
DNI: 47585475

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Encuesta 01 : Confidencialidad, elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad					✓
2.Objetividad					✓
3.Actualidad					✓
4.Organización					✓
5.Suficiencia					✓
6.Intencionalidad				✓	
7.Consistencia				✓	
8.Coherencia					✓
9.Metodología					✓

En señal de conformidad firmo la presente en la ciudad de Talara el día 30 del mes de Setiembre del 2016

Karla Priscila Castillo Vega
ING. DE SISTEMAS
R. CIP. Nº 164840

Encuesta de Confidencialidad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Mario Chuye Tavara
ESPECIALIDAD: Proyectos
DNI: 73518079

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Encuesta 01: Confidencialidad de los activos de info., elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad			✓		
2.Objetividad				✓	
3.Actualidad			✓		
4.Organización			✓		
5.Suficiencia				✓	
6.Intencionalidad				✓	
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Talara ..... el día 29 ..... del mes de Septiembre ..... del ... 2016 .....

Ing. Mario Humberto Chuye Távara
INGENIERO INDUSTRIAL
CIP Nº 184053

Encuesta de Confidencialidad de los Activos de Información
Elaboración: Propia

Validación de Encuesta de Integridad

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Carlos Augusto Correa García
ESPECIALIDAD: Tecnología y Seguridad de la Información
DNI: 02813553

Por medio de la presente hago constar que re*alicé la revisión, con fines de validación* del instrumento denominado Cuestionario 02: Integridad de Activos, elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad				✓	
3.Actualidad				✓	
4.Organización				✓	
5.Suficiencia			✓		
6.Intencionalidad				✓	
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Piura el día 30 del mes de Setiembre del 2016

CARLOS AUGUSTO CORREA GARCIA
INGENIERO INFORMATICO
Reg. CIP N° 129387

Encuesta de Integridad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Karla Castillo Vega
ESPECIALIDAD: Ingeniero de Sistemas
DNI: 47585475

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Encuesta de Integridad de los activos, elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad					✓
2.Objetividad					✓
3.Actualidad					✓
4.Organización					✓
5.Suficiencia					✓
6.Intencionalidad				✓	
7.Consistencia					✓
8.Coherencia					✓
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Talara el día 30 del mes de setiembre del 2016

Karla Fressia Castillo Vega
ING. DE SISTEMAS
R. CIP. Nº 164840

Encuesta de Integridad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Mario Chuye Tavara
ESPECIALIDAD: Proyectos
DNI: 73518078

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Encuesta 02: Integridad de los activos de Inf., elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad			✓		
2.Objetividad				✓	
3.Actualidad			✓		
4.Organización			✓		
5.Suficiencia				✓	
6.Intencionalidad			✓		
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Talara el día 29 del mes de Septiembre del 2016

Ing. Mario Humberto Chuye Távara
INGENIERO INDUSTRIAL
CIP N° 184083

Encuesta de Integridad de los Activos de Información
Elaboración: Propia

Validación de Encuesta de Disponibilidad

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Carlos Augusto Correa García
ESPECIALIDAD: Tecnología y Seguridad
DNI: 02873553

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Cuestionario 03: Disponibilidad de Activos elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad				✓	
3.Actualidad				✓	
4.Organización				✓	
5.Suficiencia				✓	
6.Intencionalidad			✓		
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Piura el día 30 del mes de Setiembre del 2016

CARLOS AUGUSTO CORREA GARCIA
INGENIERO INFORMATICO
Reg. CIP N° 129301

Encuesta de Disponibilidad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Karla Castillo Vega
ESPECIALIDAD: Ingeniero de Sistemas
DNI: 47585475

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Encuesta 03: Disponibilidad de los activos elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad					✓
2.Objetividad					✓
3.Actualidad					✓
4.Organización					✓
5.Suficiencia				✓	
6.Intencionalidad				✓	
7.Consistencia					✓
8.Coherencia					✓
9.Metodología					✓

En señal de conformidad firmo la presente en la ciudad de Talara el día 30 del mes de Setiembre del 2016.

Karla Castillo

Karla Priscila Castillo Vega
ING. DE SISTEMAS
R. CIP. N° 164840

Encuesta de Disponibilidad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Mario Chuye Tavara
ESPECIALIDAD: Proyectos
DNI: 43518073

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Encuesta 03: Disponibilidad de los activos de inf. elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad				✓	
3.Actualidad			✓		
4.Organización				✓	
5.Suficiencia			✓		
6.Intencionalidad			✓		
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Talara el día 29 del mes de Septiembre del 2016

Ing. Mario Humberto Chuye Távara
INGENIERO INDUSTRIAL
CIP Nº 184083

Encuesta de Disponibilidad de los Activos de Información
Elaboración: Propia

Validación de Lista de Cotejo de Confidencialidad

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Mario Chuye Távara
ESPECIALIDAD: Proyectos
DNI: 73518079

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Lista de Cotejo & Activo de Confidencialidad elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad				✓	
3.Actualidad				✓	
4.Organización				✓	
5.Suficiencia				✓	
6.Intencionalidad				✓	
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología			✓		

En señal de conformidad firmo la presente en la ciudad de Piura el día 15 del mes de octubre del 2016

Ing. Mario Humberto Chuye Távara
INGENIERO INDUSTRIAL
CIP N° 184083

Lista de Cotejo de Confidencialidad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Karla Castillo Vega
ESPECIALIDAD: Ingeniero de Sistemas
DNI: 47585175

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Lista de Cotejo 01: Confidencialidad, elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad					✓
2.Objetividad					✓
3.Actualidad					✓
4.Organización					✓
5.Suficiencia					✓
6.Intencionalidad					✓
7.Consistencia					✓
8.Coherencia					✓
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Talara... el día ...15... del mes de ....Octubre..... del ...2016....

Karla Fabiola Castillo Vega
ING. DE SISTEMAS
R. CIP. N° 164840

Lista de Cotejo de Confidencialidad de los Activos de Información
Elaboración: Propia

Validación de Lista de Cotejo de Integridad

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Mario Chuye Távara.
ESPECIALIDAD: Proyectos
DNI: 73518073

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Lista de Cotejo : Activos de Integridad, elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad				✓	
3.Actualidad				✓	
4.Organización				✓	
5.Suficiencia				✓	
6.Intencionalidad			✓		
7.Consistencia			✓	✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Piura el día 15 del mes de Octubre del 2016

Ing. Mario Humberto Chuye Távara
INGENIERO INDUSTRIAL
CIP N° 184083

Lista de Cotejo de Integridad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Karla Castillo Vega.
ESPECIALIDAD: Ingeniera de Sistemas
DNI: 47585475

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Lista de Cotejo 02: Integridad de los activos elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad					✓
2.Objetividad					✓
3.Actualidad					✓
4.Organización					✓
5.Suficiencia					✓
6.Intencionalidad					✓
7.Consistencia				✓	
8.Coherencia					✓
9.Metodología					✓

En señal de conformidad firmo la presente en la ciudad de Talara el día 15 del mes de Octubre del 2016

Karla Priscila Castillo Vega
ING. DE SISTEMAS
R. CIP. Nº 164840

Lista de Cotejo de Integridad de los Activos de Información
Elaboración: Propia

Validación de Lista de Cotejo de Disponibilidad

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Mario Chuye Távara
ESPECIALIDAD: Proyectos
DNI: 73518079

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Lista de Cotejo : Activo de Disponibilidad, elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad				✓	
3.Actualidad				✓	
4.Organización			✓		
5.Suficiencia			✓		
6.Intencionalidad			✓		
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Piura el día 15 del mes de octubre del 2016

Ing. Mario Humberto Chuye Tavara
INGENIERO INDUSTRIAL
CIP Nº 184083

Lista de Cotejo de Disponibilidad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Karla Castillo Vega
ESPECIALIDAD: Ingeniero de Sistemas
DNI: 47585475

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Lista de cotejo 03: Disponibilidad de los activos elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad					✓
2.Objetividad					✓
3.Actualidad					✓
4.Organización					✓
5.Suficiencia				✓	
6.Intencionalidad					✓
7.Consistencia					✓
8.Coherencia					✓
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Talara el día 15 del mes de Octubre del 2016

Karla Pressia Castillo Vega
ING. DE SISTEMAS
R. CIP. Nº 164840

Lista de Cotejo de Disponibilidad de los Activos de Información
Elaboración: Propia

Validación de Encuesta de Seguridad de la Información

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Carlos Augusto Correa García
ESPECIALIDAD: Tecnología y Seguridad de la Información
DNI: 02873553

Por medio de la presente hago constar que re*alicé la revisión, con fines de* validación del instrumento denominado Cuestionario 01 : Confidencialidad de Activos elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad				✓	
3.Actualidad				✓	
4.Organización				✓	
5.Suficiencia			✓		
6.Intencionalidad				✓	
7.Consistencia				✓	
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Piura el día 30 del mes de Setiembre del 2016

CARLOS AUGUSTO CORREA GARCIA
INGENIERO INFORMATICO
Reg. CIP N° 129301

Encuesta de Seguridad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Karla Castillo Vega
ESPECIALIDAD: Ingeniero de Sistemas
DNI: 47585475

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Encuesta 04: Seguridad de la información, elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad					✓
2.Objetividad					✓
3.Actualidad					✓
4.Organización				✓	
5.Suficiencia				✓	
6.Intencionalidad				✓	
7.Consistencia					✓
8.Coherencia					✓
9.Metodología					✓

En señal de conformidad firmo la presente en la ciudad de Talara el día 30 del mes de Setiembre del 2016

Karla Pressia Castillo Vega
INGENIERO DE SISTEMAS
R. CIP. Nº 164840

Encuesta de Seguridad de los Activos de Información
Elaboración: Propia

UNIVERSIDAD CÉSAR VALLEJO

CONSTANCIA DE JUICIO DE EXPERTO

NOMBRE DEL EXPERTO: Mario Chuye Tavara
ESPECIALIDAD: Proyectos
DNI: 43518079

Por medio de la presente hago constar que realicé la revisión, con fines de validación del instrumento denominado Encuesta 04: Seguridad de la información, elaborado por el estudiante de Ingeniería de Sistemas **AGURTO CASTILLO**, quien está realizando su desarrollo de tesis titulado: " Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido de la encuesta. De antemano agradezco su cooperación.

Luego de hacer las observaciones pertinentes, puedo formular las siguientes apreciaciones.

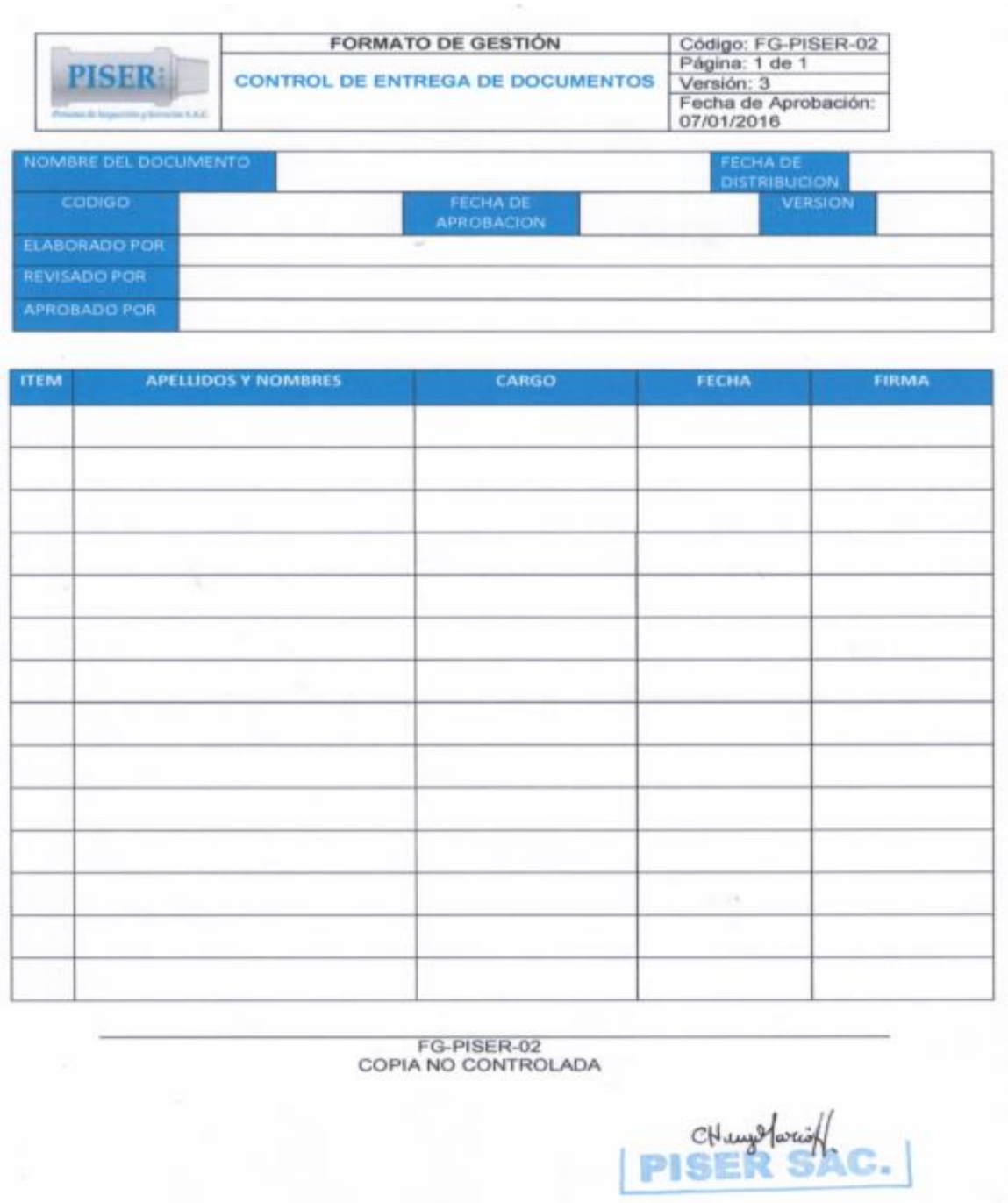
	DEFICIENTE	ACEPTABLE	BUENO	MUY BUENO	EXCELENTE
1.Claridad				✓	
2.Objetividad			✓		
3.Actualidad			✓		
4.Organización		✓			
5.Suficiencia			✓		
6.Intencionalidad			✓		
7.Consistencia			✓		
8.Coherencia				✓	
9.Metodología				✓	

En señal de conformidad firmo la presente en la ciudad de Talara el día 29 del mes de septiembre del 2016

Ing. Mario Humberto Chuye Tavara
INGENIERO INDUSTRIAL
CIP N° 184083

Encuesta de Seguridad de los Activos de Información
Elaboración: Propia

Anexo N° 03: Verificación de Formato de control de documentos y Listas Maestras del Sistema de Gestión de Calidad



PISER	FORMATO DE GESTIÓN	Código: FG-PISER-02
	CONTROL DE ENTREGA DE DOCUMENTOS	Página: 1 de 1
		Versión: 3
		Fecha de Aprobación: 07/01/2016

NOMBRE DEL DOCUMENTO		FECHA DE DISTRIBUCION	
CODIGO		FECHA DE APROBACION	VERSION
ELABORADO POR			
REVISADO POR			
APROBADO POR			

ITEM	APELLIDOS Y NOMBRES	CARGO	FECHA	FIRMA

FG-PISER-02
COPIA NO CONTROLADA

PISER SAC.

Fuente: FG-PISER-02

Verificación de Lista Maestra de documentos Externos del SIG

PISER	FORMATO DE GESTIÓN	Código	FG-PISER-03
	LISTA MAESTRA DE DOCUMENTOS EXTERNOS	Página:	1 de 1
		Versión:	02
		Fecha de Aprobación:	07/01/2016
RESPONSABLE: RAD		Fecha de actualización:	

TITULO	CODIGO	VERSION	RESPONSABLE
Process Piping - ASME Code for Pressure Piping	ASME B31.3	2008	
Pipe Flanges and Flanged Fittings NPS 1/2 Through NPS 24 Metric/Inch St	ASME B16.5	2013	
Certified Pressure Vessel Inspector Syllabus - Example Questions and Wo	API 510	2010	
Fired Heaters for General Refinery Service	ANSI/API STANDARD 560	2007	
Piping Inspection Code: In-service Inspection, Rating, Repair, and Alteratic	API 570	2009	
Inspection Practices for Pressure Vessels	API RECOMMENDED PRACTICE 572	2009	
Inspection Practices for Piping System Components	API RECOMMENDED PRACTICE 574	2009	
Risk-Based Inspection	API RECOMMENDED PRACTICE 580	2009	
Reciprocating Compressors For Petroleum, Chemical, and Gas Industry Se	API STANDARD 618	2007	
Tank Inspection, Repair, Alteration, and Reconstruction	API STANDARD 653	2009	
Recommended Practice for Machinery Installation and Installation Design	API RECOMMENDED PRACTICE 686	2009	
Steels for Hydrogen Service at Elevated Temperatures and Pressures in Petroleum Refineries and Petrochemical Plants	API RECOMMENDED PRACTICE 941	2004	
Recommended Practice for Drill Stem Design and Operating Limits	API RECOMMENDED PRACTICE 7G	1998	
Recommended Practice for Procedures for Inspections, Maintenance, Repair and Remanufacture of Hoisting Equipment	API Recommended Practice 8B	2002	
Managing System Integrity for Hazardous Liquid Pipelines	API STANDARD 1160	2001	
Damage Mechanisms Affecting Fixed Equipment in the Refining Industry	API RECOMMENDED PRACTICE 571	2011	
Material Verification Program for New and Existing Alloy Piping Systems	API RECOMMENDED PRACTICE 578	2010	
Cathodic Protection of Aboveground Petroleum Storage Tanks	API RECOMMENDED PRACTICE 651	2014	
Linings of Aboveground Petroleum Storage Tank Bottoms	API RECOMMENDED PRACTICE 652	2014	
Recommended Practice for Basic Inspection Requirements - New Pipeline	API RECOMMENDED PRACTICE 1169	2013	

Fuente: FG-PISER-03

Verificación de Lista Maestra de documentos Externos del SIG

Recommended Practice for Ultrasonic and Magnetic Examination of Offshore Structural Fabrication and Guidelines for Qualification of Technicians	API RECOMMENDED PRACTICE 2X	2004	
V NONDESTRUCTIVE EXAMINATION	ASME Boiler & Pressure Vessel Code	2013	
welding Processes, Inspection, and Metallurgy	API RECOMMENDED PRACTICE 577	2013	
Metallic Gaskets for Pipe Flanges Ring-Joint, Spiral-Wound, and Jacketed	ASME B16.20	2007	
Nonmetallic Flat Gaskets for Pipe Flanges	ASME B16.21	2011	
Buttwelding Ends	ASME B16.25	2007	
Power Piping	ASME B31.1	2012	
Pipeline Transportation Systems for Liquid Hydrocarbons and Other Liquids	ASME B31.4	2006	
Gas Transmission and Distribution Piping Systems	ASME B31.8	2012	
Hidrogen Piping and Pipelines	ASME B31.12	2008	
Building Services Piping	ASME B31.9	2008	
Pipeline Transportation Systems for Liquids and Slurries	ASME B31.4	2012	
Welded and Seamless Wrought Steel Pipe	ASME B36.10M	2004	
Rules for Construction of Power Boilers	ASME BOILER AND PRESSURE VESSEL CODE	2010	
II Part D Properties (Customary) Materials	ASME Boiler and Pressure Vessel Code	2010	
Valves - Flanged, threaded, and Welding End	ASME B16.34	2009	
VIII Rules for Construction of Pressure Vessels Division 2 Alternative Rules	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
IX Welding, Brazing, and Fusing Qualifications Qualification Standard for Welding, Brazing, and Fusing Procedures; Welders; Brazers; and Welding, Brazing, and Fusing Operators	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
Código de Soldadura Estructural - Acero	AWS D1.1/D1.1M	2010	
Factory-Made Wrought Buttwelding Fittings	ASME B16.9	2012	

PISER SAC.

Fuente: FG-PISER-03

Verificación de Lista Maestra de documentos Externos del SIG

Inspection Planning Using Risk-Based Methods	ASME PCC-3	2007	
Standard Specification for Piping Fittings of Wrought Carbon Steel and Alloy Steel for Moderate and High Temperature Service1	ASTM A234/A234M	2010	
Standard Practice for Measuring Thickness by Manual Ultrasonic Pulse-Ec	E797/E797M	2010	
Risk-Based Inspection Technology	API RECOMMENDED PRACTICE 581	2008	
Construcción, Inspección, Reparación, Modificaciones y Protección Catódica de Tanques de Acero Soldado para Almacenamiento de Petróleo	API –650, 651 & 653	2007	
Standard Specification for Heat-Treated Carbon Steel Fittings for Low-Tem	ASTM A858/A858M	2010	
Welded Tanks for Oil Storage	API STANDARD 650	2013	
Welded Tanks for Oil Storage (SP)	API STANDARD 650 (SP)	2013	
III RULES FOR CONSTRUCTION OF NUCLEAR FACILITY COMPONENTS Su	ASME Boiler & Pressure Vessel Code	2010	
III Division 1 — Appendices RULES FOR CONSTRUCTION OF NUCLEAR FACILITY COMPONENTS	ASME Boiler & Pressure Vessel Code	2010	
III Rules for Construction of Nuclear Facility Components Division 1 — Subsection NB Class 1 Components	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
III Rules for Construction of Nuclear Facility Components Division 1 — Subsection NC Class 2 Components	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
III Rules for Construction of Nuclear Facility Components Division 1 — Subsection ND Class 3 Components	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
III Division 1 — Subsection NE Class MC Components RULES FOR CONSTRUCTION OF NUCLEAR FACILITY COMPONENTS	ASME Boiler & Pressure Vessel Code	2010	
III Division 1 — Subsection NF Supports RULES FOR CONSTRUCTION OF NUCLEAR FACILITY COMPONENTS	ASME Boiler & Pressure Vessel Code	2010	
Prueba de Presión de Tuberías de Acero para el Transporte de Gas, Gas de Petróleo, Liquidos Peligrosos, Liquidos Altamen.	API PRÁCTICA RECOMENDADA 1110	2007	
III RULES FOR CONSTRUCTION OF NUCLEAR FACILITY COMPONENTS Division 1 - Subsection NG Core Support Structures	ASME Boiler & Pressure Vessel Code	2010	
III RULES FOR CONSTRUCTION OF NUCLEAR FACILITY COMPONENTS Division 1 - Subsection NH Class 1 Components in Elevated Temperature Service	ASME Boiler & Pressure Vessel Code	2010	
III Rules for Construction of Nuclear Facility Components Division 2 Code for Concrete Containments	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	

Fuente: FG-PISER-03

Verificación de Lista Maestra de documentos Externos del SIG

QUALIFICATION STANDARD FOR WELDING AND BRAZING PROCEDURES, WELDERS, BRAZERS, AND WELDING AND BRAZING OPERATORS	ASME Boiler & Pressure Vessel Code	2010	
FORM NPP-1 CERTIFICATE HOLDER'S DATA REPORT FOR FABRICATED NUCLEAR PIPING SUBASSEMBLIES* As Required by the Provisions of the ASME Code, Section III, Division 1	ASME SECTION III APPENDICES	2013	
VI Recommended Rules for the Care and Operation of Heating Boilers	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
VII Recommended Guidelines for the Care of Power Boilers	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
VIII Rules for Construction of Pressure Vessels Division 1	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
VIII Rules for Construction of Pressure Vessels Division 3 Alternative Rules for Construction of High Pressure Vessels	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
X FIBER-REINFORCED PLASTIC PRESSURE VESSELS	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
XI RULES FOR INSERVICE INSPECTION OF NUCLEAR POWER PLANT COMPONENTS	ASME Boiler & Pressure Vessel Code	2010	
XII Rules for Construction and Continued Service of Transport Tanks	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
III Rules for Construction of Nuclear Facility Components Division 1 — Subsection NB Class 1 Components	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
II Materials Part B Nonferrous Material Specifications	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
VII Recommended Guidelines for the Care of Power Boilers	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
Code Cases Boilers and Pressure Vessels	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
Stainless Steel Pipe	ASME B36.19M	2004	
II Materials Part A Ferrous Material Specifications (Beginning to SA-450)	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
PARTE QW SOLDADURA ARTICULO I REQUERIMIENTOS GENERALES DE SOLDADURA	ASME SECCIÓN IX	1998	

PISER SAC.

Fuente: FG-PISER-03

Verificación de Lista Maestra de documentos Externos del SIG

Inspección Por Particulas Magneticas	Asme Secc. V Articulo 7	1996	
A Century of Safety	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2013	
POWER PIPING Charles Becht IV	ASME B31.1	2007	
Simbolo Normalizados para Soldeo, Soldeo Fuerte y Examen no Destructivo	ANSI/AWS A2.4-93	1991	
Standard Welding Terms and Definitions Including Terms for Adhesive Bonding,Brazing,Soldering, Thermal Cutting, and Thermal Spraying	AWS A3.0	2001	
Guide for the Visual Inspection of Welds	AWS B1.11	2000	
Specification for the Qualification ofWelding Inspectors	AWS B5.1	2003	
Standard for AWS Certification of Welding Inspectors	AWS QC1	2007	
Energy API	API 1104	2012	
Code Clinic For Study of Welding of Pipelines and Related Facilities - Nineteenth Edition	AWS API 1104	1999	
Study Guide for API Standard 1104 Welding of Pipelines and Related Facilities TWENTIETH EDITION	AWS API-M	2006	
Specification for Vertical and Horizontal Emulsion Treaters	API SPECIFICATION 12L	2008	
Pressure Vessel Inspection Code: In - Service Inspection, Rating, Repair, and Alteration	API 510	2006	
Calculation of Heater-tube Thickness in Petroleum Refineries	ANSI/API STANDARD 530	2008	
Código de Inspección para Cañerias Inspección, Reparación, Alteración y Reclasificación de Sistemas de Cañerias en Servicio.	API 570	2006	
Piping Inspection Code: In-service Inspection, Rating, Repair, and Alteratic	API 570	2009	
Fitness-For-Service Example Problem Manual	API 579-2/ASME FFS-2	2009	
Fitness-For-Service	API 579-1/ASME FFS-1	2007	
Valve Inspection and Testing	API STANDARD 598	2009	
Steel Gate Valves - Flanged and Butt - Welding Ends, Bolted Bonnets	API STANDARD 600	2009	
Design and Construction of Large, Welded, Low-Pressure Storage Tanks	API STANDARD 620	2008	
Welded Steel Tanks for Oil Storage	API STANDARD 650	2007	

Fuente: FG-PISER-03

Verificación de Lista Maestra de documentos Externos del SIG

Flame Arresters for Vents of Tanks Storing Petroleum Products	API RECOMMENDED PRACTICE 2210	2000	
I Rules for Construction of Power Boilers	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL CODE	2010	
Recommended Practice for the Pressure Testing of Steel Pipelines for the transportation of gas, Petroleum Gas, Hazardous Liquids, Highly Volatile Liquids, or Carbon Dioxide	API RECOMMENDED PRACTICE 1110	2013	
Guidelines and Procedures for Entering and Cleaning Petroleum Storage T	ANSI/API RECOMMENDED PRACTICE 2016	2001	
Specification for Line Pipe	ANSI/API SPECIFICATION 5L	2007	
Technical Report on Capabilities of API Integral Flanges Under Combinatio	API TECHNICAL REPORT 6AF2	2010	
Pipe Flanges and Flanged Fittings NPS 1/2 Through NPS 24 Metric/Inch St	ASME B16.5	2009	
Code Cases: Boilers and Pressure Vessels	ASME Boiler and Pressure Vessel Code AN INTERNATIONAL COD E	2010	
Forged Fittings, Socket-Welding and Threaded	ASME B16.11	2005	
Large Diameter Steel Flanges NPS 26 Through NPS 60 Metric/Inch Standar	ASME B16.47	2011	
Process Piping	ASME B31.3	2012	
Manual for Determining the Remaining Strength of Corroded Pipelines	ASME B31G	2012	
Managing System Integrity of Gas Pipelines	ASME B31.8S	2010	
GUIDE TO LIFE CYCLE MANAGEMENT OF PRESSURE EQUIPMENT INTEG	ASME PTB-2	2009	
VIII RULES FOR CONSTRUCTION OF PRESSURE VESSELS Division 2 Alternative Rules	ASME Boiler & Pressure Vessel Code	2010	
ASME SECTION VIII - DIVISION 2 Criteria and Commentary	ASME PTB-1	2009	
Guidelines for Pressure Boundary Bolted Flange Joint Assembly	ASME PCC-1	2010	
Repair of Pressure Equipment and Piping	ASME PCC-2	2011	
Standard Test Method for Field Measurement of Soil Resistivity Using the Wenner Four-Electrode Method1	Designation: G57 – 06	2012	
Standard Guide for Three Methods of Assessing Buried Steel Tanks1	Designation: G158 – 98	2010	

PISER SAC.

Fuente: FG-PISER-03

Verificación de Lista Maestra de documentos Externos del SIG

Gas cylinders, Operational requirements for gas cylinders	ISO/TC 58/SC 4N 380	2004	
Non - Destructive testing - Qualification and Certification of personnel	ISO 9712	2005	
Gas cylinders — Refillable seamless gas cylinders — Acoustic emission testing for periodic inspection	ISO/DIS 16148	2002	
Methods for absolute calibration of acoustic emission transducers by reciprocity technique	ISO/NP TR 13115	2009	
Non-destructive testing — General terms and definitions	ISO/DIS 18173	2002	
Condition monitoring and diagnostics of machines — Acoustic emission	ISO/DIS 22096	2006	
Non-destructive testing — Qualification and certification of personnel	ISO/FDIS 9712	2004	
DRAFT TECHNICAL SPECIFICATION OR TECHNICAL REPORT	ISO/TC 135	2005	
Scheme for the Identification of Piping Systems	ASME A13.1	2007	
Standard Guide for Examination and Evaluation of Pitting Corrosion1	ASTM G46 – 94	2005	
Wrought Steel Buttwelding Short Radius Elbows and Returns	ASME B16.28	1994	
Standard Practice for Guided Wave Testing of Above Ground Steel Pipework Using Piezoelectric Effect Transduction1	ASTM E2775	2011	
Standard Practice for Magnetic Particle Testing1	ASTM E1444/E1444M	2012	

PISER SAC.

Fuente: FG-PISER-03

Verificación de Lista Maestra de documentos Internos del SIG

PISER	FORMATO DE GESTION	Código	FG-PISER-01
	LISTA MAESTRA DE DOCUMENTOS INTERNOS	Página:	1 de 1
		Versión:	02
		Fecha de Aprobación:	07/01/2016

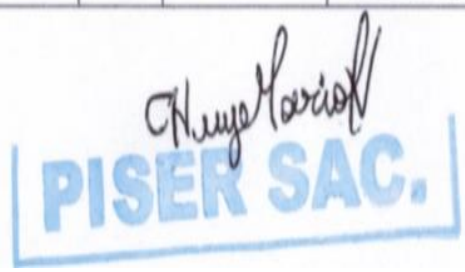
Fecha de actuzalización 30/11/2016

TITULO DEL DOCUMENTO	CODIGO	VERSION	FECHA	RESPONSABLE
DOCUMENTOS DEL SISTEMA INTEGRADO DE GESTIÓN				
POLITICA INTEGRADA DEL SISTEMA DE GESTIÓN	NO APLICA	09	28/12/2015	GERENTE GENERAL/RAD
PROGRAMA DE GESTIÓN DE CALIDAD, SEGURIDAD Y SALUD EN EL TRABAJO	NO APLICA	02	12/01/2016	GERENTE GENERAL/RAD
MAPA DE INTERACCIÓN DE PROCESOS	NO APLICA	00	09/01/2016	RAD
PROCEDIMIENTOS DE GESTIÓN				
CONTROL DE DOCUMENTOS Y REGISTROS	PG-PISER-01	03	07/01/2016	SUPERVISOR QHSE/RAD
IDENTIFICACIÓN Y EVALUACIÓN DE REQUISITOS LEGALES Y OTROS REQUISITOS	PG-PISER-02	04	09/01/2016	SUPERVISOR QHSE/RAD
IDENTIFICACIÓN DE PELIGROS, EVALUACIÓN DE RIESGOS Y DETERMINACIÓN DE CONTROLES	PG-PISER-03	04	12/01/2016	SUPERVISOR QHSE/RAD
COMPETENCIA, FORMACIÓN Y TOMA DE CONCIENCIA	PG-PISER-04	03	17/01/2016	SUPERVISOR QHSE/RAD
COMUNICACIONES	PG-PISER-05	03	15/02/2016	SUPERVISOR QHSE/RAD
PARTICIPACIÓN Y CONSULTA	PG-PISER-06	00	29/02/2016	SUPERVISOR QHSE/RAD
PERMISOS DE TRABAJO	PG-PISER-07	02	23/02/2016	SUPERVISOR QHSE/RAD
SEGUIMIENTO Y MEDICIÓN	PG-PISER-08	02	08/03/2016	SUPERVISOR QHSE/RAD
INVESTIGACIÓN DE INCIDENTES Y ACCIDENTES	PG-PISER-09	02	12/03/2016	SUPERVISOR QHSE/RAD
NO CONFORMIDADES, ACCIONES CORRECTIVAS Y PREVENTIVAS	PG-PISER-10	03	14/03/2016	SUPERVISOR QHSE/RAD
DOSSIER DE CALIDAD	PG-PISER-11	00	20/02/2016	SUPERVISOR QHSE/RAD
PRODUCTOS NO CONFORMES	PG-PISER-12	03	15/03/2016	SUPERVISOR QHSE/RAD
AUDITORIAS INTERNAS	PG-PISER-13	03	17/03/2016	SUPERVISOR QHSE/RAD
IDENTIFICACIÓN Y EVALUACIÓN DE ASPECTOS AMBIENTALES	PG-PISER-14	02	19/01/2015	SUPERVISOR QHSE/RAD
IDENTIFICACIÓN Y EVALUACIÓN DE PROVEEDORES	PG-PISER-15	01	30/04/2010	SUPERVISOR QHSE/RAD
REPARACIÓN DE EMERGENCIAS ANTE RESPUESTAS	PG-PISER-16	01	28/01/2010	SUPERVISOR QHSE/RAD
PRODUCTOS Y SERVICIOS NO CONFORMES	PG-PISER-17	01	28/01/2010	SUPERVISOR QHSE/RAD

Fuente: FG-PISER-01

Verificación de Lista Maestra de documentos Internos del SIG

PROCEDIMIENTOS OPERATIVOS				
MAESTRANZA				
FABRICACION DE HERRAMIENTAS Y ACCESOSIOS PESADOS Y LIVIANOS	PO-MAEST-PISER-01	01	20/02/2016	SUPERVISOR QHSE/RAD
MAQUINADO DE HERRAMIENTAS Y ACCESOSIOS PESADOS Y LIVIANOS	PO-MAEST-PISER-02	00	20/02/2016	SUPERVISOR QHSE/RAD
TALADRADO DE HERRAMIENTAS Y ACCESOSIOS PESADOS Y LIVIANOS	PO-MAEST-PISER-03	00	20/02/2016	SUPERVISOR QHSE/RAD
FRESADO DE HERRAMIENTAS Y ACCESOSIOS PESADOS Y LIVIANOS	PO-MAEST-PISER-04	00	20/02/2016	SUPERVISOR QHSE/RAD
OIT	PO-MAEST-PISER-05	01	15/02/2010	SUPERVISOR QHSE/RAD
SOLDADURA				
APLICACIÓN DE SOLDADURA HARD BANDING	PO-SOLD-PISER-01	02	04/03/2016	SUPERVISOR QHSE/RAD
TRANSPORTE				
OPERACIÓN CON MONTACARGAS	PO-TRANS-PISER-01	02	20/02/2016	SUPERVISOR QHSE/RAD
INSPECCIÓN				
INSPECCIÓN VISUAL Y DIMENSIONAL	PO-INSP-PISER-01	02	20/02/2016	SUPERVISOR QHSE/RAD
ACTIVIDADES DE INSPECCION DENTRO DE LOS PROCESOS	PO-INSP-PISER-01	00	20/02/2016	SUPERVISOR QHSE/RAD
INSTRUMENTACIÓN				
PROCEDIMIENTOS DE SEGURIDAD				
MEDICINA PREVENTIVA Y DEL TRABAJO	PS-QHSE-PISER-01	01	08/01/2010	SUPERVISOR QHSE/RAD
GUIAS PARA LOS PRIMEROS AUXILIOS Y ASISTENCIA MEDICA	PS-QHSE-PISER-02	01	08/01/2010	SUPERVISOR QHSE/RAD
ELEMENTOS DE PROTECCION PERSONAL	PS-QHSE-PISER-03	01	08/01/2010	SUPERVISOR QHSE/RAD



Fuente: FG-PISER-01

Verificación de Lista Maestra de documentos Internos del SIG

USO DE COMPRESORES	PS-QHSE-PISER-04	01	08/01/2010	SUPERVISOR QHSE/RAD
SIMULACROS DE EMERGENCIA	PS-QHSE-PISER-05	01	09/01/2010	SUPERVISOR QHSE/RAD
OPERACIONES DE SOLDADURA	PS-QHSE-PISER-06	01	09/01/2010	SUPERVISOR QHSE/RAD
OPERACIONES EN TALLERES	PS-QHSE-PISER-07	01	09/01/2010	SUPERVISOR QHSE/RAD
INSPECCION QHSE	PS-QHSE-PISER-08	01	13/02/2010	SUPERVISOR QHSE/RAD
IDENTIFICACION DE MARCACION Y SEÑALIZACION	PS-QHSE-PISER-09	01	13/02/2010	SUPERVISOR QHSE/RAD
MANTENIMIENTO Y CONTROL DEL MEDIO AMBIENTE	PS-QHSE-PISER-10	01	13/02/2010	SUPERVISOR QHSE/RAD
ALMACENAMIENTO DE TUBERIAS ESTIBAS Y MANTENIMIENTO	PS-QHSE-PISER-11	01	13/02/2010	SUPERVISOR QHSE/RAD
NOTIFICACION DE ACCIDENTES	PS-QHSE-PISER-12	01	10/02/2010	SUPERVISOR QHSE/RAD
INVESTIGACION DE INCIDENTES	PS-QHSE-PISER-13	01	26/02/2010	SUPERVISOR QHSE/RAD
CONDUCTAS SEGURAS EN EL TRABAJO	PS-QHSE-PISER-14	01	30/03/2010	SUPERVISOR QHSE/RAD
CONDUCCION DE VEHICULOS	PS-QHSE-PISER-15	01	30/03/2010	SUPERVISOR QHSE/RAD
PROCEDIMIENTOS DE SEGURIDAD PARA LA INSPECCION Y MANTENIMIENTO DE PSV	PS-QHSE-PISER-16	01	13/02/2010	SUPERVISOR QHSE/RAD
SALUD OCUPACIONAL	PS-QHSE-PISER-17	01	23/04/2015	SUPERVISOR QHSE/RAD
TRABAJOS EN ALTURA	PS-QHSE-PISER-18	02	15/04/2015	SUPERVISOR QHSE/RAD
INSTRUCTIVOS DE TRABAJO				
MAESTRANZA				
ALMACENAMIENTO DE PROPIEDAD DEL CLIENTE	IT-MAEST-PISER-01	00	20/02/2016	SUPERVISOR QHSE/RAD
MANUAL				
MANUAL CALIDAD	MA-PISER-01			
MANUAL DE ORGANIZACION Y FUNCIONES	MA-PISER-02			
PLAN				
PLAN DE PREPARACIÓN Y RESPUESTA ANTE EMERGENCIAS	PL-PISER-01	03	20/03/2016	SUPERVISOR QHSE/RAD
FENOMENO EL NIÑO	PL-PISER-	03		SUPERVISOR QHSE/RAD
PLAN DE CONTINGENCIA	PL-PISER-	03		SUPERVISOR QHSE/RAD

Fuente: FG-PISER-01

Verificación de Lista Maestra de documentos Internos del SIG

PROCEDIMIENTOS DE APOYO				
LOGÍSTICA				
COMPRAS	PA-LOG-PISER-01	03	20/02/2016	SUPERVISOR QHSE/RAD
RECEPCIÓN DE MATERIALES	PA-LOG-PISER-02	02	20/02/2016	SUPERVISOR QHSE/RAD
SALIDA DE MATERIALES	PA-LOG-PISER-03	02	20/02/2016	SUPERVISOR QHSE/RAD
SELECCIÓN DE PROVEEDORES	PA-LOG-PISER-04	00	25/02/2016	SUPERVISOR QHSE/RAD
FORMATOS				
FORMATOS DE GESTION				
ASISTENCIA A ENTRENAMIENTO	FG-PISER-01	02	13/01/2015	SUPERVISOR QHSE/RAD
IDENTIFICACION DE ASPECTOS Y EV. DE IMPACTOS AMBIENTALES	FG-PISER-02	01	05/01/2010	SUPERVISOR QHSE/RAD
IPERC	FG-PISER-03	01	05/01/2010	SUPERVISOR QHSE/RAD
CONTROL DE ENTREGA DE DOCUMENTOS	FG-PISER-04	03	07/01/2016	SUPERVISOR QHSE/RAD
LISTADO DE REQUISITOS LEGALES	FG-PISER-05	01	05/01/2016	SUPERVISOR QHSE/RAD
LISTADO DE DOCUMENTOS	FG-PISER-08	01	05/01/2016	SUPERVISOR QHSE/RAD
FORMATO DE CRONOGRAMA MENSUAL DE CHARLAS	FG-PISER-01			
FORMATO DE REGISTRO DE CONTROL DE ACCIONES	FG-PISER-02			
FORMATO DE SEGUIIENTO Y CIERRE DE REGISTRO DE CONTROL DE ACCIONES	FG-PISER-03			
FORMATO DE PROGRAMA DE MANTENIMIENTO DE MAQUINAS Y EQUIPOS	FG-PISER-05			
FORMATO DE IDENTIFICACIÓN DE CRITERIOS DE AUDITORIA	FG-PISER-06			

PISER SAC.

Fuente: FG-PISER-01

Verificación de Lista Maestra de documentos Internos del SIG

FORMATO DE CONSTANCIA DE ENTREGA DE DOCUMENTOS	FG-PISER-04			
FORMATO DE ASISTENCIA DE ENTRENAMIENTO	FG-PISER-07			
FORMATO DE SATISFACCIÓN DEL CLIENTE	FG-PISER-08			
FORMATO DE REPORTE DE PRODUCTO/SERVICIO NO CONFORME	FG-PISER-09			
FORMATO DE INDUCCION, CAPACITACION,ENTRENAMIENTO Y SIMULACRO DE EMERGENCIA	FG-PISER-10	03	21/01/2016	SUPERVISOR QHSE/RAD
FORMATO DE ENCUESTA DE EVALUACION AL CLIENTE	FG-PISER-14	00	15/02/2016	SUPERVISOR QHSE/RAD
FORMATO DE ANALISIS DE TRABAJO SEGURO	FG-PISER-15	02	23/02/2016	SUPERVISOR QHSE/RAD
FORMATO DE PERMISO DE TRABAJO	FG-PISER-16	02	23/02/2016	SUPERVISOR QHSE/RAD
FORMATO DE INCIDENTES PELIGROSOS E INCIDENTES DE TRABAJO	FG-PISER-18	02	12/03/2016	SUPERVISOR QHSE/RAD
FORMATO DE ACCIDENTE DE TRABAJO	FG-PISER-19	02	12/03/2016	SUPERVISOR QHSE/RAD
FORMATO DE EVALUACION DE EVALUACION Y SATISFACCION AL CLIENTE	FG-PISER-20			
FORMATO DE PROGRAMA DE CAPACITACION	FG-PISER-21			
REPORTE DE SERVICIO Y PRODUCTO NO CONFORME	FG-PISER-22	02	15/03/2016	SUPERVISOR QHSE/RAD
FORMATOS DE OPERATIVOS				
MAESTRANZA				
ORDEN INTERNA DE TRABAJO	FO-MAEST-PISER-02	03	11/05/2016	SUPERVISOR QHSE/RAD
SOLDADURA				
TRANSPORTE				
INSPECCION				
INSTRUMENTACION				
FORMATOS DE APOYO				

Fuente: FG-PISER-01

Verificación de Lista Maestra de documentos Internos del SIG

FORMATOS DE APOYO				
FORMATO DE REGISTRO DE ENTRADA DE MATERIALES	FA-LOG-PISER-01	01	15/12/2009	SUPERVISOR QHSE/RAD
FORMATO DE EVALUACIÓN DE DESEMPEÑO PROVEEDOR CRITICO	FA-LOG-PISER-02	01	30/04/2010	SUPERVISOR QHSE/RAD
FORMATO DE LISTA DE REQUISITOS PARA PROVEEDORES CRITICOS	FA-LOG-PISER-03	01	02/05/2010	SUPERVISOR QHSE/RAD
FORMATO DE INSPECCIÓN DE MATERIALES COMPRADOS	FA-LOG-PISER-04			SUPERVISOR QHSE/RAD
FORMATO DE REQUERIMIENTO DE PRODUCTO O SERVICIO	FA-LOG-PISER-05			SUPERVISOR QHSE/RAD
FORMATO DE ORDEN DE COMPRA O SERVICIO	FA-LOG-PISER-06			SUPERVISOR QHSE/RAD
RESUMEN DE PROVEEDORES CRITICOS	FA-LOG-PISER-07	01	01/05/2010	SUPERVISOR QHSE/RAD
FORMATO DE SOLICITUD DE CONVOCATORIA DE PERSONAL	FA-RRHH-PISER-01			
FORMATO INSPECCIÓN DE MONTACARGAS	FA-TRANS-PISER-01			
FORMATO CONTROL VEHICULAR	FA-TRANS-PISER-02			
FORMATO DE INSPECCIÓN VEHICULAR	FA-TRANS-PISER-03			
FORMATO DE SEGURIDAD				

PISER SAC.

Fuente: FG-PISER-01

Verificación de Lista Maestra de Registros del SIG

	FORMATO DE GESTIÓN	Código	FG-PISER-04
PISER		Página:	1 de 1
	LISTA MAESTRA DE REGISTROS	Versión:	02
		Fecha de Aprobación:	07/01/2016

Fecha de actualización: 22/02/016

REGISTRO	CODIGO	VERSIÓN	FECHA	RESPONSABLE	UBICACIÓN	TIEMPO DE RETENCION
REGISTROS DE GESTIÓN						
LISTA MAESTRA DE DOCUMENTOS INTERNOS.	FG-PISER-01	03	07/01/2016	RAD	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
CONTROL DE ENTREGA DE DOCUMENTOS	FG-PISER-02	03	07/01/2016	RAD	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
LISTA MAESTRA DE DOCUMENTOS EXTERNOS.	FG-PISER-03	03	07/01/2016	RAD	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
LISTA MAESTRA DE REGISTROS.	FG-PISER-04	03	07/01/2016	RAD	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
MATRIZ DE REQUISITOS LEGALES Y OTROS REQUISITOS	FG-PISER-05	04	09/01/2016	RAD	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
CLASIFICACIÓN DE TAREAS	FG-PISER-06	02	12/01/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
MATRIZ DE IDENTIFICACIÓN DE PELIGROS Y EVALUACIÓN DE RIESGOS	FG-PISER-07	02	12/01/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
EVALUACIÓN DE HABILIDADES	FG-PISER-08	03	21/01/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
PROGRAMA ANUALDE CAPACITACIÒN	FG-PISER-09	01	21/01/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
REGISTROS DE INDUCCIÓN, CAPACITACIÓN, ENTRENAMIENTO Y SIMULACROS DE EMERGENCIA	FG-PISER-10	03	21/01/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO

Fuente: FG-PISER-04

Verificación de Lista Maestra de Registros del SIG

REGISTRO DE COMUNICACIONES: BUZÓN	FG-PISER-13	02	15/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
ENCUESTA DE SATISFACCIÓN AL CLIENTE	FG-PISER-14	02	15/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
ANÁLISIS DETRABAJO SEGURO	FG-PISER-15	02	23/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
PERMISO DE TRABAJO	FG-PISER-16	02	23/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
PROGRAMA DE CALIBRACIÓN DE INSTRUMENTOS DE MEDICIÓN	FG-PISER-17	02	08/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
INCIDENTES PELIGROSOS E INCIDENTES DE TRABAJO	FG-PISER-18	02	12/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
ACCIDENTES DE TRABAJO	FG-PISER-19	02	12/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
ENFERMEDADES OCUPACIONALES	FG-PISER-20	02	12/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
SISTEMA DE ACCIONES CORRECTIVAS Y PREVENTIVAS	FG-PISER-21	03	14/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
REPORTE DE PRODUCTO Y SERVICIO NO CONFORME	FG-PISER-22	02	15/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
PROGRAMA ANUAL DE AUDITORIAS INTERNAS	FG-PISER-23	03	17/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
PLAN DE AUDITORIAS INTERNAS	FG-PISER-24	03	17/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
INFORME DE AUDITORIAS INTERNAS	FG-PISER-25	03	17/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
ORDEN INTERNA DE TRABAJO	FG-PISER-26	02	20/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
INDICADORES DE SEGURIDAD Y SALUD EN EL TRABAJO	FG-PISER-27	02	21/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO

PISER SAC.

Fuente: FG-PISER-04

Verificación de Lista Maestra de Registros del SIG

PISER	LISTA MAESTRA DE REGISTROS				Página:	1 de 1
					Versión:	02
					Fecha de Aprobación:	07/01/2016
ESTADÍSTICAS DE INCIDENTES, ACCIDENTES Y ENFERMEDADES OCUPACIONALES	FG-PISER-28	02	21/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
PROGRAMA DE GESTIÓN DE CALIDAD, SEGURIDAD Y SALUD OCUPACIONAL	FG-PISER-29	00	21/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
REGISTROS OPERATIVOS						
MAESTRANZA						
CHECK LIST DE TORNO, TALADRO Y FRESA	FO-MAEST-PISER-01	00	20/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
TRANSPORTE						
CHECK LIST DE MONTACARGAS	FO-TRANS-PISER-01	02	23/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
INSPECCIÓN						
REPORTE DE INSPECCIÓN DIMENSIONAL	FO-INSP-PISER-01	02	07/01/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
REPORTE DE INSPECCIÓN DE HERRAMIENTAS	FO-INSP-PISER-02	01	07/01/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
SOLDADURA						
CHECK LIST DE MAQUINA HARDBANDING	FO-SOLD-PISER-01	00	07/01/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
REGISTROS DE INSTRUCTIVOS DE TRABAJO						
REGISTROS DE MANUALES						
REPORTE OPERATIVO DE CALIDAD	FM-PISER-01	00	23/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
REGISTROS DE PLANES						
INFORME PRELIMINAR AMAGO, INCENDIO, EXPLOSIÓN O EXPLOSIÓN INCENDIO	FP-PISER-01	00	21/03/2016			
INFORME DE SINIESTROS	FP-PISER-02	00	21/03/2016			
REPORTE DE FUGA O DERRAME	FP-PISER-03	00	21/03/2016			

Fuente: FG-PISER-04

Verificación de Lista Maestra de Registros del SIG

PROGRAMA ANUAL DE SIMULACROS	FP-PISER-04	00	21/03/2016			
INFORME DE SIMULACROS	FP-PISER-05	00	21/03/2016			
REGISTRO DE EQUIPOS DE SEGURIDAD O EM	FP-PISER-06	00	21/03/2016			
REGISTROS DE APOYO						
LOGÍSTICA						
ORDEN DE COMPRA	FA-LOG-PISER-01	03	23/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
REQUERIMIENTO DE PRODUCTO O SERVICIO	FA-LOG-PISER-02	03	23/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
ORDEN DE SALIDA Y ENTREGA DE MATERIALI	FA-LOG-PISER-03	03	23/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
GUÍAS DE REMISION	N.A	01	24/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
LISTADO DE MATERIALES DE USO COMÚN	FA-LOG-PISER-04	0	26/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
EVALUACIÓN Y REEVALUACIÓN DE PROVEEDORES CRITICOS	FA-LOG-PISER-05	0	26/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
LISTADO DE REQUISITOS PARA PROVEEDORES Y CONTRATISTAS CRÍTICOS	FA-LOG-PISER-06	0	26/02/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
MANTENIMIENTO						
MANTENIMIENTO DE MÁQUINAS Y EQUIPOS	FA-MANTT-PISER-01	1	08/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
REGISTROS DE SEGURIDAD						
INPECCIONES QHSE	FA-QHSE-PISER-01	0	07/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO
CHECK LIST DE INSPECCIONES QHSE	FA-QHSE-PISER-02	1	07/03/2016	SUPERVISOR QHSE	OFICINA PRINCIPAL. ESTANTE DE FILES	1 AÑO

PISER SAC.

Fuente: FG-PISER-04

Anexo N° 07: Análisis Estadísticos

Evaluación de la confidencialidad de los activos de información

Nivel de compromiso por preservar la confidencialidad de la información del SGC	calificación	Porcentaje del nivel de compromiso por preservar la confidencialidad de la información del SGC
Alto: Existe un alto compromiso		0%
Medio. Existe un compromiso relativamente medio	2	29%
Bajo: Se demuestra poco compromiso con la confidencialidad de la información	4	57%
Nulo: No se aplica ni es asumido por los colaboradores	1	14%
Adverso: La confidencialidad de la información se percibe como una limitación al trabajo		0%
Total	7	

Figura N° 01

Elaboración: Propia

Área que establece los controles de seguridad de la información del SGC	calificación	Porcentaje del área que establece los controles de seguridad de la información del SGC
Gerencia y/o Alta Dirección	3	27%
Logística e Informática	6	55%
QHSE	2	18%
Otros		0%
Total	11	

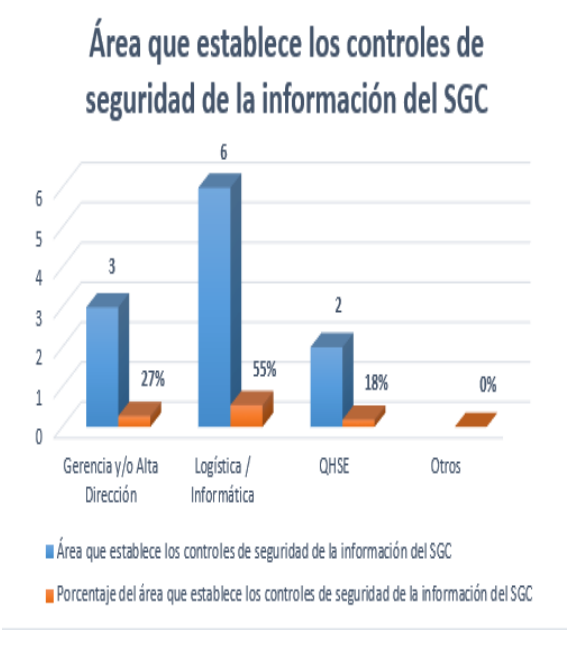


Figura N° 02

Elaboración: Propia

Incidentes de acceso indebido a la información más comunes del SGC	calificación	Porcentaje de los incidentes de acceso indebido a la información más comunes del SGC
Fuga de documentación especializada: manuales, procedimientos, documentación técnica, etc.	7	58%
Fuga de información comercial y administrativa	1	8%
Espionaje industrial de la competencia		0%
Incidencias en información de carácter personal	4	33%
Otros		0%
Desconozco este proceso		0%
Total	12	

Figura N° 03

Elaboración: Propia

Medios de fuga de información del SGC en el área QHSE	calificación	Porcentaje de medios de fuga de información del SGC en el área QHSE
Correo electrónico institucional	4	20%
Correo electrónico personal	1	5%
Dispositivos USB	5	25%
Computadora portátil	6	30%
Medios removibles	3	15%
Otros	1	5%
Total	20	

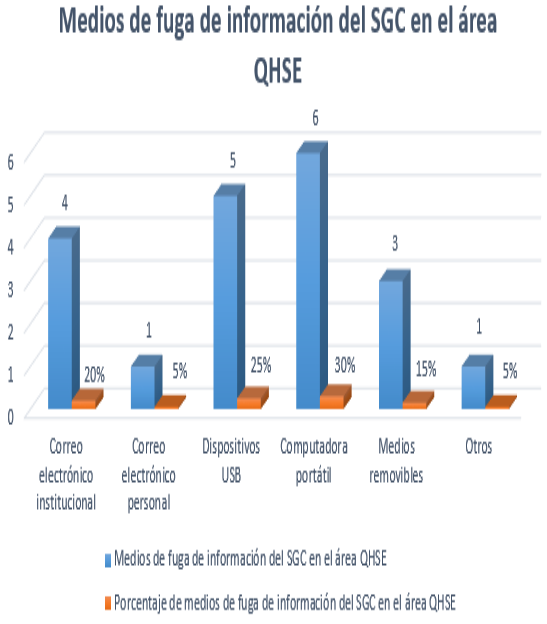


Figura N° 04

Elaboración: Propia

Vectores de fuga de información del SGC	calificación	Porcentaje de los vectores de fuga de información del SGC
Motivaciones personales, profesionales y/o laborales	1	9%
Deshonestidad/ Intereses económicos	2	18%
Desconocimiento / Falta de conciencia		0%
Exceso de confianza	7	64%
Otros	1	9%
Total	11	

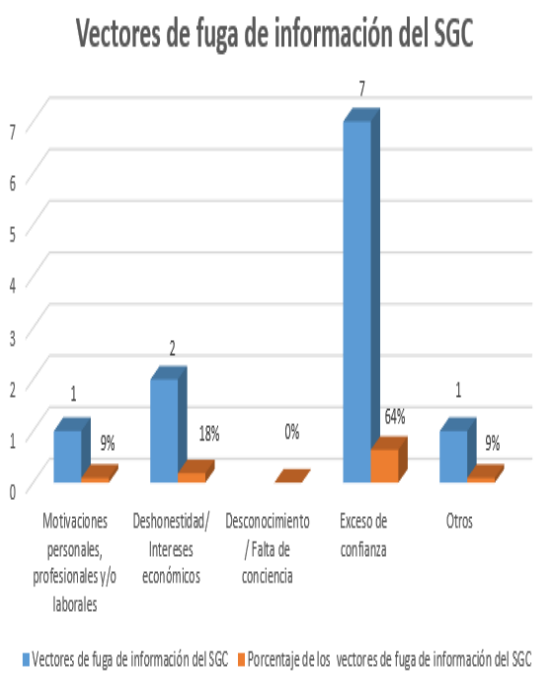


Figura N° 05

Elaboración: Propia

Nivel de frecuencia de incidentes de acceso indebido a documentos del SGC del periodo de Septiembre	calificación	Porcentaje de nivel de frecuencia de incidentes de acceso indebido a documentos del SGC del periodo de Septiembre
Baja: Entre 1y 5	1	14%
Media: Entre 6 y 10	2	29%
Alta: Más de 10	3	43%
Desconozco completamente esta información	1	14%
Total	7	

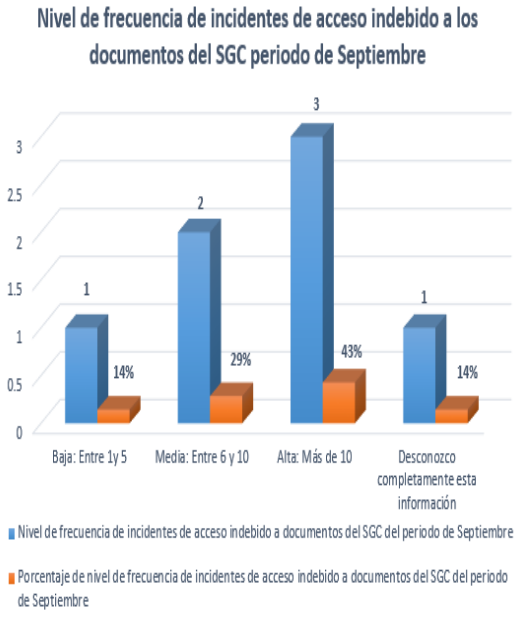


Figura: N° 06

Elaboración: Propia

Nivel de confidencialidad de las personas con acceso a la información del SGC	calificación	Porcentaje del nivel de confidencialidad accesos a la información del SGC
Controlada: Solo el área de QHSE	1	14%
Media: Área de QHSE y otras áreas estratégicas y operativas	5	71%
Alta: Toda la institución	1	14%
Extrema: Es información de dominio público		0%
Total	7	

Figura N° 07

Elaboración: Propia

Nivel de distribución de documentos del SGC	calificación	Porcentaje de distribuciones controladas del SGC
Controlada: Se distribuyen solo copias controladas	4	57%
Media: Algunas veces se distribuyen copias no controladas		0%
Baja: Se distribuyen solo copias no controladas		0%
No controlada: Actualmente no existe control de distribución de copias no controladas	3	43%
Total	7	

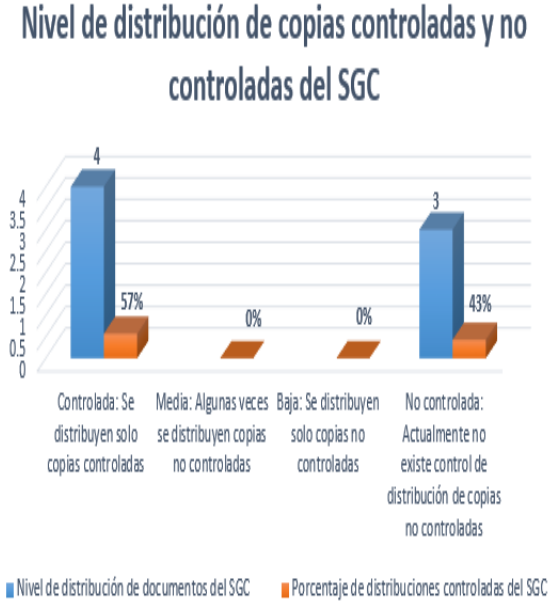


Figura N° 08

Elaboración: Propia

Evaluación de Integridad de los activos de información

Soportes de información	calificación	Porcentaje de soportes de información en el área QHSE
Equipos de Escritorio	5	20%
Equipos Portátiles	7	28%
Memorias USB	6	24%
Discos duros y otros medios removibles	5	20%
Otros	2	8%
Total	25	

Total	7

Figura N° 09
Figura N° 01
Elaboración: Propia

Incidentes de impacto a la integridad de la documentación que son más comunes del SGC	Calificación	Porcentaje de incidentes de impacto a la integridad de la documentación más comunes del SGC
Deterioro de documentos electrónicos	1	6%
Deterioro de documentos físicos	5	29%
Errores en el control de versiones	6	35%
Manipulación / Adulteración de los registros de información	5	29%
Otros		0%
Desconozco este proceso		0%
Total	17	

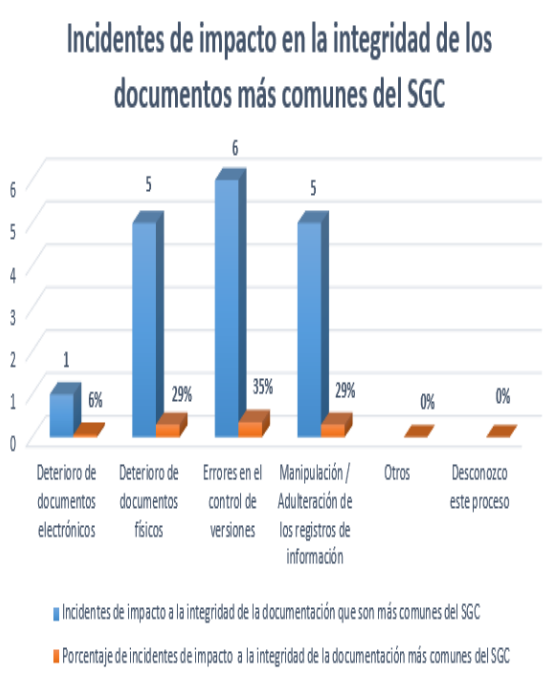


Figura N° 02
Elaboración: Propia

Vectores de pérdida de la integridad de la información del SGC	Calificación	Porcentaje de vectores pérdida de la integridad de la información del SGC
Debilidad de procedimientos y controles	2	18%
Deshonestidad / Rivalidades personales / Cultura organizacional		0%
Limitaciones en la tecnología	5	45%
Exceso de confianza	3	27%
Otros	1	9%
Total	11	

Figura N° 03

Elaboración: Propia

Nivel de frecuencia de incidentes de impacto en la integridad de los documentos del SGC	Calificación	Porcentaje del nivel de incidentes de impacto de integridad de los documentos del SGC en el periodo de Septiembre
Baja: Entre 1 y 5	1	14%
Media: Entre 6 y 10	5	71%
Alta: Más de 10		0%
Desconozco completamente esta información	1	14%
Total	7	

Figura N° 04

Elaboración: Propia

Medios de soportes de información del SGC	Calificación	Porcentaje de medios de soportes de información del SGC
Soporte físico impreso	6	25%
Soporte electrónico en PC´s	4	17%
Soporte en servidor de archivos	4	17%
Soportes de backup en medios externos	6	25%
Discos duros y otros medios removibles	4	17%
Otros		0%
Total	24	

Figura N° 06

Elaboración: Propia

Figura N° 05

Elaboración: Propia

Evaluación de la Disponibilidad de los Activos de información

Nivel de compromiso por preservar la disponibilidad de la información del SGC	Calificación	Porcentaje del nivel del compromiso por preservar la disponibilidad de la información del SGC
Alto. Existe un alto compromiso	1	14%
Medio. Existe un compromiso relativamente medio	4	57%
Bajo. Se demuestra poco compromiso con la disponibilidad de la información	2	29%
Nulo. No se aplica ni es asumido por los colaboradores		0%
Total	7	

Figura N° 01

Elaboración: Propia

Incidentes de impacto a la disponibilidad de la documentación más comunes del SGC	Calificación	Porcentaje de incidentes de impacto a la disponibilidad de la documentación del SGC
Pérdida de documentos físicos	3	30%
Indisponibilidad de servidores	5	50%
Destrucción de los registros de información		0%
Otros	1	10%
Desconozco este proceso	1	10%
Total	10	

Figura N° 02

Elaboración: Propia

Vectores de pérdida de la disponibilidad de documentos del SGC	Calificación	Porcentaje de vectores de pérdida de la disponibilidad de la información del SGC
Debilidad de procedimientos y controles	5	31%
Deshonestidad / Rivalidades personales / Cultura organizacional	1	6%
Limitaciones en la tecnología	6	38%
Exceso de confianza	4	25%
Otros		0%
Total	16	

Figura N° 03

Elaboración: Propia

Nivel de frecuencia de incidentes de impacto de la disponibilidad de los documentos del SGC del periodo de Septiembre	Calificación	Porcentaje del nivel de frecuencia de incidentes de la disponibilidad de los documentos del SGC del periodo de Septiembre
Baja: Entre 1 y 5	1	14%
Media: Entre 6 y 10	5	71%
Alta. Más de 10		0%
Desconozco completamente esta información	1	14%
Total	7	

Figura N° 04

Elaboración: Propia

Respaldos electrónicos más usados en la documentación del SGC	Calificación	Porcentaje de respaldos electrónicos más usados en la documentación del SGC
Respaldo en CD / DVD	2	20%
Respaldo en cintas tape backup		0%
Discos duros y otros medios removibles	7	70%
Otros	1	10%
Total	10	

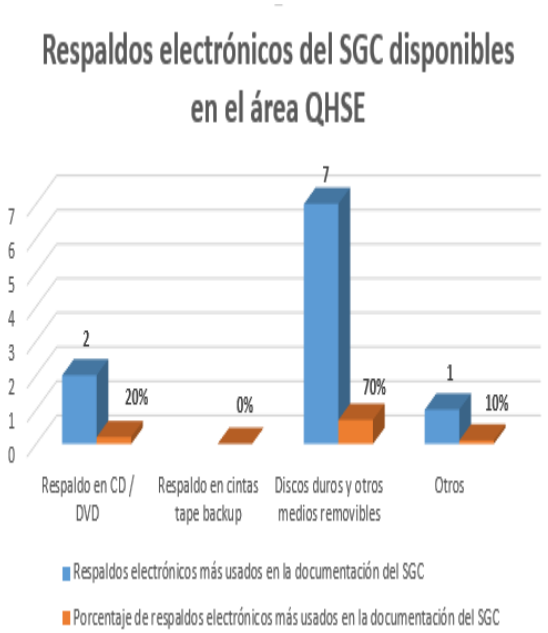


Figura N° 05

Elaboración: Propia

Anexo N° 08: Aceptación de investigación por la empresa PISER S.A.C

PISER S.A.C. Peruana de Inspección y Servicios S.A.C.

RUC: 20525568564

CONSTANCIA DE ACEPTACIÓN DE DESARROLLO DE TESIS

La Gerencia de la empresa "PERUANA DE INSPECCION Y SERVICIOS S.A.C" con RUC 20525568564, con domicilio legal Lote A-224 Parque Industrial Talara – Alta.

HACE CONSTAR

Que el alumno **MANUEL ARMANDO AGURTO CASTILLO**, identificado con DNI 46158659, estudiante de la Universidad César Vallejo de Piura, ha sido aceptado para que realice su **TESIS** con nombre **"Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001"** para fines respectivos de dicha empresa.

En razón de lo expuesto, cumplo con informar y aceptar sobre el desarrollo de la investigación del alumno.

Se expide la presente constancia a solicitud del interesado, para fines que estime convenientes.

Talara, 15 de Octubre del 2016

Ecm. Antonio Echevarría Palacios
GERENTE OPERACIONES
PISER SAC.

PISER

Lote A - 224 Parque Industrial Talara Alta (Costado de Petrex) ventasyservicios@piser.com.pe - peru.insp@hotmail.com
Telf.: 073-386013 - Cel. RPM: #983481166 - #994186561 - #981377480 / Sitio Web: www.piser.com.pe

Fuente y Elaboración: PISER S.A.C

Anexo N° 09: Actas de Reuniones

Acta de reunión para la elaboración de los controles de seguridad a los activos de información

Acta de Reunión de Elaboración de una propuesta de salvaguardas de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001

Con fecha 03 del mes de OCTUBRE del 2016 y siendo las 9:00Am horas se ha llevado a cabo la reunión ordinaria a cargo del alumno encargado de la elaboración del desarrollo de Tesis con el área de SEGURIDAD (QHSE) de la empresa: Peruana de Inspección y Servicios S.A.C, la cual tuvo como asistentes a:

Asistentes	Cargo
Mario Chuye Tavara	Sup. QHSE
Andrea Olano Zapata.	Asistente QHSE.

En la reunión se trató de:

DAR A CONOCER EL TEMA DE ELABORACIÓN DE UNA PROPUESTA DE SALVAGUARDAS.
LA PROBLEMÁTICA, LOS TRES PILARES FUNDAMENTALES DE LA NORMA ISO 27001, OBJETIVOS, VARIABLE.
RESULTADOS, ANALISÍS Y DISCUSIONES
TAMBIÉN CONVERSÓ SOBRE LOS ANÁLISIS DE LOS RESULTADOS QUE SE APLICÓ A CADA INDICADOR SEGÚN LOS TRES PILARES DE LA ISO27001

Concluyéndose y acordándose:

CONCLUYÉNDOSE CON LO EXPUESTO, CUMPLO CON INFORMAR Y ACEPTAR LA ELABORACIÓN DE UNA PROPUESTA DE SALVAGUARDAS DE LOS ACTIVOS DE INFORMACIÓN DE LOS PROCESOS IMPLEMENTADOS POR EL ESTÁNDAR ISO 9001 EN EL ÁREA QHSE, BASADO EN LA NORMA ISO 27001

Finalmente, siendo las 9:40Am horas del presente mes se levanta la sesión.

Para mayor constancia se firma la presente por:

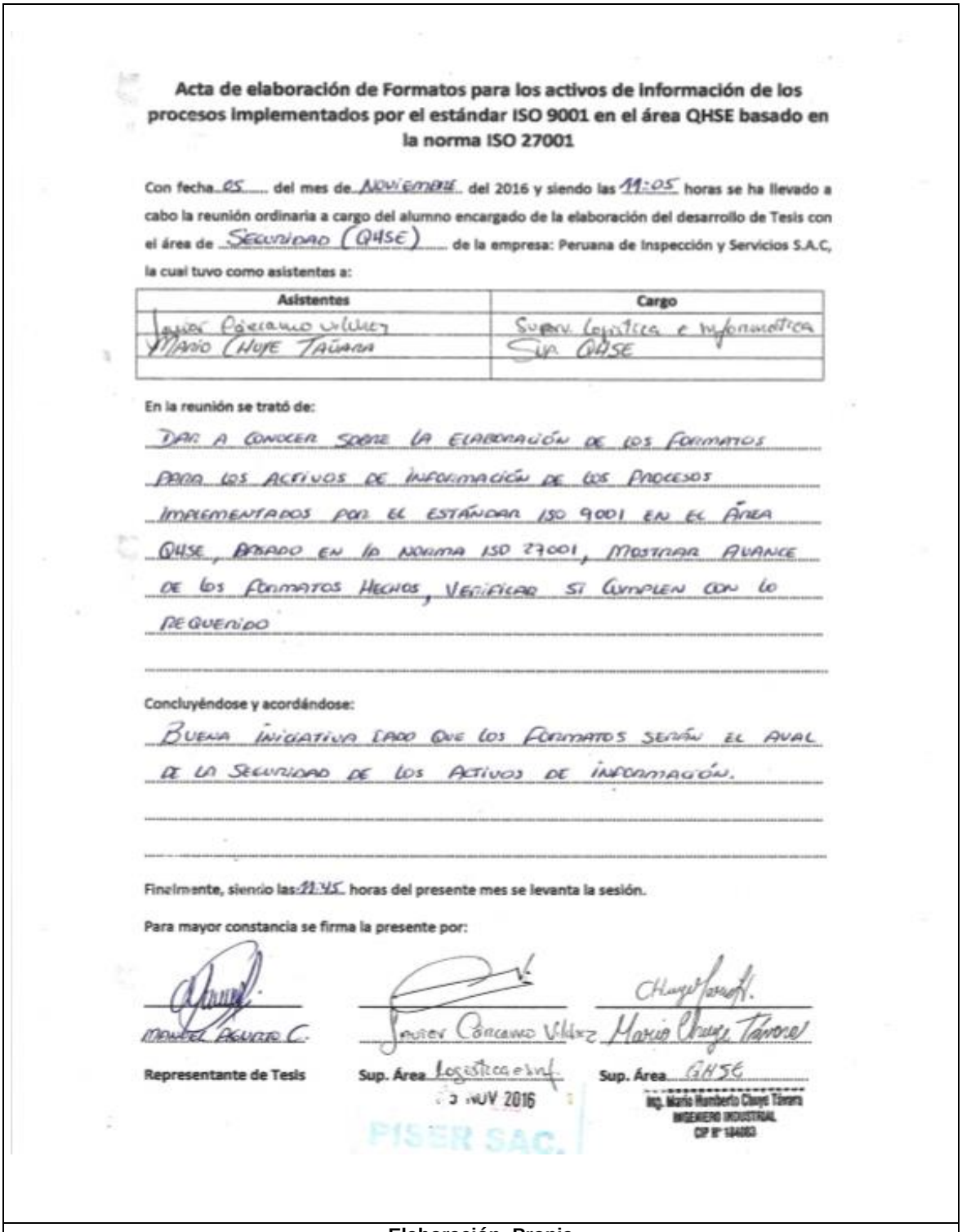
MANUEL AGURTO C.	Mario Chuye Tavara	Andrea Olano Zapata.
Representante de Tesis	**Sup. Área** Sup. QHSE	**Sup. Área** Asist. QHSE.

Ing. Mario Humberto Chuye Távara
INGENIERO INDUSTRIAL
CIP N° 184083

03 OCT 2016
PISER SAC.

Elaboración: Propia

Acta de reunión para la elaboración de formatos de seguridad a los activos de información



Acta de elaboración de Formatos para los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001

Con fecha 05 del mes de NOVIEMBRE del 2016 y siendo las 11:05 horas se ha llevado a cabo la reunión ordinaria a cargo del alumno encargado de la elaboración del desarrollo de Tesis con el área de SEGURIDAD (QHSE) de la empresa: Peruana de Inspección y Servicios S.A.C, la cual tuvo como asistentes a:

Asistentes	Cargo
Javier Palomino Valdez	Supervisor Logística e Informática
Mario Chuye Tavara	Sup. QHSE

En la reunión se trató de:

DAR A CONOCER SOBRE LA ELABORACIÓN DE LOS FORMATOS PARA LOS ACTIVOS DE INFORMACIÓN DE LOS PROCESOS IMPLEMENTADOS POR EL ESTÁNDAR ISO 9001 EN EL ÁREA QHSE, BASADO EN LA NORMA ISO 27001, MOSTRAR AVANCE DE LOS FORMATOS HECHOS, VERIFICAR SI CUMPLEN CON LO REQUERIDO

Concluyéndose y acordándose:

BUENA INICIATIVA DADO QUE LOS FORMATOS SERÁN EL AVAL DE LA SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN.

Finalmente, siendo las 11:45 horas del presente mes se levanta la sesión.

Para mayor constancia se firma la presente por:

MANUEL AGUILAR C. — Representante de Tesis

Javier Palomino Valdez — Sup. Área Logística e Inf.

Mario Chuye Tavara — Sup. Área QHSE

05 NOV 2016

Ing. Mario Humberto Chuye Tavara
INGENIERO INDUSTRIAL
CIP N° 184083

FISER SAC.

Elaboración: Propia

Acta de reunión para la finalización de investigación

Acta de Finalización de Tesis del Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE, basado en la norma ISO 27001.

Con fecha 03 del mes de DICIEMBRE del 2016 y siendo las 9:50am horas se ha llevado a cabo la reunión ordinaria a cargo del alumno encargado de la elaboración del desarrollo de Tesis con el área de SEGURIDAD (QHSE) de la empresa: Peruana de Inspección y Servicios S.A.C, la cual tuvo como asistentes a:

Asistentes	Cargo
ANTONIO ECHEVARRIA PRADOS	GERENTE DE OPERACIONES
JAVIER CÁRCAMO VILCHEZ	LOGÍSTICA E INFORMÁTICA

En la reunión se trató de:

DEMOSTRACIÓN DE LA INVESTIGACIÓN SOBRE EL DIAGNÓSTICO DE LOS ACTIVOS DE INFORMACIÓN DE LOS PROCESOS IMPLEMENTADOS POR EL ESTÁNDAR ISO 9001 EN EL ÁREA QHSE, BASADO EN LA NORMA ISO 27001. SEÑALANDO LOS RESULTADOS, OBJETIVOS, CONCLUSIONES RECOMENDACIONES, DISCUSIONES Y LOS ANEXOS.

Concluyéndose y acordándose:

LA ACEPTACIÓN Y CONFORMIDAD DE LO INVESTIGADO Y HACER ENTREGA DE LOS FORMATOS ELABORADOS PARA SU RESPECTIVA APLICACIÓN EN LA EMPRESA PISER S.A.C.

Finalmente, siendo las 11:30 horas del presente mes se levanta la sesión.

Para mayor constancia se firma la presente por:

MANUEL AGUSTO C.
Representante de Tesis

Gerente

Javier Cárcamo V.
Sup. Área Logística & Informática

PISER SAC.

Elaboración: Propia

2016

Anexo N° 10: Propuesta Técnica

Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001

MANUEL ARMANDO AGURTO CASTILLO

GENERALIDADES

Título:

- Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001

Autor:

- Manuel Armando Agurto Castillo
  Escuela de Ingeniería
  Facultad de Sistemas

Asesor:

- Ing. Carmen Quito Rodríguez
  Universidad César Vallejo - Piura

Tipo de Investigación:

- Investigación Descriptiva, porque se detalla, estudia e interpreta el proceder la variable Activos de la Información, sin manipularlos.

Línea de Investigación:

- Auditoria de Sistemas y Seguridad de la Información

Localidad:

- Lote A – 224 Parque Industrial Talara Alta (Al costado de Base Petrex)

Duración de Investigación:

- FECHA DE INICIO: (Abril 2016)
- FECHA DE FIN: (Diciembre 2016)

I. Introducción

Peruana de Inspección y Servicios S.A.C (PISER S.A.C) es una empresa ubicada Lote A-224 Parque Industrial Talara - Alta, dedicada a prestar diversos servicios en actividades industriales, petroleras y otras, desarrollando sus actividades desde el año 2007 en el rubro petrolero". (PISER S.A.C, 2014). Actualmente la información en la empresa Peruana de Inspección y Servicios S.A.C es el activo más valioso, cada vez aparecen más riesgos a los que están comprometidos los activos de información de los procesos implementados del estándar ISO 9001 la cual se debe preservar el aspecto más seguro y eficiente posible. Las dimensiones de seguridad no solo implica tecnología, también se debe tener en cuenta todos los aspectos organizativos y relativos al personal de trabajo de dicha empresa, el área seguridad en el rubro petrolero es conocida por las siglas en inglés de "Quality, Health, Safety & Environment (QHSE), en español Calidad, Salud, Seguridad y Ambiente las cuales representan las principales funciones dentro del área de seguridad". (Manual de Organización y Funciones, 2016), el área QHSE es una de las principales por lo que está inmersa a la cantidad de información tanto de personal, transporte, operaciones e implementación del estándar de calidad, siendo estos últimos uno de los más importantes por su ejecución de sus procedimientos implementados la cual genera información. Para la empresa Peruana de Inspección y Servicios S.A.C los activos de información son fundamentales y deben tratarse siempre como un proceso más de la empresa, la cual se realizará un diagnóstico a los activos de información que implica comprender los activos y operaciones a resguardar, localizar los puntos débiles de cada procedimiento ejecutado y sobre todo el reconocimiento de las amenazas posibles presentadas, determinar los indicadores de seguridad según las tres dimensiones de la norma ISO 27001 e identificar la frecuencia y porcentaje para la confidencialidad, integridad y disponibilidad para que así la empresa pueda tener continuidad dentro de los procesos implementados por el estándar ISO 9001.

II. Datos Generales

Empresa	PERUANA DE INSPECCIÓN Y SERVICIOS S.A.C
Área	Quality, Health, Safety & Environment (QHSE)
Norma para Diagnóstico	Norma ISO 27001
Alcance del Sistema	Procesos Implementados Estándar ISO 9001 - Procedimientos de Gestión. - Procedimientos Operativos. - Procedimientos de Seguridad. - Procedimientos de Apoyo.
Alcance Geográfico	Provincia de Talara y Departamento Piura
Fecha de la Propuesta	(Diciembre 2016)

III. Objetivos de la Propuesta

Objetivo General

- Elaborar un Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.

Objetivos Específicos

- Identificar los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.

- Determinar los indicadores de seguridad de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.

- Elaborar una propuesta de controles de seguridad para los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE basado en la norma ISO 27001.

IV. Propuesta Técnica

Metodología de Trabajo

Se llevó a cabo el Diagnóstico bajo la consultoría de expertos en el tema, el cual consistió en recibir asesorías en el campus universitario y en la empresa de manera continua con la finalidad de orientarse de forma oportuna y eficiente en el diagnóstico basado en la Norma ISO 27001 a los procesos implementados por el Estándar ISO 9001 en el área QHSE. Asimismo, el desarrollo obtuvo una duración estimada de ocho (8) meses, además se realizó la aplicación de instrumentos para la recolección de datos a lo largo de todo el desarrollo del proyecto a fin de garantizar la calidad de la investigación.

Finalmente, la empresa Peruana de Inspección y Servicios S.A.C, como parte de su compromiso, pondrá a disponibilidad la información del Área QHSE y el tiempo posible para poder interactuar para la recolección de información para dicho diagnóstico basado en la norma ISO 27001.

Etapas de Propuestas

En base a la elaboración del diagnóstico de los activos de información de los procesos implementados en el área se preparó, en conjunto con el líder del área QHSE, toda la base documental necesaria que fue revisada y firmada para mayor validez, para cumplir todos los requisitos de la norma ISO 27001 para dicho diagnóstico. Se realizaron reuniones con el Supervisor y Asistente del área QHSE, cuyo propósito era identificar los activos de información de los procesos implementados, para su respectivo diagnóstico, donde se realizó unas listas de cotejo para su verificación, seguimiento y revisar la lista maestra de documentos internos, externos y la lista maestra de registros de todo los procesos implementados, posteriormente determinar los indicadores según los tres pilares fundamentales de la norma ISO 27001, confidencialidad, integridad y disponibilidad que se obtiene a través del análisis dado su frecuencia y porcentaje de incidencias, además como último objetivo se elaboró una propuesta de controles de seguridad de los activos de información con las conclusiones y recomendaciones a seguir del diagnóstico.

Equipo Profesional

Universidad César Vallejo pondrá a disposición el siguiente personal:

- **Mg. Carmen Zulema Quito Rodríguez**. Asesora Líder. Responsable de liderar el desarrollo de investigación, realizar coordinaciones y seguimiento de la continuidad del proyecto con la finalidad de garantizar el cumplimiento de los objetivos.
- **Ing**. **Jaime Leandro Madrid Casariego.** Asesor experto. Responsable, habilitación y aceptación del proyecto de investigación.
- **Ing. Rubén More Valencia.** Asesor experto. Asesoría en el planteamiento del problema.

Asesor experto en la línea de investigación de Auditoria de sistemas y Seguridad de la Información:

- **Ing. Carlos Augusto Correa García.** Asesor experto. Asesoría en el tema de investigación.

Peruana de Inspección y Servicios S.A.C pondrá a disposición el siguiente personal:

- **Ing. Jorge Cruzado Cortez.** Gerente general de la empresa PISER.S.A.C.
- **Econ. Antonio Echevarría Palacios.** Gerente de operaciones. Responsable y seguimiento en operaciones en la empresa.
- **Ing. Mario Chuye Távara.** Supervisor QHSE. Responsable en la certificación del estándar ISO 9001 y responsable de actualización de documentos.
- **Adm. Andrea Olano Zapata.** Asistente QHSE. Responsable en los activos de información de los procesos implementados por el estándar ISO 9001.
- **Ing. Javier Cárcamo Vílchez.** Supervisor De logística e informática. Responsable en TI y seguridad de información.

Cronograma de Actividades

Elaboración: Propia

V. Propuesta Económica

Se detalla en el siguiente cuadro el monto total que se invirtió para el desarrollo de la investigación, el total ascendió a s/. 2688.00, no incluye los costos generados en pasajes de viaje de Talara a Piura y de la movilidad.

Rubro / Material / Actividad	MONTO
BIENES	
Papel	s/.30.00
Folder	s/.10.00
USB	s/.60.00
Laptop	s/.1,990.00
SERVICIOS	
Fotocopiado	s/.20.00
Digitado – Escaneo	10.00
Impresiones	s/.248.00
Anillado	s/.20.00
REMUNERACIONES	
Validación por expertos	s/.300.00
Total	s/2688.00

Elaboración: Propia

Se detalla en el siguiente cuadro el monto invertido en los pasajes de Talara – Piura de ida y regreso, también se incluye el monto de la movilidad y refrigerio, estos gastos fueron invertidos para la asesoría por los expertos de la universidad César Vallejo tal como se nombró en el equipo profesional que estará en disposición del campus universitario, el total del monto ascendió a s/.702.00 tal como se demuestra en el cuadro.

Pasajes / Movilidad / Refrigerio (Setiembre – Diciembre)	TOTAL
EPPO / Talara – Piura	
Ida – Regreso	s/.360.00
Movilidad / Talara – Piura	
Moto taxi para agencia y UCV Ida - Regreso	s/.252.00
Refrigerio / Piura	
Energizantes, agua, etc.	s/.90.00
Total	s/. 702.00

Elaboración: Propia

2016

Anexo N° 11:

Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001

MANUEL ARMANDO AGURTO CASTILLO

Diagnóstico de la Situación Actual en el área QHSE

Breve Reseña Histórica de la empresa PISER S.A.C

"Peruana de Inspección y Servicios S.A.C (PISER S.A.C) es una empresa ubicada Lote A-224 Parque Industrial Talara - Alta, dedicada a prestar diversos servicios en actividades industriales, petroleras y otras, desarrollando sus actividades desde el año 2007 en el rubro petrolero". (PISER S.A.C, 2014). Actualmente la información en la empresa Peruana de Inspección y Servicios S.A.C es el activo más valioso, cada vez aparecen más riesgos a los que están comprometidos los activos de información de los procesos implementados del estándar ISO 9001, la cual se debe preservar el aspecto más seguro y eficiente posible.

Misión y Visión de la empresa PISER S.A.C

En la empresa PISER S.A.C se plantea una Misión y una Visión claramente definidas, las cuales son tomadas como el núcleo central de la orientación organizacional. A continuación, son presentadas.

Misión

Brindar servicios de calidad a la industria petrolera, a través del uso eficiente de recursos y capital humano especializado, comprometido con la seguridad y cuidado del medio ambiente. (Brochure PISER, 2016)

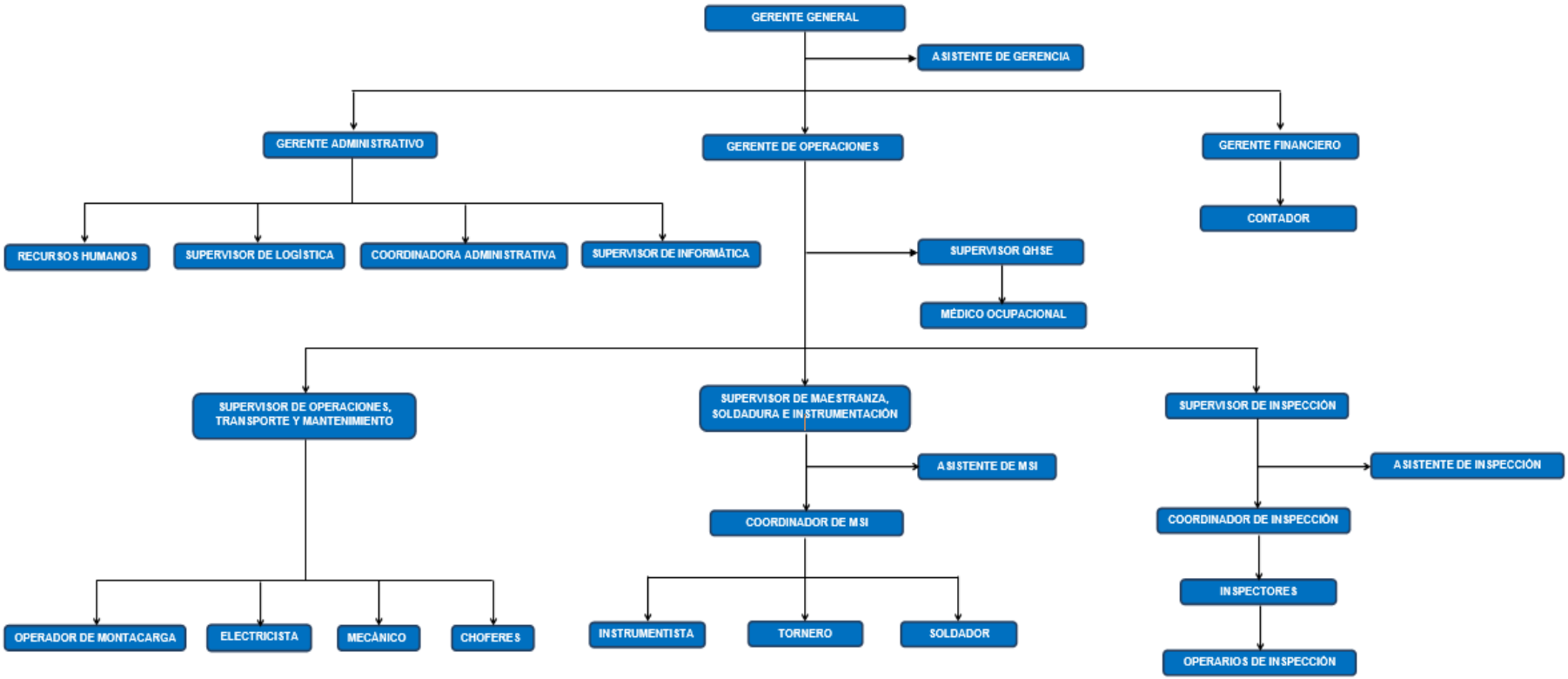
Visión

Ser una empresa líder, a nivel nacional, en la prestación de servicios a la industria petrolera, manteniendo elevados estándares de calidad y competitividad; aplicando una política que promueva la salud, la seguridad y el cuidado del medio ambiente, bajo un entorno de mejora continua. (Brochure PISER, 2016)

Cabe destacar que las tecnologías de Información y Comunicaciones – TIC's deben brindar el soporte necesario para cumplir con la misión y coadyuvar al alcance de la visión empresarial.

Organización y Funciones Generales

A continuación, se muestra el organigrama de PISER S.A.C



Fuente: MA-PISER-02

Diagnóstico de la situación actual operativo y tecnológico

El diagnóstico de la situación incluye la revisión y el análisis de la situación actual de la organización, tomando como referencia aspectos internos desde el punto operativo y tecnológico.

En primera instancia, se presenta un Diagnostico de la Situación Actual de manera general de la empresa PISER S.A.C mediante un FODA.

Fortalezas	**Debilidades**
-Personal del área QHSE con alta capacidad técnica y experiencia profesional. **-**Permanente coordinación entre los colaboradores del área QHSE. **-**Capacidad del área de TI y QHSE para gestionar las necesidades de TIC con la Alta Dirección. **-**Profesionalismo, compromiso y vocación de servicio del personal del área QHSE.	**-**Falta de planificación integral y cooperativa de las TIC. **-**Gestión de Servicios de TIC no estructurado. **-**Limitada infraestructura de TI, se cuenta con un servidor de limitadas capacidades que atienda los servicios del área QHSE. **-**Deficiente integración a nivel de arquitectura de datos y sistemas TI. **-**Niveles de seguridad con alto grado de riesgo en la seguridad de la información.
Oportunidades	**Amenazas**
-Alta dirección comprometida con la mejora de los procesos y servicios soportados por las TIC y la seguridad de su información. **-**Desarrollo de nuevas tecnologías en el mercado; tendencias tecnológicas y buenas prácticas en la seguridad de los activos de información. **-**Conocimiento del colaborador común en uso de TI, tecnología móvil, internet y otros. **-**Modelos de tercerización de servicios de TIC consolidados en el mercado.	**-**Insatisfacción del área QHSE en función a algunos servicios de TI que brinda el área de TI por la falta de seguridad de su información. **-**Limitaciones presupuestales. **-**Procedimientos administrativos con intereses particulares que podrían afectar el principio de transparencia.
Elaboración: Propia	

Área QHSE

Las dimensiones de seguridad no solo implica tecnología, también se debe tener en cuenta todos los aspectos organizativos y relativos al personal de trabajo de dicha empresa, el área seguridad en el rubro petrolero es conocida por las siglas en inglés de “Quality, Health, Safety & Environment (QHSE), en español Calidad, Salud, Seguridad y Ambiente las cuales representan las principales funciones dentro del área de seguridad”. (Manual de Organización y Funciones, 2016), QHSE es una de las principales áreas por lo que está inmersa a la cantidad de información tanto de personal, transporte, operaciones e implementación del estándar de calidad, siendo estos últimos uno de los más importantes por su ejecución de sus procedimientos implementados la cual genera información**.**

Perfil de Puesto del Encargado del Área QHSE y del Estándar ISO 9001

1.- DATOS GENERALES

Título del Puesto: Supervisor QHSE

2.- RELACION CON OTROS PUESTOS

Puesto al que reporta: Gerente de Operaciones

Puestos que le reportan: Médico Ocupacional

3.- COMPETENCIAS

Educación:	**Mínima**	**Óptima**
Tipo:	Superior	Superior
Grado:	Técnico	Universitario Titulado, Colegiado.
Especialidad:	Administrador Industrial, Medio Ambiente	Ing. Industrial – Biólogo.
Formación:	**Mínima**	**Óptima**
Tipo	Cursos	Cursos Especializados al giro del negocio.
Especialidad	Seguridad y Salud Ocupacional.	Sistema Integrado de Gestión.

Experiencia	Mínima	Óptima
	01 año de Supervisión SSO	03 años de Supervisión SSO.

Habilidades

- Establecer y fomentar las relaciones interpersonales positivas del personal.
- Capacidad de Diálogo.
- Manejo de Personal.
- Concertación de situaciones conflictivas.
- Disposición para integrar equipos de trabajo y trabajar en equipo.
- Capacidad para la toma de decisiones, supervisión y coordinación de proyectos.

4.- PRINCIPALES FUNCIONES Y RESPONSABILIDADES

- Desarrollar e implementar Políticas de Calidad, Seguridad, Salud ocupacional y Medio Ambiente en Manuales y Procedimientos.
- Elaborar las pautas y lineamientos básicos en materia de Calidad, Seguridad, Salud ocupacional y Medio Ambiente.
- Coordinar las Auditorías Externas de Calidad, Seguridad, Salud ocupacional y Medio Ambiente.
- Realizar inspecciones periódicas de seguridad.
- Paralizar cualquier labor en operación, que se encuentra con evidentes condiciones sub-estándares que atente contra la integridad de las personas, equipos e instalaciones, hasta que se eliminen dichas condiciones.
- Decretar, evaluar y reportar a la Gerencia General y de Operaciones, acciones y/o condiciones sub – estándar que puedan generar incidentes o accidentes de trabajo. Así mismo deberá proponer las medidas correctivas y realizar el seguimiento de su aplicación.
- Poner en funcionamiento y mejorar el Programa Anual de Actividades de Seguridad.
- Coordinar con los Miembros del Comité de Seguridad para la ejecución de actividades.

- Elaborar y coordinar Planes de Contingencias y Emergencias.
- Participar y representar a la Empresa en foros y grupos de trabajo sobre Seguridad y Medio Ambiente.
- Identificar los riesgos contra la seguridad y salud que existan en las actividades que desarrolla PISER S.A.C.
- Ejecutar el plan de primeros auxilios.
- Elaborar en proyectos nuevos la factibilidad ambiental, en los casos que fuese aplicable.
- Capacitar y auditar en temas de Calidad, Seguridad, Salud ocupacional y Medio Ambiente a las áreas de la Empresa.
- Tener al día el Libro de Actas, describiendo el control del cumplimiento de los acuerdos y propuestas del Comité.
- Responsable de la administración del SIG entre las demás dependencias de la empresa.
- Compromiso con el mejoramiento continuo del desempeño del SIG.
- Realizar y analizar las estadísticas de los incidentes, accidentes y enfermedades ocupacionales ocurridos en la empresa emitiendo las recomendaciones respectivas.
- Asegurarse de que se establecen, implementan y mantienen los procesos necesarios para el Sistema de Gestión de la Calidad, Seguridad, Salud ocupacional y Medio Ambiente.
- Elaborar, Implementar, Controlar, Difundir y Resguardar toda la documentación (Registros, Formatos, Objetivos, Programa y Planes de Gestión) relevante del SIG.
- Mantener actualizada la información referida al Sistema Integrado de Gestión.
- Aplicar técnicas de monitoreo y medición del desempeño del SIG.
- Mantener informado al Comité de SST y a la Alta dirección, del avance en la implementación, mantenimiento y mejora del Sistema Integrado de Gestión.
- Difusión de los Procedimientos de Gestión del SIG.
- Informar a la Alta Dirección sobre el desempeño del SIG y de cualquier necesidad de mejora.

- Coordinar los planes de acción con los responsables de las distintas áreas de los sistemas de gestión.
- Coordinar y planificar las Auditorias del SIG, en los servicios de los clientes, así como en las instalaciones de la empresa (Oficina y Talleres).
- Facilitar la labor de planear, organizar, dirigir, ejecutar y controlar el cumplimiento de estándares, procedimientos, prácticas, reglamento interno en coordinación con Gerencia General y de Operaciones.
- Llevar el control del cumplimiento de las disposiciones legales aplicables.
- Ejecutar y coordinar actividades relacionadas con el registro, procesamiento, Clasificación, verificación y archivo del movimiento documentario.
- Implementar Directivas Especificas de la organización.
- Revisar la estructura organizativa, proponer mejoras y ajustes.
- Realizar el Programa Anual de Capacitaciones.
- Realizar reportes regulares del avance en la implementación de los objetivos de la Organización.
- Otras funciones que le asigne la Gerencia General.

Tipo de Empresa, Razón Social y Giro del Negocio

Nombre **:** Peruana de Inspección y Servicios S.A.C (PISER S.A.C).

Dirección **:** Lote A-224 Parque Industrial Talara Alta (Costado Petrex)

Gerente General **:** Ing. Jorge Cruzado Cortez

Teléfono **:** 981377480

Rubro al que se dedica: Servicios Petroleros a diversas empresas en Talara

Metodología

La Norma ISO 27001

ISO 27001 se ha desarrollado con el propósito de ocuparse como molde para la organización; La implementación, operación, monitorización y mejoramiento de un Sistema de Gestión de Seguridad de la Información (SGSI) para la ejecución de cualquier empresa; Al respecto, (Cañizares, y otros, 2011) señala que, “Cada

empresa tiene que proteger con tres de las características incorporadas a la información, las cuales son de mucha utilidad". Es decir, la proposición de esta norma está enfocada a gestionar la seguridad de la información.

Procesamiento de la información

Herramienta

La herramienta que se utilizó para el procesamiento de la información fue el Excel 2013 quien brinda buena esencia para la utilización de enorme capacidad de información y posibilita desarrollar con exactitud estudios estadísticos asertivos que ayudaran al desarrollo del diagnóstico de los activos de información de los procesos implementados del estándar ISO 9001 de forma apropiada.

Resumen de Resultados de Seguridad de la Información

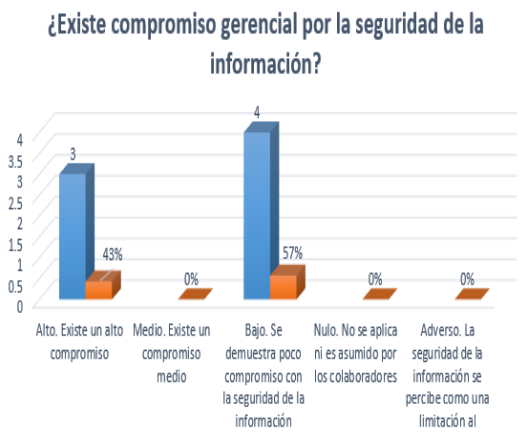
Después de haber aplicado los instrumentos de cada dimensión según la Norma ISO 27001, se realizó también un instrumento para la recolección de información para ver cuán importante es la seguridad por parte de alta gerencia y colaboradores.

Como se aprecia en la figura N° 01de la encuesta, se observó que el 57% de los colaboradores reveló que se demuestra poco compromiso gerencial con la seguridad de la información, mostrándose que el nivel de compromiso gerencial por la seguridad de la información sea considerada como baja, seguidamente con el 43% se mostró que existe un alto compromiso gerencial por la seguridad de la información, revelándose que el nivel de compromiso gerencial por la seguridad de la información sea considerable alto.

Como se aprecia en la figura N° 02 de la encuesta, se obtuvo que el 57% de los colaboradores reveló que no existe compromiso gerencial por la seguridad de la información, seguidamente con un parecido porcentaje de 14% se mostró que se demuestra el compromiso gerencial por la seguridad de la información es con la aplicación políticas de seguridad, otro es con difusión de boletines o

Compromiso gerencial por la seguridad de la información	Calificación	Porcentaje del compromiso gerencial por la seguridad de la información
Alto. Existe un alto compromiso	3	43%
Medio. Existe un compromiso medio		0%
Bajo. Se demuestra poco compromiso con la seguridad de la información	4	57%
Nulo. No se aplica ni es asumido por los colaboradores		0%

Existe Compromiso gerencial	Calificación	Porcentaje del compromiso gerencial por la seguridad de la información
Políticas de seguridad	1	14%
Charlas de sensibilización		0%
Difusión de boletines o recomendaciones de seguridad de la información	1	14%
Normatividad de seguridad de la información	1	14%
Otros		0%
No Existe	4	57%
Total	7	



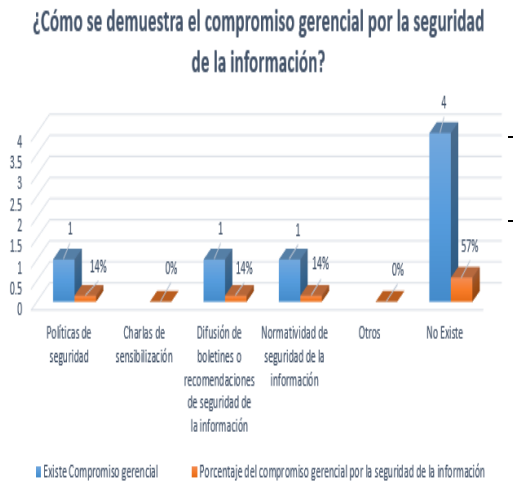


Figura N° 02

Elaboración: Propia

recomendaciones de seguridad de la información y por último señaló que es con la normatividad de seguridad de la información que demuestra gerencia.

Tal como se demuestra en la figura N° 03 de la encuesta, el 57% de los colaboradores reveló que hay conciencia pero no está generalizada en todos los colaboradores, demostrándose que el nivel de existencia de conciencia en la seguridad de la información en los colaboradores sea considerada como media, la cual el 29% se obtuvo que por lo general no existe conciencia en la seguridad de la información, demostrándose un nivel bajo en la existencia de conciencia en la seguridad y finalmente se detectó que el 14% de los colaboradores indicó que no existe conciencia en la seguridad de la información o no asume un nivel de compromiso, es decir, este es nulo.

Existe conciencia en la seguridad de la información en los trabajadores	Calificación	Porcentaje de conciencia en la seguridad de la información en los trabajadores
Alta. En general existe conciencia en la seguridad de la información		0%
Media. Hay conciencia pero no está generalizada en todos los colaboradores	4	57%
Baja. Por lo general no existe conciencia en la seguridad de la información	2	29%
Nula. En general no existe conciencia en la seguridad de la información	1	14%
Total	7	

Figura N° 03

Elaboración: Propia

En la pregunta N° 04 de la encuesta, se apreció que el área que estable los controles de seguridad de la información es logística e informática con un porcentaje de 67% demostrado por los colaboradores, por debajo con el 22% se mostró que el área QHSE es la que establece los controles de seguridad de la información y por último con un porcentaje de 11% se indicó que gerencia y/o alta dirección son quienes establece los controles de seguridad de la información.

En la figura N° 05 de la encuesta, se observó que el 55% de los colaboradores QHSE y logística e informática se limita a realizar su trabajo técnico. No aborda el tema de seguridad de la información, seguidamente con el 27% demostró que la participación de QHSE y logística e informática si demuestran su compromiso con la seguridad de la información y finalmente ambos con el mismo porcentaje de 9% revelaron que aplican políticas de seguridad de la información y realizan charlas de conocimiento y sensibilización.

Tal como se aprecia en la figura N° 06 de la encuesta, se identificó que el 71% de los colaboradores desconoce el proceso de la aplicación de controles de seguridad de la información, demostrándose ambas con el 14% de los

Participación de QHSE y Logística e Informática en la seguridad de la información	Calificación	Porcentaje de participación de QHSE y Logística e informática en la seguridad de la información
Demuestra su compromiso con la seguridad de la información	3	27%
Aplica políticas de seguridad de la información	1	9%
Realiza charlas de conocimiento y sensibilización	1	9%
Difusión de boletines y/o recomendaciones de la seguridad de la información		0%
Se limita a realizar su trabajo técnico. No aborda el tema de seguridad de la información	6	55%
Otro		0%
Total	11	

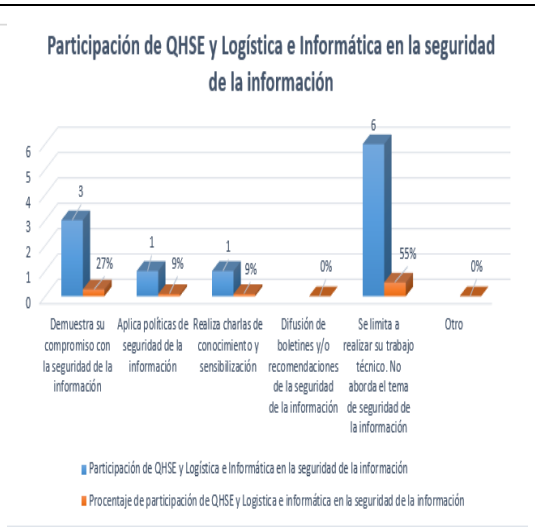


Figura N° 05
Elaboración: Propia

Figura N° 04
Elaboración: Propia

colaboradores que se aplican controles en base a una adecuada evaluación de riesgos y por último también con el mismo porcentaje se revelo que muy pocos saben de controles y sin una adecuada evaluación de riesgos.

Controles de seguridad de la información	Calificación	Porcentaje de aplicación de controles de seguridad de la información
Se aplican controles en base a una adecuada evaluación de riesgos	1	14%
Se aplican controles sin una adecuada evaluación de riesgos		0%
Se muy pocos controles y sin una adecuada evaluación de riesgos	1	14%
Desconozco este proceso	5	71%
Total	7	

Figura N° 06

Elaboración: Propia

Situación Tecnológica de PISER S.A.C

PISER S.A.C cuenta actualmente con una infraestructura tecnológica que permite la comunicación y el acceso a la información de las diferentes áreas. Sin embargo, aspectos como seguridad de la información, control y eficacia en los procesos desarrollados son aspectos que no han sido cubiertos en su totalidad.

A continuación, se presentan la distribución de equipos tecnológicos usados en PISER S.A.C

Hardware y Software de la empresa PISER S.A.C

SITUACIÓN INFORMÁTICA ACTUAL DE PISER S.A.C

Área: Dpto. Sistemas e Informatica

1. **Características de Hardware Utilizado por los usuarios.**

	Equipos	Total	Cantidad Por Procesador						Observaciones
Hardware	PC's	05	Intel core i7	Intel core i5	Intel core i3	Intel dual core			Ubicados en Base Op. Piser
		Tiempo en uso			5 4 años.				
	Laptops	04	Intel core i7	Intel core i5	Intel core i3	Intel dual core			Ubicados en Base Op. Piser.
		Tiempo en uso		4 3 años.					
	Impresoras	04	Fotocopiadora		Multifuncional				01 Matricial 01 HP. Scaner / printers
		Tiempo en uso			2.				
	Otros	Nombre	Nro.	Tiempo en uso	Características generales				Observaciones

2. **Características de Software Utilizado por los usuarios.**

		Nombres	Licenciado	Libre	Observaciones
Software	Sistemas Operativos	Windows 7, 8	Si		Windows 8 producto de Update.
	Software de Ofimática	Microsoft OFFICE 2010	Si		
	Firewall/ Antivirus	NOD 32	Si		
	Otros	Acrobat		Si	Winrar, Winzip. Sin licencia en Versión Prueba

Representante del área

Consultor

Elaboración Propia

Hardware y Software en el área QHSE
Hardware 02 laptop Core I7. 01 computadora de mesa HP. 01 impresora Epson de sistema continúo. 01 disco Duro Toshiba. Memorias USB. **Software** Sistemas operativos licenciados - Windows 7 y 8. Ofimática – Microsoft office 2010. Antivirus – NOD 32. Acrobat – Software libre. WinRar – WinZip – Software libre.

Características Técnicas del Servidor
• Sistema Operativo: Windows Server 2008 R2 • Procesador: Intel Xeon • Memoria RAM: 8 GB • Tamaño de Disco Duro: 3 TB • Nro. de UPS: 1 *Nota: El servidor es utilizado para el almacenamiento de archivos e información que es accedida por las áreas de PISER S.A.C.

Riesgos y Debilidades en la seguridad de la información por parte de Equipos Hardware y Software
• Área de servidores, infraestructura y accesos no implementados. • Ausencia de un SO que administre la red (no hay active directory, usuarios, perfiles de acceso) • Los equipos informáticos no cuentan con una estricta seguridad de la información. • Uso y regulación de software licenciado. • Monitoreo de la red e instalación de cortafuegos. • Administración de cuentas corporativas para e-mail. • Política de uso, seguridad y traslado de equipos de cómputo. • Clasificación de documentos digitales y certificados de seguridad. • Concientización al personal del manejo de la información. • Uso de software malintencionado tales como p2p, torrent, lime, etc. • Uso de laptops o pc´s es informal, cualquier usuario tiene acceso a la información. • No existe formato para la salida de equipos informáticos fuera del área o de la empresa PISER S.A.C. • Los equipos de respaldo de información son utilizados para algunas áreas de la empresa. • No existe compromiso de confidencialidad, integridad y disponibilidad de la información por parte de alta gerencia y de colaboradores. • El servidor es libre para todas las áreas sin cuidado a la pérdida de la información. • La indisponibilidad del internet deja sin acceso a la información almacenada en el servidor.

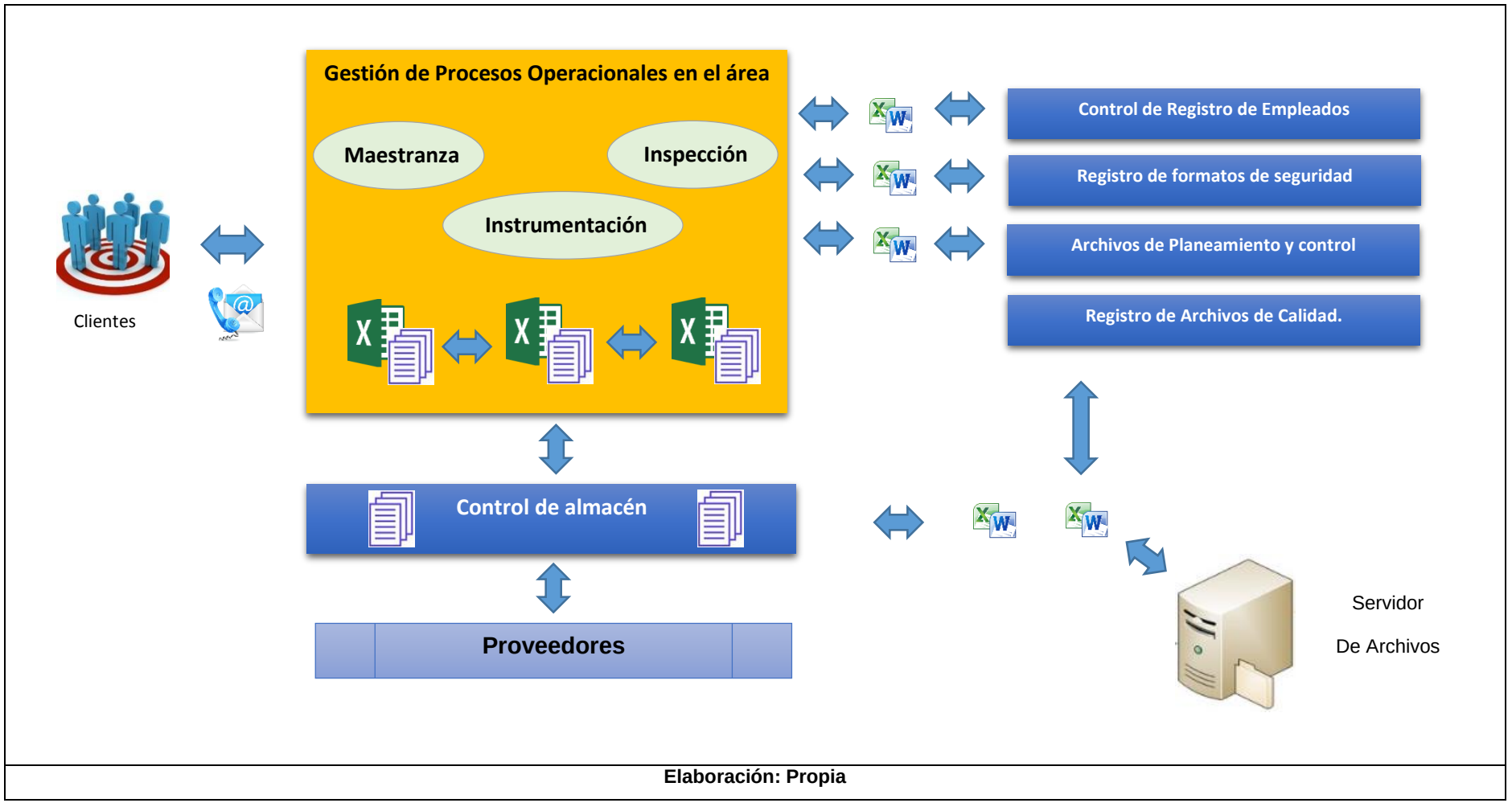
Determinación de las Necesidades del área de QHSE

El registro de los procedimientos implementados por el ISO 9001 se lleva a cabo mediante formatos de control manual (físicos y digitales), lo que demanda esfuerzos en llevar un control estricto y eficiente en cuanto su seguridad a los procesos implementados, luego dicha información es procesada, estructurada y ejecutada para la continuidad del estándar de calidad ISO 9001. Controlar de forma eficiente esta información es un proceso crítico para determinar los niveles de calidad de los servicios que brinda la organización.

Modelo de Operación en el área QHSE

La arquitectura de sistemas actual que soporta los procesos del estándar ISO 9001 en el área QHSE, se puede revisar tomando como base la forma como opera actualmente el área como modelo de operación. Cabe destacar que todos los procesos operativos que maneja el área QHSE son soportados en hojas de cálculo EXCEL, y también se destaca que no cuenta con un Sistema de gestión que permita llevar un control eficiente de sus procesos implementados tanto administrativos como operacionales. En la siguiente figura se muestra un modelo de operación actual del área QHSE donde toda la información es almacenada a un servidor de archivos, corriendo el riesgo que la información almacenada sea eliminada, modificada o extraída para fines desconocidos.

Modelo de Operación actual en el área QHSE:



Elaboración: Propia

Evaluación de Listas de Cotejo

Los siguientes instrumentos fueron aplicados para la verificación y seguimiento de los activos de información en el área QHSE.

PISER S.A.C.

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

Área: QHSE Fecha: 30-09-2016

LISTA DE COTEJO N° 01: CONFIDENCIALIDAD DE LOS ACTIVOS DE INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa correcta
Objetivo: Determinar los indicadores de seguridad de Confidencialidad
Elaboración: Propia

SITUACIÓN A EVALUAR	SI	NO	OBSERVACIONES
CONFIDENCIALIDAD			
Los documentos se encuentran archivados en sus debidos portafolios.		X	NO TODOS LOS DOCUMENTOS
Existe acumulaciones de documentos del SGC en el área.	X		SÍ EXISTE
Existe solicitud o formato de confidencialidad.		X	NO EXISTE SOLICITUD
Existe incidentes de acceso indebido a los documentos.	X		SÍ : ATS - PT - OIT
Existe formato de control de distribución de copias controladas.	X		SÍ EXISTE
Aplican el formato de control de distribución de copias controladas.	X		SÍ A COPIAS CONTROLADAS
Existe formato de control de distribución de copias no controladas.		X	NO EXISTE NINGÚN FORMATO
Existe medios de fuga de información en el área.	X		SÍ EN LOS DOCUMENTOS
Existe autorización de ingreso de personas al área QHSE.		X	NO EXISTE
Existe políticas de Confidencialidad en el área.		X	NO EXISTE
Existe compromiso por preservar la confidencialidad en el área.		X	NO EXISTE
Existe soportes de información en el área.	X		SOPORTES INFORMÁTICOS
Los controles de seguridad de la información los brinda QHSE.		X	NO
Existe inventario de los procesos implementados por el SGC.	X		SÍ LISTAS MAESTRAS
Existe estadística de incidentes de seguridad de la información que tenga impacto sobre la confidencialidad.		X	NO EXISTE NADA.

PISER SAC.
15 NOV 2016

Lista de cotejo de Confidencialidad de los activos de información
Elaboración: Propia

PISER

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

Área: QHSE **Fecha:** 30 - 09 - 2016

LISTA DE COTEJO N° 02: INTEGRIDAD DE LOS ACTIVOS DE INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa correcta
Objetivo: Determinar los indicadores de seguridad de Integridad
Elaboración: Propia

SITUACIÓN A EVALUAR	SI	NO	OBSERVACIONES
INTEGRIDAD			
Existe compromiso por preservar la integridad.		X	NO EXISTE
Existe incidentes de impacto a la integridad en documentos.	X		SÍ EXISTE
Se presentan incidentes en el control de versiones de la documentación del SGC.	X		SÍ EXISTE
Existe incidentes por los colaboradores en el SGC.	X		SÍ EXISTE
Existe modificaciones de documentos en el área QHSE.	X		SÍ EXISTE
Existe procedimientos para la elaboración de documentos.	X		SÍ EXISTE
Existe algún formato o registro para las incidencias de integridad de información.		X	NO EXISTE NADA
Existe autorización para la actulización de documentos del SGC.	X		SÍ EXISTE
Existe control incidencias de modificaciones de información del servidor.		X	NO EXISTE CONTROL
Existe pérdida o eliminación de información en el servidor.	X		SÍ EXISTE
Existe control incidencias de modificaciones de información del servidor.		X	NO EXISTE
Existe estadística de impacto sobre la integridad de la información.		X	NO EXISTE
Existe normas o políticas en el área QHSE para la integridad de la información.		X	NO EXISTE

C Hugo Mario H.
PISER SAC.
15 NOV 2016

Lista de cotejo de Integridad de los activos de información
Elaboración: Propia

PISER

EVALUACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

SISTEMA DE GESTIÓN DE CALIDAD (SGC) - ISO 9001

Área: QHSE **Fecha:** 30-09-2016

LISTA DE COTEJO N° 03: DISPONIBILIDAD DE LOS ACTIVOS DE INFORMACIÓN

Instrucciones: Marque con un aspa (X) la alternativa correcta
Objetivo: Determinar los indicadores de seguridad de Disponibilidad
Elaboración: Propia

SITUACIÓN A EVALUAR	SI	NO	OBSERVACIONES
DISPONIBILIDAD			
Los documentos se encuentran a disponibilidad en el área QHSE.	X		Sí: CAMOS - ATS - PT - PASES
Las laptops cuentan con contraseña de seguridad.	X		SÍ TIENEN CONTRASEÑA
Existe formatos de impacto a la disponibilidad de los documentos.	X		SI PÉRDIDA DE DOCUMENTOS
Los respaldos electronicos del SGC están disponibles en el área QHSE.		X	NO, ESTÁN ACARGO DEL SUP.
Existe inconvenientes relacionados con la indisponibilidad de servidores	X		SI NADIE TENDRÍA ACCESO.
Existe estadística de impacto sobre la disponibilidad de la información.		X	NO EXISTE NADA
El personal administrativo puede acceder a la base de datos del SGC.	X		SI TIENEN ACCESO
Existe control de disponibilidad de los equipos informáticos para salida del área.		X	NO HAY CONTROL
Existe disponibilidad de equipos informáticos a colaboradores.		X	NO
Existe disponibilidad de acceso al servidor de la empresa a practicantes.	X		SÍ
Existe backup para un rápido respaldo de información en el área QHSE.	X		SÍ EXISTEN
Existe formatos o registros de seguimiento de copias de respaldo del SGC.		X	NO EXISTE SEGUIMIENTO

PISER SAC.

15 NOV 2016

Lista de cotejo de Disponibilidad de los activos de información
Elaboración: Propia

Descripción de lista de cotejo de Confidencialidad

Situación de Confidencialidad	Observaciones
-Los documentos se encuentran archivados en sus debidos portafolios.	-No todos los documentos se encontraron archivados. -Falta de portafolios. -Los documentos de gestión de pases de los trabajadores están a disposición en el área QHSE. -Los documentos de procesos operativos se encuentran acumulados en los escritorios.
-Existen acumulaciones de documentos del SGC en el área.	-Si por la falta de espacio en la oficina. -Falta de portafolios. -Todo se trabaja física y manualmente en la aplicación de procedimientos operativos. -Falta de armarios y estantes.
-Existe solicitud o formato de confidencialidad.	-No existe solicitud ni formato de confidencialidad en el área QHSE. -Todos acceden a la información de los procesos implementados sin autorización.
-Existen incidentes de acceso indebido a los documentos.	-Si existen incidentes de acceso por parte de colaboradores a los documentos: -Permisos de trabajo. -Análisis de trabajo seguro. -Orden interna de trabajo.
-Existe formato de control de distribución de copias controladas.	-Si existe formato de control de distribución de copias controladas de documentos del SGC por parte del estándar ISO 9001.
-Aplican el formato de control de distribución de copias controladas.	-Si se aplica el formato de control de distribución de copias controladas por parte del estándar ISO 9001.
-Existe formato de control de distribución de copias no controladas.	-No existe ningún formato para el control de distribución de copias no controladas. -Solo las copias controladas son las que tienen un control en el área QHSE.
-Existen medios de fuga de información en el área.	-La fuga de información es por medio de la documentación en el área QHSE. -La existencia de acumulación de los procedimientos aplicados en base PISER.

Situación de Confidencialidad	Observaciones
-Existe autorización de ingreso de personas al área QHSE.	-No existe ninguna autorización de ingreso a personas al área QHSE. -No existen normas o políticas que restrinja el ingreso de personal no autorizado.
-Existen políticas de Confidencialidad en el área.	-No existen políticas de confidencialidad en ninguna de las áreas de la empresa PISER S.A.C.
-Existe compromiso por preservar la confidencialidad en el área QHSE.	-El compromiso existe por parte del supervisor y la asistente QHSE, pero las demás áreas estratégicas no tienen el compromiso por la preservación de la confidencialidad en el área QHSE.
-Existen soportes de información en el área QHSE.	-Si los equipos informáticos: Laptops, Disco Duro, servidor y Memorias USB.
-Los controles de seguridad de la información los brinda QHSE.	-No, según colaboradores y supervisor QHSE, los controles de seguridad de la información deben trabajarlos el área de Logística e Informática junto con Alta Gerencia.
-Existe inventario de los procesos implementados por el SGC.	Si existen: -Listas Maestras de Documentos Externos e Internos. -Listas Maestras de Registros. -Las listas maestras deben ser actualizadas y verificadas por los procesos implementados por el estándar ISO 9001.
-Existe estadística de incidentes de seguridad de la información que tenga impacto sobre la confidencialidad.	-No existe absolutamente nada que muestre la situación de la seguridad de la información del área QHSE y mucho menos de la empresa PISER S.A.C.

Descripción de lista de cotejo de Integridad

Situación de Integridad	Observación
-Existe compromiso por preservar la integridad.	-El compromiso por el supervisor existe, pero por parte de los colaboradores encargados a la ejecución de los procedimientos no tienen el compromiso por la preservación de la integridad.
-Existen incidentes de impacto a la integridad en documentos.	Si existen incidentes: -En el deterioro de los documentos físicos. -Destrucción de documentos en el área y base de PISER S.A.C. -Confusiones y modificaciones en los documentos. -Pérdida de los documentos por los colaboradores.
-Se presentan incidentes en el control de versiones de la documentación del SGC.	-Si presentan incidentes por las modificaciones que existen en la implementación del estándar ISO 9001. -Actualizaciones de procedimientos en el área QHSE.
-Existen incidentes por los colaboradores en el SGC.	Si existen incidentes: -Equivocaciones por parte de los colaboradores en los procedimientos operativos del SGC en el almacenamiento del servidor.
-Existen modificaciones de documentos en el área QHSE.	-Si existen modificaciones en los procesos implementados del estándar ISO 9001. -En los análisis de trabajo seguro.
-Existen procedimientos para la elaboración de documentos.	-Si los procedimientos del SGC por parte del estándar ISO 9001.
-Existe algún formato o registro para las incidencias de integridad de información.	-No existe ningún formato o registros para las incidencias de integridad de la información. -No hay control en los incidentes de integridad de la información física y digital. -No existen normas ni políticas que resguarde la integridad en el área QHSE.

Situación de Integridad	Observación
-Existe autorización para la actualización de documentos del SGC.	-Si por parte del supervisor QHSE y alta gerencia. -Existe el respaldo de los consultores de apoyo para la implementación del SGC.
-Existe control de incidencias de modificaciones de información del servidor.	-No existe ningún control. -No hay Formatos o registros del seguimiento de modificaciones en el servidor. -No existe la importancia por preservar la integridad de sus procesos implementados por los colaboradores de las áreas estratégicas.
-Existe pérdida o eliminación de información en el servidor.	-Si pérdidas de carpetas almacenadas en el servidor. -Perdidas de documentos de los procesos implementados (digitalizados). -Modificación de ruta de almacenamiento de archivos en el servidor.
-Existe control de incidencias de modificaciones de información del servidor.	-No existe formato o registros de seguimiento de incidencias de modificación de archivos en el servidor.
-Existe estadística de impacto sobre la integridad de la información.	-No existe estadística de impacto sobre la integridad de la información. -No existe el interés por la preservación de la seguridad de la información en sus colaboradores.
-Existen normas o políticas en el área QHSE para la integridad de la información.	-No existen normas ni políticas en el área QHSE para la integridad de la información.

Descripción de lista de cotejo de Disponibilidad

Situación de Disponibilidad	Observación
-Los documentos se encuentran a disponibilidad en el área QHSE.	Documentos disponibles en el área QHSE: -Certificado de Aptitud Medico Ocupacional (CAMO) -Análisis de trabajo seguro. -Permisos de Trabajo. -Pases de colaboradores para servicios.
-Las laptops cuentan con contraseña de seguridad.	-Si cuentan con contraseñas cada laptop.
-Existen formatos de impacto a la disponibilidad de los documentos.	-Si en la pérdida de documentos de procesos operativos. -Pases de colaboradores para servicios a clientes.
-Los respaldos electrónicos del SGC están disponibles en el área QHSE.	-No. Estás a cargo del Supervisor QHSE encargado de la implementación.
-Existen inconvenientes relacionados con la indisponibilidad de servidores.	-Si cuando no hay internet nadie puede acceder a la información compartida en el servidor.
-Existe estadística de impacto sobre la disponibilidad de la información.	-No existe ningún diagnóstico y mucho menos cuadros estadísticos de la disponibilidad de la información.
-El personal administrativo puede acceder a la base de datos del SGC.	-Si a la información compartida que se encuentra en el servidor.
-Existe control de disponibilidad de los equipos informáticos para salida del área.	-No hay formatos o registros que controlen la salida de equipos informáticos.
-Existe disponibilidad de equipos informáticos a colaboradores.	-No existe disponibilidad de los equipos informáticos en el área QHSE.
-Existe disponibilidad de acceso al servidor de la empresa a practicantes.	-Si existe el acceso al servidor de la empresa PISER S.A.C.
-Existe backup para un rápido respaldo de información en el área QHSE.	-Si hay backup de emergencia.
-Existen formatos o registros de seguimiento de copias de respaldo del SGC.	-No existe seguimiento -No existen formatos o registros.

Cuadro de Debilidades identificadas y Controles Recomendados de los activos de información en el Área QHSE de la empresa PISER S.A.C

Debilidad Identificada	Control Recomendado
-No existe estadística de incidentes de seguridad de la información que tengan impacto sobre la confidencialidad, integridad y disponibilidad de la información	C01: Implementar procedimiento de gestión de incidentes de seguridad de la información.
-Existe un bajo compromiso con la seguridad de la información	C02: Implementar acuerdo de confidencialidad que sea firmado por todos los colaboradores de PISER S.A.C.
-Se percibe mayoritariamente que los controles seguridad de la información los establece Logística/Informática	C03: Documentar política de seguridad de la información que demuestre compromiso gerencial, y difundirla con todo el personal.
-Los principales medios de fuga de información son correo electrónico y dispositivos USB	C04: Evaluar necesidad de restricciones en el correo electrónico institucional y uso de dispositivos USB. Se debe realizar un análisis del caso de acuerdo a funciones y responsabilidades en la empresa.
-Se percibe que entre los principales vectores de fuga de información el exceso de confianza es el que mayor incidencia tiene	C05: Desarrollar programa de sensibilización difusión de la política y lineamientos de seguridad de la información en toda la empresa. C06: Implementar procedimiento de control de acceso a los sistemas de información de PISER S.A.C.
-Existe la percepción de un alto número de incidentes de fuga y acceso indebido a información, y también existe una cantidad relativamente alta de equipos portátiles usándose en la empresa.	C07: Implementar procedimiento de autorización para los siguientes casos: 1. Uso de equipos portátiles fuera de las instalaciones de PISER S.A.C. 2. Uso de equipos particulares dentro de las instalaciones de PISER S.A.C.
-La documentación del SGC podría ser usada por otras personas ajenas a el área de QHSE y áreas estratégicas	C08: Mejorar el procedimiento de distribución de copias controladas de la documentación del SGC.
-Se percibe que algunas veces se presentan incidentes en el control de versiones de la documentación del SGC	C09: Mejorar procedimiento de control de versiones de la documentación del SGC. Se recomienda el uso de tecnología como por ejemplo una intranet de documentación definitiva.

Debilidad Identificada	Control Recomendado
-La documentación del SGC está soportada principalmente en medios físicos (documentación impresa) y en medios externos.	C10: Implementar procedimiento de respaldo de información del SGC para mitigar riesgo de pérdida de integridad y disponibilidad de la información.
-Se percibe que existen inconvenientes relacionados con la indisponibilidad de servidores y sistemas de información	C11: Implementar procedimiento de mantenimiento preventivo y correctivo de servidores y equipos informáticos críticos. C12: Implementar procedimiento de monitoreo de servidores y equipos informáticos críticos.

2016

Anexo N° 12: Controles de Seguridad

Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001

MANUEL ARMANDO AGURTO CASTILLO

Según (NTP-ISO/IEC 27001, 2014) **los controles de referencia son definidos:**

TABLA A.1 CONTROLES DE SEGURIDAD		
A.5 Políticas de seguridad de la información		
A.5.1 Dirección de la gerencia para la seguridad de la información		
Objetivo: Proporcionar dirección y apoyo de la gerencia para la seguridad de la información en su concordancia con los requisitos del negocio y las leyes y regulaciones relevantes.		
A.5.1.1	Políticas para la seguridad de la información.	Control -Implementar procedimiento de autorización para los siguientes casos: 1. Uso de equipos portátiles fuera de las instalaciones de PISER S.A.C. 2. Uso de equipos particulares dentro de las instalaciones de PISER S.A.C. -Implementar acuerdo de confidencialidad que sea firmado por todos los colaboradores de PISER S.A.C. -Implementar procedimiento de control de acceso a los sistemas de información de PISER S.A.C. -Implementar procedimiento de respaldo de información del SGC para mitigar riesgo de pérdida de integridad y disponibilidad de la información. -Implementar procedimiento de mantenimiento preventivo y correctivo de servidores y equipos informáticos críticos. -Implementar procedimiento de monitoreo de servidores y equipos informáticos críticos. Implementar procedimiento de gestión de incidentes de seguridad de la información.
A.5.1.2	Revisión de las políticas para la seguridad de la información.	Control Alta gerencia debe: -Documentar política de seguridad de la información que demuestre compromiso gerencial, y difundirla con todo el personal. -Desarrollar programa de sensibilización difusión de la política y lineamientos de seguridad de la información en toda la empresa. -Desarrollar procedimientos de cambios de modificación de documentos, así como el procedimiento de control de versiones por parte del estándar ISO 9001.
A.6 Organización de la seguridad de la información		

A.6.1 Dispositivos móviles y teletrabajo		
Objetivo: Asegurar la seguridad del teletrabajo y el uso de los dispositivos móviles.		
A.6.1.1	Política de dispositivos móviles.	-Política de uso de celular en el área QHSE Control -Se prohíbe el uso de dispositivos móviles para la utilización de redes sociales en la jornada laboral. -Implementar un registro de uso de dispositivos móviles solo a personal autorizado. -Implementar controles criptográficos para autenticar el código del dispositivo móvil.
A.7 Seguridad de los recursos humanos		
A.7.1 Antes del empleo		
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades y son convenientes para los roles para los que se considera.		
A.7.1.1	Selección	Control -Implementar una lista maestra de todos los datos de los colaboradores para la gestión de pases a empresas que requieran el servicio. -Implementar un procedimiento de verificación de la integridad y precisión en todos los datos de los colaboradores constatando junto con la lista maestra.
A.7.1.2	Términos y condiciones del empleo	Control Dentro de la confidencialidad de los procesos implementados del estándar ISO 9001: -Se debe implementar un formato de solicitud de confidencialidad donde el colaborador se comprometa a guardar seguridad a información confidencial dentro del área QHSE.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas sean conscientes y cumplan con sus responsabilidades de seguridad de la información.		
A.7.2.1	Conciencia, educación y capacitación sobre la seguridad de la información	Control -Se debe realizar un análisis del caso de acuerdo a funciones y responsabilidades en el área QHSE.
A.7.2.2	Proceso disciplinario	Control -Se debe realizar un procedimiento para asegurar un tratamiento correcto, teniendo como referencia el artículo 16 seguridad de tratamiento de datos personales de la ley N° 29733.

		-Se debe realizar también un procedimiento adecuado, teniendo como referencia el artículo 17 confidencialidad de los datos personales de la ley N° 29733, ya que el área QHSE es la encargada de la gestión de pases de los colaboradores.
A.7.3 Terminación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo.		
A.7.3.1	Terminación o cambio de responsabilidades del empleo	Control -Se debe realizar la preservación de la información de los colaboradores. -El área QHSE en conjunto con la empresa tiene la responsabilidad de mantener seguro la información del personal así no labore en la empresa. -Para la mayor seguridad según el artículo 28 de la ley 962 de 2005, se dice que debe conservar mínimo 10 años, sea físicamente o en medios electrónicos, etc.
A.8 Gestión de activos		
A.8.1 Responsabilidad por los activos		
Objetivo: Identificar los activos de la organización y definir responsabilidades de protección apropiadas.		
A.8.1.1	Inventario de activos	Control -Identificar los activos de información aplicando inventarios en el área QHSE. -Implementar listas maestras de todos los activos de información en el área QHSE: Hardware, software, datos, usuarios, servicios, etc. -Implementar registros de los activos de información asociados con la lista maestra a implementar, designados en el área QHSE.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe un nivel apropiado de protección en concordancia con su importancia para la organización.		
A.8.2.1	Clasificación de la información	Control -Realizar una evaluación completa. -Implementar los enfoques como la norma ISO 27005 o algún otro enfoque metodológico orientado específicamente a la gestión y tratamiento de riesgos para el grado de sensibilidad y criticidad de la información. -Realizar registros de confianza para resguardar la información del área QHSE.

		-Realizar un plan de seguridad del SGC para otorgar una perspectiva amplia de los requerimientos de seguridad.
A.8.3 Manejo de los medios		
Objetivos: Prevenir la divulgación, modificación, remoción o destrucción no autorizada de información almacenada en medios.		
A.8.3.1	Gestión de medios removibles	Control -Implementar procedimientos de seguridad en medios informáticos para el SGC en el área QHSE: -Uso de equipos portátiles fuera de las instalaciones de la empresa PISER S.A.C. -Uso de equipos particulares dentro las instalaciones de la empresa PISER S.A.C.
A.9 Control de acceso		
A.9.1 Requisitos de la empresa para el control de acceso Objetivo: Limitar el acceso a la información y las instalaciones de procesamiento de la información.		
A.9.1.1	Política de control de acceso	-Política de control de acceso a información del SGC. Control -Desarrollar programa de sensibilización difusión de la política y lineamientos de seguridad de la información en toda la empresa. -Implementar procedimiento de control de acceso a los sistemas de información del SGC en el área QHSE. -Realizar que exista el compromiso por la confidencialidad, integridad y disponibilidad en la información del SGC.
A.9.2 Gestión de acceso de usuario		
Objetivo: Asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas y servicios.		
A.9.2.1	Registro y baja de usuarios	Control -Implementar procedimiento de seguridad por medios de técnicas de autenticación y autorización de usuarios. -Implementar un registro de control en la entrada que impida el ingreso de personal extraño a las instalaciones del área QHSE. -Aplicar el formato o solicitud de compromiso de confidencialidad de la información del SGC.
A.9.3 Control de acceso a sistemas y aplicación		
Objetivo: Prevenir el acceso no autorizado a los sistemas y aplicaciones.		
		Control

A.9.3.1	Restricción de acceso a la información	Deshabilitar inmediatamente el acceso al servidor de la empresa PISER S.A.C. -Implementar un registro donde se determina la des habilitación de colaboradores que han sido desvinculados de los derechos de acceso al servidor de la empresa PISER S.A.C. -Realizar solicitud para los colaboradores donde se establezcan sanciones si los colaboradores prestan información a la competencia o intentan acceder a información no autorizada.
A.10 Seguridad física y ambiental		
A.10.1 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.		
A.10.1.1	Controles de ingreso físico	Control -Diseñar y aplicar una defensa contra ataque malicioso o accidentes en las instalaciones del área QHSE. -Implementar un formato que registre la hora y la fecha de ingreso y salida de las personas visitantes.
A.10.1.2	Protección contra amenazas externas y ambientales	Control -Se debe prestar atención a cualquier advertencia en contra la seguridad brindada por las áreas, en caso de un amago en el exterior de la empresa, se tiene que implementar rociadores de agua en el techo de cada área para cualquier incidente fuera del área o de la empresa PISER S.A.C.
A.10.1.3	Trabajo en área seguras	Control -Implementar un plan para eludir la entrada física no autorizada, deterioro o impertinencia en las instalaciones del área QHSE y al sistema de gestión de calidad.
A.11 Equipos		
Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos e interrupción de las operaciones de la organización.		
A.11.1.1	Emplazamiento y protección de los equipos	Control -Realizar un plan de contingencia de antes, durante y después a los equipos informáticos en caso de un desastre natural. -Implementar un planeamiento estratégico de tecnologías de información con sistemas de accesos no autorizados.
		Control

A.11.1.2	Servicios de suministro	-Establecer un procedimiento para implementar una estrategia de respaldo de datos de emergencia. -Implementar la infraestructura tecnológica con sistema de alimentación interrumpida para el almacenamiento respectivo de energía limitada en el momento del corte de fluido eléctrico.
A.11.1.3	Mantenimiento de equipos	Control -Realizar un inventario de todos los equipos informáticos del área. -Implementar una arquitectura de situación actual de todos los equipos informáticos. -Sólo el encargado de mantenimiento seleccionado debe realizar las soluciones en el servicio de equipos informáticos. -Implementar registro de mantenimiento por el encargado del área de logística e informática. -Implementar un checklist de seguimiento y verificación de mantenimiento prolongado para el sustento del área QHSE.
A.11.1.4	Seguridad de equipos y activos fuera de las instalaciones	Control -Implementar un registro para la salida de equipos informáticos fuera del área o de la empresa con autorización y firmado por gerencia.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos y responsabilidades operativas		
Objetivo: Asegurar que las operaciones de instalaciones de procesamiento de la información sean correctas y seguras.		
A.12.1.1	Procedimientos operativos documentados	Control -Implementar los procedimientos para la elaboración de documentos en el área QHSE. -Realizar un inventario de toda la información obtenida en el área QHSE.
A.12.2 Respaldo		
Objetivo: Proteger contra la pérdida de datos		
A.12.2.1	Respaldo de la información	Control -Implementar registro de respaldos electrónicos autorizados para la información del sistema de gestión de calidad. -Implementar procedimiento de respaldo de información del SGC para mitigar riesgo de pérdida de integridad y disponibilidad de la información.
A.14 Gestión de incidentes de seguridad de la información		

A.14.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque consiste y efectivo a la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos de seguridad y debilidades.		
A.14.1.2	Reporte de debilidades de seguridad de la información.	Control -Realizar diagnósticos a los indicadores de los activos de información en el área QHSE para el análisis análisis correspondiente. -Realizar reportes de debilidades de seguridad de la información del área QHSE después de obtener el análisis del diagnóstico a los activos de información.
A.15 Cumplimiento		
A.15.1 Cumplimiento de 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.		
A.15.1.2	Protección de los registros	Control -Realizar procedimientos que resguarde la información adquirida durante el cumplimiento de la aplicación de registro de seguridad de la información en el área QHSE.
A.15.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información esta implementada y es operada de acuerdo con las políticas y procedimientos organizativos.		
A.15.1.3	Cumplimiento de políticas y normas de seguridad	Control -Implementar registros para el cumplimiento y seguimiento por parte de alta gerencia de la empresa PISER S.A.C

Anexo N° 13: Glosario

- ✓ **PISER:** Peruana de Inspección y Servicios.
- ✓ **QHSE:** Quality, Health, Safety & Environment. (Calidad, Salud, Seguridad y Ambiente).
- ✓ **CAMO:** Certificado de Aptitud Medico Ocupacional.
- ✓ **ISO:** International Organization for Standardization (Organización Internacional de Normalización).
- ✓ **ATS:** Análisis de Trabajo Seguro.
- ✓ **PT:** Permiso de Trabajo.

- ✓ **OIT:** Orden Interna de Trabajo.
- ✓ **TIC:** Tecnología Informática y Comunicaciones.
- ✓ **TI:** Tecnología Informática.
- ✓ **MOF:** Manual de Organización y Funciones.
- ✓ **SGC:** Sistema de Gestión de Calidad.

Anexo N° 14: Formatos para la seguridad de la información en el Área QHSE

PISER S.A.C.	FORMATO DE ACUERDO DE CONFIDENCIALIDAD

ACUERDO DE CONFIDENCIALIDAD

Yo _____ con DNI N° _____

DECLARO:

1. Que me comprometo a utilizar los recursos informáticos y de comunicación vía electrónica para el desarrollo de las labores o servicios encomendados por PISER S.A.C. y para uso privado siempre y cuando no interfieran con ellos ni ocasione perjuicios a PISER S.A.C.
2. Que he leído y comprendido la normatividad interna de Seguridad de la Información de PISER S.A.C., que comprende mis obligaciones como usuario de la información, por lo que me comprometo a cumplir con los lineamientos descritos en dicho marco normativo interno.
3. Que me comprometo a guardar confidencialidad y reserva sobre la información que pueda tener conocimiento en función de mi puesto de trabajo y del uso de los recursos informáticos y de comunicación que me han sido asignados.
4. Que me comprometo a cumplir los procedimientos e instrucciones de seguridad dictadas por las áreas competentes de PISER S.A.C. y las que establezca con carácter general la legislación vigente.
5. Que autorizo al administrador de los recursos informáticos a la realización de cuantas acciones y operaciones técnicas sean necesarias sobre los recursos informáticos y de comunicación, bajo mi custodia, para garantizar la seguridad y el buen uso de los mismos. Estas acciones se llevarán a cabo con conocimiento y coordinación de mi persona.

Talara, _____ de _____ del 20 _____

Firma: _____

DNI: _____ Hora: _____

Formato de acuerdo de Confidencialidad
Elaboración: Propia

PISER S.A.C.	FORMATO DE REPORTE DE INCIDENTE DE SEGURIDAD DE LA INFORMACIÓN

FORMATO DE REPORTE DE INCIDENTE	N° Control:

A. DATOS DE SOLICTUD (A ser llenado por quien reporta el incidente)

Fecha Reporte: ____/_____/_____ Hora Reporte: _____:_____ _____

Persona que Reporta: _____

Tipo Persona: ☐ Interno ☐ Externo / Empresa: _____

Área: _____

Detalle del Incidente:

_____

_____

Fecha Incidente: ____/_____/_____ Hora Incidente: _____:_____ _____

Tipo Incidente: ☐ Evento ☐ Incidente

Clase Incidente: ☐ Administrativo ☐ Técnico/Informático ☐ Técnico/No Informático

Urgencia: ☐ Baja ☐ Media ☐ Alta

Categoría Incidente: _____

Sub-Categoría Incidente: _____

B. DATOS DE GESTIÓN (A ser llenado por quien atiende el incidente)

Respuesta/Solución _____

_____

Tipo Solución: ☐ Definitiva ☐ Temporal ☐ Sin solución

Recibido por:	Atendido por:
Fecha: : ____/_____/_____	Fecha: ____/_____/_____ Hora: _____:_____ _____

Formato de reporte de incidente de seguridad de la información
Elaboración: Propia

PISER S.A.C.	FORMATO DE SOLICITUD DE AUTORIZACION DE USO DE EQUIPO FUERA DE INSTALACIONES

SOLICITUD DE AUTORIZACION DE USO DE EQUIPO FUERA DE LAS INSTALACIONES	N° Control:

A. DATOS DE SOLICTUD

Solicitado por: _____ Fecha de Solicitud: ____/_____/_____

Cargo: _____ Área: _____

A ser usado en: _____

Tipo Uso: ☐ Propio ☐ Terceros ☐ Otros/ Explique: _____

Fecha Desde: ____/_____/_____ Fecha Hasta: ___/_____/_____ Nº de Registro: _____

Marca: _____ Modelo: _____

Nº de Serie: _____

Justificación de Solicitud: _____

_____

REQUERIMIENTOS ADICIONALES	SI	No
a) ¿Se requiere conexión a la red informática de PISER S.A.C.?	☐	☐
b) ¿Se requiere usar software proporcionado por PISER S.A.C.?	☐	☐

B. DATOS DE ATENCIÓN

	SI	No
a) ¿Existe de información comprometida o expuesta?	☐	☐
b) ¿Se configuró conexión de acceso remoto a la red informática de PISER S.A.C.?	☐	☐
c) ¿Se instaló algún aplicativo? Especifique en las anotaciones adicionales.	☐	☐

Anotaciones Adicionales:

_____

Solicitado por:	Autorizado por:	Atendido por
Fecha: ____/_____/_____	Fecha: ____/_____/_____	Fecha: ____/_____/_____

Formato de solicitud de autorización de uso de equipo fuera de instalaciones
Elaboración: Propia

FORMATO DE SOLICITUD DE AUTORIZACIÓN DE USO DE EQUIPO PARTICULAR

PISER SAC

FORMATO SOLICITUD DE ACCESO A RECURSOS INFORMÁTICOS

SOLICITUD DE ACCESO A RECURSOS INFORMÁTICOS	Nº Control:

APELLIDOS Y NOMBRES:	CARGO:	FECHA:
CONDICIÓN: ☐ PLANILLA ☐ RECIBO ☐ EXTERNO ☐ OTRO: _____		
ÁREA:		LUGAR TRABAJO:

☐ INGRESO	☐ RENOVACIÓN	☐ ANULACIÓN	☐ BLOQUEO	☐ SUSPENSIÓN TEMPORAL
☐ ESTA SOLICITUD ANULA Y REEMPLAZA A LA ANTERIOR				DESDE: / /
				HASTA: / /

AUTORIZACIÓN / ELIMINACIÓN DE ACCESO A LOS SIGUIENTES RECURSOS:

FIRMAS Y FECHAS:		
SOLICITADO POR:	AUTORIZADO POR:	EJECUTADO POR:
FECHA: ____/____/_____	FECHA: ____/____/_____	FECHA: ____/____/_____

Formato de solicitud de autorización de uso de equipo particular
Elaboración: Propia

Formato de solicitud de acceso a recursos informáticos
Elaboración: Propia

PISER

REGISTRO DE SOPORTE DE SEGURIDAD DE LA INFORMACIÓN

COPIAS DE ALMACENAMIENTO DE SEGURIDAD DE LA INFORMACIÓN

DATOS DEL ENCARGADO DE LA SEGURIDAD DE LA INFORMACIÓN

APELLIDOS Y NOMBRES:	CARGO:	N° CONTROL

SE REVISÓ Y ALMACENÓ COPIA DE INFORMACIÓN

ITEM	NOMBRE DEL RESPALDO ALMACENADO	SOPORTE INFORMÁTICO	FIRMA	FECHA

Registro de Soporte de Seguridad de la Información
Elaboración: Propia