FACULTAD DE INGENIERÍA Y ARQUITECTURA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

“Análisis de Factores Críticos de Éxito para la Implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) en la Empresa Inversiones Prisco S.A.C – Sechura”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Ingeniera de Sistemas

AUTORA:

Zapata Moran, Diana Stefany (ORCID: 0000-0003-0894-3487)

ASESORA:

Mg. Quito Rodríguez, Carmen Zulema (ORCID: 0000-0002-4340-5732)

LÍNEA DE INVESTIGACIÓN:

Auditoria De Sistemas y Seguridad De La Información

PIURA – PERU

2021

DEDICATORIA

El siguiente trabajo está dedicado a mis Padres y familia que hicieron lo posible de alguna u otra manera, apoyándome incondicionalmente en todo momento, con el único fin de culminar satisfactoriamente este proyecto, la cual fue llevado a cabo con mucho esfuerzo y dedicación.

AGRADECIMIENTO

Agradezco a Dios por haberme guiado en mi carrera profesional, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes. Les doy gracias a mis padres por haberme brindado el apoyo y los valores esenciales; como también agradezco a mis profesores en general por haber compartido sus conocimientos y experiencias.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

RESUMEN

El presente trabajo tuvo como objetivo analizar los factores críticos de éxito para la implementación de un sistema de gestión de seguridad de la información en la empresa Inversiones Prisco SAC – Sechura, empleando la metodología de tipo descriptiva. Para identificar los factores críticos de éxito en la empresa se realizó una entrevista con cada jefe de área además de un checkList que fue suministrado al equipo de trabajo conformado por el responsable de dirección, la gerencia, involucrados en la toma de decisiones. En cuanto a los resultados se tuvo que los factores identificados en la empresa fueron 5: compromiso de la gerencia, cultura organizacional, alcance de la seguridad de la información, evaluación de desempeño, sensibilización. Después de haber realizado un análisis de los resultados obtenido podemos concluir que cada factor debe generar estrategias para así llegar a una implementación de un sistema de gestión de seguridad de la información en la empresa Inversiones PRISCO SAC – SECHURA, como también se concluye que el factor más importante es sensibilización, teniendo un impacto de 77.8%, debido que para medir los demás factores primero se tiene que sensibilizar y así generar una buena actitud para una implementación de un SGSI dentro de la entidad.

.

Palabras Clave: Factores Críticos de Éxito, SGSI.

ABSTRACT

The present work aimed to analyze the critical success factors for the implementation of an information security management system in the company Inversiones Prisco SAC - Sechura, using a descriptive methodology. To identify the critical success factors in the company, an interview was conducted with each area manager in addition to a checkList that was provided to the work team made up of the head of management, the management, involved in decision making. Regarding the results, the factors identified in the company were 5: management commitment, organizational culture, scope of information security, performance evaluation, awareness. After having carried out an analysis of the results obtained, we can conclude that each factor must generate strategies in order to reach an implementation of an information security management system in the company Inversiones PRISCO SAC - SECHURA, as it is also concluded that the factor The most important is awareness, having an impact of 77.8%, because in order to measure the other factors, awareness must first be raised and thus generate a good attitude for the implementation of an ISMS within the entity.

Keywords: Critical Success Factors, ISM.

I. INTRODUCCIÓN

Las diferentes organizaciones a nivel mundial, tanto públicas como privadas día a día generan información de diferente importancia dentro de la organización y sus clientes, representando un flujo de vital importancia para su funcionamiento. Este volumen de información en forma frecuente es almacenado en diferentes medios sean estos físicos o electrónicos, para posteriormente estar disponible en los formatos y según las necesidades requeridas (Andress, 2015). Por tanto, sabiéndose de su valía, es importante protegerla y para ello es necesario adoptar mecanismos y estrategias que estén basadas en normas altamente recomendadas, tales como la norma ISO 27001. En este contexto se considera importante que, la seguridad de la información, es un compromiso, que no solo les atañe a sistemas o a un conjunto de controles que se construyan para salvaguardar los activos de información, Siendo ello un compromiso de todas las personas en la organización, al fin al cabo quienes cumplen o ejecutan los procedimientos son las mismas personas (Yañez Caceres, 2017).

Inversiones PRISCO SAC, es una entidad que se dedica a la extracción, procesamiento y exportación de productos hidrobiológicos, que constantemente intercambia información privilegiada y sensible con otras empresas del rubro: acuerdos comerciales, contratos, información de clientes potenciales, etc. No obstante, existiendo una legislación que regula el tratamiento de los datos, medidas de seguridad para protegerlos y que garantizan los derechos fundamentales de los titulares de dicha información, en Prisco SAC existe un malestar por los constantes inconvenientes generados en el tratamiento de la información, tales como: Propiedad de la información; donde todo se da por asumido, pero no hay documentación que tipifique quienes son los responsables de la creación de los datos, de las modificaciones y de la generación de la información. Escalamiento de privilegios de acceso a la información; porque cualquiera que acceda al sistema puede hacer cambios. Además, denegación de servicio, si el servidor se satura se bloquea y todos se quedan sin servicio. Backups inexistentes; no se sabe a ciencia cierta cuál es ultimo Backups a usar

si se necesita restaurar la información. Puertos vulnerables abiertos; no existe una política de control y acceso a los servicios mediante medios inalámbricos. Destrucción de equipamiento; las personas no tienen el sentido de cuidado del parque informático y asumen que no es su función. Violación de contraseñas; los controles de acceso, recuperación y modificación no siguen patrones y/o esquemas que permitan identificar que la creación, cambio y/o modificación es y pertenece al usuario correcto. Presencia de Virus; los usuarios de sistemas se quejan constantemente de la pérdida de información por presencia de virus informático. Ingeniería social; no existen esquemas fidedignos de generación de contraseñas. Empleados deshonestos, al no existir mecanismos que permitan salvaguardar la información, las personas aprovechan de ello y vulneran la confidencialidad de la información y nadie es responsable de fallos generados por entregar información que no es fidedigna (Cuervo Alvarez, 2017).

En tal sentido, surge la imperiosa necesidad de identificar y analizar los factores críticos de éxito para la implementación de un sistema de gestión de la seguridad de información y que ayude a Prisco SAC salvaguardar la confidencialidad, disponibilidad e integridad del activo más importante, la información.

La presente investigación se centrará en identificar y analizar los factores críticos de éxitos adecuados que serán aplicados para la implementación de un sistema de gestión de la seguridad de la información para la empresa Inversiones PRISCO SAC. Como resultado de ello se propondrá un conjunto de estrategias que permitirá asegurar una implementación en dicha institución. Por ello se formula la siguiente pregunta de tesis ¿Cómo el análisis de los factores críticos de éxito permitirá implementar un sistema de gestión de seguridad de la información en la empresa Inversiones Prisco SAC – Sechura?, y como preguntas específicas ¿Cuáles son los factores críticos de éxito relacionados a la implementación de un SGSI en la empresa inversiones Prisco SAC – Sechura?, ¿Cómo se evalúa los factores críticos de éxito identificados relacionados a la implementación un SGSI en la empresa inversiones Prisco SAC – Sechura?, ¿Qué estrategias permite implementar un SGSI en la empresa inversiones Prisco SAC – Sechura?

El trabajo de investigación se justifica porque se pretende dejar una línea de acción ante toda implementación de una SGSI, para ello se establece que debe identificarse y analizarse los factores críticos de éxito y posterior a ello elaborar un conjunto de estrategias que sirvan en la implementación de un SGSI en la organización (Jason, 2015). Se justifica para su área profesional a corto plazo, al asumir la capacidad de analizar cada factor en la empresa y así mismo encontrar hallazgos dentro de ella permitiéndome tener la accesibilidad y la facilidad de conocer más las debilidades de la empresa estudiada y así elaborar una investigación de éxito (Solarte, y otros, 2015). Se justifica en el contexto institucional, pues el desarrollo de este proyecto sirvió para identificar los elementos críticos de éxito, proceso preliminar a la implementación de un sistema de gestión de la seguridad de la información, teniendo en cuenta experiencias similares de implementación, así como otros trabajos de investigación; aspectos que se contrastarán con la realidad y cultura organizacional de la impresa Inversiones Prisco SAC - Sechura.

Se plantea como objetivo general analizar los factores críticos de éxito para la implementación de un sistema de gestión de seguridad de la información en la empresa Inversiones Prisco SAC – Sechura, y como objetivos específicos se plantea Identificar los factores críticos de éxito relacionados a la implementación de un SGSI en la empresa inversiones Prisco SAC– Sechura, evaluar los factores críticos de éxito identificados relacionados a la implementación de un SGSI en la empresa inversiones Prisco SAC– Sechura y diseñar estrategias que permitan implementar un SGSI en la empresa inversiones Prisco SAC – Sechura.

II. MARCO TEÓRICO

Gambin Carreño, y otros (2017) realizo una investigación en la Universidad Pública Colombiana, relacionada con un espacio de trabajo para gestionar de la seguridad de los sistemas de información en la Universidad Pública Colombiana, su objetivo fue delinear una estrategia de gestión de tecnología de información como base de la seguridad y privacidad de esta en la organización, tomando como referencia la norma ISO/IEC27001:2013 y NTGP 1000:2009. Entre sus resultados se tiene que para una correcta implementación de un SGSI depende de establecer los elementos críticos de éxito y una guía de trazabilidad de las actividades a realizar. Se concluye que para garantizar el tratamiento en forma adecuada los riesgos para la implementación del SGSI, es imprescindible definir proyectos estratégicos de seguridad.

Aguirre Ventura (2018), presentó una investigación en la empresa de Servicios Informáticos S.A.C – La Molina, un aplicativo web para gestionar la seguridad de la información, fundamentada en la norma ISO/IEC 27001, como objetivo se planteó establecer cómo afecta un aplicativo web fundamentado en la norma ISO/IEC 27001 en la gestión de la seguridad de la información. Entre sus resultados se determinó que, utilizando la aplicación web, mejoró porcentualmente la entrega correcta de los reportes confidenciales de 77.39% a 96.67%.

Cruz Diaz, y otros (2017), realizó una investigación en la Clínica Medcam Perú cuyo objetivo fue la implementación de un sistema de gestión de seguridad de la información (SGSI), para la protección de los activos de información. Entre sus resultados se tuvo que la sensibilización debe ir en forma paralela a la implementación del SGSI, debido a la importancia que implica que los colaboradores de la organización conozcan la relevancia de esto en el desarrollo de sus aactividades diarias. El el 96% considera la importancia de la seguridad de la información, y el 72% posee conocimiento de la importancia de la seguridad de la informaación y el 83% posee conocimiento de los riesgos de los activos con los cuales trabaja.

Molano Espinel (2017), realizó una investigación para la empresa Market Mix, cuyo objetivo fue la propuesta de una estrategia de implementación de un SGSI,

basado en la norma ISO 27001. El enfoque de esta investigación es de carácter mixto cualitativo, cuantitativo; la muestra estuvo conformada por 200 colaboradores de las diferentes áreas, tanto administrativos como operarios, y para la muestra se consideran 20. Entre los resultados se evidencia que en cuanto al conocimiento de la seguridad de la informacion 7% lo considera excelente, 29 % bueno, 13% muy deficiente, 32% regular y 20% no poseen conocimiento de ello, por tanto se puede establecer que el 65% de los colaboradores considera que posee bajos niveles de conocimiento de seguridad de la información. Finalmente mediante el método de triangulación se establece que existe un alto desconocimiento de seguridad de la información por parte de los colaboradores.

Moscaiza Moncada (2018), realizó una investigacion en la Cooperativa de Ahorro y Crédito ABC, cuya finalidad consistió en el diseño de sistema de gestión de la seguridad de la información (SGSI), fundamentado en la norma ISO 27001:2013. Entre los resultados se tiene que el estado de visualización del semaforo de la organización está en rojo que representa el 20%; debiéndose estos resultados a la ausencia de lineamientos, procedimientos u politicas en cuanto a seguridad de la información se refiere. Se valido el modelo, elaborando el plan estratégico de seguridad de la información. En sus conclusiones se tuvo que se logro validar que los planes de seguridad elaborados estaban alineados a la SGSI de la CAC.

Yañez Caceres (2017), en la subsecretaria de economía realizó un SGSI para empresas de menor tamaño, bajo un enfoque de mejora continua, cuyo objetivo fue su definición e implementación de sistemas pero considerando software open source basado en la norma ISO27001:2013. Entre sus resultados se tiene que en lo que respecta a la sensibilización, se resalta lo necesario que implica la difusion de las politicas y procedimientos para la protección de la información en toda la empresa; por tanto es menester institucionalizar en la subsecretaria de economía la seguridad de la información

Benites Durand (2019) realizó en la planta de la Fábrica Radiadores Fortaleza la Implementación de un SGSI - Norma ISO 27001, en la oficina de proyectos. La investigación es de nivel documental – correlacional y un diseño de tipo experimental. En sus resultados obtuvo que entre los FCE esta el esfuerzo y el

desempeño considerando los niveles más altos de la jerarquía de la organización, otro factor es el compromiso de los jefes de cada una de las áreas involucradas. Además de la concientización mediante protocoles de comportamiento y sanciones a los colaboradores, con el proposito de hacerles sentir la necesidad del cumplimiento del SGSI. Se concluye que durante el desarrollo del SGSI se debe tener una serie de inducciones y capacitaciones tanto tecnicas como informativas y diversas reuniornes inopinadas con los colaboradores para asegurar el éxito en su implementación del SGSI.

Nieves (2017) realizó bajo la normativa ISO/IEC 27001:2013, un trabajo de investigación para el diseño de un SGSI. Se consideró la metodología cuantitativa y cualitativa. Entre sus FCE se considera la capacitación a los colaboradores de la empresa, con respectos a los terminos de la normatividad; concientizándolo además con el uso responsable de los certificados de acceso a la plataforma, como el usuario y la clave respectivamente. Además sensibilizar a los colaboradores mediante catálogos bien estructurados para la enseñanza de Seguridad de la Información, brindando materiales de apoyo constantemente para crear condiciones de compromiso. Se concluye que uno de los FCE es la sensibilización acerca de la responsabilidad de los activos de la información y de la información que se maneja.

Castillo Collazo (2016) Según el portal Web Institucional de Inversiones Prisco SAC (2016), es una empresa pesquera, que en sus inicios se forjó como productora de conservas. Actualmente se ha posicionado en el norte del Perú, con 04 plantas, 02 especializadas en aceite y harina de pescado, 01 planta de congelados e IQF y la última en conservas. Las líneas de productos son línea de conservas, línea de Congelados, línea de Semi conservas (iPrisco, 2016).

Según define las Normas Internacionales ISO (2015), proporciona soluciones y beneficios para una gran cantidad de sectores. Según la familia de normas ISO/IEC 27000 (Iso27000, 2015), son estándares de seguridad que publica la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC), poseen varias denominaciones ISO/IEC 27000, 27001, 27002, 27003, 27004, 27005 entre otros.

En cuanto a Sistema de Gestión de Seguridad de la Información (SGSI) se define por información como una agrupación de datos que están organizados y son de gran importancia dentro de una organización, sin importar la manera que se almacena o transmite (oral, escrita, imagen, papel, electrónica entre otras), de cómo se originó (fuente interna o externa).

Según la ISO 27001 (2015), la seguridad de la información, no es más que la preservación de los principios de integridad, disponibilidad y confidencialidad. Por tanto, en estos 03 principios se fundamenta los cimientos de la seguridad de la información.

Los beneficios de la seguridad de la información, según el Instituto Nacional de Tecnologías de la comunicación (INTECO, 2015), son reducción de costes, pues influye directamente sobre la rentabilidad económica al descubrir las fallas y errores con el propósito de reducirlos y hasta eliminarlos si fuera el caso, se evitan costosos incidentes de seguridad; se optimizan recursos e inversiones en tecnología, pues con su implementación las decisiones se tomarán en base a información fiable y segura; mejorando con ello la competitividad e imagen corporativa, pues así los clientes tomaran el concepto de empresa responsable, involucrada en la mejora de sus procesos, servicios y/o productos que ofrece.

Rockart (Rockart, 2015) , define factores críticos de éxito (FCE) como: “cantidad de áreas limitadas en una organización, donde los resultados son satisfactorios, asegurando competitividad y éxito”, debido a que aportan información relevante para la consecución del propósito o misión de la empresa, deben considerarse durante la realización de un proyecto.

Es por ello que para tener una aproximación válida de cuáles son los FCE se debe de considerar que son subjetivos y temporales, deben tener relación con la supervivencia de la empresa, específicos de acuerdo al giro del negocio, enmarcados en el horizonte de planeación de la empresa y deben relacionarse con sus amenazas, debilidades, oportunidades y fortalezas.

Según Villamizar R. (2015) los FCE dependen de las características propias del negocio y considera según sus casos de éxito en implementación de SGSI, los siguientes a. compromiso de la alta dirección, cultura organizacional, definición del alcance, los controles no son garantía por sí solos, Involucrarse en el

desarrollo del SGSI, métricas de desempeño en el SGSI, sensibilizar al recurso humano, asegurar su continuidad en el tiempo, mejora continua, plan de automatización con el soporte de herramientas informáticas.

Para la identificación los factores críticos de éxito, la técnica a desarrollarse, se basó en el método de los FCE propuesto por (Rockart, 2015). El propósito de la técnica es el soporte para planificar actividades, recursos y delimitación de las áreas claves, facilitando la asignación de prioridades. Primero determinar los FE y FCE. En cuanto al aspecto procedimental una parte corresponde a los responsables del proyecto, quienes recogen información y sugerencias; aquí se obtiene una lista de factores iniciales, los mismos que se analizan, discuten y se depuran. Luego se agrupan los FE de acuerdo a los objetivos, eliminando la redundancia, posteriormente se elimina los factores no críticos de éxito, obteniéndose como un producto final los FCE, así como los atributos para poderlos medir, para finalmente se asignan los recursos que son necesarios

III. METODOLOGÍA

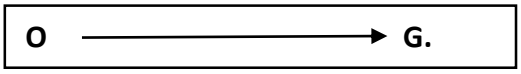
3.1. Tipo y diseño de investigación

3.1.1 Tipo de investigación

La investigación está basada en el paradigma cuantitativo pues los datos fueron examinados de manera numérica, todo ello con el fin de analizar y describir los resultados. Es por ello que el tipo de investigación se establece como descriptiva, donde busca identificar los factores críticos de éxito, realizar un análisis estos para una implementación exitoso de un SGSI (Hernández Sampieri, y otros, 2018).

3.1.2. Diseño de la investigación

El tipo de diseño corresponde a un modelo descriptivo; en el cual el investigador busca y recoge información. El esquema es el siguiente:



Dónde “G” corresponde al grupo control, o corresponden a los factores críticos de éxito considerados para la implementación del SGSI (Esteban Nieto, 2015).

3.2. Variables y operacionalización

Factores críticos de éxito

Según Rockart (2015), cantidad de áreas limitadas en una organización, donde los resultados son satisfactorios, asegurando competitividad y éxito.

3.3. Población, muestra, muestreo y unidad de análisis

3.3.1. Población

Según Arias (2015), lo define como un conjunto limitado o ilimitado de individuos u objetos con características en común. En la presente investigación está constituida por los trabajadores

seleccionados de Inversiones PRISCO SAC, el lugar de la investigación es Sechura (Departamento de Piura).

Tabla 1 Población

Informantes	**Cantidad**
Gestión Talento Humano	10
Contabilidad y Administración	14
Producción	4
Acuicultura	4
Laboratorio Aseguramiento de Calidad	4
Asistente Gerencia	3
Gerente	1
Sistemas	4
Almacén	6
Producción Congelados	7
Almacén Productos terminados	8
TOTAL POBLACIÓN	**65**

Fuente: Empresa inversiones PRISCO SAC – SECHURA

3.3.2. Muestra

Según Arias (2015), se considera a la colección de individuos u objetos que se sustrae de la población, con el propósito de realizar la investigación estadística. En la investigación se considera toda la población, por tanto, tenemos una muestra censal.

3.3.3. Muestreo

Para este caso, como se considera que no existe muestreo, pues la muestra que se consideró es la total de la población de los trabajadores de la empresa de Inversiones PRISCO SAC.

3.3.4. Unidad de análisis

La unidad de análisis, está representada por los informantes de las áreas de la empresa de Inversiones PRISCO SAC.

3.4. Técnicas e instrumentos de recolección de datos

3.4.1. Técnicas

En cuanto a los instrumentos, según Hernández Escobar, y otros (2018) son medios mediante los cuales se recolecta y almacena información de las unidades de análisis. Se aplica de acuerdo al contexto de la investigación, se consideran encuesta, entrevista y observación.

Tabla 2 Técnicas e Instrumentos

TÉCNICAS	INSTRUMENTOS
Encuesta	Cuestionario
Entrevista	Entrevista
Observación	ChekList

Fuente: Empresa inversiones PRISCO SAC – SECHURA

3.4.2. Instrumentos

El cuestionario, instrumento de recopilación de información, conformado por una serie de interrogantes, con una serie de alternativas valorativas que servirá para cuantificar el resultado de su aplicabilidad (Hernández Escobar, y otros, 2018 p. 57).

El chekList, también denominadas listas de chequeo o de control, son elaborados mediante ítems de requerimientos de un determinado contexto de aplicabilidad, con el propósito de realizar comprobaciones o verificaciones de cumplimiento, para ello se cuantifica con valoraciones de los ítems Dicotómicos (Hernández Sampieri, y otros, 2018 p. 75).

La entrevista, técnica de recolección de datos, el mismo que se ejecuta mediante un diálogo coloquial entre el sujeto en estudio y el investigador, mediante el planteamiento de interrogantes, con el fin de obtener respuestas en forma verbal sobre la temática en investigación (Hernández Sampieri, y otros, 2018 p. 78).

Tabla 3 Técnicas e Instrumentos

N°	Indicador	Técnica	Instrumento
1	Compromiso de la gerencia	Encuesta	Cuestionario N° 01
2	Cultura organizacional		
3	Alcance de la seguridad de la información		
4	Evaluación del desempeño		
5	Sensibilización		

Fuente: Empresa inversiones PRISCO SAC – SECHURA

3.4.3. Validez

Para determinar si instrumentos cuantifican las variables, se consideró la validez del constructo y el criterio de experticia de los jueces.

3.5. Procedimientos

Para identificar los factores críticos de éxito (FCE) se realizó una entrevista con cada jefe de las áreas de Gestión Talento Humano, Contabilidad y Administración, Producción, Acuicultura, y otros de la empresa.

Mediante el instrumento checkList aplicado al equipo de trabajo conformada por el responsable de dirección, la gerencia, involucrados en la toma de decisiones, se identificó los factores críticos de éxito.

Asimismo, a la población conformada por 65 trabajadores de la empresa Inversiones PRISCO SAC., se le aplicó un cuestionario, para la valoración cuantitativa de los factores críticos de éxito. Finalmente, los resultados fueron analizados e interpretados lo cual resultó que los factores identificados en la empresa fueron 5: compromiso de la gerencia, cultura organizacional, alcance de la seguridad de la información, evaluación de desempeño, sensibilización.

3.6. Métodos de análisis de datos

Para el análisis de los datos se organizaron los resultados mediante tablas estadísticas y establecer tendencias de esta mediante la visualización de gráficos.

La información se analizará utilizando los siguientes métodos:

Tabla 4 Métodos de análisis de datos

MÉTODO	DESCRIPCIÓN
Análisis estadístico	Para la recolección, análisis e interpretación de datos.
Tabulación	Aplicado a los cuestionarios aplicados.
Análisis descriptivo por frecuencias	Se aplicará para analizar los datos obtenidos en las encuestas y observaciones realizadas a los trabajadores.

Fuente: Elaborado por el autor

Para el procesamiento se utilizó Excel 2013, allí se registraron las encuestas aplicadas a la muestra, mediante el formato presentado en anexo. Para las gráficas se utilizó diagrama de barras.

3.7. Aspectos éticos

Los resultados no son manipulados y se garantiza que la realización de las operaciones (análisis de frecuencias, histogramas que se está usando), son reales y fidedignos.

IV. RESULTADOS

4.1. Identificar los factores críticos de éxito relacionados a la implementación de un SGSI en la empresa inversiones Prisco SAC– Sechura. En lo que respecta a los factores identificados en la empresa fueron 5: compromiso de la gerencia, cultura organizacional, alcance de la seguridad de la información, evaluación de desempeño y sensibilización.

En lo que respecta al primer factor compromiso gerencial: El 92.31% de los trabajadores responden que nunca han sido participes en acciones de concientización de políticas de seguridad de la información (Tabla N° 1 anexo Nº 5). El 100% de los trabajadores responden que nunca han sido participes cuando se han asignado roles y responsabilidades en seguridad de la información. (Tabla N°2 Anexo Nº 5). El 100% de los trabajadores responden que nunca han sido conscientes en que la seguridad de la información debe de cumplir criterios de aceptación del riesgo. (Tabla N°3 anexo Nº 5). El 98.4% de los trabajadores responden que nunca han sido conscientes en que se debe de asignar presupuesto a temas de seguridad de la información. (Tabla N°4 anexo Nº 5). El 100% de los trabajadores responden que nunca han realizado auditorías internas en seguridad de la información. (Tabla N°5 anexo Nº 5). El 100% de los trabajadores responden que nunca han realizado revisiones de manera periódicas a las políticas de seguridad de la información, argumentando su desconocimiento. (TABLA N°6 Anexo Nº 5). Por tanto, se concluye que, es necesario establecer estrategias y mecanismos que permitan atender el FCE compromiso de la alta gerencia en referencia a la implementación del SGSI. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

En cuanto al segundo factor cultura organizacional: El 92.31% de los trabajadores responden que nunca son conscientes que proteger la seguridad de la información es una parte importante de su trabajo. (Tabla N°7 anexo Nº 5). El 95.38% de los trabajadores responden que nunca son conscientes del riesgo de no seguir políticas de seguridad de la información. (Tabla N°8 anexo

Nº 5). El 100% de los trabajadores responden que nunca se han definido procedimientos para reportar las violaciones de seguridad de la información. (Tabla N°9 anexo Nº 5). Por tanto, se concluye que, es necesario establecer estrategias y mecanismos que permitan atender el FCE Cultura Organizacional en referencia a la implementación del SGSI. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

En lo que respecta al tercer factor alcance de la seguridad de la información: El 100% de los trabajadores responden que nunca la empresa ha establecido objetivos para salvaguardar la información. (Tabla n°10 anexo Nº 5). El 100% de los trabajadores responden que nunca se han definido equipos, grupo o departamento responsable de la seguridad de la información. (Tabla N°11 anexo Nº 5). El 100% de los trabajadores responden que nunca se definen fechas para alcanzar las metas propuestas en seguridad de la información. (Tabla N°12 anexo Nº 5). Por tanto, se concluye que, es necesario establecer estrategias y mecanismos que permitan atender el FCE en referencia a la implementación del SGSI. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

En cuanto al cuarto factor evaluación del desempeño: El 64.6% de los trabajadores responden que la mayoría de las veces sí y un 23.1% que siempre se ha resquebrajado la confianza en temas de seguridad de la información. (Tabla N°13 anexo Nº 5). El 60% de los trabajadores respondieron que nunca y un 40% la mayoría de las veces no efectivas las tecnologías de seguridad de la información existentes en la empresa. (Tabla N°14 anexo Nº 5). Un 43.1% de los trabajadores respondieron que siempre y un 56.9% que la mayoría de las veces sí se han presentado incidentes de seguridad en la organización. (Tabla N°15 anexo Nº 5). Por tanto, se concluye que, es necesario establecer estrategias y mecanismos que permitan atender el FCE evaluación del desempeño en referencia a la implementación del SGSI. Puesto que se está observando que cada atributo medido del presente factor nos muestra el

conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

En el quinto factor de sensibilización: El 100% de los trabajadores respondieron que nunca se ha realizado un diagnóstico del estado de la seguridad de la información. (Tabla N°16 anexo Nº 5). 26.2% de los trabajadores respondieron que siempre y un 55.4% que la mayoría de las veces sí, la continuidad del negocio se ha visto afectada cuando se ha presentado violaciones de la seguridad de la información. (Tabla N°17 anexo Nº 5). El 50.8% de los trabajadores respondieron que nunca y un 49.2% que La mayoría de las veces no, es cuidadoso en administrar y/o manipular información del negocio (Tabla N°18 anexo Nº 5). Por tanto, se concluye que, es necesario establecer estrategias y mecanismos que permitan atender el FCE sensibilización en referencia a la implementación del SGSI. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

4.2. Evaluar los factores críticos de éxito identificados relacionados a la implementación de un SGSI en la empresa inversiones Prisco SAC– Sechura

Posterior a la evaluación de los atributos medibles relacionados a los factores crítico de éxito respectivamente, se procedió a suministrar al grupo de interés formado por el responsable de la dirección, la gerencia, tomadores de decisiones, la siguiente pregunta:

¿Qué factor crítico de éxito, considera Ud. que es el más estratégico e importante en el éxito de implementación del SGSI?

Tabla 5 Estadísticos

Moda		5
Percentiles	25	3,00
	50	5,00
	75	5,00

Fuente**:** Elaborado por el autor

Tabla 6 Importancia de lo FCE

¿Que factor crítico de éxito, considera Ud. que es el más estratégico e importante en el exito de implementación del SGSI?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Compromiso de la Alta Gerencia	2	22,2	22,2	22,2
	Sensibilización	7	77,8	77,8	100,0
	Total	9	100,0	100,0	

Fuente: **Elaborado por el autor**

Ilustración 1 Importancia de los FCE

Fuente: Elaborado por el autor

Por tanto, se observa que un 77.8% de los encuestados optan por considerar a la Sensibilización como el factor más importante porque se considera una oportunidad que contribuye a que los trabajadores de la empresa estén informados y concientizados en la importancia de la implementación de un SGSI. Además, el 22.2% de los encuestados considera el Compromiso de la alta gerencia.

4.3. Diseñar estrategias que permitan implementar un SGSI en la empresa inversiones Prisco SAC – Sechura.

Habiendo definido, evaluado y analizado los criterios críticos de éxito para la implementación de un sistema de gestión para la seguridad de la información en la empresa Prisco, se considera necesario:

NIVEL I: INICIAL

- Concientizar a los colaboradores de lo necesario e importante de la ejecución de actividades alineadas a los planes de Seguridad de la Información.
- Preparar a los colaboradores para cumplimiento de su compromiso con la organización con respecto a la seguridad de la información.
- Implementar controles de seguridad en cada una de las áreas de la empresa y a nivel general para toda la organización.
- Garantizar el cumplimiento de las políticas de seguridad mediante la verificación constante de los controles
- Implementación de métodos para la valoración de los controles propuestos para el cumplimiento de las políticas de seguridad.

NIVEL II: REVISIÓN Y EVALUACIÓN DEL DESEMPEÑO

Para la implementación de un SGSI, es imprescindible la caracterización de métricas e indicadores, los mismos que permitirán una valoración cuantitativa y seguimiento del esfuerzo; direccionando estrategias para el logro de los objetivos propuestos por la organización. Para la medición de instrumentos es menester el diagnóstico correcto y hay que corregir para un diagnóstico, para ello es preciso la consideración de las siguientes acciones:

a. Revisar en forma periódica según los indicadores propuestos.
b. Reconocimiento de riesgos.

c. Ejecución de auditorías internas y/o externas.

d. Comunicar los resultados de las auditorías.

Se ejecutará los procedimientos de revisión, los mismos que serán evaluados mediante instrumentos. Los objetivos de estos son:

- Evaluación de la efectividad de implementar los controles de seguridad
- Evaluar la eficiencia del SGSI, con inclusión de mejoras continuas.
- Comunicación efectiva de seguridad a la organización.
- Utilizar el resultado de los análisis como entradas para el tratamiento de riesgos.

Para la mejora continua de la gestión del Sistema de Seguridad de la Información, es importante tener la trazabilidad para la valoración, observando los niveles de madurez en su implementación.

En este sentido, se recomienda posterior a la implementación del SGSI:

- Diagnosticar tanto en forma presencial y remota de la seguridad.
- Evaluar los resultados de los registros analizados en las auditorias.
- Analizar los reportes y alarmas, de los sistemas de seguridad}
- Realizar análisis de incidencias de seguridad generada a partir de los resultados obtenidos

V. DISCUSIÓN

De acuerdo a los objetivos de la investigación se consideró importante considerar investigaciones que permitan orientar el camino en cuanto a la labor de identificar los FCE en la implementación de SGSI, evaluar y proponer estrategias de implementación efectiva de SGSI. En este sentido se ha creado el siguiente ámbito de discusión con el fin de profundizar en la explicación de los descubrimientos, confrontar propuestas, elaborar conclusiones y en todo sentido contribuir a enriquecer el conocimiento.

En lo que respecta a los FCE identificados en la empresa, el resultado fueron 5 factores: compromiso de la gerencia, cultura organizacional, alcance de la seguridad de la información, evaluación de desempeño y sensibilización. Estos resultados coinciden con los encontrados por Gambin Carreño, y otros **(2017)** En base a las consideraciones del investigador, es muy ligero suponer la aplicabilidad de los FCE a todo ámbito, debido a que la realidad del cada negocio exige el estudio de sus formas de trabajo, reglas de negocio, visión, misión, objetivos, necesidades y por tanto los factores críticos que se han de proponer son aplicables al interés de cada negocio en particular y no a nivel general. Además, coincide con Cruz Díaz, y otros **(2017)** pues se tuvo que la sensibilización debe ir en forma paralela a la implementación del SGSI, debido a la importancia que implica que los colaboradores de la organización conozcan la relevancia de esto en el desarrollo de sus actividades diarias. De los encuestados el 96% considera la importancia de la seguridad de la información, y el 72% posee conocimiento referente a la seguridad de la información y el 83% posee conocimiento de los riesgos de los activos con los cuales trabaja. Así también Yáñez Cáceres **(2017)**, entre sus resultados se tiene que en lo que respecta a la sensibilización, se resalta lo necesario que implica la difusión de las políticas y procedimientos para la protección de la información en toda la empresa; por tanto, es menester institucionalizar en la subsecretaria de economía la seguridad de la información. También concuerda con Benites Durand **(2019)** que los FCE está el esfuerzo y el desempeño considerando los niveles más altos de la jerarquía de la organización, otro factor es el

compromiso de los jefes de cada una de las áreas involucradas. Además de la concientización mediante protocoles de comportamiento y sanciones a los colaboradores, con el propósito de hacerles sentir la necesidad del cumplimiento del SGSI. Finalmente se concuerda con los resultados obtenidos por Nieves (2017) entre sus FCE se considera la capacitación a los colaboradores de la empresa, con respectos a los terminos de la normatividad; concientizándolo además con el uso responsable de los certificados de acceso a la plataforma, como el usuario y la clave respectivamente. Además sensibilizar a los colaboradores mediante catálogos bien estructurados para la enseñanza de Seguridad de la Información, brindando materiales de apoyo constantemente para crear condiciones de compromiso.

En la evaluación de los factores críticos de éxito identificados relacionados a la implementación de un SGSI en la empresa inversiones Prisco SAC– Sechura, se procedió a suministrar al grupo de interés formado por el responsable de la dirección, la gerencia. Se determinó que el 22% considera que el FCE es el compromiso de gerencia y el 77.8% la sensibilización. Los resultados obtenidos concuerdan con Moscaiza Moncada (2018), quien en sus resultados se tiene que el estado de visualización del semáforo de la organización está en rojo que representa el 20%; debiéndose estos resultados a la ausencia de lineamientos, procedimientos u políticas en cuanto a seguridad de la información se refiere. Se validó el modelo, elaborando el plan estratégico de seguridad de la información. En base a los valores obtenidos se pudieron determinar los planes de seguridad pertinentes. Además, concuerdan con Benites Durand **(2019)** que sostiene que entre los FCE está el esfuerzo y el desempeño considerando los niveles más altos de la jerarquía de la organización, otro factor es el compromiso de los jefes de cada una de las áreas involucradas. Además de la concientización mediante protocoles de comportamiento y sanciones a los colaboradores, con el propósito de hacerles sentir la necesidad del cumplimiento del SGSI.

En el diseño de estrategias que permitan implementar un SGSI en la empresa inversiones Prisco SAC – Sechura, habiendo definido, evaluado y analizado los

criterios críticos de éxito para la implementación de un SGSI en la empresa Prisco, se considera necesario Nivel I: inicial, Nivel II: establecimiento de métricas e indicadores para la evaluación del desempeño. Estos resultados concuerdan con los obtenidos por Molano Espinel **(2017)**, pues se evidencia que en cuanto al conocimiento de la seguridad de la información 7% lo considera excelente, 29 % bueno, 13% muy deficiente, 32% regular y 20% no poseen conocimiento de ello, por tanto, se puede establecer que el 65% de los colaboradores considera que posee bajos niveles de conocimiento de seguridad de la información. Finalmente, mediante el método de triangulación se establece que existe un alto desconocimiento de seguridad de la información por parte de los colaboradores. Asimismo concuerda con Benites Durand **(2019)** pues en sus resultados determina que como parte de la estrategia, Además de la concientización mediante protocoles de comportamiento y sanciones a los colaboradores, con el proposito de hacerles sentir la necesidad del cumplimiento del SGSI. Asimismo en esa misma linea Condori Alejo **(2012)** desarrolla un modelo estructural, con el fin de determinar el grado de influencia de los FCE y propone un conjunto de factores críticos que deben de considerarse cada vez que se desee implementar un SGSI.

VI. CONCLUSIONES

Tomando en cuenta los fundamentos teóricos y los resultados de la investigación, se concluye:

- Se identificó los Factores Críticos de Éxito en la Implementación de Seguridad de Sistemas de Información, se propuso y desarrollo un modelo basado en la propuesta de identificación de FCE de **(Rockart, 2015)**, los factores críticos de éxito identificados en la empresa Inversiones Prisco SAC – Sechura fueron los siguientes: Cultura Organizacional, Compromiso de la Alta Gerencia, Evaluación del desempeño y Sensibilización y Alcance de la seguridad de la información.

- Asimismo, se logró evaluar los FCE identificados antes dicho y se determinó que cada factor nos muestra el conjunto de carencias que existen en el negocio con respecto a la seguridad de la información siendo esto una debilidad para la organización; como dando resultado que el factor que se debe tener en cuenta y factor principal es la sensibilización, ya que este factor promueve a los demás factores identificados.

- Se logró el diseño de las estrategias que se detallan a continuación:

  - ✓ Diagnosticar tanto en forma presencial y remota de la seguridad.
  - ✓ Evaluar los resultados de los registros analizados en las auditorias.
  - ✓ Analizar los reportes y alarmas, de los sistemas de seguridad.
  - ✓ Realizar análisis de incidencias de seguridad generada a partir de los resultados obtenidos.

VII. RECOMENDACIONES

- Para futuras investigaciones se debe contemplar el alineamiento entre la política de seguridad, el plan estratégico institucional y las políticas de la organización.
- Considerar La norma 27001 como una guía para la aplicabilidad de controles, determinar los riesgos; realizando un análisis de los procesos para determinar en cada uno de ellos aspectos de seguridad.
- Implementar más casos de estudios a otras empresas del rubro y validar la aplicabilidad de los FCE encontrados en las mismas; pudiendo ajustarlos de acuerdo de los dominios considerados en la norma.
- Desarrollar una herramienta de software, con base estadística, que permita automatizar aplicabilidad del método planteado.
- Implementar talleres de Auditoria con respecto a la seguridad de información.

REFERENCIAS

1. **Aguirre Ventura, José Miguel. 2018.** *Sistema web para la gestión de la seguridad de la información alineada a la norma ISO/IEC 27001 en la empresa de Servicios Informáticos S.A.C – La Molina.* Lima, Parú : s.n.

2. **Andress, J. 2015.** *The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice. .* Massachusetts, Estados : Elsevier.

3. **Arias, Fidias G. 2015.** *El Proyecto de Investigación.* Caracas, Venezuela : Ediciones El Pasillo, 2015. 980-07-8529-9.

4. **Barrantes Porras, Carlos Eduardo y Hugo Eduardo, Javier Eduardo. 2012.** *Diseño e Implementacion de un Sistema de Gestion de Seguridad de Informacion en Procesos Tecnologicos .* Lima : s.n.

5. **Benites Durand, César Augusto. 2019.** *Implementación de un Sistema de Gestión de Seguridad de la Información - Norma ISO 27001 para la Fábrica Radiadores Fortaleza.* Lima, Perú : s.n.

6. **BENITES, NIEVES. 2013.** *Evaluacion de la seguridad de las tecnologias de la informacion en la empresa consolidate Group del Peru SAC basado en la NTP – ISO / EIC 17799:2007.* 2013.

7. **Castillo Collazos, Roxana Elida. 2016.** *Sistema de gestión de seguridad de la información en la municipalidad distrital de pira aplicando la norma iso/iec 27001:2013.* Huaraz, Perú : s.n.

8. **CONDORI ALEJO, HENRY IVAN. 2012.** *Tesis de postgrado: un modelo de evaluacion de factores criticos de exito en la implementacion de la seguridad en sistemas de informacion para determinar su influencia en la intencion del usuario*.

9. **CONDORI ALEJO, HENRY IVAN. 2012.** Tesis de postgrado: un modelo de evaluacion de factores criticos de exito en la implementacion de la seguridad en sistemas de informacion para determinar su influencia en la intencion del usuario. *http://repositorio.concytec.gob.pe/bitstream/concytec/115/1/condori_ah.pdf.* [en línea].

10. **Cruz Diaz, Miguel Angel y Fukusaki Infantas, Senyi. 2017.** *Diseño e implementación de un sistema de gestión de seguridad de la información para proteger los activos de información de la Clínica Medcam Perú,.* Lima, Perú : s.n.

11. **Cuervo Alvarez, Sara. 2017.** *Implementación ISO 27001*.

12. **ESPINOZA AGUINAGA, HANS RYAN. 2013.** *Analisis y diseño de un sistema de gestion de seguridad de informacion basado en la norma iso/iec 27001:2005 para una empresa de produccion y comercializacion de productos de consumo masivo.* lima : s.n.

13. **Esteban Nieto, Nicomedes Teodoro. 2015.** *Tipos de Investigación*.

14. **FLORES, GUERRERO. 2015.** *Adaptacion del estandar internacional iso – iec-27002 para la gestion de la seguridad de la informacion en la oficina de informatica, telecomunicaciones y estadisticas de la diresa"*.

15. **Gambin Carreño, Bladimir y Macias Villamizar, Liliana. 2017.** *Marco de trabajo para la gestión de la seguridad de los sistemas de información en la Universidad Pública Colombiana- caso de estudio Universidad del Magdalena.* Barranquilla : s.n.

16. **Griful Ponsati, Eulalia Y Canela Campos, Miguel Angel. 2016.** *Gestion de la calidad*.

17. **Guíñez Fernández, Jorge Andrés. 2017.** *Sistema de gestión de seguridad de la información [SGSI] : revisión sistemática y propuesta*.

18. **Hernández Escobar, Arturo Andrés, y otros. 2018.** *Metodología de la Investigación Cientifíca.* 2018. 978-84-948257-0-5.

19. **Hernández Sampieri, Roberto y Mendoza Torres, Christian Paulina. 2018.** *Metodologia de la Investigación: Las rutas cuantitativa, cualitativa y mixta.* México : McGRAW-HILL.

20. **HUAMAN MONZON, FERNANDO MIGUEL. 2015.** *Diseño de procedimientos de auditoria de cumplimiento de la norma ntp-iso/iec 17799:2007 como parte del proceso de implantacion de la norma tecnica ntp-iso/iec 27001:2008 en instituciones del estado peruano*.

21. **INDECOPI. 2017.** *INDECOPÍ.* Lima : INDECOPI.

22. **INTECO, Instituto Nacional de Tecnologías de la comunicación. 2015.** *Seguridad de la Información.* Lima : INTECO,.

23. **IPRISCO. 2016.** http:/www.iprisco.com.pe/. [en línea] 2016.

24. **iPrisco. 2016.** iPrisco. [En línea] 15 de Enero de 2016. [Citado el: 22 de Julio de 2020.] http://www.iprisco.com.pe/.

25. **ISO tools Excellence. 2015.** *La norma ISO 27001.* 2015.

26. **—. 2015.** *La norma ISO 27001.* 2015.

27. **Iso27000. 2015.** Sistema de Gestión de la Seguridad de la Información. *Iso27000.es.* [En línea] 2015. http://www.iso27000.es/download/doc_sgsi_all.pdf.

28. **Jason, Andress. 2015.** *The Basics of Information Security.* Massachusetts, Estados : Elsevier, 2015.

29. **KARL, THOMAS. 2015.** http://www.welivesecurity.com/la-es/2015/08/19/impact-team-publica-los-datos-robados-de-ashley-madison/. [En línea] 15 de 08 de 2015.

30. **Molano Espinel, Rafael Antonio. 2017.** *Estrategia para implementar un sistema de gestión de la seguridad de la información basada en la norma iso 27001 en el área de ti para la empresa Market Mix.* Bogotá, Colombia : s.n., 2017.

31. **Moscaiza Moncada, Omar Israel. 2018.** *Diseño de un sistema de gestión de la seguridad de la información (SGSI) para la Cooperativa de Ahorro y Crédito ABC, basado en la norma ISO 27001:2013.* 2018.

32. **Nieves, Arlenys Carolina. 2017.** *Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma ISO/IEC 27001:2013.* Colombia : s.n., 2017.

33. **Prisco SAC, Inversiones.** http://www.anchoasperu.com/priscoperu/enlace1.htmly. [En línea]

34. **Rockart, John F. 2015.** Factores criticos de éxito. *LPSI.* [En línea] Julio de 2015. http://www.lpsi.eui.upm.es/webing/tfcmetrica/gtfce.html.

35. **Salcedo B, Robin J. 2015.** *plan de implementación del sgsi basado en la norma iso 27001:2013*.

36. **Solarte, F., Enriquez, E. y enavidez, M. 2015. 2015.** *Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. .* Guayaquil, Ecuador : Revista Tecnológica.

37. **Villamizar R, Carlos. 2015.** consejos practicos para la implementacion de su sgsi. *http://www.magazcitum.com.mx/?p=2597.* [en línea] julio de 2015.

38. **Yan Carranza, Freddy Y Zavala Vasquez, Cinthia Llliliana. 2013.** *Plan de mejora de la seguridad de la informacion y continuidad del centro de datos de la gerencia regional de educacion la libertad aplicando lineamiento iso 27001 y buenas practicas cobit.* trujillo : s.n.

39. **Yañez Caceres, Nelson Alejandro. 2017.** *Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño.* Santiago, Chile : s.n., 2017.

40. **—. 2017.** *Sistema de gestión de seguridad de la información para la subsecretaria de economía y empresas de menor tamaño.* Santiago de Chile : Universidad de Chile, 2017.

ANEXOS

Anexo Nº 1: Tabla de operacionalización

Variables de estudio	Definición conceptual	Definición operacional	Dimensión	Indicadores	Escala de medición
IDENTIFICACIÓN FACTORES CRÍTICOS DE EXITO	Número limitado de áreas en las cuales, los resultados si son satisfactorios, aseguraran un funcionamiento competitivo y exitoso para la organización.	Factores críticos de éxito que el negocio considera aceptable.	Factor crítico de éxito		Ordinal
		Descripción cada factor identificado y aceptado para la organización.	Evaluación del factor crítico de éxito.		Ordinal
		Estrategias que se debe considerar antes de implementar un sistema de gestión de la seguridad de la información y que está supeditado a la evaluación de los factores críticos de éxito.	Estrategia de implementación de SGSI en base a FCE		Ordinal

Fuente: Empresa inversiones PRISCO SAC – SECHURA

Elaborado por el autor

Anexo Nº 2: Instrumentos

Formatos de Instrumentos

- Para la evaluación de FCE para los trabajadores de empresa Inversiones Prisco SAC (65 personas)

Encuesta

Instrucciones: Responda las siguientes preguntas:
Marque con ✔ o una ✗ o rellenando el circulo que más se acerque a su respuesta, la alternativa a escoger

Dimensión	Pregunta
COMPROMISO DE LA ALTA GERENCIA	¿Ha sido participe en la concientización de políticas de seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Ha sido participe en la asignación de roles y responsabilidades en seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Es usted consiente que la seguridad de la información debe de cumplir con criterios de aceptación del riesgo? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Es usted consiente que se debe de asignar presupuesto a temas de seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**

	¿La institución ha realizado auditorías internas en seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿La institución realiza revisiones periódicas de las políticas de seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**

Dimensión	Pregunta
CULTURA ORGANIZACIONAL	¿Es Usted consiente que proteger la seguridad de la información es una parte importante de su trabajo? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Es usted consciente del riesgo de no seguir políticas de seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Se han definido procedimientos para reportar las violaciones de seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**

Dimensión	Pregunta
ALCANCE DE LA SEGURIDAD DE LA INFORMACIÓN	¿La empresa ha establecido objetivos para salvaguardar la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Se definen constantemente equipos, grupo o departamento responsable de la seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Se definen fechas para alcanzar las metas propuestas en seguridad de la información?

	1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.

Dimensión	Pregunta
EVALUACIÓN DEL DESEMPEÑO	¿Se ha resquebrajado la confianza en temas de seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Son efectivas las tecnologías de seguridad de la información que hay en la organización? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Se presentan incidentes de seguridad en la organización? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**

Dimensión	Pregunta
SENSIBILIZACIÓN	¿Se ha realizado un diagnóstico del estado actual de la seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿La continuidad del negocio se ha visto afectada cuando se ha presentado una violación de la seguridad de la información? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**
	¿Es cuidadoso en administrar y/o manipular información del negocio? **1) Nunca. 2) La mayoría de las veces no. 3) Algunas veces sí, algunas veces no 4) La mayoría de las veces sí. 5) Siempre.**

- Formato de entrevista para la identificación de FCE dirigido a cada jefe de área

ENTREVISTA

¿Cuáles son las políticas que hay en el tema seguridad de la información?

¿Cuáles son los roles y responsabilidades dentro de la gerencia?

¿De qué manera se realizan los criterios de aceptación de riesgos?

¿Cuántas auditorias hay anual, o mensual en la empresa?

¿Cuántas revisiones periódicas hay en el tema de seguridad de información y de qué forma?

¿Qué Importancia tiene en la seguridad de la información?

_____
_____
_____
_____

¿De qué manera se manifiesta la concientización del riesgo?

_____
_____
_____
_____

¿Cómo son los procedimientos para reportar las violaciones de seguridad de la información?

_____
_____
_____
_____

¿Qué objetivos utilizan para salvaguardar la información?

_____
_____
_____
_____

¿Donde más se encuentran los incidentes de seguridad?

_____
_____
_____
_____

¿Cuáles son los diagnósticos de estado en la seguridad de la información existen al mes?

_____
_____
_____

- Formato de CheckList para la identificación de FCE dirigido a 6 personas (responsable de la dirección, la gerencia, tomadores de decisiones y responsable de proyecto).

  ***¿El cumplimiento o existencia de este factor contribuirá al logro o cumplimiento del objetivo del negocio*?**

Factores de éxito	**Pregunta**
Compromiso de la gerencia en seguridad de la información.	
Cultura organizacional en seguridad de la información.	
Misión de la organización	
Alcance de la seguridad de la información.	
Recursos y presupuesto	
Evaluación del desempeño.	
Formación y capacitación	

Sensibilización en seguridad de la información.	
Existencia de capital humano capacitado	
Transferencia tecnológica adecuada.	

- **P01:** ¿Es el factor esencial para cumplir los objetivos?
- **P02:** ¿Requiere especial cuidado en su realización, es decir, recursos especialmente cualificados?

Factor	P01	P02	¿Es Crítico?
Compromiso de la gerencia en seguridad de la información.			
Cultura organizacional en seguridad de la información			
Alcance de la seguridad de la información			
Evaluación del desempeño			
Sensibilización en seguridad de la información			

- **P01:** ¿Es el Factor de Éxito esencial para cumplir los objetivos?

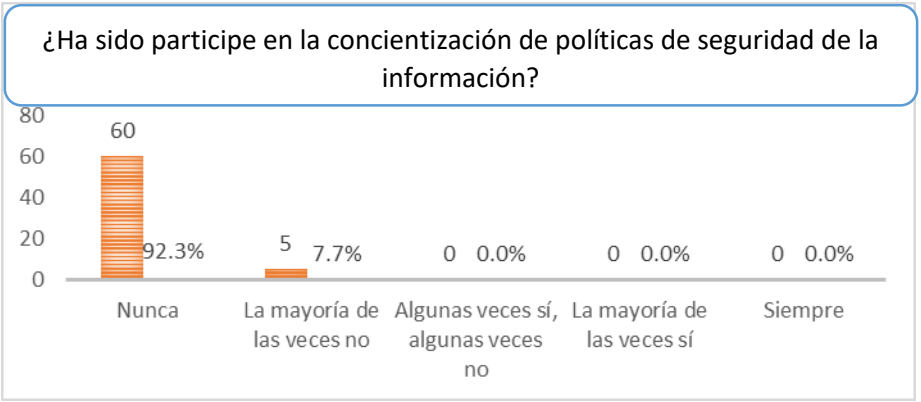
- **P02:** ¿Hay una probabilidad significativa de que el Factor de Éxito no ocurra?
- **P03:** Si no ocurre el Factor de Éxito ¿Podrían alterarse las estrategias con el fin de minimizar el impacto de dicho incumplimiento, suponiendo que hubiese suficiente tiempo disponible?

Factor	P01	P02	P03	¿Es Crítico?
Existencia de capital humano capacitado.				
Transferencia tecnológica adecuada.				

Anexo Nº 3: Tablas y Gráficos de Resultados

1) TABLA N°1

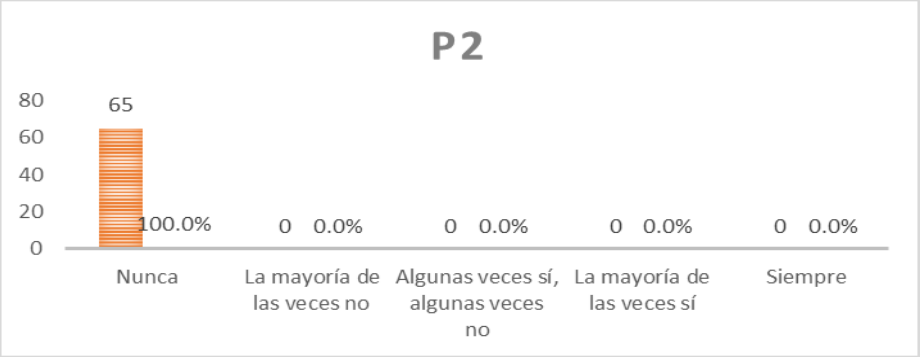
	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	60	92.3%
La mayoría de las veces no	2	5	7.7%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%



2) TABLA N°2

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

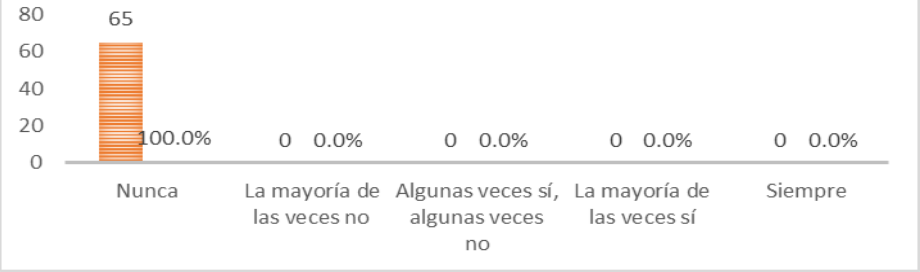
¿Ha sido participe en la asignación de roles y responsabilidades en seguridad de la información?



3) TABLA N°3

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

¿Es usted consciente que la seguridad de la información debe de cumplir con criterios de aceptación de riesgos?

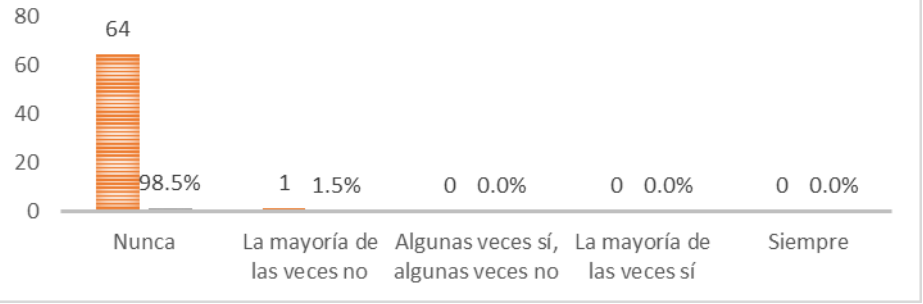


4) TABLA N°4

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	64	98.5%
La mayoría de las veces no	2	1	1.5%
Algunas veces sí, algunas veces no	3	0	0.0%

La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

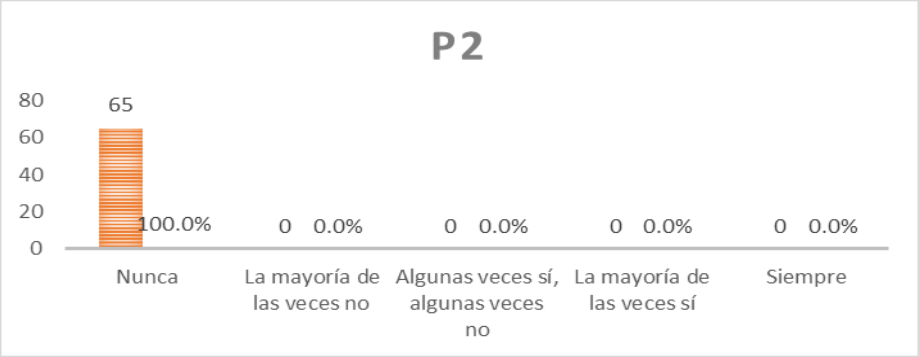
¿Es usted consciente que se debe de asignar presupuesto a temas de seguridad de la información?



5) TABLA N°5

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

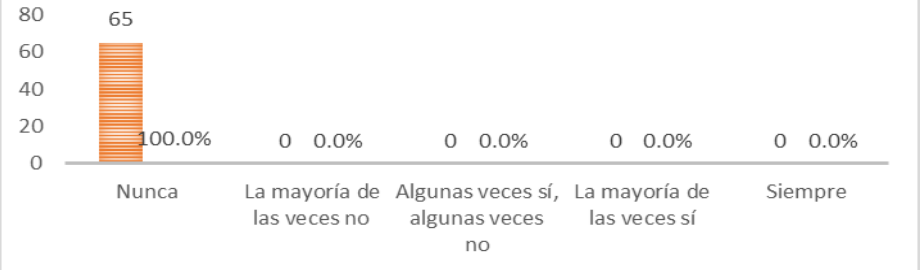
¿La institución ha realizado auditoria internas en seguridad de la información?



6) TABLA N°6

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

¿La institución realiza revisiones periódicas de las políticas de seguridad de la información?

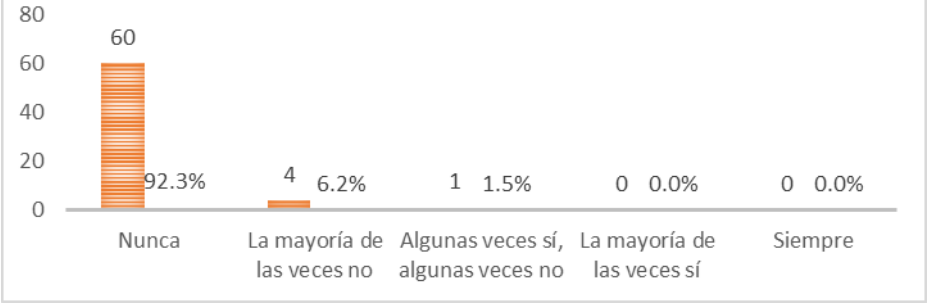


7) TABLA N°7

	CLASE	FRECUENCIA	ACUMULADO

Nunca	1	60	92.3%
La mayoría de las veces no	2	4	6.2%
Algunas veces sí, algunas veces no	3	1	1.5%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

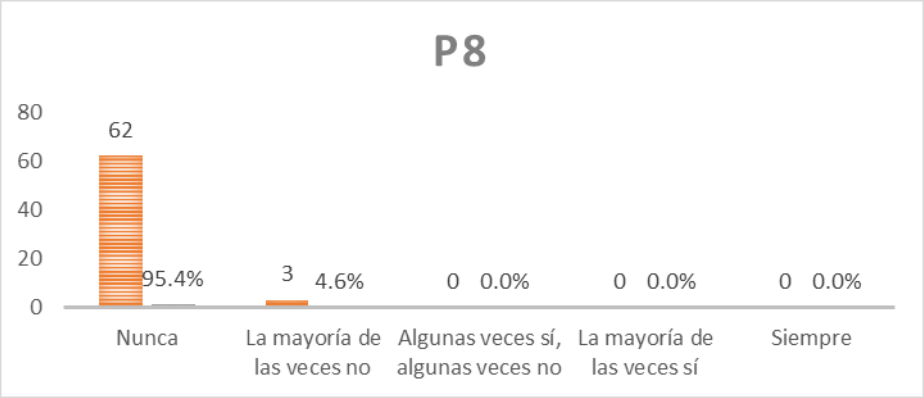
¿Es usted consciente que proteger la seguridad de la información es una parte importante de su trabajo?



8) TABLA N°8

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	62	95.4%
La mayoría de las veces no	2	3	4.6%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

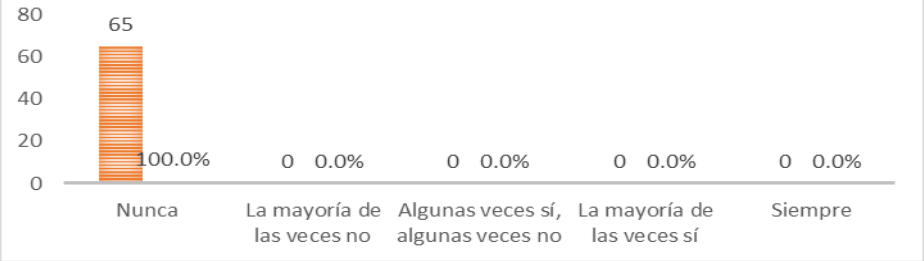
¿Es usted consciente del riesgo de no seguir políticas de seguridad de la información?



9) TABLA N°9

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

¿Se han definido procedimiento para reportar las violaciones de la seguridad de la información?

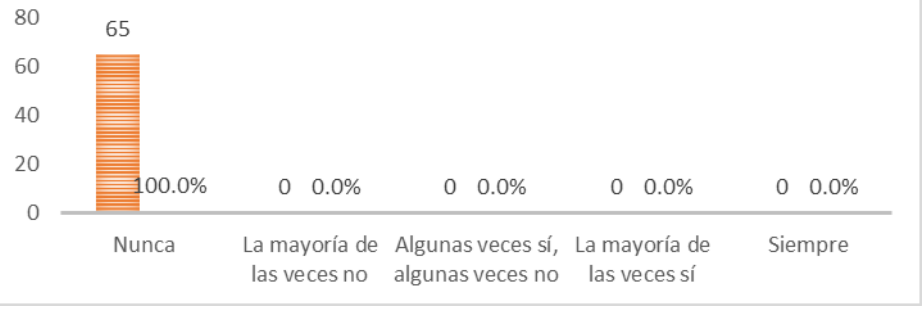


10)TABLA N°10

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%

Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

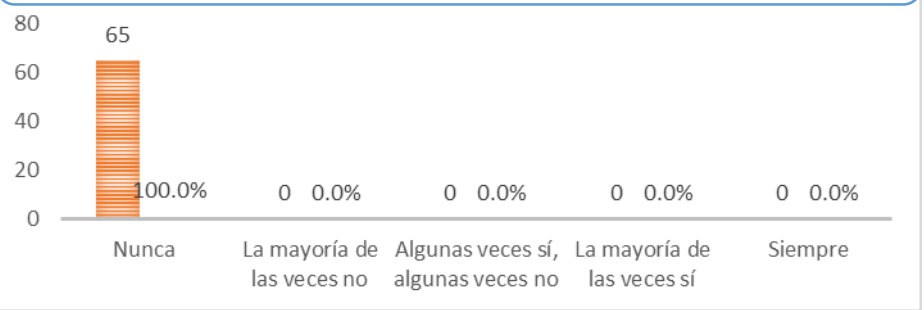
¿La empresa ha establecido objetivos para salvaguardar la información?



11)TABLA N°11

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

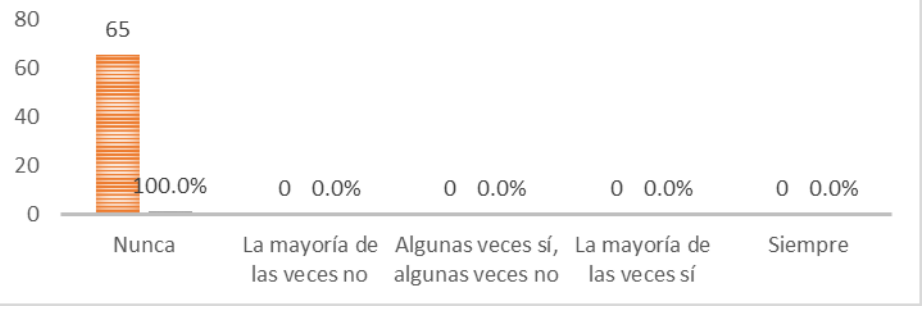
¿Se definen constantemente equipos, grupo o departamento responsable de la seguridad de la información?



12)TABLA N°12

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

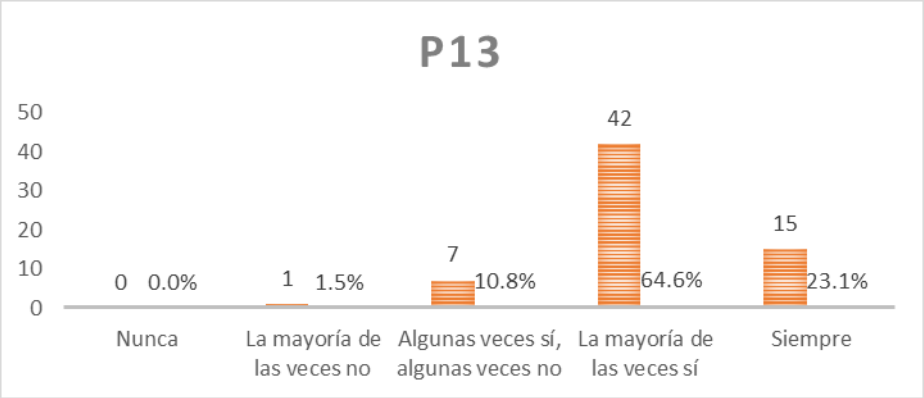
¿Se define fechas para alcanzar las metas propuestas en seguridad de la información?



13)TABLA N°13

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	0	0.0%
La mayoría de las veces no	2	1	1.5%
Algunas veces sí, algunas veces no	3	7	10.8%
La mayoría de las veces sí	4	42	64.6%
Siempre	5	15	23.1%
N° DE ENCUESTADOS		65	100.0%

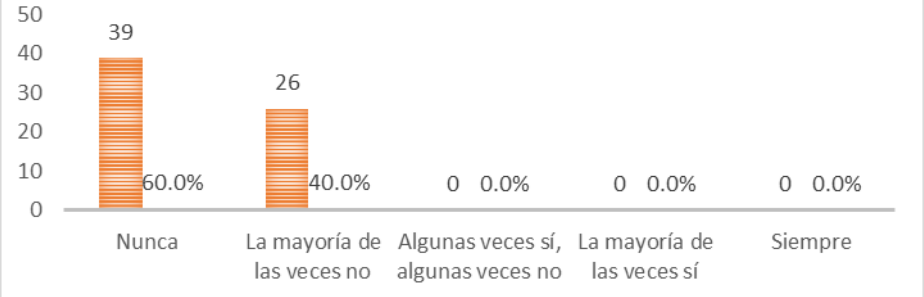
¿Se ha resquebrajado la confianza en temas de seguridad de la información?



14)TABLA N°14

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	39	60.0%
La mayoría de las veces no	2	26	40.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

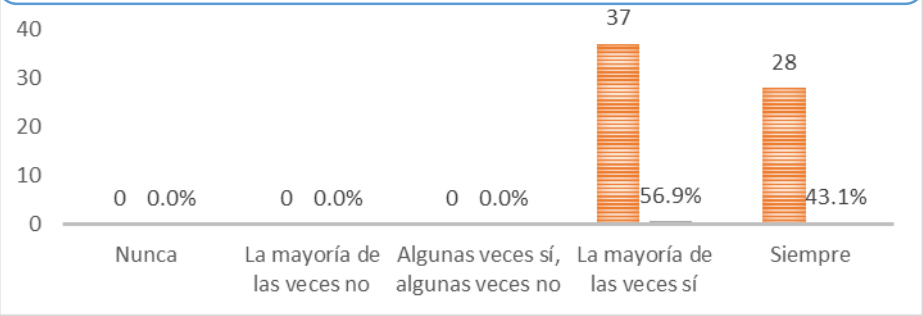
¿Son efectivas las tecnologías de seguridad de la información que hay en la organización?



15)TABLA N°15

	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	0	0.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	37	56.9%
Siempre	5	28	43.1%
N° DE ENCUESTADOS		65	100.0%

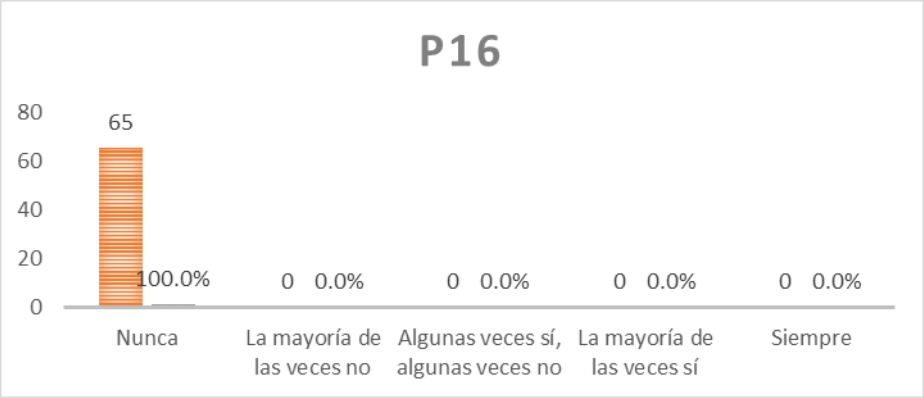
¿Se presentan incidentes de la seguridad en la información?



16)TABLA N°16

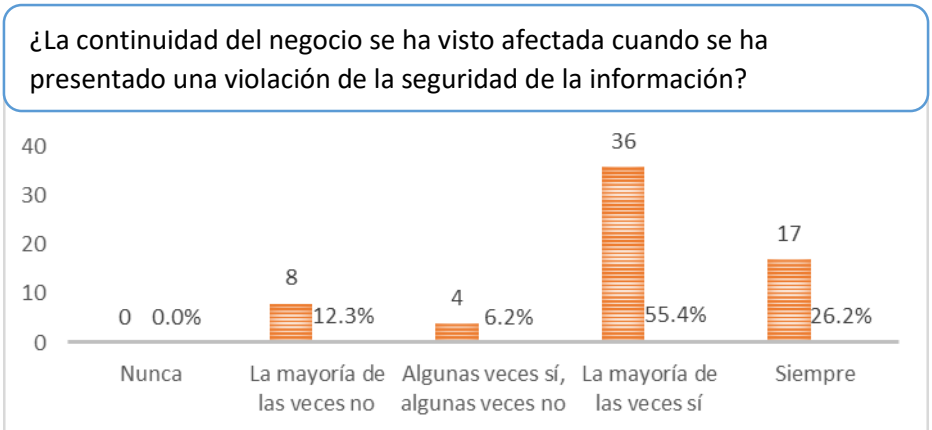
	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	65	100.0%
La mayoría de las veces no	2	0	0.0%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%

¿Se ha realizado un diagnóstico del estado actual de la seguridad de la información?



17)TABLA N°17

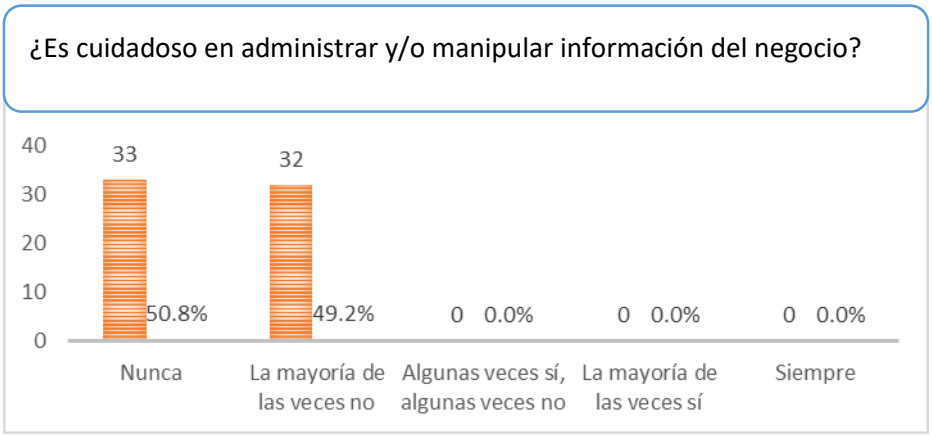
	CLASE	FRECUENCIA	ACUMULADO
Nunca	1	0	0.0%
La mayoría de las veces no	2	8	12.3%
Algunas veces sí, algunas veces no	3	4	6.2%
La mayoría de las veces sí	4	36	55.4%
Siempre	5	17	26.2%
N° DE ENCUESTADOS		65	100.0%



18)TABLA N°18

	CLASE	FRECUENCIA	ACUMULADO

Nunca	1	33	50.8%
La mayoría de las veces no	2	32	49.2%
Algunas veces sí, algunas veces no	3	0	0.0%
La mayoría de las veces sí	4	0	0.0%
Siempre	5	0	0.0%
N° DE ENCUESTADOS		65	100.0%



Anexo Nº 4: PROPUESTA

IDENTIFICACION DE LOS FACTORES CRÍTICOS DE ÉXITO.

La **identificación** de los factores críticos de éxito aplicados a la implementación de Sistemas de gestión de la seguridad de la Información, se ha realizado mediante el uso del método de los factores críticos de éxito propuesto por el Dr. John F. Rockart.

En este apartado se desarrolla la técnica para realizar una correcta identificación de los FCE, considerando que es una labor que está relacionada a la particularidad del negocio que se intenta estudiar.

En principio partimos recordando:

- Un factor de éxito es algo que debe ocurrir (o no ocurrir) para conseguir un objetivo.

- Tiene la característica de ser crítico cuando su cumplimiento es absolutamente necesario para cumplir los objetivos de la organización.
- Por tanto, se debe de requerir especial atención por parte de los órganos gestores con el fin de asegurar que se dedican los mejores recursos a la ejecución o realización de dicho factor.

3.2. DEFINICIÓN DE OBJETIVOS

Según **(Rockart, 2015)**, es conveniente ser muy explícitos en la especificación de objetivos, debido a que estos son los fines hacia donde se dirige la organización.

A continuación, se describe la misión, visión, objetivos de la empresa Prisco SAC.

Misión

Ser una organización responsable de la extracción, transformación y comercialización de productos alimentarios, con el propósito de cumplir con los estándares de calidad y servicios de nuestros clientes, trabajando en armonía con la sociedad y el medio ambiente.

Visión

INVERSIONES PRISCO S.A.C. Será una empresa líder y de prestigio internacional, basada en la elaboración de alimentos Hidrobiológicos, cumpliendo con la expectativa de satisfacción de nuestros clientes con calidad, seguridad alimentaria, mejoramiento continuo, innovación, tecnología e investigación.

Objetivos

- Ser la empresa **líder en ventas** en la industria pesquera nacional y tener una importancia relevante internacionalmente, tanto en la producción de congelados, conservas y harina de pescado.
- Prevalecer la **importancia del cliente y la calidad del servicio** que le brindamos.
- Llegar a **colocar nuestros productos en todos los continentes**.
- Brindar a nuestro personal el **mejor ambiente de trabajo** y la mejor **calidad institucional**.

3.3. DEPURACIÓN DE OBJETIVOS CLAVES

En este apartado se ha revisado la lista de objetivos obtenida en el paso anterior, con el fin de asegurar que dichos objetivos constituyen un fin en sí mismos y no un medio para obtener otro objetivo identificado, en cuyo caso se consideraría como un factor de éxito (FE).

En trabajo conjunto con la dirección y gerencia se analizó los objetivos inicialmente establecidos y se definió la siguiente lista depurada:

- Líder de ventas.
- Calidad del servicio.

- Diversificación de mercado.
- Calidad Institucional.

3.1.1. IDENTIFICACIÓN DE FACTORES DE ÉXITO

En este paso se obtuvo un listado de factores de éxito, aplicados a la implementación de sistemas de gestión de la seguridad de la información, como medio necesario para conseguir los objetivos claves del negocio, su cumplimiento o existencia contribuirá a logro o éxito del mismo.

En primer término, se hizo uso una lista de chequeo (**checklist**), la cual fue suministrada al equipo de trabajo, conformada por el responsable de la dirección, la gerencia, tomadores de decisiones y el responsable del proyecto (6 personas).

Se consideró que el **checklist** debía considerar preguntas basadas en las recomendaciones sugeridas por **INDECOPI (2009)** y **Villamizar R, Carlos (2014)**. Esto debido a que era necesario tener un punto de referencia sobre la cual generar un espacio de discusión.

La temática se basó en organizar y ejecutar 3 sesiones, que se llevaron acabo de la siguiente manera:

Primera sesión: Se revisaron los objetivos del negocio, se propusieron los factores críticos para el logro de cada objetivo, se relacionan objetivos vs. factores críticos de éxito para clarificar, combinar, eliminar o redefinir estos últimos y se aproximan medidas para esos factores.

Segunda sesión. Se revisaron los resultados de la primera sesión, se discutieron en profundidad varias medidas para los factores críticos de éxito y su naturaleza.

Tercera sesión. Se llegó a un acuerdo final acerca de los FCE, medidas y se creó una secuencia de estos elementos.

Cada taller demandó 2 horas para su ejecución, esto generó un espacio de discusión de 6 horas, en la cual se desarrollaron todos los pasos que demanda la técnica de John F. Rockart.

En principio por cada factor crítico propuesto, se le suministró al grupo de trabajo la siguiente la pregunta a resolver: ***¿El cumplimiento o existencia de este factor contribuirá al logro o cumplimiento del objetivo del negocio*?**

Tabla N° 06: Cumplimiento

Factores de éxito	Pregunta
Compromiso de la gerencia en seguridad de la información.	**SI**
Cultura organizacional en seguridad de la información.	**SI**
Misión de la organización	**NO** Se estableció que debe ser absorbida por la **Cultura organizacional**.
Alcance de la seguridad de la información.	**SI**
Recursos y presupuesto	**NO** Se estableció que debe ser absorbida por el **compromiso de la gerencia**.
Evaluación del desempeño.	**SI**

Formación y capacitación	**NO** Se estableció que debe ser absorbida por la **Sensibilización en seguridad**.
Sensibilización en seguridad de la información.	**SI**
Existencia de capital humano capacitado	**SI**
Transferencia tecnológica adecuada.	**SI**

Fuente: Elaborado por el autor

Resultado de ello se organizó los factores de éxito de la siguiente manera:

Tabla N° 07: Cumplimiento

Factores de éxito bajo el control de la organización	Factores de éxito fuera del control de la organización
Compromiso de la gerencia en seguridad de la información.	Existencia de capital humano capacitado.
Cultura organizacional en seguridad de la información.	Transferencia tecnológica adecuada.
Alcance de la seguridad de la información.	
Evaluación del desempeño.	
Sensibilización en seguridad de la información.	

Fuente: Elaborado por el autor

3.1.2. AGRUPAR LOS FACTORES DE ÉXITO DE ACUERDO A LOS OBJETIVOS

En la siguiente tabla se agrupa los factores de éxito en implementación de sistemas de gestión de la seguridad identificados en el apartado anterior, como medios para cumplir los objetivos propuestos ya depurados en el punto 3.1.2.

Tabla N° 08: implementación de sistemas de gestión

Objetivo	Factor de éxito
Líder de ventas	Compromiso de la gerencia en seguridad de la información
Calidad del servicio	Cultura organizacional en seguridad de la información. Alcance de la seguridad de la información. Existencia de capital humano capacitado.
Diversificación de mercado	Evaluación del desempeño. Transferencia tecnológica adecuada.
Calidad Institucional	Sensibilización en seguridad de la información.

Fuente: Elaborado por el autor

3.1.3. ELIMINACIÓN DE FACTORES DE ÉXITO NO CRÍTICOS

En este apartado se pasa a depurar los factores de éxito dejando solo los que presentan la característica de “críticos”.

Según Rockart, para depurarlos se considera si los factores se encuentran dentro o fuera del control de la organización y según ello se suministran las siguientes preguntas:

Grupo 01: factores de éxito bajo el control de la organización.

- **P01:** ¿Es el factor esencial para cumplir los objetivos?
- **P02:** ¿Requiere especial cuidado en su realización, es decir, recursos especialmente cualificados?

Si la respuesta a alguna de estas preguntas es NO, el factor de éxito no es "critico".

La siguiente tabla muestra las respuestas por cada pregunta planteada a los factores de éxito que están bajo del control de la organización, la última columna muestra si el factor es crítico o no.

Tabla N° 09: implementación de sistemas de gestión

Factor	P01	P02	¿Es Crítico?
Compromiso de la gerencia en seguridad de la información.	SI	SI	SI
Cultura organizacional en seguridad de la información	SI	SI	SI
Alcance de la seguridad de la información	SI	SI	SI
Evaluación del desempeño	SI	SI	SI
Sensibilización en seguridad de la información	SI	SI	SI

Fuente: Elaborado por el autor

Grupo 02: factores de éxito fuera del control de la organización.

- **P01:** ¿Es el Factor de Éxito esencial para cumplir los objetivos?
- **P02:** ¿Hay una probabilidad significativa de que el Factor de Éxito no ocurra?
- **P03:** Si no ocurre el Factor de Éxito ¿Podrían alterarse las estrategias con el fin de minimizar el impacto de dicho incumplimiento, suponiendo que hubiese suficiente tiempo disponible?

Si la respuesta a alguna de estas preguntas es NO, el factor de éxito no es "crítico".

Esto se hace para no considerar aquellos factores de éxito que ocurren casi con toda seguridad (en caso de una respuesta negativa a la segunda pregunta) o aquellos factores de éxito cuyo no cumplimiento impide cualquier tipo de acción correctiva (en el caso de una respuesta negativa a la tercera pregunta)

La siguiente tabla muestra las respuestas por cada pregunta planteada a los factores de éxito que están fuera del control de la organización, la última columna muestra si el factor es crítico o no.

Tabla N° 10: análisis de datos

Factor	P01	P02	P03	¿Es Crítico?
Existencia de capital humano capacitado.	SI	SI	NO	NO
Transferencia tecnológica adecuada.	SI	SI	SI	SI

Fuente: Elaborado por el autor

Resultado de esta evaluación estableció como factores críticos de éxito los siguientes:

- **Compromiso de la gerencia** en seguridad de la información.
- **Cultura organizacional** en seguridad de la información.
- **Alcance** de la seguridad de la información.
- **Evaluación del desempeño**.
- **Sensibilización** en seguridad de la información.
- **Transferencia tecnológica** adecuada.

3.1.4. IDENTIFICACION DE ATRIBUTOS A MEDIR DIRECTAMENTE RELACIONADOS CON CADA FACTOR CRÍTICO DE ÉXITO

En esta parte se determina un número limitado de atributos, específicamente los que tienen relación con la implementación de sistemas de seguridad de la información.

Tabla N° 11: Atributos

Factor crítico de éxito	Atributos
Compromiso de la gerencia en seguridad de la información.	Políticas de seguridad de la información. Roles y responsabilidades. Criterios de aceptación de riesgos. Asignación de recursos. Auditorías Internas. Revisiones Periódicas del SGSI.
Cultura organizacional en seguridad de la información.	Importancia de la seguridad de la información. Concientización del riesgo.

	Procedimientos para reportar las violaciones de seguridad de la información.
Alcance de la seguridad de la información.	Objetivos para salvaguardar la información. Fijación de responsables de la seguridad de la información. Metas a alcanzar de SGSI.
Evaluación del desempeño.	Confianza en temas de seguridad de la información. Tecnologías de seguridad de la información. Incidentes de seguridad.
Sensibilización en seguridad de la información.	Diagnóstico del estado de la seguridad de la información. Continuidad del negocio. Manipulación de información.

Fuente: Elaborado por el autor

3.1. EVALUACION DE LOS FACTORES CRITICOS DE ÉXITO,

Posterior a la definición de los factores críticos de éxito (**FCE**), se elaboró una batería de preguntas basadas en los atributos medibles establecidos en el apartado anterior. Se considera la siguiente escala

(1) Nunca, (2) La mayoría de las veces no, (3) Algunas veces sí, algunas veces no, (4) La mayoría de las veces sí, (5) Siempre

En los resultados de la evaluación:

- Es necesario establecer estrategias y mecanismos que permitan atender el FCE compromiso de la alta gerencia respecto a la implementación de Sistemas de Gestión de la Seguridad de la Información. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

- Es necesario establecer estrategias y mecanismos que permitan atender el FCE Cultura Organizacional respecto a la implementación de Sistemas de Gestión de la Seguridad de la Información. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

- Es necesario establecer estrategias y mecanismos que permitan atender el FCE alcance de la seguridad de la información respecto a la implementación de Sistemas de Gestión de la Seguridad de la Información. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

- Es necesario establecer estrategias y mecanismos que permitan atender el FCE evaluación del desempeño respecto a la implementación de Sistemas de Gestión de la Seguridad de la Información. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

- Es necesario establecer estrategias y mecanismos que permitan atender el FCE sensibilización respecto a la implementación de Sistemas de Gestión de la Seguridad de la Información. Puesto que se está observando que cada atributo medido del presente factor nos muestra el conjunto de carencias que existen en el negocio respecto a la seguridad de la información.

Posterior a la evaluación de los atributos medibles que están directamente relacionados con cada factor crítico de éxito, se procedió a suministrar al grupo de interés formado por el responsable de la dirección, la gerencia, tomadores de decisiones, la siguiente pregunta ¿Que factor crítico de éxito, considera Ud. que es el más estratégico e importante en el éxito de implementación del SGSI?

Tabla N° 11: Factores críticos de éxito

Estadísticos

¿Qué factor crítico de éxito, considera Ud. que es el más estratégico e importante en el éxito de implementación del SGSI?

N	Válido	9
	Perdidos	0
Moda		5
Percentiles	25	3,00
	50	5,00
	75	5,00

Fuente: Elaborado por el autor

Tabla N° 12: Factores críticos de éxito

¿Que factor crítico de éxito, considera Ud. que es el más estratégico e importante en el exito de implementación del SGSI?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Compromiso de la Alta Gerencia	2	22,2	22,2	22,2
	Sensibilización	7	77,8	77,8	100,0
	Total	9	100,0	100,0	

Fuente: Elaborado por el autor

Por tanto, se observa que un 77.8% de los encuestados optan por considerar a la **Sensibilización** como el factor más importante porque se considera una oportunidad que contribuye a que los trabajadores de la empresa estén informados y concientizados en la importancia de la implementación del sistema de Seguridad de la Información.

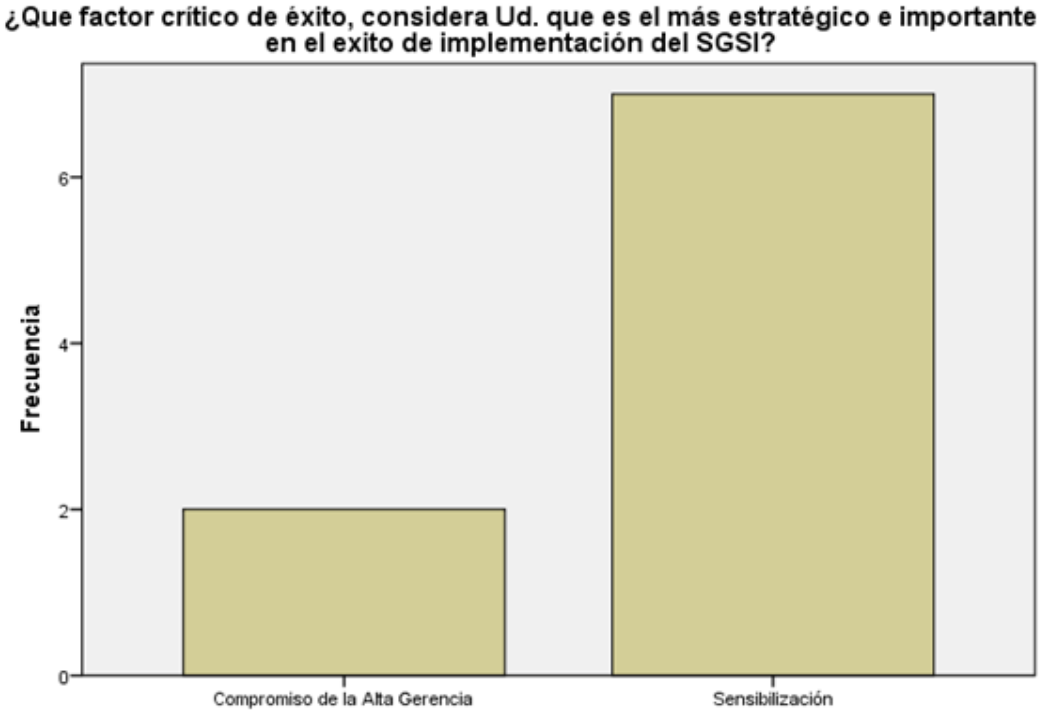


Ilustración 2-: Gráficos

Anexo Nº 5: Validación de Expertos

Validez de contenido del cuestionario sobre Análisis de los factores críticos de éxito para la implementación de un sistema de gestión de seguridad de información en la empresa I.Prisco SAC - Sechura.

Estimado(a) Ingeniero/Maestro/Doctor:

DR. VÍCTOR ANCAJIMA HIÑÁN .

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para analizar los factores críticos de éxito y con ello 6 dimensiones respecto al compromiso de la gerencia, cultura organizacional, misión de la organización, recursos y presupuesto, formación y capacitación, conciencia de la necesidad de seguridad de la información en la empresa inversiones Prisco SAC. A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

A. Información sobre el especialista

Sexo	: Varón (X) Mujer ( )
Edad	: 52 Años
Profesión o especialidad	: DR. EN TECNOLOGIAS INFORMACIÓN
Años de experiencia laboral	: 18 AÑOS
No. ID. Colegio Profesional	: CIP 86817

B. Definición de conceptos y pertinencia de cada ítem

Analizar los factores críticos de éxitos : El compromiso de la gerencia, la cultura organizacional que se da en la empresa, misión de organización, recursos y presupuesto, formación y capacitación, conciencia de la necesidad de la seguridad de información; con estos 6 dimensiones vamos analizar..

Ítems relacionados con los factores críticos de éxito.	¿Es pertinente con el concepto?		¿Necesita mejorar la redacción?		¿Es tendencioso, aquiescente?		¿Se necesita más ítems para medir el concepto?	
	SÍ	NO	SÍ	NO	SÍ	NO	SI	NO
Ha sido participe en la concientización de políticas de seguridad de la información	✓		✓			✓		✓
Ha sido participe en la asignación de roles y responsabilidades en seguridad de la información	✓			✓		✓		✓
Es usted consciente que la seguridad de la información debe de cumplir con criterios de aceptación del riesgo	✓			✓		✓		✓
Es usted consciente que se debe de asignar presupuesto a temas de seguridad de la información	✓			✓		✓		✓
La institución ha realizado auditorías internas en seguridad de la información	✓			✓		✓		✓
La institución realiza revisiones periódicas de las políticas de seguridad de la información	✓			✓		✓		✓
Es usted consciente que proteger la seguridad de la información es una parte importante de su trabajo	✓			✓		✓		✓
Es usted consciente del riesgo de no seguir políticas de seguridad de la información	✓			✓		✓		✓
Se han definido procedimientos para reportar las violaciones de seguridad de la información	✓			✓		✓		✓
La empresa ha establecido objetivos para salvaguardar la información	✓			✓		✓		✓
Se definen constantemente equipos, grupo o departamento responsable de la seguridad de la información	✓			✓		✓		✓
Se definen fechas para alcanzar las metas propuestas en seguridad de la información .	✓			✓		✓		✓
Se ha resquebrajado la confianza en temas de seguridad de la información.	✓			✓		✓		✓

Son efectivas las tecnologías de seguridad de la información que hay en la organización	✓		✓			✓		✓
Se presentan incidentes de seguridad en la organización	✓			✓		✓		✓
Se ha realizado un diagnóstico del estado actual de la seguridad de la información.	✓			✓		✓		✓
La continuidad del negocio se ha visto afectada cuando se ha presentado una violación de la seguridad de la información.	✓			✓		✓		✓
Es cuidadoso en administrar y/o manipular información del negocio.	✓			✓		✓		✓

Muchas gracias por su colaboración!

Carta emitida por el juez experto que cierra el procedimiento de la validez y fiabilidad

Yo VÍCTOR ANCAJIMA MIÑÁN especialista en INGENIERÍA SISTEMAS, ostento el grado de DOCTOR y ejerzo la carrera profesional en DOCENCIA UNIVERSITARIA VALIDÓ el instrumento denominado FACTORES CRÍTICOS DE ÉXITO, el mismo que consta del análisis de factores críticos de éxito para la implementación de un sistema de gestión de seguridad de la información en la empresa inversiones Prisco SAC – Sechura.

Fecha

30/09/2016

Firma y pos firma

VÍCTOR A. ANCAJIMA MIÑÁN
INGENIERO DE SISTEMAS
DOCTOR EN TIC
CIP N° 86817

Validez de contenido del cuestionario sobre Análisis de los factores críticos de éxito para la implementación de un sistema de gestión de seguridad de información en la empresa I.Prisco SAC - Sechura.

Estimado(a) Ingeniero/Maestro/Doctor:

Ing. Miguel Arcajima Holgín

Siendo conocedor de su trayectoria académica y profesional, me he tomado la libertad de elegirlo como JUEZ EXPERTO para revisar el contenido del cuestionario que pretendo utilizar para analizar los factores críticos de éxito y con ello 6 dimensiones respecto al compromiso de la gerencia, cultura organizacional, misión de la organización, recursos y presupuesto, formación y capacitación, conciencia de la necesidad de seguridad de la información en la empresa inversiones Prisco SAC. A continuación presento una lista de afirmaciones (ítems) relacionadas a cada concepto teórico. Lo que se le solicita es marcar con una X el grado de pertenencia de cada ítem con su respectivo concepto, de acuerdo a su propia experiencia y visión profesional. No le pido que responda las preguntas de cada área, sino que indique si cada pregunta es apropiada o congruente con el concepto o variable que se pretende medir.

Los resultados de esta evaluación servirán para determinar los coeficientes de validez de contenido del presente cuestionario. De antemano agradezco su cooperación.

A. Información sobre el especialista

Sexo	: Varón (x) Mujer ( )
Edad	: ...28... Años
Profesión o especialidad	: ...Ing. Sistemas.
Años de experiencia laboral	: ...5 años...
No. ID. Colegio Profesional	: ...131339...

B. Definición de conceptos y pertinencia de cada ítem

Analizar los factores críticos de éxitos : El compromiso de la gerencia, la cultura organizacional que se da en la empresa, misión de organización, recursos y presupuesto, formación y capacitación, conciencia de la necesidad de la seguridad de información; con estos 6 dimensiones vamos analizar..

Ítems relacionados con los factores críticos de éxito.	¿Es pertinente con el concepto?		¿Necesita mejorar la redacción?		¿Es tendencioso, aquiescente?		¿Se necesita más ítems para medir el concepto?	
	SÍ	NO	SÍ	NO	SÍ	NO	SI	NO
Ha sido participe en la concientización de políticas de seguridad de la información	4			4		4		4
Ha sido participe en la asignación de roles y responsabilidades en seguridad de la información	4			4		4		4
Es usted consciente que la seguridad de la información debe de cumplir con criterios de aceptación del riesgo	4			4		4		4
Es usted consciente que se debe de asignar presupuesto a temas de seguridad de la información	4			4		4		4
La institución ha realizado auditorías internas en seguridad de la información	4			4		4		4
La institución realiza revisiones periódicas de las políticas de seguridad de la información	4			4		4		4
Es usted consciente que proteger la seguridad de la información es una parte importante de su trabajo	4			4		4		4
Es usted consciente del riesgo de no seguir políticas de seguridad de la información	4			4		4		4
Se han definido procedimientos para reportar las violaciones de seguridad de la información	4			4		4		4
La empresa ha establecido objetivos para salvaguardar la información	4			4		4		4
Se definen constantemente equipos, grupo o departamento responsable de la seguridad de la información	4			4		4		4
Se definen fechas para alcanzar las metas propuestas en seguridad de la información .	4			4		4		4
Se ha resquebrajado la confianza en temas de seguridad de la información.	4			4		4		4

Son efectivas las tecnologías de seguridad de la información que hay en la organización	4			4		4		2
Se presentan incidentes de seguridad en la organización	4			4		2		2
Se ha realizado un diagnóstico del estado actual de la seguridad de la información.	4			4		2		0
La continuidad del negocio se ha visto afectada cuando se ha presentado una violación de la seguridad de la información.	4			4		2		2
Es cuidadoso en administrar y/o manipular información del negocio.	4			4		2		2

Muchas gracias por su colaboración!

Carta emitida por el juez experto que cierra el procedimiento de la validez y fiabilidad

Yo. Miguel Abelardo Ancajima H. especialista en. Ingeniería de Sistemas.,
ostento el grado de Ingeniero Sistemas y ejerzo la carrera profesional en
Empresa Equicom SAC. VALIDO el instrumento
denominado. Análisis de factores críticos de éxito., el mismo que consta del análisis de factores críticos de éxito para la implementación de un sistema de gestión de seguridad de la información en la empresa inversiones Prisco SAC – Sechura.

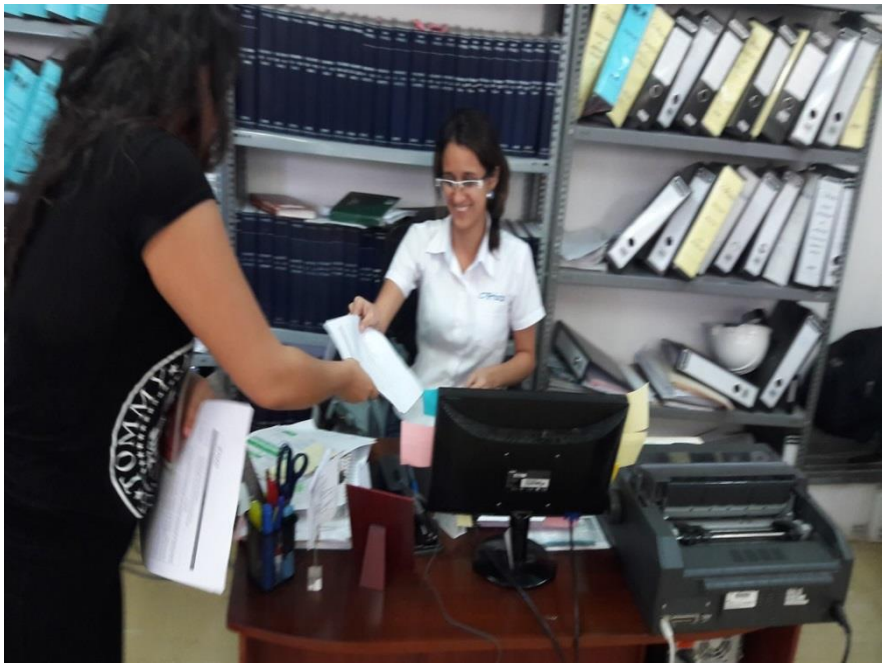
Fecha

30/09/2016

MIGUEL ABELARDO
ANCAJIMA HOLGUIN
INGENIERO DE SISTEMAS
Reg. CIP N° 131334

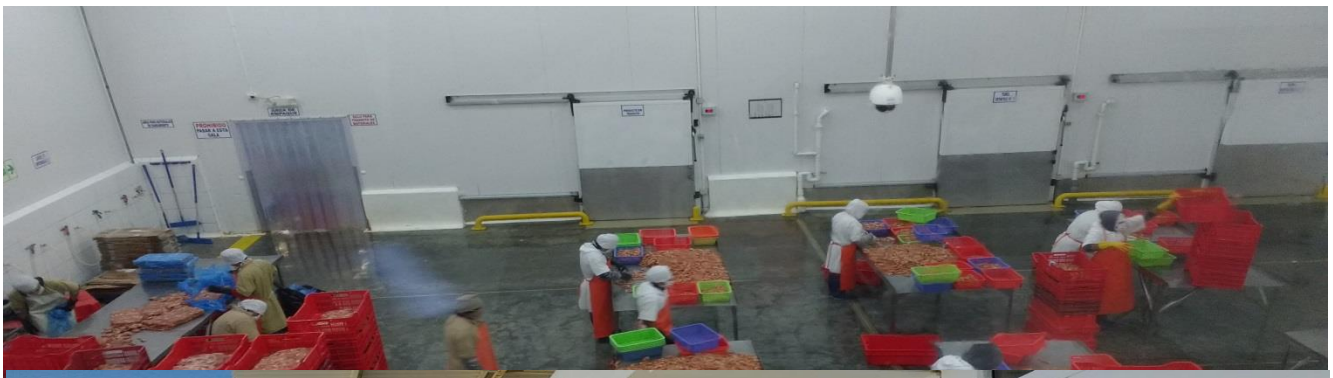
Firma y pos firma

Anexo Nº 6: Fotos de Encuestas




2014
SC 3178
SC 3201
600 cjo Mix
440 cjo Rojos
560 cubos
1600
1500X6 Mixtura
450X12 Mixtura
800X12 Rojos
160X12 Rojos
160X6 cubos
410 X24 cubos


SALIDA




Inversiones Prisco

Anexo Nº 7: Carta de Realización de Proyecto

iPrisco
Av. Victor Temoche S/N Sector 04
Sechura - Piura
Teléfono: 073 - 377138

"Año de la Consolidación del Mar de Grau"

Constancia de Realización de Proyecto

Hace Constar:

ZAPATA MORAN, DIANA STEFANY

Estudiante del X ciclo de la escuela de Ingeniería de sistemas de la Universidad Cesar Vallejo de Piura, ha realizado el proyecto titulado: "ANÁLISIS DE FACTORES CRÍTICOS DE ÉXITO PARA LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) EN LA EMPRESA INVERSIONES PRISCO SAC – SECHURA"

Se expide la presente constancia para los fines que crean conveniente.

Sechura, 20 de Octubre del 2016

INVERSIONES PRISCO S.A.C.