UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN DEL GOBIERNO REGIONAL PIURA; 2020.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERO DE SISTEMAS

AUTOR:

GARCIA CRUZ RODOLFO AUGUSTO

ORCID: 0000-0001-5213-990X

ASESOR:

MORE REAÑO RICARDO EDWIN

ORCID: 0000-0002-6223-4246

PIURA – PERÚ

2020

EQUIPO DE TRABAJO

AUTOR

GARCIA CRUZ RODOLFO AUGUSTO

ORCID ID: 0000-0001-5213-990X

Universidad Católica Los Ángeles de Chimbote, Estudiante de Pregrado, Piura, Perú

ASESOR

MORE REAÑO RICARDO EDWIN

ORCID ID: 0000-0002-6223-4246

Universidad Católica Los Ángeles de Chimbote, Facultad de Ingeniería, Escuela Profesional de Ingeniería de Sistema, Piura, Perú

JURADO

SULLÓN CHINGA JENNIFER DENISSE

ORCID: 0000-0003-4363-0590

SERNAQUÉ BARRANTES MARLENY

ORCID:0000-0002-5483-4997

GARCÍA CÓRDOVA EDY JAVIER

ORCID:0000-0001-5644-4776

HOJA DE FIRMA DEL JURADO Y ASESOR

MGTR. SULLÓN CHINGA JENNIFER DENISSE
PRESIDENTE

MGTR. SERNAQUÉ BARRANTES MARLENY
MIEMBRO

MGTR. GARCÍA CÓRDOVA EDY JAVIER
MIEMBRO

MGTR. MORE REAÑO RICARDO EDWIN
ASESOR

DEDICATORIA

Este trabajo está dedicado a mi madre.

Rodolfo Augusto García Cruz

AGRADECIMIENTO

Agradezco a mi familia, a aquellos que siempre están a mi lado incondicionalmente, a la vida por conocer y seguir conociendo, a mis educadores gracias por sus enseñanzas y a mis amigos por todo lo vivido y lo que aún falta por venir……

Rodolfo Augusto García Cruz

RESUMEN

Esta tesis fue desarrollada bajo la línea de investigación: Sistemas de Gestión de la Calidad y Seguridad de la Información, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote; tuvo como objetivo Realizar una propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, para minimizar la pérdida de información, la investigación fue desarrollada cuantitativamente bajo el diseño descriptivo de transcripción no experimental. La población de la muestra de la tesis fue constituida por los 23 trabajadores; de los cuales se obtuvo como resultado: el 91% de los trabajadores encuestados expresaron NO están satisfacción con la situación actual; mientras el 9% indicó que, SI se encuentran satisfacción con la situación actual, el 100.00% de los trabajadores encuestados expresaron SI necesitan la seguridad de información con norma ISO 27001. El alcance abarca un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 para preservar la confidencialidad, integridad y disponibilidad de la información en la oficina de tecnologías de información del Gobierno Regional Piura. En conclusión, se determinó que la propuesta de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura mejoro sus procesos de seguridad de la información y comunicación.

Palabras clave: Confidencialidad, Información, ISO, Integridad, Seguridad, TI.

ABSTRACT

This thesis was developed under the research line: Information Security and Quality Management Systems, from the Professional School of Systems Engineering of the Los Ángeles de Chimbote Catholic University; Its objective was to make a proposal for an information security management system based on the ISO 27001 standard for the information technology office of the Piura Regional Government; 2020, to minimize the loss of information, the research was developed quantitatively under the descriptive design of non-experimental transcription. The population of the thesis sample was constituted by 23 workers; of which the result was: 91% of the workers surveyed expressed NO satisfaction with the current situation; While 9% indicated that IF they are satisfied with the current situation, 100.00% of the workers surveyed expressed IF they need information security with ISO 27001 standard. The scope includes an information security management system based on the ISO / IEC 27001 standard to preserve the confidentiality, integrity and availability of information in the information technology office of the Piura Regional Government. In conclusion, it was determined that the proposal for an information security management system based on the ISO 27001 standard for the information technology office of the Piura Regional Government improved its information and communication security processes.

Keywords: Confidentiality, Information, ISO, Integrity, Security, IT.

ÍNDICE DE CONTENIDO

ÍNDICE DE GRÁFICOS

ÍNDICE DE TABLAS

I. INTRODUCCIÓN

En una economía donde las tecnologías de la información están cada día cada vez más en auge y más extendidas, las organizaciones deben definir políticas de seguridad más exhaustivas en sus sistemas de información para evitar el acceso a ellos por personal no autorizado y para impedir un uso malintencionado de sus datos (1).

La seguridad de la información es una regla asociada tradicionalmente a la gestión de TIC, cuyo propósito es mantener niveles admisibles de riesgo de la información organizacional y de los dispositivos tecnológicos que aprueban su recolección, procesamiento, acceso, intercambio, almacenamiento, transformación y adecuada presentación. La norma ISO/IEC 27001 que permite la garantía, la confidencialidad y la integridad de los datos e información (2).

La evolución de la tecnología en los sistemas de Información ha disminuido en su costo y ofrecen una mayor facilidad para incorporarla y difundirla en las organizaciones. Sin embargo, estos cambios no fueron asimilados en las empresas que no cuentan con una disposición financiera y/o organizativa para tener una aplicación completa o avanzada tecnológicamente, las cuales no han evolucionado a la misma velocidad.

En la actualidad se verifica variedad de tropiezos, como se menciona a continuación: salida de datos e información; su intención es obtener el contenido privado de mucha importancia para dicha institución o empresa, lo que ocasionaría es una diversidad de dificultades como organización, así mismo se recomienda contar con estrategías establecidas para solucionar estas circunstancias y que no afecte a profundidad.

Por lo tanto, cada vez hay más conciencia y consenso en la importancia de la Seguridad de la Información en las empresas y Organizaciones cualquiera sea el sector de la economía o rol en la sociedad que desempeñen, en particular en las empresas medianas y grandes. Sin embargo, existen diversas industrias y estructuras empresariales que hacen que algunos temas deban ser analizados y estudiados con una estrategia diferente, ya sea por la criticidad de la información que manejan, su dimensión o su estructura empresarial.

Hay una nueva tendencia, pero igual surgen problemas de confidencialidad de los datos y pérdida de control de los mismos. Dichos riesgos se incrementan al usar las plataformas más conocidas, como las de Microsoft, Google, teniendo en cuenta que la privacidad de la información y las comunicaciones.

Es así como surge la necesidad de realizar una propuesta de mejora para regular el acceso de los usuarios a la infraestructura y servicios TIC y otros aspectos afines. Para conducir el proceso de seguridad de informática orientado a cautelar la integridad de la información digital del Gobierno Regional de Piura. Conducir el proceso de calidad informática orientado a cautelar la integridad de la información digital del Gobierno (data) generación de copias de respaldo de (BACKUP), Regular el acceso de los usuarios a la infraestructura y servicios TIC y otros aspectos afines.

De acuerdo a lo mencionado en los párrafos anteriores sobre la problemática se procede a plantear el enunciado del problema: ¿De qué manera la propuesta de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, minimiza la pérdida de información?

Posteriormente el objetivo fue Realizar una propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, para minimizar la pérdida de información.

En base al objetivo general mencionado anteriormente se deduce los objetivos específicos:

1. Analizar la seguridad actual de la información, en la oficina de tecnologías de información del Gobierno Regional Piura.

2. Evaluar los marcos de referencias que ayuden a mejorar la seguridad de la información en la oficina de tecnologías de información del Gobierno Regional Piura.

3. Proponer la aplicación de la Norma ISO / IEC 27001, para mejorar la seguridad de la información.

En cuanto a la justificación académica, se tiene en cuenta el conocimiento adquirido durante los ciclos académicos en la Universidad Católica los Ángeles de Chimbote, mediante ello ayudará a plantear y desarrollar una propuesta diseñada para la problemática encontrada en la oficina de tecnologías de información del Gobierno Regional de Piura.

Con respecto a la justificación operativa, se basa en los objetivos específicos de la presente investigación, que permitirá al Gobierno Regional tener una mejor gestión en seguridad de la información, organización de TIC y gestión de activos.

En cuanto a la justificación económica, su finalidad es ahorrar tiempo y dinero con respecto a la seguridad de la información, cual hoy en día no solo es importante para el Gobierno Regional de Piura, sino también para las universidades y organizaciones en general.

Con respecto a la justificación tecnológica, en la oficina de tecnologías de información del Gobierno Regional de Piura, se diferencia de otras instituciones en el mejoramiento de la gestión de las TIC.

En cuanto a la justificación institucional, otorgará a la oficina de tecnologías de información del Gobierno Regional de Piura, proteger la viabilidad, confiabilidad y seguridad de las informaciones.

La presente investigación se manifiesta en una propuesta de sistema de seguridad de información, cuya finalidad es brindar respaldo, amplitud y totalidad de la privacidad en el Gobierno Regional de Piura para garantizar que los riesgos sean conocidos, asumidos, gestionados y minimizados por la institución de una forma documentada, sistemática, estructurada, eficiente y adaptada en los cambios que se produzcan.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

Ararat (3), realizó su investigación titulada: "Diseño de un SGSI basado en la norma ISO 27001 para la empresa MA PEÑALOSA CÍA. S.A.S. sede principal Cúcuta" en el año 2018, El presente proyecto pretende contribuir al mejoramiento de la seguridad de los activos informáticos de MA PEÑALOSA CÍA. S.A.S. en la sede Principal de Cúcuta, manteniendo controlados los riesgos a los que pueden estar expuestos ellos, ya sean por diversos factores humanos intencionales o no intencionales, averías de origen físico o lógico, ambientales o de origen industrial que pueden ocasionar desastres, accidentes o contaminación. Algunas de las causas de estas amenazas se originan por el desconocimiento y la falta de concientización de los usuarios para dar un adecuado manejo a los mismos activos; también por la falta de controles y procedimientos que apoyen los procesos. Se planteará una propuesta de Sistema de Gestión de Seguridad de la información a MA PEÑALOSA CÍA. S.A.S. que establezca políticas y lineamientos para proteger los activos informáticos y permita mitigar los riesgos y vulnerabilidades que puedan afectar la operatividad del negocio.

Meneses, Ramírez, Merchan y Suarez (4), realizaron su investigación titulada: "Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para los procesos soportados por el área de sistemas en la cámara de comercio de Aguachica, Cesar" en el año 2016, El objetivo principal de este proyecto consiste en la elaboración del Diseño del Sistema de Gestión de Seguridad de la Información para los procesos que son soportados por el Área de Sistemas de la Cámara de Comercio de Aguachica, Cesar, basado

en la norma internacional ISO/IEC 27001: 2013, en donde seguimos el ciclo PHVA, llegando solo a la fase del Plan, en donde identificamos los activos, salvaguardas y planteamos las políticas de seguridad pertinentes para la entidad, el motivo que inspiro el mismo es determinado por el valor que representa la información para la cámara de comercio, y el análisis de resultados determinando las deficiencias en las buenas prácticas por parte del personal encargado de la seguridad de la información y demás funcionarios. Partiendo del análisis realizado a la información que se recolecto, aplicado a los funcionarios, se determinó que existen falencias; se ha determinado que no existen políticas actualizadas, que los empleados desconocen de buenas prácticas y que a la información no se le están garantizando las características básicas de la seguridad como son Disponibilidad, Confidencialidad e Integridad. Seguido de lo descrito anteriormente se realizó el análisis de riesgos, basados en la metodología Magerit V3, en donde se identificaron los activos de acuerdo a la clasificación sugerida por la misma, se realizó caracterización de amenazas y salvaguardas y finalmente se estimó el impacto potencial y riesgo potencial que cada amenaza conlleva al sistema. Como fase final y pilar de este proyecto se realiza las Políticas de Seguridad de la Información, como marco de trabajo de la organización en lo referente al uso adecuado de los recursos tecnológicos, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

Tola (5), desarrollo su tesis titulada: “Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la Norma ISO/IEC 27001” en el año 2015. En el proyecto de titulación se pretende dar una adecuada solución de seguridad a la empresa A&CGroup S.A., la cual consiste en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), tomando como base el estándar ISO 27001:2005. El primer capítulo, el marco teórico, se refiere a revisar los

conceptos básicos que van a permitir tener una visión clara del conjunto de acciones necesarias para que la entidad involucrada pueda contar con un sistema para la seguridad y gestión de riesgos de la información. Por otra parte, en el segundo capítulo se presentan los antecedentes del proyecto, en donde se describirá el problema, la solución propuesta, el objetivo general y los objetivos específicos. En el tercer capítulo, se detalla el levantamiento de información necesario para la implementación del SGSI (Sistema de Gestión de Seguridad de la Información). El cuarto capítulo trata sobre la metodología PDCA (Plan – Do – Check - Act) y los conceptos por cada una de las etapas implicadas en el modelo. Se detalla el alcance que se desea establecer, indicando los lineamientos y principios a implementar, mantener y así mejorar la gestión de la seguridad de la información dentro de la empresa; continuando con una breve descripción de las políticas generales que se deben aplicar. El quinto capítulo describe la metodología para la gestión del riesgo con el concepto y ventajas principales de su implementación, se detalla el inventario de activos de información dentro de la organización y se especifica el análisis de riesgo con sus apropiados criterios de valoración; de igual manera se realiza la evaluación del riesgo dentro del cual se procede a describir la metodología para calcular los valores de riesgo y la selección de las estrategias para el tratamiento de los mismos. El desarrollo del sexto capítulo se centra en la explicación de la implementación de las políticas y el plan de tratamiento a utilizar para la debida gestión de riesgos que se encontraron. Por último, en el séptimo capítulo se muestra el análisis de los resultados obtenidos y las estrategias de difusión aplicadas en la empresa. Se presentan las conclusiones y recomendaciones, así como los anexos del trabajo realizado.

2.1.2. Antecedentes a nivel nacional

Torres (6), realizó su tesis titulada: “Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/IEC 27001:2013,

para el proceso de servicio post-venta de un integrador de soluciones en Telecomunicaciones" en el año 2018. El presente trabajo de tesis describió los conceptos involucrados al diseño de un Sistema de Gestión de Seguridad de la Información (SGSI) y su despliegue asociado al proceso de Servicio Post-Venta de un Integrador de Telecomunicaciones. Asimismo, este diseño contempló la adopción de los procedimientos y lineamientos indicados en la norma internacional ISO/IEC 27001 en su versión 2013 y los controles de seguridad asociados en el Anexo A de la misma. Por otro lado, el presente trabajo buscó demostrar que los beneficios de este diseño al proceso de servicio Post-Venta en estudio fueron: La clasificación de los principales activos de información, la determinación de los principales riesgos a lo que los activos de información están expuestos, la propuesta de un Plan de Tratamiento de Riesgos (PTR) sobre los activos de información, y la definición de roles y responsabilidades dentro de la adopción de una estructura organizacional de un Sistema de Gestión de Seguridad de la Información (SGSI), los cuales se ajustaron a los requerimientos de seguridad y negocios definidos por la organización. Por último, cabe destacar que todo lo comentado se logró mediante establecimiento de una metodología de la gestión de la seguridad de la información propia y adaptada de las buenas prácticas en el mercado, así como su puesta en marcha dentro del alcance definido en el presente trabajo.

Santos (7), realizó su tesis titulada: "Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de Consultoría de Software" en el año 2016. Actualmente, las empresas de consultoría de desarrollo de software cuentan con muchos retos propios de este tipo de negocio. Entre estos, destacan los relacionados a la seguridad de información, pues, debido al constante intercambio de información entre la empresa y sus clientes, aparecen riesgos potenciales que pueden comprometer el éxito e incluso la subsistencia de la organización. La solución planteada para

este problema es un Sistema de Gestión de Seguridad de Información (SGSI), el cual cuenta con el estándar ISO 27001:2013 como marco formal de requisitos a cumplir. Este sistema permitirá que los directivos y demás involucrados gestionen y tomen decisiones adecuadas respecto a la seguridad de información de la organización, para asegurar que cuente con niveles adecuados respecto a la confidencialidad, integridad y disponibilidad de la información crítica que se maneja como parte de su operación. En este informe se especifican las cuatro fases cíclicas del SGSI: el establecimiento, donde las bases del sistema se integran a los procesos del negocio; la implementación, que desarrolla los mecanismos para la adecuada administración de la seguridad; el mantenimiento, donde se detectan fallos que pueden existir en la organización o en el propio sistema; y la mejora, que finalmente permite cerrar el ciclo mediante la aplicación de todas las correcciones y optimizaciones significativas que han sido detectadas. Este modelo permite que el sistema opere bajo un principio de mejora continua, que beneficia permanentemente a la organización, propiciando un manejo adecuado de la seguridad de su información.

Castillo (8), en su tesis de maestría titulada "Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la norma ISO/IEC 27001:2013"; en el año 2016, realizado en la Universidad Católica Los Ángeles de Chimbote , el presente trabajo de tesis tiene como objetivo principal es evaluar el sistema de gestión de seguridad de la información en la Municipalidad Distrital de Pira basado en la norma ISO/IEC 27001:2013; la cual permitirá una mejor administración en los activos de información. El autor define la metodología de investigación por el grado de cuantificación reúne las condiciones de una investigación cuantitativa, el investigador para la presente investigación, se tomó como población a todo el personal administrativo que consta de 16 trabajadores que labora en la oficina matriz de la Municipalidad Distrital de Pira, que son aquellos involucrados directamente en los procesos,

para cada una de las variables en estudio sobre sistemas de gestión de seguridad de la información, al finalizar el proceso de evaluación. Según los resultados de la encuesta aplicada a los trabajadores se determinó que no cuentan con el conocimiento y las medidas adecuadas para salvaguardar los activos de información. Con el Autodiagnóstico General para la evaluación de madurez, el 93% consideran por conocimiento que, en la Municipalidad, este proceso está en el nivel Inexistente, según los niveles de madurez de la ISO/IEC 27001:2013, lo que significa que se reconoce la necesidad de recolectar y evaluar información sobre los procesos de monitoreo. El 7% No se han identificado procesos estándar de recolección y evaluación. En conclusión, esta evaluación permite a la empresa tomar medidas preventivas y correctivas en los procesos que necesitan ser atendidos con mayor brevedad a nivel de seguridad para el mejor funcionamiento de los mismos.

2.1.3. Antecedentes a nivel regional

Vegas (9), realizó su tesis titulada: "Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001" en el año 2019. La Universidad Nacional de Piura tiene la necesidad de proteger sus activos e información frente amenazas, que son importantes y cruciales para el desarrollo de sus actividades académicas. De ahí que la presente investigación tiene como objetivo diseñar un Sistema de Gestión de Seguridad de la Información, para los Procesos Académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001, con el fin de garantizar la confiablidad, integridad, disponibilidad y auditabilidad de la información. Para ello, se realizaron varias reuniones con el personal estratégico, operativo del Centro de Informática y Telecomunicaciones y Facultades que permitió definir el alcance del Sistema de Gestión de Seguridad de la Información e identificar y valorar los activos de la institución. Posteriormente se analizó la Situación Actual de Seguridad de los

procesos académicos y evaluó los riesgos a los cuales estan sometidos los activos, siguiendo la metodología de la NTP ISO/IEC 27001. Los resultados de esta investigación indican que existen políticas y controles mínimos implementados, pero estos no están documentados, un bajo porcentaje de cumplimiento de la seguridad de la información, y un alto valor de criticidad de la información y activos en los procesos académicos. A partir de esto se diseñó el Sistema de Gestión de Seguridad de la Información, con los controles propuestos, basado en la NTP ISO/IEC 27001.

Lara (10), desarrollo su tesis titulada: "Propuesta para la seguridad informática basado en la norma ISO /IEC 27001 en la clínica Simedic diagnóstica S.A.C – Piura; 2018. Esta tesis fue desarrollada bajo la línea de investigación en tecnología de la información y comunicación para la mejora continua de las organizaciones del Perú, de la escuela profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote Sede en Piura. La investigación tuvo como objetivo realizar la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018, permitirá mejorar la gestión en los activos de información. La investigación tuvo un diseño de tipo no experimental porque los datos no se manipularán y de corte transversal porque se realiza en un determinado tiempo; la población de esta investigación fue de 28 empleados de los cuales se tomó en conciencia que esta investigación no se delimitará debido a que se verán beneficiados en su totalidad de empleados, a quien se les aplicó el instrumentos donde se lograron obtener los siguientes resultados: En la dimensión 01: Situación actual; que el 61% de los trabajadores encuestados opinaron que la situación actual NO cuenta con la adecuada gestión en los procesos de la clínica Simedic Diagnóstica S.A.C, mientras que el 39% SI está conforme con la situación actual de la clínica. Y en la dimensión 02: seguridad de información; se observó que el 68% de los trabajadores encuestados opinaron que, SI están de acuerdo con la que se debería realizar la propuesta

para la seguridad informática para la clínica Simedic Diagnóstica S.A.C, mientras que el 32% NO cree necesario la propuesta para la seguridad informática. Se concluyó la propuesta para la seguridad informática basada en la norma ISO/IEC 27001 en la clínica Simedic Diagnóstica S.A.C – Piura; 2018, para la seguridad de información queda aceptada en su totalidad para brindar mayor seguridad en la clínica, trabajadores y clientes.

Albán (11), realizó su tesis titulada: "Gestión de seguridad de información basado en la norma ISO/IEC 27000 en la Municipalidad Provincial de Talara año 2016". El presente informe de Tesis está desarrollado bajo la línea de investigación en Tecnología de la Información y Comunicación, de la escuela profesional de Ingeniería de Sistemas de la Universidad Los Ángeles de Chimbote (ULADECH CATÓLICA). El objetivo principal fue Realizar la gestión de seguridad de información basada en la norma ISO/IEC 27000 en la Municipalidad Provincial de Talara año 2016; permitirá ayudar en la seguridad de los activos de información, de acuerdo a las características, la investigación fue cuantitativa, de diseño no experimental, tipo descriptiva y de corte transversal; la cual tiene una población que está constituida por 13 trabajadores administrativos, donde se tomó una muestra similar a la cantidad de la población, es decir 13 trabajadores; convirtiéndose esta en una población muestral. En la investigación se obtuvo que el 92.00% de los encuestados están insatisfechos con la situación actual y por lo tanto el 100% de los encuestados expresaron una necesidad de la realización de gestión de seguridad de información; para solucionar los inconvenientes presentados en la realización de cualquier proceso o consulta.

2.2. Bases teóricas de la investigación

2.2.1. Gobierno Regional de Piura

¿QUIÉNES SOMOS?

El Gobierno Regional Piura es un organismo que emana de la voluntad popular. Tiene personería jurídica de derecho público, con autonomía política, económica y administrativa en asuntos de su competencia, constituyendo, administrativa, económica y financieramente un Pliego Presupuestal.

Realiza una aplicación coherente y eficaz de las políticas e instrumentos de desarrollo económico, social, poblacional, cultural y ambiental, a través de planes, programas y proyectos, orientados a generar condiciones que permitan consolidar el proceso de descentralización del país y el crecimiento económico armonizado con la dinámica demográfica, el desarrollo social equitativo y la conservación de los recursos naturales y el ambiente en el territorio regional, orientado hacia el ejercicio pleno de los derechos de hombres y mujeres en igualdad de oportunidad.

MISIÓN

Conducir y promover el desarrollo sostenible e integral de la población del departamento de Piura, mediante la provisión de servicios públicos e infraestructura de calidad, con énfasis en reducir la vulnerabilidad.

VISIÓN

Piura, departamento seguro e inclusivo, desarrolla una economía competitiva, diversificada e innovadora, gracias al aprovechamiento sostenible y

responsable de los recursos naturales, potencialidades y diversidad de su territorio.

Su población goza de servicios públicos de calidad y sus productores y productoras han fortalecido sus capacidades para la innovación y transformación productiva.

BREVE RESEÑA HISTORICA

La modificación del Capítulo XIV del Título IV de la Constitución Política del Perú, permitió la creación de los Gobiernos Regionales, iniciando así la política de Descentralización de la estructura del estado aplicada por el gobierno del Dr. Alejandro Toledo Manrique.

Esta política que tiene como objetivo fundamental el desarrollo integral del país se da con la Ley Nº 27680 del 07 de marzo de 2002. Luego con la Ley de Descentralización Nº 27783 del 20 de julio 2002, se regula la estructura y organización del Estado en forma democrática, descentralizada y desconcentrada, correspondiente al Gobierno Nacional, Gobierno Regional y Gobierno Local, y con La ley Orgánica de Gobierno Regionales Nº 27867, del 18 de noviembre de 2002 se establece y norma la estructura, organización, competencias y funciones de los gobiernos regionales. La estructura organizacional del nuevo Gobierno Regional fue en base al organismo creado transitoriamente mediante Decreto Ley Nº 25432 del 11 de abril de 1992, por el Gobierno de turno, denominado Consejo de Administración Regional Piura.

En concordancia con el Decreto Ley Nº 26109 del 24 de diciembre de 1992, que declara en reorganización y reestructuración administrativa a los Gobiernos Regionales, posteriormente, queda definido el CTAR Piura por aplicación de la Resolución Ministerial Nº 032-93-PRES del 04 marzo de 1993, el que es

incorporado al Ministerio de la Presidencia, mediante Ley Nº 26499 del 13 de julio de 1995.

CTAR Piura sustituyó a la Asamblea y Consejo Regional de la Región Grau, que fuera creada con Ley Nº 24793 el 16 de febrero de 1988, como un organismo descentralizado con personería jurídica y de derecho público interno, con autonomía administrativa y económica, siendo creado sobre la base de los departamentos de Piura y Tumbes

DENOMINACIONES DEL GOBIERNO REGIONAL:

1936 – 2003

Tabla Nro. 1: Denominación del Gobierno Regional Piura

DENOMINACIÓN	AÑO
Junta de Obras Públicas	1936
Corporación de Desarrollo de Piura – CORPIURA	1963
Sistema Nacional de Movilización Social – SINAMOS	1969
Organismos de Desarrollo del Norte – ORDENORTE	1978
Corporación de Desarrollo de Piura - CORPIURA	1981
Asamblea y Consejo Regional de la Región Grau	1988
Consejo Transitorio de Administración Regional Piura – CTAR Piura	1992
Gobierno Regional Piura	2003

Fuente: Elaboración propia.

OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN

- Proponer, formular, organizar, dirigir e implementar las políticas y planes de aplicación y uso de tecnologías de la información y de las comunicaciones, de manera que estos prevean soporte a la operación del Gobierno Regional Piura.

- Formular, actualizar, proponer y evaluar la normatividad interna de los sistemas de soporte informático, a través de Reglamentos, Directivas, Manuales de Procedimientos y otros documentos, con el asesoramiento de la Sub Gerencia Regional de Desarrollo Institucional, dentro del marco de sus competencias.

- Conducir y ejecutar las actividades, servicios y proyectos en concordancia con los lineamientos de política y objetivos generales institucionales aprobados y con la Política Nacional Informática.

- Formular, implementar, ejecutar y supervisar los planes de contingencia y de seguridad de la información que garanticen la continuidad de la gestión, basados de acuerdo a normas establecidas que brindan una excelente seguridad.

Tabla Nro. 2: Plan Estratégico de Tecnologías de la Información

Documento de Aprobación	Plan	Periodo	Fecha de Aprobación
RE N° 191-2017	VIGENTE	2017-2019	29/03/2017

Fuente: Elaboración propia.

Tabla Nro. 3: Plan Operativo Informático

Documento de Aprobación	Plan	Periodo	Fecha de Aprobación
RE N° 269-2018	VIGENTE	2018	08/05/2018

Fuente: Elaboración propia.

Tabla Nro. 4: Plan Estratégico Institucional de Gobierno Electrónico - PEGE

Documento de Aprobación	Plan	Periodo	Fecha de Aprobación
RE N° 853-2017	VIGENTE	2018-2020	29/12/2017

Fuente: Elaboración propia.

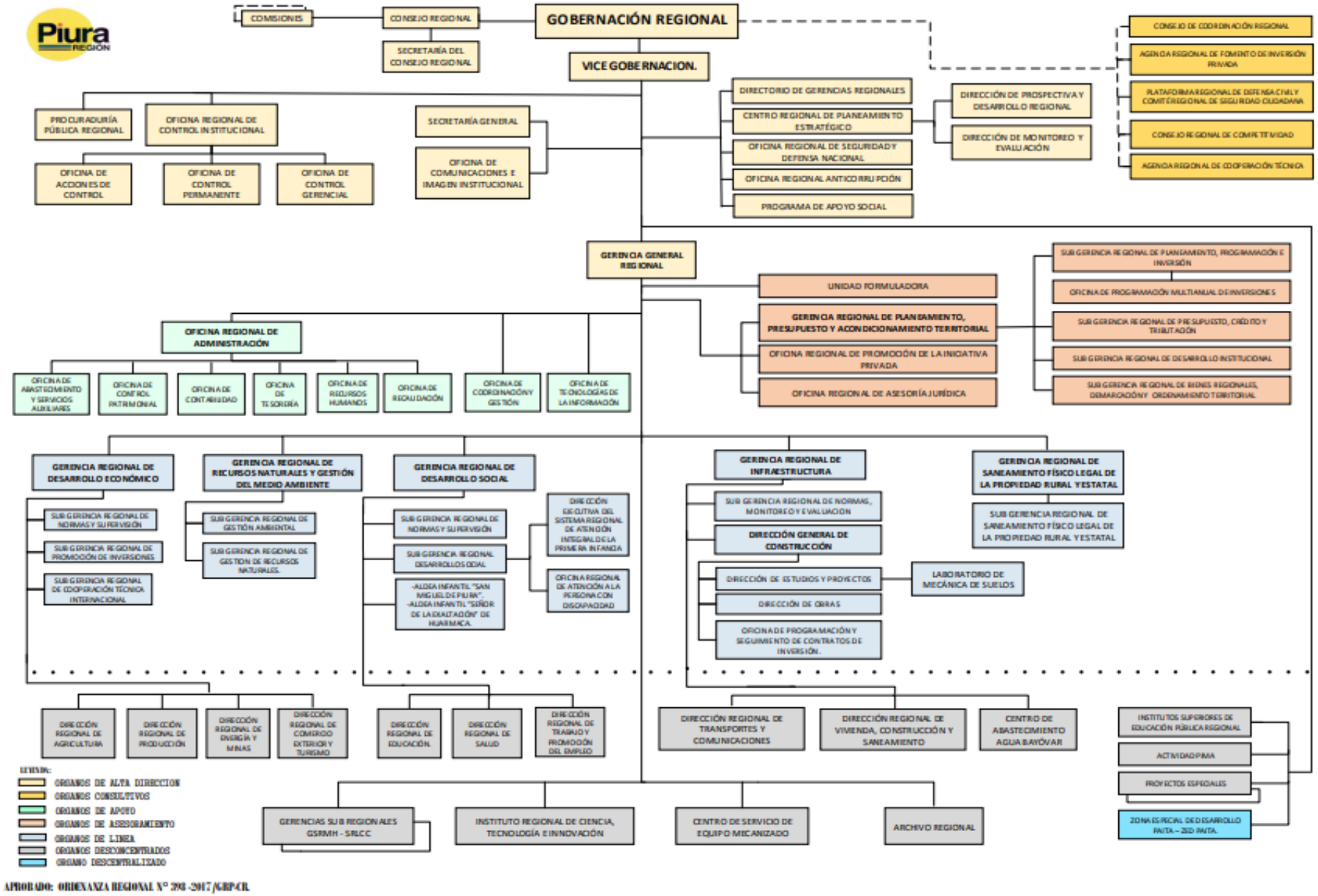


Gráfico Nro. 1: Organigrama del Gobierno Regional Piura

2.2.2. Las tecnologías de la información y comunicaciones

La Tecnología de Información es conjunto de instrumentos para la tecnología que accede a la adquisición, fabricación, almacenamiento, procesamiento, exploración y finalmente para los procesos de información que contiene único propósito de señalización acústica, óptica o electromagnética (12).

Gráfico Nro. 2: El Proceso de la Información

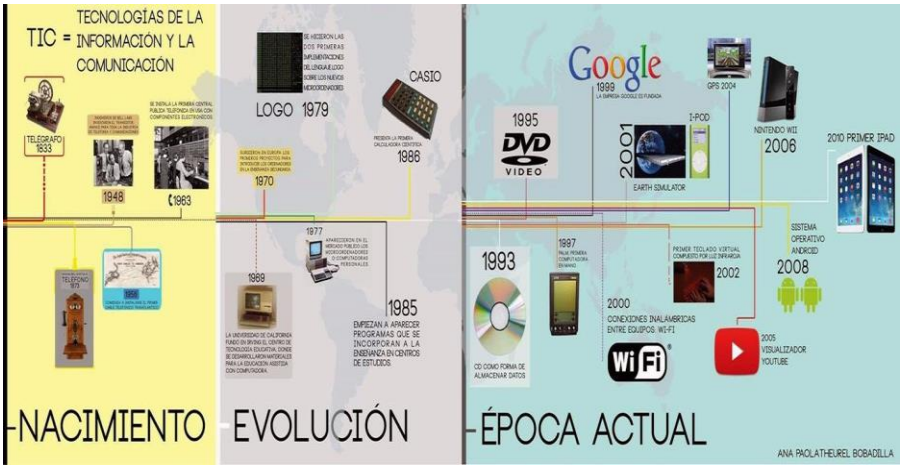
Fuente: TI, Un enfoque interdisciplinario (13).

Evolución de las TIC

Comenzando en los años 70, donde se empezó a desarrollar la era de la digitalización se hizo con los progresos científicos para la electrónica era importante combinar principalmente electrónicos y software, pero también en los años 80, desarrolló una autorización de la electrónica, además con las telecomunicaciones y también las interconexiones entre redes. El cambio evolutivo de la TIC comenzó con el beneficio para la economía nueva que tenga que ver con criterios de éxito en las organizaciones o incluso la sociedad para entrar en las innovaciones tecnológicas y dar una capacidad para aprender a explotarlos para su propio beneficio, ha facilitado esta tecnología están en la preparación de documentos, enviar y recibir correo electrónico y otras funciones

importantes. El punto de similitud entre la revolución de la tecnología es verdaderamente en la revolución industrial, que fue la mayor diferencia en materia prima, es decir, la explosión social basada en la utilización de empresas de energía. Incluidos las áreas, está ciencias como microelectrónica, computación, telecomunicaciones e ingeniería genética (14).

Gráfico Nro. 3: Origen y Evolución de la TIC



Fuente: Sutori (15).

Áreas de herramientas de Aplicación de las TIC

La agenda digital peruana, dijo que el gobierno peruano se enfrenta al desafío de promover el trabajo del gobierno donde la situación tiene una mayor población, además obtiene un bajo nivel socioeconómico que verifica una gama de propuestas en servicios en instituciones bancarias limitadas para realizar un nivel de alfabetización digital en ocasiones especiales en áreas rurales y remotas, con el cálculo precISO ilimitado para tener un que proponer en las TIC por reconociendo en entidades generales y a su vez obtiene un sistema de información, además con la integración en sus sistemas informáticos, que procede a la última integración en áreas de electrónica entre agencias en él estad (16).

2.2.3. Normas Técnicas Peruanas

Es variedad de archivos importantes conformados por individuos legales referentes a reglas establecidas bajo la supervisión de Indecopi, cumpliendo con sus respectivos proyectos establecidos dependiente su fuente de origen (17).

Seguridad de Información

La protección tiene como finalidad la integridad y disponibilidad de los medios de información, para tener un seguro muy efectivo que sea accesible sólo a las personas aceptables, para que ello exija cambios no deseados y que los usuarios sean accedidos cuando precisen (18).

La Organización Internacional de Normalización (ISO) define la seguridad de la información (SI) como:

La preservación de la privacidad, integridad y disponibilidad de información; así como los sistemas involucrados en su tratamiento dentro de una organización. Además, otras propiedades también pueden estar involucradas, tales como: autenticidad, responsabilidad, no repudio y confiabilidad (18).

- Es decir, estos tres términos constituyen la base de la seguridad de la información, de la que se resume la explicación a continuación.

- Privacidad: la información no está disponible o revela individuos, dispositivos.

- Mantenga precisión e integridad de la información.

- Integridad: Mantener integridad y precisión de la información y sus procedimientos. Esto puede ser afectado por hardware o productos de virus de malware.

- Acceso: entrada y uso de un sistema de información por parte de las mismas personas y procesos permitidos cuando lo requieran.

Sistema de Gestión de Seguridad de Información

SGSI tiene capacidad de crear, realizar, manejar, monitorear y mejora la protección de la información que busca para poder identificar el mismo contenido con integridad y disponibilidad, integridad y descarte en la información, minimizando los riesgos de seguridad del ordenador (19).

Gráfico Nro. 4: Ciclo Deming o circulo PDCA

Fuente: SQL Consultores (20).

Análisis y Evaluación de Riesgo

El análisis de riesgos como la elección de los mecanismos de protección, permite estimar la posible pérdida de información y ayuda a reducirla al facilitar su elección. El método para analizar y gestionar los riesgos del sistema de información es el núcleo de las medidas de análisis, evaluación y gestión de riesgos (21).

En 2008, se definieron tres riesgos, como los riesgos estratégicos asociados con la seguridad de la información, que se centran más en los beneficios y la reputación de la organización, teniendo en cuenta la decisión estratégica tomada por la corporación (22).

2.2.4. Vulnerabilidades y Riesgos

Estos términos están interrelacionados, la manifestación de una inseguridad analizada y detectada surge con atentados al informe influyente en un sistema establecido. Esto es lo que para los expertos en cuestiones de seguridad de la información se conoce como la relación de causa y efecto entre los elementos del análisis de riesgo. Por lo tanto, el siguiente paso será integrar estos elementos para analizar y definir los niveles de riesgo que permitirán implementar los procedimientos que ayudarán a mitigar estos riesgos y eliminar las vulnerabilidades (23).

Cálculo de Riesgo

Después de que los activos se enumeran y se clasifican y las amenazas y vulnerabilidades se identifican, se calcula el riesgo. Este cálculo utilizará valores cuantitativos porque el valor de un activo de información se evalúa en el impacto sobre las pérdidas económicas que genera si es violado (23). Se detecta de dos puntos diferentes:

- Análisis cuantitativo. Con base en los valores de métricas y calculando que determinan el cálculo de costo-beneficio.

- Análisis cualitativo ¿Es más flexible, pero el resultado es más subjetivo, no está basado? En número y contiene análisis simples.

Tratamiento de Riesgos

A partir del informe de evaluación de riesgos se procede a examinar cual es el tratamiento más adecuado para cada uno de los riesgos que han sido identificados (23).

Los siguientes lineamientos de la norma ISO 27001:2005, el procedimiento de riesgos incluye los siguientes enfoques:

Para definir los controles que se realizarán según el análisis de riesgo, se deben realizar los siguientes pasos:

- Prepare un Documento de Declaración de Aplicabilidad (DDA) donde la lista de controles que se va a implementar es detallada.

- Determine el nivel de inseguridad que es accesible para la empresa.

- Obtenga la aprobación de la dirección de la DDA y los riesgos que no están cubiertos.

- Formular un plan de tratamiento de riesgos cuando sea necesario para reducir los riesgos a un nivel aceptable y realizar los controles considerados necesarios de acuerdo con los requisitos de las acciones de ISO / IEC 27001: 2005 en 4.2.1. f, g y h.

- Preparar los procedimientos con la necesidad de realizar controles.

Control

Los controles se enfocan en manejar el riesgo y además incluyendo políticas, estructuras organizacionales (18).
En estas se clasificaciones en:

- Preventivos: Reducir las vulnerabilidades.

- Detectivos: Detectan amenazas o escenarios antes de permitir que se activen otros controles.

- Correctivos: contrarrestar el efecto del acontecimiento de un riesgo.

- Persuasivos: reducir el riesgo o amenazas.

2.2.5. Norma ISO/IEC 27000

Norma ISO

Según el International Organization for Standardization nos proporciona las siguientes definiciones (24):

¿Qué es ISO?

ISO (Organización Internacional de Normalización) es una organización no gubernamental, independiente, cuyos 163 miembros son los organismos nacionales de normalización. A través de sus miembros, la organización reúne a expertos que ponen sus conocimientos conjuntamente para desarrollar estándares internacionales, apoyo a la innovación relevante para el mercado, basado en el consenso voluntario y que ofrecen soluciones a los problemas mundiales.

¿Qué es un estándar?

Una norma es un documento que proporciona requisitos, especificaciones, directrices o características que pueden ser utilizadas consistentemente para asegurar que los materiales, productos, procesos y servicios son adecuados para su propósito. Hemos publicado más de 19 500 Normas Internacionales que se pueden comprar en la tienda de la ISO o de nuestros miembros.

Beneficios de las Normas Internacionales

Normas Internacionales de traer beneficios tecnológicos, económicos y sociales. Ayudan a armonizar las especificaciones técnicas de los productos y servicios que hacen la industria más eficiente y rompiendo las barreras al comercio internacional. Conformidad con las Normas Internacionales de ayuda a tranquilizar a los consumidores que los productos sean seguros, eficientes y bueno para el medio ambiente.

La Organización Internacional de Normalización (ISO) define el SGSI como un enfoque sistemático para gestionar la información confidencial en la empresa, para garantizar su seguridad. Abarca personas, procesos y sistemas de TI a través de la aplicación de un proceso de gestión de riesgos. Puede ayudar a pequeñas, medianas y grandes empresas en todas las industrias a mantener la información segura (25).

Tipos de Serie de Normas ISO/IEC 27000

ISO / IEC 27000: es una familia de estándares destinados a ayudar a las organizaciones a mantener sus tareas seguras. Su aplicación hace posible manejar la seguridad de los activos, como información financiera, propiedad intelectual, detalles de empleados o información de terceros (25).

ISO/IEC 27001: ISO / IEC 27001: es un marco internacional reconocido para las mejores prácticas para un sistema de gestión de seguridad de la información. Le ayuda a identificar los riesgos con su información importante e inserta controles apropiados para ayudarlo a reducir el riesgo.

ISO/IEC 27002: ISO / IEC 27001: es un marco internacional reconocido para las mejores prácticas para un sistema de gestión de seguridad de la información. Le ayuda a identificar los riesgos con su información importante e inserta controles apropiados para ayudarlo a reducir el riesgo.

ISO / IEC 27003: determinado en una guía para la implementación del SGSI e información sobre el uso del modelo PDCA y los requisitos de sus diferentes fases.

ISO / IEC 27004: esta norma específica cómo medir el sistema de medición, qué parámetros medir, cuándo y cómo medirlos. Además, ayuda a las empresas a determinar los objetivos relacionados con los criterios de rendimiento y éxito.

ISO / IEC 27005: la norma internacional que trata la gestión de riesgos de seguridad de la información. La norma proporciona pautas para gestionar los riesgos de seguridad de la información en una empresa, en particular para cumplir con los requisitos del sistema de gestión de seguridad de la información tal como se define en la norma ISO 27001.

ISO / IEC 27006: esta norma se complementa con ISO / IEC 17021 y proporciona los requisitos de certificación necesarios para una organización que certifica SGSI de acuerdo con ISO / IEC 27001.

ISO / IEC 27007: es el estándar más conocido en la familia que requiere un sistema de gestión de seguridad de la información (SGSI). Es una norma internacional para la cual una organización puede ser certificada, incluso si la certificación es voluntaria.

ISO / CEI TR 27008: proporciona orientación sobre la auditoría de la implementación y operación de los controles, incluida la verificación del cumplimiento técnico de los controles del sistema de información, de acuerdo con las normas de seguridad establecidas por una organización.

ISO / IEC 27010: esta norma proporciona controles y directrices que están específicamente relacionados con el inicio, la implementación, el mantenimiento y la mejora de la seguridad de la información en las comunicaciones entre organizaciones y sectores.

ISO / IEC 27011: Consiste en una guía de administración de seguridad de la información específica para las telecomunicaciones.

ISO / IEC 27013: se enfoca solo en la implementación integrada de un SGSI según ISO / IEC 27001 y un sistema de gestión de servicios (SMS) ISO / IEC 20000-1.

ISO / IEC 27014: proporciona orientación sobre conceptos y principios para controlar la seguridad de la información a través de los cuales las organizaciones pueden evaluar, monitorear y comunicar dentro de la organización.

ISO / IEC TR 27015: proporciona una guía de seguridad para la información adicional y las disposiciones de seguridad de ISO / IEC 27002: 2005 Información para iniciar, implementar, y prosperar lo fundamental en organizaciones que brindan servicios financieros.

ISO/IEC TR 27016: Proporciona orientación sobre cómo una organización puede tomar decisiones para proteger la información y comprender las consecuencias financieras de estas decisiones en relación con los requisitos de recursos en competencia.

ISO / IEC 27799: 2008: proporciona pautas para los estándares de seguridad de la información para la organización y los métodos de gestión de la seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo para la seguridad de la información de la organización.

2.2.6. Beneficios de ISO 27001

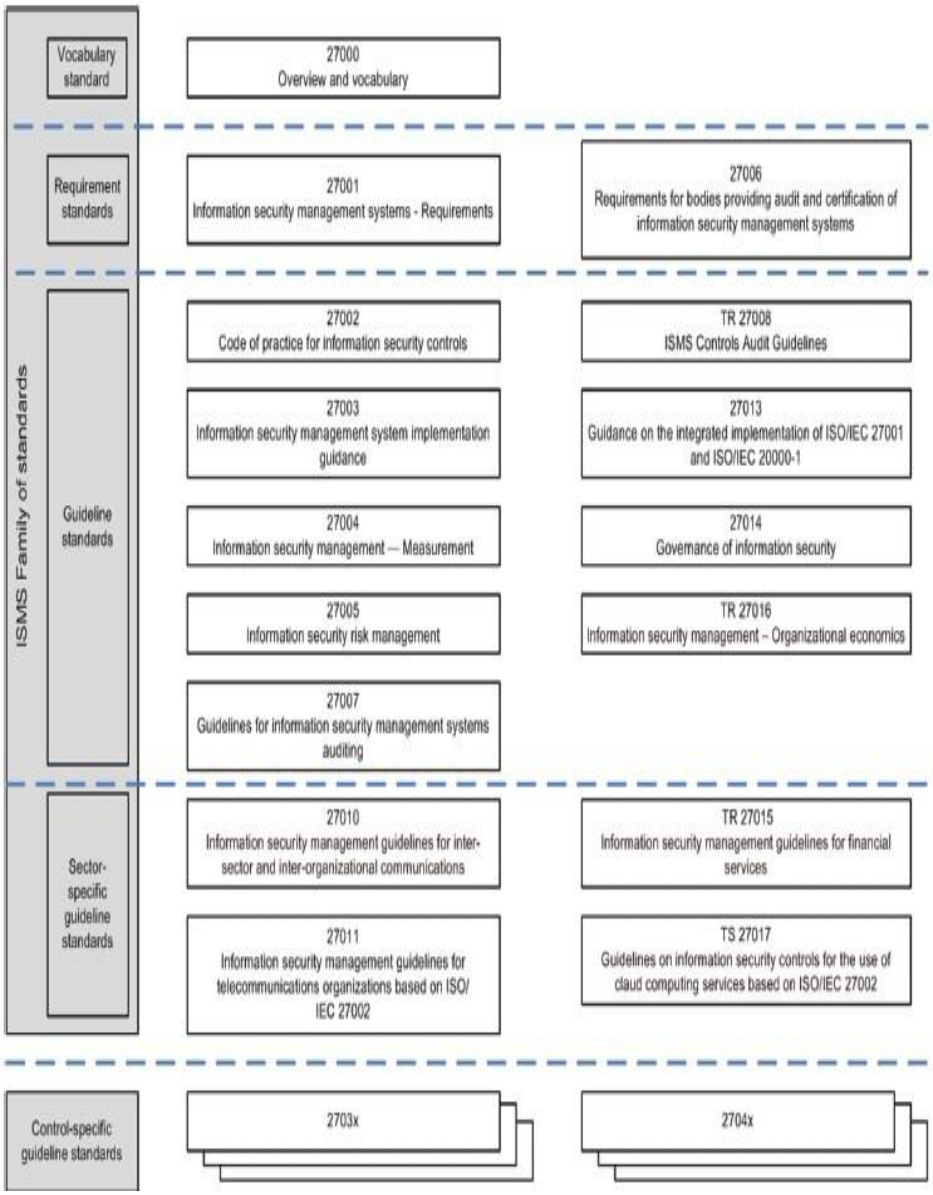
Para 27001 Academy especialistas en brindar asesoramiento mencionan 4 ventajas comerciales fundamentales que una empresa puede obtener con la implementación de esta norma para la seguridad de la información:

- Cumplir con los requerimientos legales.
- Obtener una ventaja comercial.

- Menores costos.
- Una mejor organización.

La seguridad de la información es parte de la gestión global del riesgo en una empresa (25), en el siguiente grafico observamos que áreas interviene:

Gráfico Nro. 5: Relaciones de la familia de estándares ISMS



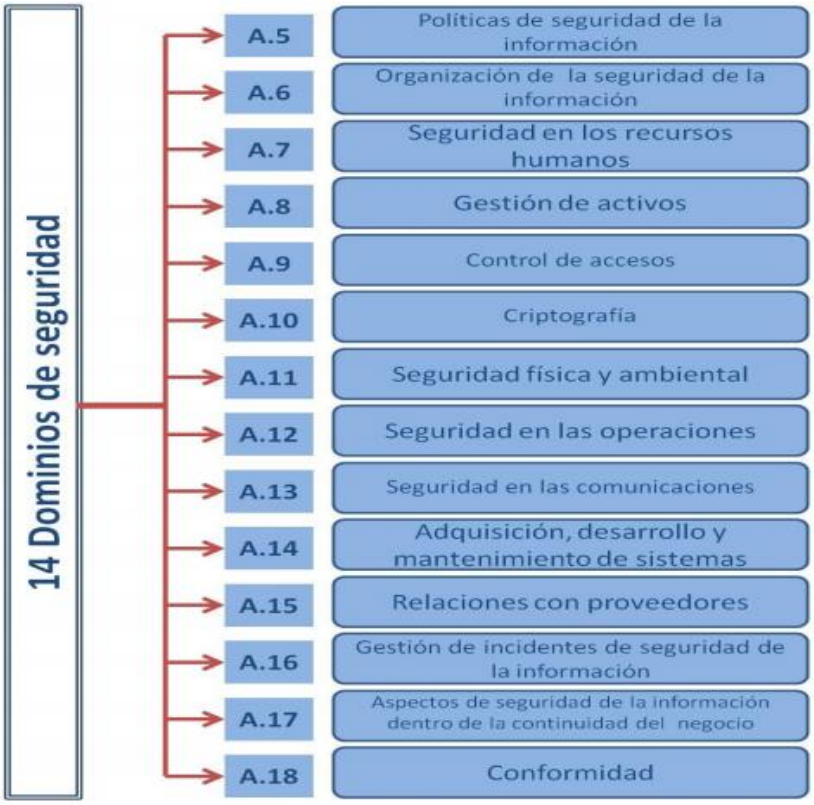
Fuente: ISO/IEC 27000:2014 (19).

2.2.7. Ley de Información de gestión de datos técnicos 27001

La Ley Técnica Peruana reemplaza a la norma ISO 27001:2008 verificada en el año 2013 como después a sumiria la norma ISO 27001:2013 y además la ISO 27001:2013/COR (26).

El uso obligatorio de la norma ISO 27001:2014 ha sido aprobado en la fecha 14 de enero del 2016. Técnicos de Seguridad, Tecnologías de la Información (27).

Gráfico Nro. 6: El nuevo enfoque de la ISO/IEC 27001: 2013



Fuente: ISACA MADRID CHAPTER (28).

Ventajas del ISMS

Las SGSI son importantes para permitir que tener un plan de negocios destinado a controlar el control de las dificultades en las acciones de negocios y también preservar los métodos graves de Todas las empresas asociadas a fallas importantes en sistemas de formación de desastres (28).

Casos del éxito

En 2014 llevó a cabo la investigación sobre "Análisis de la norma ISO / IEC 27001 en el diseño e implementación de la red corporativa" de la Universidad Católica de Santiago de Guayaquil, que tiene una seguridad en la aplicación del análisis de la norma ISO / IEC 27001 equipos tener una formación en una empresa o una organización. En el estudio de seguridad de datos, la caracterización general de la Ley ISO 27000 se lleva a cabo para desarrollar a fondo ISO 27001, que es responsable de las tecnologías de seguridad, en última instancia, los requisitos importantes. El plan de seguridad de TI de la compañía está en análisis de riesgo. Este estudio se basa en determinar si la seguridad de la empresa cumple con los parámetros establecidos, lo que permite la mejora y la obtención de la certificación (29).

2.2.8. Metodologías de gestión de riesgos

Hoy en día las empresas sufren de riesgos informáticos que afecta su funcionamiento, una forma de prevenir estos riesgos es realizando una evaluación de riesgos informáticos. Esta evaluación se puede llevar acabo aplicando algunas de las siguientes metodologías:

MAGERIT

El método MAGERIT, son las siglas de Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de la Administraciones, dicho método cubre la fase AGR (Análisis y Gestión de Riesgos). Si hablamos de Gestión global

de la Seguridad de un Sistema de Seguridad de la Información basado en ISO 27001, MAGERIT, es el núcleo de toda actuación organizada en dicha materia, ya que influye en todas las fases que sean de tipo estratégico y se condiciona la profundidad de las fases de tipo logístico. El Consejo Superior de Informática ha sido el encargado de elaborar la primera versión de MAGERIT, con lo que promueve su utilización como respuesta a la dependencia creciente de toda la sociedad respecto a las Tecnologías de la Información. MAGERIT se encuentra muy relacionada con la generación en la que se utilizan los medios electrónicos, informáticos y telemáticos, lo que genera grandes beneficios para los empleados y los ciudadanos, aunque también puede dar lugar a diferentes riesgos que se tienen que minimizar con medidas de seguridad que generan confianza (30).

OCTAVE

Giménez (31), nos da a conocer sobre Octave que significa Operationally Critical Threat, Asset and Vulnerability Evaluation. El método está desarrollado por la universidad de Canegie Mellon, y define un conjunto de criterios, para poder emplear métodos más flexibles según la empresa. Existen tres métodos muy comunes que cumplen esos criterios de compatibilidad: El método de Octave original, el Octaves-s para pequeñas empresas, y el Octave-Allegro, especialmente centrado en los activos de información.

Los criterios son bastantes generales, e incluyen; que las medidas sean adaptables a las necesidades, que el proceso de análisis esté definido, sea continuo y tenga visión de futuro, y que el proceso se centre en un conjunto reducido de riesgos críticos.

Los resultados se dividen en diferentes fases: fase organizativa (activos críticos y sus requerimientos, amenazas, y prácticas de seguridad habituales), una fase tecnológica (componentes clave y vulnerabilidades), es una tercera y última fase estratégico, o de desarrollo del plan de riesgo.

CRAMM

Es el método de análisis y control de riesgos del Gobierno Británico (CCTA Risk Analysis and Management Method). CRAMM es un método estructurado y coherente para la identificación y la evaluación de riesgos en redes y sistemas de información. Abarca escenarios técnicos y no técnicos (por ejemplos, aspectos físicos de la seguridad de la tecnología de la información) y proporciona un método riguroso por etapas que permite programar adecuadamente las revisiones. Hay herramientas de software disponibles para CRAMM. La última versión es CRAMM Versión 5 de enero de 2013 (32).

Es una metodología de la Agencia Central de Cómputo y Telecomunicaciones del Reino Unido, que data de los años 80. El modelo es muy similar al visto (31):

- Una fase de análisis en la se estudian los activos, las vulnerabilidades, y las amenazas para generar unos riesgos.
- Una fase de gestión, que incluye unas contramedidas, una implantación, y por último una fase de auditoría.

III. HIPÓTESIS

La propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, minimizará la pérdida de información.

IV. METODOLOGÍA

4.1. Diseño de la Investigación

4.1.1. Tipo

El tipo de la presente investigación fue determinada como investigación cuantitativa. Según Daniel C. (35) ,la Investigación Cuantitativa, en cambio, es aquella que utiliza preferentemente información cuantitativa o cuantificable. Algunos ejemplos de investigaciones cuantitativas son: diseños experimentales, diseños cuasi – experimentales, investigaciones basadas en la encuesta social.

Según Barragán (36), la investigación cuantitativa es perteneciente o relativo a la cantidad, y de su análisis se determina las porciones de cada elemento analizado.

4.1.2. Nivel

Verificando las características de este proyecto en investigación se define de nivel descriptivo. Según Namakforoosh M. (33), la investigación descriptiva busca observar y describir el comportamiento del sujeto de estudio sin influir sobre él de modo alguno. Su objetivo es calcular la proporción de gente de una población específica que posee ciertas características. Una investigación descriptiva es simple cuando se considera una variable.

El nivel es descriptivo, para Naghi (34), la investigación descriptiva es una forma de estudio para saber quién, donde, cuándo, cómo y porqué del sujeto del estudio. En otras palabras, la información obtenida en un estudio descriptivo, explica perfectamente a una organización el consumidor, objetos, conceptos y cuentas.

4.1.3. Diseño de la Investigación

EL diseño de la investigación es no experimental y por la característica de la su ejecución es de corte transversal.

Hernández R., Fernández C. y Baptista P. (37), afirmaron que la investigación no experimental es la investigación que se realiza sin manipular intencionalmente las variables a fin de ver el efecto que pueden producir en otras variables. En la investigación no experimental solo se observa un fenómeno para su posterior análisis. La presente investigación cumple esta característica, debido a que no hay manipulación alguna de la variable, y tampoco se busca hacer algún cambio al fenómeno estudiado durante la investigación.

Es corte transversal porque se analizan las variables en un periodo de tiempo determinado, según en una edición de investigación de la Universidad de Michigan (38), el corte Trasversal ya que el estudio se circunscribe a un momento puntual, recolectando dato en un tiempo único, describiendo variables y analizando su incidencia.

4.2. Población y muestra

Para la presente investigación la población se delimito a 23 trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura.

Muestra

Para la presente investigación, la muestra se seleccionó a 23 trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura, no se utilizó ninguna técnica estadística por ser los involucrados directos en la seguridad de información.

Hernández R, Fernández C y Baptista P. (37), definieron a la muestra como un subgrupo de la población. Un subconjunto de elementos dentro de un conjunto que posee características similares, a la cual se le considera la población. Adicionalmente, estos autores mencionaron que cuando en el caso se incluye todos los elementos del universo o población, se le denomina censo.

4.3. Definición y Operacionalización de variables e Indicadores

Tabla Nro. 5: Matriz de Operacionalización de Variables

Variable	Definición Conceptual	Dimensiones	Indicadores	Definición Operacional
Propuesta de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001	Es una familia de estándares destinados a ayudar a las organizaciones a mantener sus tareas seguras. Su aplicación hace posible manejar la seguridad de los activos, como información financiera, propiedad intelectual, detalles de empleados o información de terceros (25).	− Satisfacción de la situación actual.	− Confiabilidad en la información − Satisfacción del actual servicio.	Documento que consiste en una propuesta para contar con lista de verificación y directivas basado en normas para asegurar la Seguridad de la Información
		− Necesidad de seguridad de la Información.	− Uso de la norma ISO 27001 − Necesidad de seguridad de la información − Conformidad con la seguridad	

Fuente: Elaboración propia.

4.4. Técnicas e Instrumentos de recolección de datos

En la presente investigación se utilizo la encuesta como técnica y el cuestionario como instrumento de tipo cerrado dicotómico, que quiere decir solo de dos opciones; si o no.

La técnica que se maneja es la encuesta.

Encuesta: Es el conjunto de preguntas especialmente diseñadas y pensadas para ser dirigidas a una muestra de población, que se considera por determinadas circunstancias funcionales al trabajo, representativa de esa población, con el objetivo de conocer la opinión de la gente sobre determinadas cuestiones corrientes y porque no también para medir la temperatura de la gente acerca de algún hecho específico que se sucede en una comunidad determinada y que despierta especial atención entre la opinión pública y que capaz requiere de la realización de una encuesta para conocer más a fondo cuál es la sensación de la gente (39)**.**

El instrumento que se utiliza es el cuestionario

Cuestionario: Es un procedimiento considerado clásico en las ciencias sociales para la obtención y registro de datos. Su versatilidad permite utilizarlo como instrumento de investigación y como instrumento de evaluación de personas, procesos y programas de formación. Es una técnica de evaluación que puede abarcar aspectos cuantitativos y cualitativos. Su característica singular radica en que, para registrar la información solicitada a los mismos sujetos, ésta tiene lugar de una forma menos profunda e impersonal, que el "cara a cara" de la entrevista. Al mismo tiempo, permite consultar a una población amplia de una manera rápida y económica (40)**.**

4.5. Plan de análisis

La información recopilada es procesada, tabulada y presentada por medio de estadísticas, para las cuales se elaboran tablas y gráficos de distribución estadística definida. Para facilitar el procesamiento de los datos, se utilizó Excel, que clasifico sistemáticamente la información. De acuerdo con los resultados encontrados en las tablas de distribución de frecuencia, en los gráficos estadísticos utilizados y en la confianza de los indicadores estadísticos; los resultados son analizados de acuerdo con el comportamiento de las variables en relación a los elementos de estudio, detallando las figuras o resultados más importantes de las informaciones correspondientes.

4.6. Matriz de consistencia

Tabla Nro. 6: Matriz de Consistencia

<table>
<tr><th>Problema</th><th>Objetivo general</th><th>Hipótesis</th><th>Metodología</th></tr>
<tr><td rowspan="3">¿De qué manera la propuesta de un Sistema de Gestión de Seguridad de la Información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, minimiza la pérdida de información?</td><td>Realizar una propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, para minimizar la pérdida de información.</td><td rowspan="3">La propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, minimizará la pérdida de información.</td><td rowspan="3">Tipo: Cuantitativa
Nivel: Descriptiva
Diseño: No experimental y de corte transversal</td></tr>
<tr><td>Objetivos específicos</td></tr>
<tr><td>1. Analizar la seguridad actual de la información, en la oficina de tecnologías de información del Gobierno Regional Piura.
2. Evaluar los marcos de referencias que ayuden a mejorar la seguridad de la información en la oficina de</td></tr>
</table>

	tecnologías de información del Gobierno Regional Piura. 3. Proponer la aplicación de la Norma ISO / IEC 27001, para mejorar la seguridad de la información.		

Fuente: Elaboración propia.

4.7. Principios éticos

Durante el desarrollo del presente trabajo de investigación denominado "Propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020" se ha considerado el código de ética para la investigación versión 002, el cual tiene por finalidad establecer los principios y valores éticos que guíen las buenas prácticas y conducta responsable de los estudiantes, graduados, docentes, formas de colaboración docente, y no docentes, en la Universidad, que se canaliza a través del Comité Institucional de Ética en Investigación (CIEI).

También se ha respetado los derechos de autor y propiedad intelectual de las diferentes piezas literarias que se ha citado, reproduciendo fielmente sus contenidos para brindar un macro teórico basto para la presente investigación

Siguiendo el código de ética se ha respetado completamente las respuestas y opiniones brindadas por los trabajadores del la empresa GOBIERNO REGIONAL PIURA, para crear un análisis e interpretación honesta de la realidad actual de los procesos de la empresa. Así mismo se ha mantenido anónima la identidad de los colaboradores para obtener respuestas objetivas.

La investigación cuenta la manifestación de voluntad, informada, libre, inequívoca y específica; mediante la cual las personas como sujetos investigados o titular de los datos consiente el uso de la información para los fines específicos establecidos en el proyecto.

V. RESULTADOS

5.1. Resultados

Dimensión 01: Nivel de satisfacción de la situación actual

Tabla Nro. 7: Datos seguros

Distribución de frecuencias y respuestas relacionadas con los datos registrados en el sistema actual; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	3	13
No	20	87
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Cree Usted que los datos registrados en el sistema actual son seguros?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 7 se puede observar que el 87% de los trabajadores encuestados expresaron que NO son seguros los datos registrados, mientras que el 13% de los encuestados indicó que sí.

Tabla Nro. 8: Información de usuarios

Distribución de frecuencias y respuestas relacionadas con políticas y procedimientos para seguridad; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	1	4
No	22	96
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Existen políticas y procedimientos para asegurar que se proporciona seguridad en la información de sus usuarios?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 8 se puede observar que el 96% de los trabajadores encuestados expresaron que NO existen políticas ni procedimientos para la seguridad, mientras que el 4% de los encuestados indicó que sí.

Tabla Nro. 9: Desechar información

Distribución de frecuencias y respuestas relacionadas con desechar la información que ya no necesita; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	2	9
No	21	91
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Usted desecha la información que ya no necesita?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 9 se puede observar que el 91% de los trabajadores encuestados expresaron que NO desechan la información que ya no necesitan, mientras que el 9% de los encuestados indicó que sí.

Tabla Nro. 10: Copias de seguridad

Distribución de frecuencias y respuestas relacionadas con realizar copias de seguridad; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	-	-
No	23	100
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Se realizan copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 10 se puede observar que el 100% de los trabajadores encuestados expresaron que NO realizan copias de seguridad en su información.

Tabla Nro. 11: Documentación visible

Distribución de frecuencias y respuestas relacionadas con dejar documentación visible en escritorio; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	3	13
No	20	87
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Cuándo no se encuentra en su oficina deja documentación visible en su escritorio?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 11 se puede observar que el 87% de los trabajadores encuestados expresaron que NO dejan documentación visible en su escritorio durante su ausencia, mientras que el 13% de los encuestados indicó que sí.

Tabla Nro. 12: Clave de acceso

Distribución de frecuencias y respuestas relacionadas con la clave de acceso para los equipos de cómputo; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	1	4
No	22	96
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿La clave de acceso es la misma para ingresar a todos los equipos de cómputo?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 12 se puede observar que el 96% de los trabajadores encuestados expresaron que NO es la misma clave de acceso para ingresar a los equipos de cómputo, mientras que el 4% de los encuestados indicó que sí.

Tabla Nro. 13: Estado de antivirus

Distribución de frecuencias y respuestas relacionadas con el estado del antivirus; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	3	13
No	20	87
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Usted ha detectado que el antivirus del Gobierno Regional Piura funciona y se encuentra actualizado?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 13 se puede observar que el 87% de los trabajadores encuestados expresaron que NO han detectado su actualización del antivirus, mientras que el 13% de los encuestados indicó que sí.

Tabla Nro. 14: Existencia de alarma

Distribución de frecuencias y respuestas relacionadas con existencia de algún tipo de alarmas; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	1	4
No	22	96
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Existe alguna alarma contra incendios, robos u otros?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 14 se puede observar que el 96% de los trabajadores encuestados expresaron que NO existe ninguna alarma en la oficina, mientras que el 4% de los encuestados indicó que sí.

Tabla Nro. 15: Plan de contingencia

Distribución de frecuencias y respuestas relacionadas con tener algún plan de contingencia; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	3	13
No	20	87
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿El Gobierno cuenta con algún plan de contingencia para dar solución a algún incidente tanto interno o ajeno de la organización?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 15 se puede observar que el 87% de los trabajadores encuestados expresaron que NO cuentan con algún plan de contingencia para incendios u otros incidentes, mientras que el 13% de los encuestados indicó que sí.

Tabla Nro. 16: Ingerir alimentos cerca de una computadora

Distribución de frecuencias y respuestas relacionadas con ingerir alimentos cerca a cualquier computadora; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	1	4
No	22	96
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Usted ha observado que alguno de sus compañeros a ingerido alguna bebida o alimentos cuando realiza su trabajo en cualquiera de las computadoras del Gobierno Regional?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 16 se puede observar que el 96% de los trabajadores encuestados expresaron que NO han observado a sus compañeros ingerir alimentos o bebidas cerca a una computadora, mientras que el 4% de los encuestados indicó que sí.

Dimensión 02: Necesidad de la seguridad de información

Tabla Nro. 17: Seguridad de Información

Distribución de frecuencias y respuestas relacionadas con tener conocimientos de seguridad de información; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	22	96
No	1	4
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Conoce el tema seguridad de información?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 17 se puede observar que el 96% de los trabajadores encuestados expresaron que, SI tienen conocimientos sobre el tema de seguridad de información, mientras que el 4% de los encuestados indicó que no.

Tabla Nro. 18: Controles de seguridad

Distribución de frecuencias y respuestas relacionadas con aplicar controles de seguridad para evitar pérdidas; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	N	%
Si	23	100
No	-	-
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Cree que es necesario aplicar controles de seguridad para evitar pérdida o daño de información importante para el Gobierno Regional?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 18 se puede observar que el 100% de los trabajadores encuestados expresaron que, SI creen que es necesario aplicar controles de seguridad para evitar pérdidas o daños de información.

Tabla Nro. 19: Responsable de oficina de TIC

Distribución de frecuencias y respuestas relacionadas con responsable de área de la seguridad de información; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	N	%
Si	23	100
No	-	-
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Existe en el Gobierno Regional un responsable del área de la seguridad de información?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 19 se puede observar que el 100% de los trabajadores encuestados expresaron que, SI existe un responsable del área de la seguridad de información.

Tabla Nro. 20: Incidente ocurrido

Distribución de frecuencias y respuestas relacionadas con ocurrir algún incidente de seguridad; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	22	96
No	1	4
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Ha ocurrido algún incidente de seguridad en su puesto de trabajo en el último año?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 20 se puede observar que el 96% de los trabajadores encuestados expresaron que, SI ha ocurrido incidentes de seguridad en su puesto de trabajo, mientras que el 4% de los encuestados indicó que no.

Tabla Nro. 21: Importancia a la seguridad

Distribución de frecuencias y respuestas relacionadas con dar importancia al tema de seguridad; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	21	91
No	2	9
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Considera que el Gobierno Regional le da importancia al tema de seguridad?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 21 se puede observar que el 91% de los trabajadores encuestados expresaron que, SI consideran que el Gobierno Regional debe darle importancia al tema de seguridad, mientras que el 9% de los encuestados indicó que no.

Tabla Nro. 22: Seguridad de Información vital

Distribución de frecuencias y respuestas relacionadas con seguridad de información vital; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	23	100
No	-	-
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Considera que la seguridad de información debe ser vital en el Gobierno Regional?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 22 se puede observar que el 100% de los trabajadores encuestados expresaron que, SI consideran seguridad de información vital en el Gobierno Regional.

Tabla Nro. 23: Protocolos de seguridad

Distribución de frecuencias y respuestas relacionadas con seguir con protocolos de seguridad; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	22	96
No	1	4
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Usted como trabajador tiene la cultura de seguir con protocolos de seguridad?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 23 se puede observar que el 96% de los trabajadores encuestados expresaron que, SI tienen la cultura de seguir con protocolos de seguridad, mientras que el 4% de los encuestados indicó que no.

Tabla Nro. 24: Norma ISO 27001

Distribución de frecuencias y respuestas relacionadas con tener conocimientos sobre la norma ISO 27001; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	20	87
No	3	13
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Conoce Usted sobre la norma ISO 27001 en la seguridad de información?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 24 se puede observar que el 87% de los trabajadores encuestados expresaron que, SI tienen conocimientos sobre la norma ISO 27001 en la seguridad de información, mientras que el 13% de los encuestados indicó que no.

Tabla Nro. 25: Capacitaciones de seguridad

Distribución de frecuencias y respuestas relacionadas con impartir capacitaciones de seguridad; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	21	91
No	2	9
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿El Gobierno Regional imparte constantemente capacitaciones de seguridad?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 25 se puede observar que el 91% de los trabajadores encuestados expresaron que, SI imparte constantemente capacitaciones de seguridad el Gobierno Regional, mientras que el 9% de los encuestados indicó que no.

Tabla Nro. 26: Capacitación sobre norma ISO 27001

Distribución de frecuencias y respuestas relacionadas con recibir capacitaciones basado en la norma ISO 27001; respecto a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

Alternativas	n	%
Si	23	100
No	-	-
Total	23	100

Fuente: Origen del instrumento aplicado a los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura; 2020; para responder a la pregunta: ¿Desea recibir capacitaciones sobre la seguridad de información y la norma ISO 27001?

Aplicado por: García, R.; 2020.

En la Tabla Nro. 26 se puede observar que el 100% de los trabajadores encuestados expresaron que, SI desean recibir capacitaciones sobre la seguridad de información y la norma ISO 27001.

RESUMEN GENERAL

Tabla Nro. 27: Resumen General por Dimensiones

Niveles de satisfacción de los trabajadores, respecto a la propuesta establecida basado a la problemática detectada para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.

DIMENSIONES	ALTERNATIVAS DE RESPUESTAS				TOTAL MUESTRA	
	SI	%	NO	%	n	%
Satisfacción de la situación actual	2	9	21	91	23	100
Necesidad de la seguridad de la información	23	100	--	--	23	100

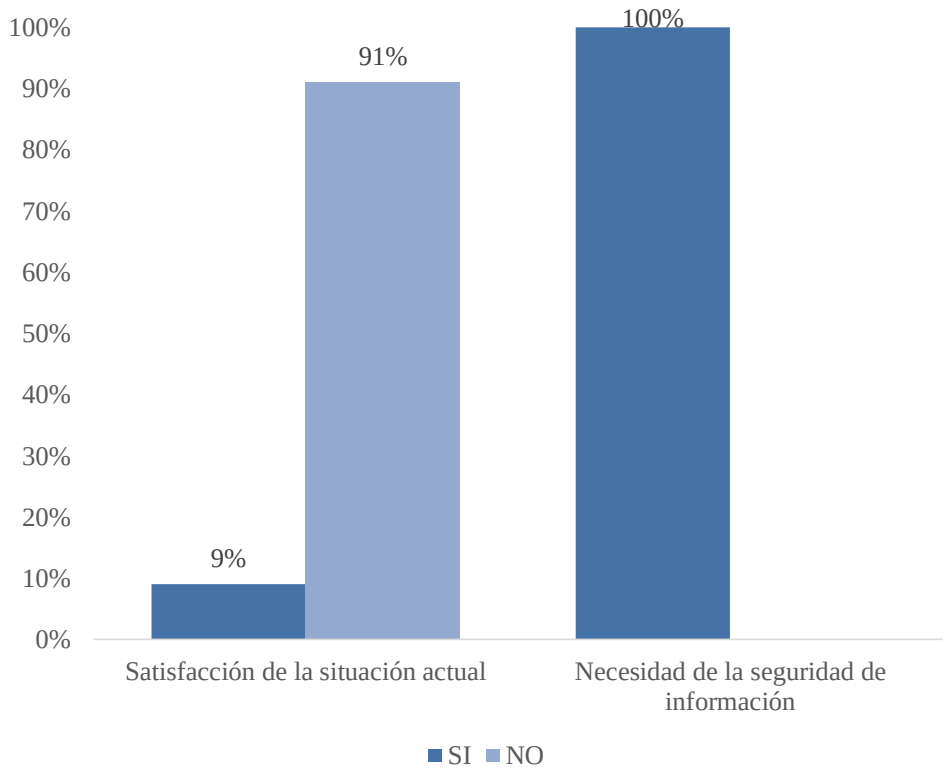
Fuente: Desarrollo del cuestionario para obtener entendimiento por parte de los trabajadores encuestados acerca de la satisfacción y la necesidad de un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de información de Gobierno Regional Piura; 2020.

Aplicado por: García, R.; 2020.

En la Tabla Nro. 27 se puede observar que en la primera dimensión NO están satisfechos con la situación actual y en la segunda dimensión SI necesitan un sistema de gestión de seguridad de la información basado en la norma ISO 27001 para la oficina de tecnologías de información de Gobierno Regional Piura; 2020.

Gráfico Nro. 7: Resumen general de dimensiones

Niveles de satisfacción de los trabajadores, respecto a la propuesta establecida basado a la problemática detectada para la oficina de tecnologías de información del Gobierno Regional Piura; 2020.



Fuente: Tabla Nro. 27.

5.2. Análisis de resultados

Posteriormente de indicar desarrollar el instrumento en los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura, se realiza el análisis de los datos obtenidos como resultado.

1. En la primera dimensión: Satisfacción de la Situación Actual de seguridad de información en la Tabla Nro. 27 podemos visualizar que el 91.00% de los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura, manifestaron que la situación actual NO brinda seguridad de la información que maneja cada trabajador, como consecuencia se concluyó la alternativa de un sistema de gestión de seguridad de información basado en la norma ISO 27001, por lo tanto, el 9.00% de los encuestados expresó que SI. Este producto obtenido tiene similitud con los logrados en el informe de investigación de Vegas (9), y en el informe de investigación de Lara (10), manifestando su contenido en sus informes y para una dimensión semejante determinan que manifiestan insatisfacción por parte de los trabajadores en su satisfacción actual. Esta similitud se evidencia con el análisis respectivo en las organizaciones investigadas se propone un sistema de gestión de seguridad de la información basado en la Norma ISO 27001.

2. Respectivamente en la segunda dimensión: Necesidad de la seguridad de información, en la Tabla Nro. 27 se verifica el resultado que el 100% de los trabajadores de la oficina de tecnologías de información del Gobierno Regional Piura, manifestaron que SI requieren la propuesta sobre un sistema de gestión de seguridad de información basado en la norma ISO 27001. Este resultado de esta dimensión tiene similitud con los logrados en el informe de investigación de Vegas (9), y en el informe de investigación de Lara (10), quienes en sus investigaciones y para una dimensión similar concluyeron un alto nivel de necesidad de implementación de un sistema de gestión de seguridad de información.

5.3. Propuesta de Mejora

Después de realizar el análisis de los datos extraidos por medio de las dos dimensiones: Satisfacción de la situación actual y la necesidad de la seguridad de información. Se propone la aplicación de la norma ISO / IEC 27001, el mismo que permitirá mejora los siguientes procesos:

- Establecer políticas de seguridad, con respecto a la adquisición, distribución y uso de las TI en la oficina de tecnologías de información del Gobierno Regional Piura.
- Que la Alta gerencia, muestre compromiso con las innovaciones tecnológicas que soportan los procesos de la oficina de tecnologías de información del Gobierno Regional Piura.
- Determinar procesos que aseguren la Seguridad de la información en la oficina de tecnologías de información del Gobierno Regional Piura.
- Establecer procedimientos que aseguren la confidencialidad de la información en la oficina de tecnologías de información del Gobierno Regional Piura.
- Establecer políticas que aseguren la factibilidad y protección de brindar información a terceros.
- Definir procesos documentados para el registro de inventarios de activos de TI en la oficina de tecnologías de información del Gobierno Regional Piura.
- Realizar el registro automatizado de la asignación de responsables de activos en la oficina de tecnologías de información del Gobierno Regional Piura.
- Determinar los roles y responsabilidades del personal en la oficina de tecnologías de información del Gobierno Regional Piura.
- Establecer las responsabilidades de los usuarios que hacen uso de las TI de acuerdo a las funciones establecidas en la oficina de tecnologías de información del Gobierno Regional Piura.
- Planificar capacitaciones y entrenamientos al personal en la oficina de tecnologías de información del Gobierno Regional Piura.

- Documentar las políticas para sanciones por uso indebido de los sistemas de información.
- Definir los procesos de seguridad de ambientes físicos y ambientales para los activos de TI en la oficina de tecnologías de información del Gobierno Regional Piura.
- Determinar los procesos para operaciones y transacciones de TI que realiza las unidades operativas de la oficina de tecnologías de información del Gobierno Regional Piura.
- Definir los procesos para solicitudes y atención de soporte de TI en la oficina de tecnologías de información del Gobierno Regional Piura.

Tabla Nro. 28 Tabla de evaluación del sistema de gestión de seguridad

OJETIVO DE CONTROL	**CONTROLES**	**VERIFICACIÓN**	
		SI	**NO**
POLITICA DE SEGURIDAD	Se verifica las políticas de seguridad de información.		
	Existen Perfiles que asegure la seguridad de la información.		
	La alta gerencia está comprometida con la seguridad de la información.		
	Existe coordinación entre la gerencia de TI y las otras áreas a fin de mejorar la seguridad de información.		
	Existen asignación de responsabilidades, respecto a la seguridad de la información.		
	Se define sucesiones de consentimiento para las modificaciones presentadas.		

	Se evidencias normas de confidencialidad.		
	Existe un proceso de coordinación con autoridades.		
	Existe registro de Contacto de los grupos de interés.		
	Se realiza revisiones periódicas que aseguren la seguridad de la información.		
	Se identifica la existencia de riesgos relacionados con entidades externas.		
	Hay archivos de respaldos para presentara clientes.		
	Se evidencia criterios para garantizar la seguridad de la información, frente a terceros.		
GESTION DE ACTIVOS	Existe inventarios de activos.		
	Los activos, son verificados de manera periódica, para asegurar su estado.		
	Se verifica el uso aceptable de los activos.		
	Se clasifican los activos de acuerdo a categorías.		
	Existe técnicas para la atomización del registro de activos.		
SEGURIDAD DE LOS RECURSOS HUMANOS	Se verifica Roles y responsabilidades de los usuarios.		

	Existe un proceso de selección para asignar responsables de las copias de seguridad de información.		
	Se verifica términos y condiciones de empleo.		
	Existe una gestión de Responsabilidades		
	Se detalla y plantea preparación en la seguridad.		
	Existen procedimientos disciplinarios con respecto a la vulnerabilidad de la seguridad de la información.		
	Se registran las incidencias de vulnerabilidad y/o amenazas de la seguridad de la información.		
	Se evidencia la devolución de activos, por parte del recurso humano cesado o asignado a otras funciones.		
	Se verifica la eliminación de derechos de acceso al usuario cesado.		
SEGURIDAD FÍSICA Y AMBIENTAL	El perímetro de la seguridad de la información, representa seguridad para los equipos de la seguridad de la información.		
	Existen controles en las entradas de ambientes físicos.		
	Se verifica la seguridad de oficinas, ambientaciones y medios.		

	Existe protección contra amenazas externas, respecto a los ambientes.		
	Se comprueba los trabajos en áreas seguras.		
	Se comprueba las áreas de acceso público, entrega y carga.		
	Se evidencia la ubicación y protección de equipos.		
	Se verifica la existencia de algunos servicios públicos.		
	Existe alguna seguridad en el cableado.		
	Existe mantenimiento de equipo.		
	Existe verificación de seguridad del equipo fuera del local.		
	Se comprueba eliminación segura o rehusó del equipo.		
	Se comprueba el traslado de propiedades.		
GESTIÓN DE LA COMUNICACIÓN Y OPERACIONES	Existe procedimientos de operación documentadas.		
	Le verifica gestión de cambio.		
	Existe la segregación de deberes.		
	Se verifica la separación de los medios de desarrollo y operacionales.		
	Existe alguna Entrega de servicios.		
	Se comprueba monitoreo y revisión de los servicios de terceros.		

	Se verifica el manejo de los cambios en los servicios de terceros.		
	Existe alguna gestión de la capacidad.		
	Se comprueba la aceptación del sistema.		
	Existe algún control sobre Software maliciosos.		
	Se evidencia los controles contra códigos móviles.		
	Existen evidencias de Backup o controles de la información.		
	Existe algún control de Red.		
	Se comprueba la seguridad de los servicios de Red.		
	Se verifica la gestión de los medios removibles.		
	Se comprueba la eliminación de medios.		
	Existe algún Procedimientos de los manejos de información.		
	Se comprueba la seguridad de documentación del sistema.		
	Existen procedimientos y políticas de información y Software.		
	Se verifica el registro de acuerdos de intercambios.		
	Se comprueba medios físicos en tránsito.		
	Se verifican los mensajes electrónicos.		
	Existe algunos sistemas de información comercial		

	Existe verificación de registro de comercio electrónico.		
	Se comprueba Transacciones en línea.		
	Se verifica la información disponible públicamente.		
	Existe algún Registro de auditoria		
	Se verifica la existencia del sistema de monitoreo.		
	Existe alguna protección del sistema de monitoreo.		
	Se vírica la protección de la información del registro.		
	Se comprueba los registros del administrador y operador.		
	Existe algún Registro de fallas.		
	Existe verificación de sincronización de relojes.		
	Se comprueba las políticas del control de accesos.		
	Existe alguna inscripción del usuario.		
	Existe una verificación de gestión de privilegios.		
	Existe alguna gestión de clave de usuarios.		
	Revisión de los accesos de los derechos del usuario.		
	Existe algún uso de clave.		
	Equipamiento de usuario desatendido.		

CONTROL DE ACCESO	Existe alguna política de pantalla y escritorio limpio.		
	Existe alguna política sobre el uso de servicios en Red.		
	Se comprueba Autenticación del usuario para conexiones externas.		
	Se comprueba la identificación del equipo en Red.		
	Existe alguna protección del puerto de diagnóstico remoto.		
	Segregación en redes.		
	Existe algún control de conexiones en redes.		
	Se comprueba el control de routing en redes.		
	Existe algún procedimiento de registro en el terminal.		
	Se verifica la identificación y autenticación del usuario.		
	Se comprueba el sistema de gestión de claves.		
	Se verifica el uso de utilidades del sistema.		
	Existe alguna sesión inactiva.		
	Se comprueba la limitación de tiempo de conexión.		
	Existe alguna restricción al acceso a la información.		
	Existe algún aislamiento del sistema sensible.		

	Se verifica la existencia de computación móvil y comunicación.		
	Existe algún Tele-trabajo.		

Fuente: Elaboración Propia.

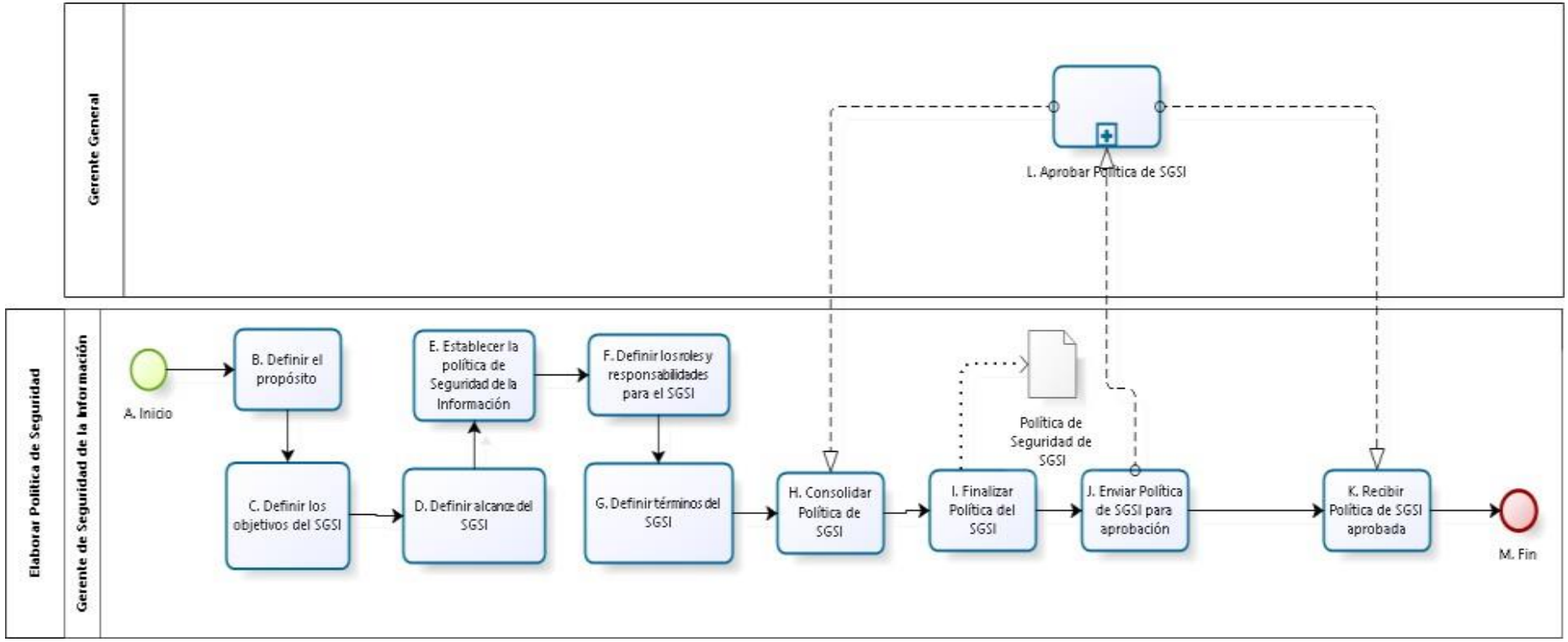
La incorporación de los presentes objetos de control, permitirá calcular el nivel de riesgo que considera y las metodologías de otros. Sin embargo, aquí veremos una fórmula simple y rápida para entender, basada en dos parámetros fundamentales en la gestión de riesgos: Probabilidades y Amenazas.

El Plan de Tratamiento de Riesgos debe contener una serie de informaciones básicas: Responsable del control: Persona responsable por la correcta implementación del control, Recursos: Personas, técnicos, empresas externas o materiales que serán utilizados para la implementación del control, Acciones a realizar: Acciones que serán necesarias para la implementación del control, Prioridad: Todos los controles no tienen la misma prioridad, ya que, por un lado, el nivel de riesgo no será el mismo, ni el valor de cada activo para la Organización. Por lo tanto, es necesario establecer prioridades, que pueden determinarse hasta la fecha de contabilización implementación de cada control.

Proceso – Elaborar Política de seguridad de la información

Por supuesto, se detalla el proceso de implementación de la política de seguridad de la información:

Gráfico Nro. 8: Elaborar Política de seguridad de la información



Fuente: Elaboración Propia

Una propuesta eficaz para hacer una implementación adecuada de la ISO 27001, es analizar las fortalezas y debilidades de los elementos más importantes que proponga en la imagen.

Gráfico Nro. 9: Propuesta de Fortalezas y Debilidades de TI

Fuente: Elaboración Propia.

Para lograr un eficiente trabajo, primeramente se debe plantear los puntos con debilidades propias para ser absueltas todas y brinde una seguridad plena, en base a lo establecido se ha planteado las fases mencionadas a continuación.

Primera Fase:

Esta primera fase comprende el inicio del plan de gestión de la seguridad de la información, donde se establecen responsabilidades, estándares y procedimientos sobre la dirección del plan de gestión de seguridad.

- Designar formalmente al Responsable de Seguridad de la información y/o Seguridad Informática.
- Definir y establecer las responsabilidades y objetivos del Responsable de Seguridad de la información y/o Seguridad Informática.
- Conformar el Comité de Gestión de la Seguridad de la Información.
- Analizar cada una de las recomendaciones dadas, de tal forma que se dé prioridad de implementación a los controles de seguridad que puedan disminuir el riesgo de mayor impacto.
- Diseñar el manual de políticas de seguridad de la información en base a los controles implementados actualmente y considerando nuevos controles que podrán ser implementados dentro de la oficina de tecnologías de información del Gobierno Regional Piura.
- Elaborar un catálogo de Clasificación de la información por área, el cual debe ponerse en conocimiento de todos los empleados (categorización: confidencial o pública).
- Evaluar con personal especializado todo lo referente a requerimientos legales, tomando en cuenta organismos de control que regulan a la oficina de tecnologías de información del Gobierno Regional Piura.

Segunda Fase:

Esta fase comprende la aplicación de los controles de seguridad anteriormente definidos, se realizan las actividades que han sido diseñadas con el propósito de disminuir el riesgo actual.

- Crear e implementar un programa de capacitación para los empleados de la oficina de tecnologías de información del Gobierno Regional Piura acerca de temas relacionados con la seguridad informática (charlas, boletines, seminarios, entre otros).
- Implementar los controles de seguridad recomendados en la matriz de situación actual y activos de la información, tomando en cuenta la protección física y lógica de la información y de los sistemas de procesamiento de información.
- Definir y establecer políticas y responsabilidades sobre la administración de accesos de los sistemas de información.
- Estandarizar los user ID, de tal forma que los empleados utilicen un solo usuario para el ingreso a los diferentes aplicativos de la oficina de tecnologías de información del Gobierno Regional Piura.
- Definir el proceso para gestionar los cambios que se necesiten realizar en los aplicativos de la oficina de tecnologías de información del Gobierno Regional Piura.
- Incorporar la seguridad de la información en la Gestión de la continuidad del negocio.
- Administrar y registrar los incidentes de seguridad de la información que se presente.
- Analizar la posibilidad de implementación de sistemas de video vigilancia, detectores de humo, sistemas contra incendios.
- Registrar pistas de auditorías en los sistemas de información de la oficina de tecnologías de información del Gobierno Regional Piura.
- Definir un backup para cada funcionario que desempeñe un rol crítico dentro de las actividades del área de sistemas.

Tercera Fase:

- Dar seguimiento la seguridad brindada, resaltar su capacidad con la intenci´n de cumplir lo establecido.
- Verificar constantemente las pautas de seguridad concretados para desviar todo inconveniente.
- Examinar el punto de contraer utensilios para dirigir con mas exactitud.
- Guiar los pasos respectivos para concretar un ejemplo de trabajo.

- Finalmente anotar el fruto logrado exitosamente.

Cuarta Fase:

- Cambiar en prosperidad la gestión de la seguridad basándose en las causas encontradas detectads durante el análisis respectivo.
- Reconocer y agregar pautas de ayuda a superar las causas perjudicables.
- Actualizar el manual de políticas de seguridad de la información cuando ocurran cambios significativos.
- Capacitar al personal que maneja la seguridad de la información, así como al personal técnico del área de Sistemas (administradores, desarrolladores, entre otros).

VI.CONCLUSIONES

Teniendo en cuenta los resultados obtenidos en el presente trabajo de investigación, se concluye que la oficina de tecnologías de información del Gobierno Regional Piura, la misma que permitirá mejorar los procesos de seguridad, confiabilidad y disponibilidad de la información. La interpretación realizada coincide con la hipótesis general a la propuesta de un sistema de gestión de seguridad de la información basado en la Norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura; 2020, minimizará la pérdida de información, por lo tanto, concluyo diciendo que la hipótesis general es debidamente aceptada.

1. Para la propuesta de seguridad de información, se evaluó la situación actual de los procesos de seguridad tomando en cuenta la norma ISO 27001 para la oficina de tecnologías de información del Gobierno Regional Piura, permitiendo identificar los problemas de seguridad en la información.

2. Se demostró que la evaluación de los marcos de referencia nos permitió proponer mejoras en la seguridad de la información en la oficina de tecnologías de información del Gobierno Regional Piura los cuales se refuerza con los resultados de la dimensión Necesidad de la propuesta de un sistema de la información con normas ISO 27001.

3. Se logró realizar la propuesta de la aplicación de la Norma ISO/IEC 27001, la cual mejora la seguridad de la información en la oficina de tecnologías de información del Gobierno Regional Piura.

Como principal aporte es mejorar la seguridad de información y por ende mejorar la perdida de información da la oficina de tecnologías de información del Gobierno Regional Piura.

RECOMENDACIONES

1. Es importante considerar que el Sistema de Gestión de Seguridad de la Información es un proceso de mejoramiento continuo, en donde los nuevos requerimientos de seguridad se ajusten a los cambios de la oficina de tecnologías de información del Gobierno Regional Piura.

2. Evaluar periódicamente la seguridad de la información, utilizando las normas ISO 27001, en la oficina de tecnologías de información del Gobierno Regional Piura. A fin de garantizar la aplicación de procesos preventivos que contribuyan a la continuidad de los servicios y de este modo el Gobierno se fortalezca en su reputación a través del uso de los sistemas de información.

3. Capacitación continua para el personal de TI en métodos y procesos de seguridad de la información y comunicación de la oficina de tecnologías de información del Gobierno Regional Piura a fin de mejora sus competencias y actualización en nuevas metodologías y herramientas para la aplicación de la seguridad de la información.

4. La oficina de tecnologías de información del Gobierno Regional Piura, debe proponer la realización de la gestión para la Certificación de la norma ISO / IEC 27001, a fin de garantizar la implementación de acuerdo con las normas y protocolos establecidos por la empresa de certificación.

REFERENCIAS BIBLIOGRÁFICAS

1. Chicano E. Gestión de Incidentes de Seguridad Informática. Primera edición ed. Málaga: Editorial I, editor; 2015.
2. Alemán Novoa CI. Metodología para la Implementación de un SGSI en la JDC: Aplicación de la norma ISO 27001 - SGSI en la Fundación Universitaria Juan de Castellanos de Tunja. Primera ed. España: Editorial Académica Española; 2017.
3. Ararat J. Diseño de un SGSI basado en la norma ISO 27001 para la empresa MA PEÑALOSA CÍA. S.A.S. sede principal Cúcuta. San José de Cúcuta, Norte de Santander: Universidad Nacional Abierta y a Distancia, Escuela de ciencias básicas, tecnología e ingeniería; 2018.
4. Meneses A, Ramírez E, Merchan M, Suarez Y. Diseño del sistema de gestión de seguridad de la información SGSI basado en el estándar ISO 27001, para los procesos soportados por el área de sistemas en la cámara de comercio de Aguachica, Cesar. Tesis pregrado. Colombia: Universidad Francisco de Paula Santander Ocaña, Facultad de Ingenierias; 2016.
5. Tola D. Implementación de un sistema de gestión de seguridad de la información para una empresa de consultoría y auditoría, aplicando la Norma ISO/IEC 27001. Tesis de pregrado. Ecuador: Escuela Superior Politécnica del Litoral, Facultad de Ingeniería en Electricidad y Computación ; 2015.
6. Torres M. Diseño de un sistema de gestión de la seguridad de la información (SGSI), basada en la norma ISO/IEC 27001:2013, para el proceso de servicio post-venta de un integrador de soluciones en Telecomunicaciones. Tesis pregrado. Lima - Perú: Universidad Peruana de Ciencias Aplicadas (UPC), Facultad de Ingeniería - Carrera de Ingeniería de Redes y Comunicaciones; 2018.
7. Santos D. Establecimiento, implementación, mantenimiento y mejora de un sistema de gestión de seguridad de la información, basado en la ISO/IEC 27001:2013, para una empresa de Consultoría de Software. Tesis de pregrado. Lima - Perú: Pontificia Universidad Católica del Perú, Facultad de Ciencias e Ingeniería; 2016.
8. Castillo R. Sistema de Gestión de Seguridad de la Información en la Municipalidad Distrital de Pira aplicando la norma ISO/IEC 27001:2013. Tesis de pregrado. Huaraz -

Ancash: Universidad Católica los Ángeles de Chimbote, Ingenieria de Sistemas; 2016.

9. Vegas I. Diseño de un sistema de gestión de seguridad de la información para los procesos académicos de la Universidad Nacional de Piura según la NTP ISO/IEC 27001. Tesis de pregrado. Piura: Universidad Nacional de Piura, Facultad de Ingeniería Industrial - Escuela Profesional de Ingeniería Informática; 2019.
10. Lara. Propuesta para la seguridad informática basado en la norma ISO /IEC 27001 en la clínica Simedic diagnóstica S.A.C – Piura; 2018. Tesis de pregrado. Piura: Universidad Católica los Ángeles de Chimbote, Ingeniería de Sistemas; 2018.
11. Albán E. Gestión de seguridad de información basado en la norma ISO/IEC 27000 en la Municipalidad Provincial de Talara año 2016. Tesis Magíster. Piura: Universidad Católica los Ángeles de Chimbote, Ingeniería de Sistemas; 2017.
12. Vasconcelos Santillan J. Tecnologia de la Información. Segunda ed. Patria GE, editor. Mexico: Patria; 2015.
13. Gutiérrez González. Introducción a la Ingeniería. Primera ed. Marcombo , editor. Madrid: Alfaomega; 2016.
14. Cubillos Ospina D. Tecnología De La Información Y Comunicación - Yopal. [Online].; 2012 [cited 2018 Nobiembre 11. Available from: https://sites.google.com/site/ticsyopal5/assignments/homeworkforweekofoctober18th.
15. Arturo Betancourt S. Origen y evolución de las TIC y aportes a la educación. [Online].; 2012 [cited 2018 Abril 1. Available from: https://www.sutori.com/story/origen-y-evolucion-de-las-tic-y-aportes-a-la-educacion.
16. Villafuerte Quiroga D. solucionespracticas. [Online]. Lima; 2009 [cited 2018 marzo 1. Available from: https://solucionespracticas.org.pe/Descargar/398/3726.
17. Instituto Nacional de Calidad. INACAL. [Online].; 2016 [cited 2018 Octubre 30. Available from: https://www.inacal.gob.pe/principal/categoria/ntp.
18. Garre Gui S, Tortajada Gallego , Segovia Henares , Cruz Allende. Sistema de gestión de la seguridad de la información. Primera ed. España: Editorial UOC; 2018.
19. Vidalina De Freitas FN. Sistema de Gestion de Seguridad de La Informacion. Primera ed. Venezuela: Eae; 2012.
20. sbqconsultores. Consultora de Sistemas de Gestión y Normas ISO. [Online].; 2015

[cited 2018 Enero 27. Available from: https://www.sbqconsultores.es/el-ciclo-de-deming-o-circulo-pdca/.

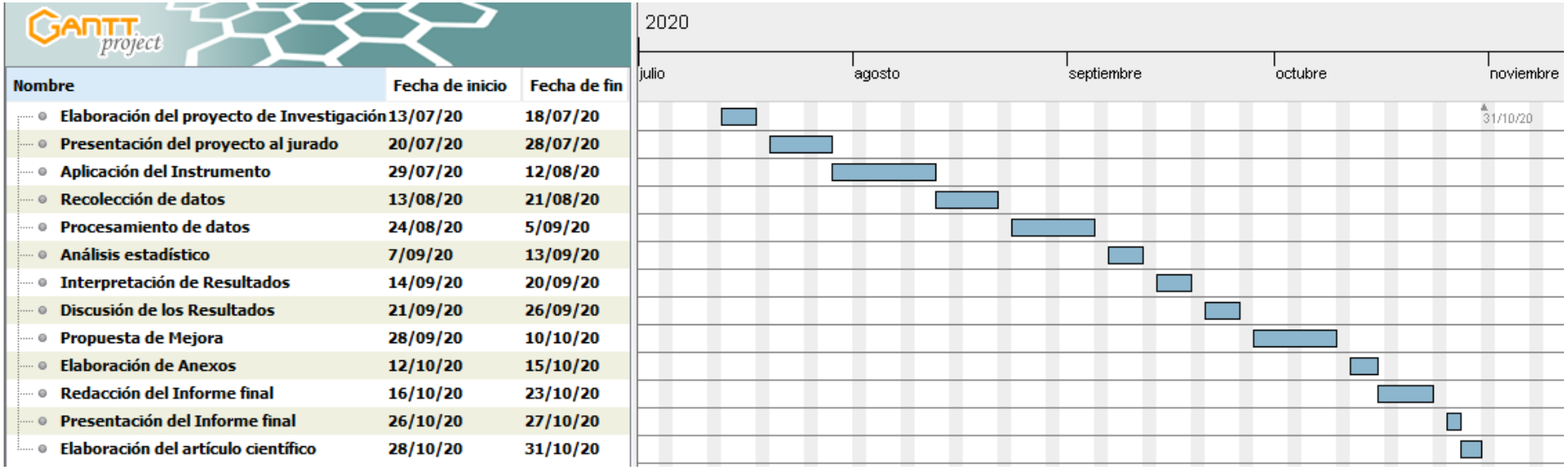
21. Daltabuit Godas , Hernandez Audelo. La seguridad de la información. Primera ed. México: Limusa; 2007.
22. Harold F. Tipton MK. Information security management handbook. Sexto ed. Tipton HF, editor. Nueva york: Auerbach; 2008.
23. Miguel Pérez C. Protección de datos y seguridad de la información. Cuarta ed. España: Ra-Ma ; 2015.
24. ISO. ISO. [Online]. [Online]. [cited 2017 agosto 01. Available from: Available from: http://www.iso.org/.
25. iso27000. Portal de ISO 27001 en español. [Online].; 2017 [cited 2017 Marzo 27. Available from: http://www.iso27000.es/iso27000.html.
26. Núñes Ponce J. JULIO NUNEZ DERECHO INFORMATICO. [Online].; 2016 [cited 2016 Marzo 1. Available from: http://julionunezderechoinformatico.blogspot.com/2016/01/.
27. elperuano. aprueban el uso obligatorio de la norma tecnica peruana NTP resolucion ministerial n° 004 2016 pcm. [Online].; 2016 [cited 2016 Enero 8. Available from: https://busquedas.elperuano.pe/normaslegales/aprueban-el-uso-obligatorio-de-la-norma-tecnica-peruana-ntp-resolucion-ministerial-no-004-2016-pcm-1333015-1/.
28. Rubio JA. isaca. [Online].; 2013 [cited 2013 Noviembre 11. Available from: http://www.isaca.org/chapters7/Madrid/Events/Documents/Principales%20Novedades%20de%20la%20ISO27001ISO%2027002%20-%20Paloma%20Garcia.pdf.
29. Sandoval Vargas C. Análisis de la norma ISO/IEC 27001. Diseño de Implementación en la red de una empresa. Tesis de Grado. Guayaquil: Universidad Católica de Santiago de Guayaquil, Sistema de Posgrado; 2014.
30. Excellence. I. Blog especializado en Sistemas de Gestión. [Online].; 2015 [cited 2017 agosto 05. Available from: http://www.pmg-ssi.com/2015/03/iso-.
31. Giménez Albacete. Seguridad en equipos informáticos. IFCT0109.. editor. Malaga: IC Editorial. primera ed., IC Editorial 2; 2015.
32. Fernández Barcell M. Estudio de una estrategia para la implementación de los sistemas

de gestión de la seguridad de información.. Doctoral.. Cadíz: Universidad de Cadíz, Ingeniería en Automática; 2003.

33. Namakforoosh M. Metodología de la investigación. Segunda ed. Mexico: Limusa; 2012.
34. Naghi M. Metología de la Investigación. Limusa E, editor. México:; 2005.
35. Cauas D. Definicion de la Variables, enfoque y tipo de Investigacion. 2006. Articulo - Manual.
36. Barragán R, Ayllón V V, Sanjinés J, Langer E, Córdova J, Rojas R. Guía para la Formulación y Ejecución de Proyectos de Investigación. Tercera Edición ed. ed. Bolivia : Offser Boliviana Ltda; 2016.
37. Hernandez Sampieri , Fernandez Collado , Baptista Lucio. Metodología de la investigación. Sexta ed. España: McGraw-Hill Interamericana; 2014.
38. Hernández Sampieri R, Fernández Collado C, Baptista Lucio P. Metodología de la investigación: Componentes de los Materiales de entrenamiento para Análisis de Corte Transversal. Primera ed. S.A PFeI, editor. Canada: MCGRAW-HILL; 1991.
39. definicionabc. Definición de Encuesta. [Online].; 2016 [cited 2017 abril 23. Available from: http://www.definicionabc.com/comunicacion/encuesta.php.
40. Muñoz Almendralejo TG. El Cuestionario como instrumento de investigación /evaluación. Tesis. España: Universitario Santa Ana, Sociologia; 2003.

ANEXOS

ANEXO N° 01 CRONOGRAMA DE ACTIVIDADES



Nombre	Fecha de inicio	Fecha de fin
Elaboración del proyecto de Investigación	13/07/20	18/07/20
Presentación del proyecto al jurado	20/07/20	28/07/20
Aplicación del Instrumento	29/07/20	12/08/20
Recolección de datos	13/08/20	21/08/20
Procesamiento de datos	24/08/20	5/09/20
Análisis estadístico	7/09/20	13/09/20
Interpretación de Resultados	14/09/20	20/09/20
Discusión de los Resultados	21/09/20	26/09/20
Propuesta de Mejora	28/09/20	10/10/20
Elaboración de Anexos	12/10/20	15/10/20
Redacción del Informe final	16/10/20	23/10/20
Presentación del Informe final	26/10/20	27/10/20
Elaboración del artículo científico	28/10/20	31/10/20

Fuente: Elaboración propia.

ANEXO N° 02 PRESUPUESTO

TITULO: PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN DEL GOBIERNO REGIONAL PIURA; 2020.

ESTUDIANTE: GARCIA CRUZ RODOLFO AUGUSTO

INVERSIÓN: S/. 1,047.00

FINANCIAMIENTO: RECURSOS PROPIOS

DESCRIPCIÓN	UNIDAD	CANT.	COSTO UNITARIO	COSTO TOTAL
VIÁTICOS Y ASIGNA CIONES				
Movilidad	Días	10	40.00	400.00
ALIMENTACIÓN				
Almuerzos	Días	30	10.00	300.00
SERVICIO DE INTERNET				
Internet	Mes	03	90.00	270.00
Fotocopias	Unidad	400	0.10	40.00
MATERIALES VARIOS				
Lapiceros	Unidad	10	1.50	15.00
Lápiz	Unidad	5	1.00	5.00
Hojas	Unidad	500	0.025	12.00
Folder Manila	Unidad	10	0.50	5.00
		TOTAL,	S/	1,047.00

ANEXO N° 03 CUESTIONARIO

TITULO: PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001 PARA LA OFICINA DE TECNOLOGÍAS DE INFORMACIÓN DEL GOBIERNO REGIONAL PIURA; 2020.

ESTUDIANTE: GARCIA CRUZ RODOLFO AUGUSTO

DIMENSIÓN 01: Satisfacción de la situación actual			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Cree Usted que los datos registrados en el sistema actual son seguros?		
2	¿Existen políticas y procedimientos para asegurar que se proporciona seguridad en la información de sus usuarios?		
3	¿Usted desecha la información que ya no necesita?		
4	¿Se realizan copias de seguridad (diariamente, semanalmente, mensualmente, etc.)?		
5	¿Cuándo no se encuentra en su oficina deja documentación visible en su escritorio?		
6	¿La clave de acceso es la misma para ingresar a todos los equipos de cómputo?		
7	¿Usted ha detectado que el antivirus del Gobierno Regional Piura funciona y se encuentra actualizado?		
8	¿Existe alguna alarma contra incendios, robos u otros?		
9	¿El Gobierno cuenta con algún plan de contingencia para dar solución a algún incidente tanto interno o ajeno de la organización?		
10	¿Usted ha observado que alguno de sus compañeros a ingerido alguna bebida o alimentos cuando realiza su trabajo en cualquiera de las computadoras del Gobierno Regional?		

DIMENSIÓN 02: Necesidad de la seguridad de información			
NRO.	**PREGUNTA**	**SI**	**NO**
1	¿Conoce el tema seguridad de información?		
2	¿Cree que es necesario aplicar controles de seguridad para evitar pérdida o daño de información importante para el Gobierno Regional?		
3	¿Existe en el Gobierno Regional un responsable del área de la seguridad de información?		
4	¿Ha ocurrido algún incidente de seguridad en su puesto de trabajo en el último año?		
5	¿Considera que el Gobierno Regional le da importancia al tema de seguridad?		
6	¿Considera que la seguridad de información debe ser vital en el Gobierno Regional?		
7	¿Usted como trabajador tiene la cultura de seguir con protocolos de seguridad?		
8	¿Conoce Usted sobre la norma ISO 27001 en la seguridad de información?		
9	¿El Gobierno Regional imparte constantemente capacitaciones de seguridad?		
10	¿Desea recibir capacitaciones sobre la seguridad de información y la norma ISO 27001?		