UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS

IMPLEMENTACIÓN DE AUDITORÍA INFORMÁTICA CON LA ISO 27001 EN LA MUNICIPALIDAD DISTRITAL DE SUYO-PIURA; 2020.

TESIS PARA OPTAR EL TÍTULO PROFESIONAL DE INGENIERA DE SISTEMAS

AUTORA:

COSIOS AVILA, TANIA VERÓNICA

ORCID:0000-0002-7715-6922

ASESOR:

MORE REAÑO, RICARDO EDWIN

ORCID:0000-0002-6223-4246

PIURA – PERÚ

2020

EQUIPO DE TRABAJO

AUTOR

Cosios Avila Tania Verónica

ORCID:0000-0002-7715-6922

Universidad Católica Los Ángeles de Chimbote, Estudiante de Pregrado,

Piura, Perú

ASESOR

More Reaño, Ricardo Edwin

ORCID: 0000-0002-6223-4246

Universidad Católica Los Ángeles de Chimbote, Facultad de Ingeniería,

Escuela Profesional de Ingeniería de Sistemas, 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. JENNIFER DENISSE SULLÓN CHINGA
PRESIDENTE

MGTR. MARLENY SERNAQUÉ BARRANTES
MIEMBRO

MGTR. EDY JAVIER GARCÍA CÓRDOVA
MIEMBRO

ING. RICARDO EDWIN MORE REAÑO
ASESOR

DEDICATORIA

A Dios porque tanto me ama por concederme sabiduría, salud, amor, fe y esperanza, por ser mi fuerza espiritual, mi guía por regalarme cada día el milagro de la vida y permitir así luchar por mis sueños que tanto anhelo.

A mis padres, los cuales me apoyaron de manera incondicional, por sus consejos, sus valores que me ayudan hacer una persona de bien, por su infinito amor y comprensión lo que motiva a salir adelante y poder afrontar cada obstáculo que se me presenta en el camino.

A mis hermanitas que están en el cielo y a mis hermanos, que aún están con vida, porque con su amor y enseñanzas me mostraron que estudiando se puede conseguir varias metas y ser felices por ello.

A mis pequeñas sobrinas Yamilet y Edita que con su hermosa sonrisa, sus abrazos y sus muestras de cariño me motivan a seguir cada día adelante.

Tania verónica cosios Ávila

AGRADECIMIENTO

Agradezco a Dios por su infinito amor, su paciencia, por darme la oportunidad de vivir y guiarme en cada momento de mi vida y tomar buenas decisiones, a mi familia por apoyarme en cada momento, por su amor, su comprensión.

Así mismo agradecer a los docentes que gracias a sus conocimientos, experiencias obtenidas compartieron con nosotros en sus aulas, siempre motivándonos a ser cada día mejores profesionales y que con humildad se pueden lograr grandes cosas.

Agradezco, a la Municipalidad Distrital de Suyo-Piura, por haberme dado la oportunidad de llevar acabo mi informe de tesis, facilitándome la información necesaria y su tiempo empleado para lograr el desarrollo de mi investigación.

Y un especial agradecimiento a mi asesor ING. Ricardo More Reaño, por su paciencia, su tiempo dedicado por brindarme sus conocimientos, asesorías durante el desarrollo de mi tesis y así lograr un buen resultado.

Tania verónica cosios Ávila

RESUMEN

La presente investigación ha sido desarrollada bajo la línea de investigación desarrollo de modelos y aplicación de las tecnologías de información y comunicaciones para la mejora continua de calidad de las organizaciones del Perú de la escuela profesional de Ingeniería de Sistemas, la cual estuvo basada en realizar una Implementación de Auditoría Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura; 2020.El tipo de investigación fue no experimental, descriptiva y de corte transversal, teniendo como objetivo general Implementar una Auditoria Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura; para mejorar el sistema de información. Con una muestra de 40 miembros. Los resultados obtenidos en el primer nivel de conocimiento de la información de Implementación de auditoria informática con la ISO 27001, el 50% de los trabajadores encuestados indicaron que NO tienen conocimiento de seguridad informática y seguridad de un sistema de información. En la segunda dimensión seguridad de la información, el 55% de los trabajadores encuestados indicaron que NO hay seguridad de la información en dicha municipalidad, se puede concluir que en la municipalidad los trabajadores desconocen acerca lo que es seguridad de información y por lo cual no se realiza una buena seguridad de la información en el sistema.

Palabras Clave: Auditoria, Información, ISO 27001, Seguridad.

ABSTRACT

The present investigation has been developed under the line of investigation development of models and application of the information and communication technologies for the continuous improvement of quality of the organizations of Peru of the professional school of Systems Engineering, which was based on carrying out a Implementation of a Computer Audit with ISO 27001 in the District Municipality of Suyo-Piura; 2020.JThe type of investigation was non-experimental, descriptive and cross-sectional, with the general objective of implementing a Computer Audit with ISO 27001 in the District Municipality of Suyo-Piura; to improve the information system. With a sample of 40 members. The results obtained in the first level of knowledge of the information of Implementation of a computer audit with ISO 27001, 50% of the surveyed workers indicated that they have NO knowledge of computer security and security of an information system. In the second dimension of information security, 55% of the surveyed workers indicated that there is NO information security in said municipality, so it can be concluded that in the municipality, workers are unaware of what information security is and why which does not make a good security of the information in the system.

Key Words: Audit, Information, ISO 27001, Security.

ÍNDICE DE CONTENIDO

EQUIPO DE TRABAJO ii
HOJA DE FIRMA DEL JURADO Y ASESOR iii
DEDICATORIA iv
AGRADECIMIENTO v
RESUMEN vi
ABSTRACT vii
ÍNDICE DE CONTENIDO viii
ÍNDICE DE TABLAS x
ÍNDICE DE GRÁFICOS xii
I. INTRODUCCIÓN 1
II. REVISIÓN DE LA LITERATURA 4
2.1. Antecedentes 4
2.1.1. Antecedentes a nivel internacional 4
2.1.2. Antecedentes a nivel nacional 6
2.1.3 Antecedentes a nivel regional 7
2.2. Bases teóricas 10
2.2.1. Información de la empresa 10
2.2.1.1. Definición municipalidad 10
2.2.2. Municipalidad Investigada 15
2.2.3. Las TIC 20
2.2.4.La Tecnología de la Investigación 23
III. HIPÓTESIS 48
IV. METODOLOGÍA 49
4.1. Tipo y nivel de la investigación 49

4.1.1. Tipo de Investigación 49
4.1.2 Nivel de Investigación 50
4.2. Diseño de la Investigación 51
4.3. Población y Muestra 52
4.3.1. Población 52
4.3.2. Muestra 52
4.5. Técnicas e Instrumentos 58
4.4.1. Técnica 58
4.4.2. Instrumento 59
4.4.3 Procedimiento de recolección de datos 59
4.6. Plan de análisis de datos 60
4.8. Principios éticos 63
V. RESULTADOS 64
5.1. Resultados 64
5.1.1. Dimensión 01: Nivel de conocimiento 64
de la información 74
5.1.2. Dimensión 02: Seguridad de la información 76
5.2. Análisis de Resultados 90
5.3. Propuesta de mejora 92
V. CONCLUSIONES 175
RECOMENDACIONES 176
REFERENCIAS BIBLIOGRÁFICAS 177
Anexo Nº 1: Cronograma de actividades 183
Anexo Nº 2: Presupuesto 184
Anexo Nº 3: Cuestionario 185

ÍNDICE DE TABLAS

Tabla Nro. 1: Infraestructura Tecnológica 19
Tabla Nro.2: División de trabajadores de la Municipalidad de Suyo 54
Tabla Nro.3: Definición Operacional 56
Tabla Nro. 4: Matriz de consistencia 61
Tabla Nro. 5: Sistemas de información 64
Tabla Nro. 6:Norma de Seguridad 65
Tabla Nro. 7: Políticas de seguridad 66
Tabla Nro. 8: Mecanismos para la comunicación a los trabajadores 67
Tabla Nro. 9: Programas de formación en seguridad 68
Tabla Nro.10: Roles y responsabilidades 69
Tabla Nro.11: Confidencialidad de la información 70
Tabla Nro.12: Proceso Disciplinario 71
Tabla Nro.13: Áreas restringidas 72
Tabla Nro. 14: Incidente de seguridad 73
Tabla Nro. 15: Resumen de la dimensión 01-Nivel de conocimiento 74
Tabla Nro.16: Método para reducir el mal uso de los sistemas 76
Tabla Nro.17: Asentadores para la gestión de los sistemas de Información 77
Tabla Nro.18: Copias de seguridad 78
Tabla Nro.19: Documentación de los sistemas de información 79
Tabla Nro. 20: Seguridad en el comercio electrónico 80
Tabla Nro. 21: Encriptación de password 81
Tabla Nro. 22: Capacidad de proceso y almacenamiento de la Informaciòn 82
Tabla Nro. 23: Logs 83
Tabla Nro.24: Control de accesos 84
Tabla Nro.25:Controles criptográficos 85
Tabla Nro.26: Resumen de la dimensión 02-Seguridad de la información 86
Tabla Nro.27: Resumen General de las Dimensiones 88
Tabla Nro. 28: Evaluación de los controles de la Normativa ISO/IEC 27002:2013Control de la normativa ISO/IEC 27001:2013 94
Tabla Nro. 29: Inventario de los activos 150

Tabla Nro. 30:Valor de los activos 152
Tabla Nro.31:Escala de valoración 153
Tabla Nro.32: Valoración de seguridad de los activos 153
Tabla Nro.33: AMENAZAS 156
Tabla Nro.34: Relación de proyectos 164

ÍNDICE DE GRÁFICOS

Grafico Nro.1: Ubicación de la municipalidad Distrital de Suyo 15
Grafico Nro.2:Organigrama Institucional 18
Grafico Nro.3:Tipo de Auditorias de Sistemas de Información 24
Grafico Nro.4:Relación entre mecanismos y servicios de seguridad 28
Grafico Nro.5:Evolución de la norma 32
Grafico Nro.6: Niveles de Organización Documentada 36
Grafico Nro.7: Modelo del SGSI de la Norma ISO 27001 40
Grafico Nro. 8: Metodología Magerit 41
Grafico Nro. 9:Enfoque de los controles de la Norma ISO 27001 43
Grafico Nro.10: Actividades para alcanzar la certificación ISO 27001 del SGSI .. 47
Grafico Nro.11:Resultados de la Dimensión 01 75
Grafico Nro.12: Resultados de la Dimensión 02 87
Grafico Nro. 13:Resumen General de las Dimensiones 89
Grafico Nro. 14:Salvaguardas en primer nivel 170
Grafico Nro15:Salvaguardas de mejoras en la gestión 171
Grafico Nro.16:Tiempo de realización 174

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).

Hay numerosas motivaciones por las que un atacante puede actuar en una organización: desde motivos económicos, por simple diversión, por disconformidad con sus directrices o valores o por la mera autorrealización personal, entre muchas otras (1).

La municipalidad distrital de Suyo, provincia Ayabaca se encuentra ubicada en Jr. Leoncio Prado Nro.S/N, de la cual cuenta un total de 20 laptops, 70 equipos de cómputo, 12 impresoras. Todas las computadoras poseen Sistema operativo Windows 10. El utilitario de antivirus que se usa es el Eset nod 32, las aplicaciones que poseen son: Microsoft office 2013, para todos los trabajos de oficina, Skype, para realizar llamadas, navegadores como Firefox, google Chrome e internet explorer, aplicaciones multimedia entre otros.

Actualmente la municipalidad cuenta con políticas y controles de seguridad de la información mínimos para realización de sus actividades, pero éstas no se encuentran documentadas. Sin embargo, debido a la sensibilidad y criticidad y seguridad de la información, no son suficientes para reducir los riesgos en el manejo, almacenamiento y distribución de la información contenida en los diversos sistemas informáticos, equipos de cómputo, procesos con falla de seguridad, perjudicando la integridad, confiabilidad y disponibilidad de la información.

Hoy en día los constantes cambios tecnológicos, el manejo de la seguridad de información a todo nivel; se convierte en un problema grave y tiende a ser motivo de descuido en las instituciones cuando no se le brinda el control y tratamiento apropiado.

En lo cual se deduce, respecto a la seguridad de la información, existe una gran inconsistencia, en dicha municipalidad los trabajadores no tienen conocimiento sobre seguridad informática y seguridad de la información, se ignora los riesgos que llevan a mantener la confiabilidad, integridad y disponibilidad de la información.

De acuerdo a la problemática establecida se expresó el siguiente enunciado del problema:

¿La implementación de auditoria informática con la ISO 27001; mejora la seguridad de información en la Municipalidad Distrital de Suyo-Piura?

Para el desarrollo de esta investigación se planteó el siguiente objetivo general

Implementar Auditoria Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura; para mejorar la seguridad de la información. Lo cual se definieron los siguientes objetivos específicos:

1. Identificar los activos de información de los procesos implementados basados en la norma ISO 27001.
2. Evaluar los riesgos a dichos activos en la municipalidad.
3. Elaborar los controles adecuados de acuerdo a los riesgos identificados.

La justificación de esta investigación se basa que en la Municipalidad distrital de Suyo la implementación de Auditoria Informática con la ISO 27001 mejora la seguridad de la información de los posibles riesgos y ataques que están expuestos, así también los trabajadores deben estar capacitados para cooperar en la seguridad informática y de la información.

Justificación académica es usar los conocimientos adquiridos a través de todos los años de estudio en la UNIVERSIDAD CATÓLICA LOS ÁNGELES DE CHIMBOTE, lo cual nos servirá para implementar auditoria informática con las ISO 27001 para mejorar el sistema de información en la municipalidad distrital de Suyo.

Con respecto a la justificación operativa, la implementación de una auditoria informática ayudara a mejorar la seguridad de la información de posibles ataques tanto físicos y lógicos en dicha municipalidad.

En lo que respecta a la justificación económica fue factible puesto que con la implementación de auditoria se pueden prevenir o minimizar costos extremos, de acuerdo a los riesgos que se dan en los sistemas de información.

Como justificación tecnología, la municipalidad tiene una infraestructura tecnológica, que permite evaluar, monitorear y mejorar posibles ataques que puedan afectar la confidencialidad, integración de la información.

La justificación institucional tomo en cuenta que la municipalidad distrital de Suyo necesita conocer acerca de auditoria informática con la ISO 27001 para la mejora en la seguridad de la información.

El alcance del presente trabajo de investigación será desarrollado en la Municipalidad Distrital de Suyo – Piura. Asimismo, esta investigación abarcara la implementación de Auditoria Informática con la ISO 27001 para evitar posibles riesgos de seguridad informática y las vulnerabilidades que están expuestas el sistema de información.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes a nivel internacional

Aguilar (2), en el año 2017, en su tesis titulada Plan de Seguridad Informática Basado en Estándar ISO-IEC 27001 para Proteger la Información y Activos del Gad Cantonal de Pastaza ,sostiene que la información que forma parte de un gobierno seccional, se la considera el activo más valioso para su correcto desempeño dentro de la política pública y su relación con los conciudadanos en este nuevo siglo, porque ésta será elemento fundamental en el cumplimiento de sus objetivos, es por ello que, resguardar todo tipo de Información de cualquier posibilidad de alteración, mal uso, pérdida, entre otros muchos eventos, puede significar un respaldo para el normal desarrollo de sus actividades. Sin embargo, pese a la falta de conocimiento sobre cómo protegerla adecuadamente, o debido a la complejidad de las normas internacionales que indican los procedimientos para lograr un adecuado nivel de protección, muchas organizaciones, en especial el sector de los Gobiernos Locales, no logra alcanzar este objetivo. Por lo tanto, este estudio propone una forma de aplicar la seguridad de la información para la gestión de riesgo informático aplicable al entorno de pequeñas y medianas empresas como a los gobiernos seccionales del Ecuador. Para el efecto, se utilizó la herramienta proporcionada por Microsoft denominada Herramienta de Evaluación de Seguridad de Microsoft (MSAT).Esta herramienta es internacionalmente utilizada en la gestión del riesgo de la información, concomitante a los parámetros de referencia de la norma: ISO 27001, 27002 y 27005, con los informes resultantes de esta herramienta, se generó el Plan de Seguridad de la Información, que deberá ser aplicado para mejorar

los controles internos del Gobierno Seccional en lo relacionado a seguridad informática.

Bermúdez,Bailón (3),en el año 2015, en su tesis titulada "Análisis en Seguridad Informática y Seguridad de la Información Basado en la Norma ISO/IEC 27001- Sistemas de Gestión de Seguridad de la Información Dirigido a una Empresa de Servicios Financieros", para obtener el título de ingeniero de sistemas manifestó, durante muchos años las empresas se han preocupado por perfeccionar todos los sistemas informáticos, dejando en una prioridad casi nula la seguridad de la información. La evolución de los sistemas computacionales, del internet y de las comunicaciones en general han abierto una puerta para que las personas empiecen a descubrir el valor de la información y la facilidad de acceder a los datos. Desafortunadamente ese fácil acceso a la información la expone a que también sea utilizada por personas no autorizadas. Existen miles de personas que se dedican a realizar ataques informáticos con la finalidad de obtener información para cometer actos ilícitos, de tal manera que puede llegar a perjudicar una empresa.

Landázuri (4), en el año 2015,en su tesis titulada "Auditoria a la Seguridad del Sistema de Información Sivigila de la Alcaldía de San Andrés de Tumaco Basado en el Estándar ISO 27001", tuvo como objetivo proponer planes de mejoramiento que redunden en la gestión de la información mediante la aplicación de procesos de auditoría a la seguridad basada en el estándar ISO 27001 en el sistema de información SIVIGILA de la Secretaria de Salud de la alcaldía de Tumaco. De esta como la primera meta es identificar el lugar a auditar que permita desarrollar una investigación completa y verídica que dé lugar a un plan de auditoria completo y acorde con las necesidades de la entidad que se está evaluando, seguido del

desarrollo de un plan de auditoria acorde con la investigación hecha en el lugar a auditar, una vez hecho esto desarrollar herramientas, técnicas y procedimientos para la recolección de información y obtención de evidencias en el proceso de auditoría, las cuales permitieron obtener evidencias mediante la ejecución del plan de auditoria, sintetizar y sistematizar los hallazgos del resultado del proceso de auditoría, haciendo posible la socialización del informe final de auditoria a la alcaldía de Tumaco.

2.1.2. Antecedentes a nivel nacional

Celis (5),en el año 2018, en su tesis titulada Plan de Seguridad de la Información Aplicado a la Central Hidroeléctrica Carhuaquero, manifestó que el Plan de Seguridad compromete la organización de los procesos de la citada Unidad, puesto que la correcta gestión de seguridad de la información puede marcar la diferencia entre la eficacia y la inoperancia. En cuanto a la metodología utilizada debemos señalar que después de una sutil comparación con las ya existentes en este campo, se optó por aquella denominada MAGERIT; la misma que permitió el análisis y gestión de riesgos. También, se utilizó la herramienta EAR-PILAR que ayudó en la toma de las mejores decisiones frente al problema de seguridad de la información.

Ccesa (6), en su tesis titulada, Diseño de un Sistema de Gestión de Seguridad de la Información Bajo la NTP ISO/IEC 27001:2014 Para la Municipalidad Provincial de Huamanga en el año 2016,sostiene que la información es considerada hoy en día el mayor activo que posee cualquier organización y en consecuencia requiere de una protección adecuada. En el Perú, con el objetivo de establecer una adecuada gestión de la seguridad de la información que ayude a

preservar la confidencialidad, integridad y disponibilidad de la misma, se exige a las entidades públicas integrantes del sistema nacional de informática la implementación de la Norma Técnica Peruana NTP ISO/IEC 27001:2014 (Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información), pero el desconocimiento por parte de la alta dirección, la falta de presupuesto y falta de personal especializado ha ocasionado que no se cumplan con el cronograma establecido por el estado para su implementación.

García (7) ,en el año 2016,en su tesis titulada "Implementación de un Sistema de Gestión de Seguridad de la Información, Aplicado a los Riesgos Asociados a los Activos de Información en la Empresa Net – Consultores S.A.C", tiene como objetivo fundamental, diseñar un SGSI para la empresa NET- Consultores bajo la Norma ISO/IEC 27001 con el fin de clasificar la información, identificar vulnerabilidades y amenazas en el área de informática; valorar los riesgos y con base en estos definir controles y políticas de seguridad que deben ser de conocimiento de la empresa, instrucciones de los procedimientos a realizarse y la v documentación que se debe desarrollar en todo el proceso para la posterior implementación del SGSI, aplicando el modelo PDCA (Planificar, hacer, verificar y actuar).

2.1.3 Antecedentes a nivel regional

Vegas (8), en el año 2019,en 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",sostiene 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 audibilidad de la información. 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 (9) , en el año 2018,en 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, indico que la presente tesis fue desarrollada bajo la línea de investigación en tecnología de la información y comunicación, 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; 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.

Agurto (10), en el año 2017 , en su tesis titulada Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001,manifestó que esta investigación tuvo como objetivo elaborar un diagnóstico de los activos de información, donde se planteó como tema de investigación debido que el área QHSE es la encargada de la estandarización y ejecución de procedimientos del estándar ISO 9001, generando gran cantidad de información la cual está expuesta a deteriorarse, perderse, ser modificada o llegar a manos de la competencia, ya que para la ISO 27001, en toda empresa, el activo fundamental es su información. Se realizaron constantes reuniones con los colaboradores del área de logística e informática y el área QHSE para identificar y valorar los activos de información de los procesos implementados bajo la norma ISO 27001, se utilizaron cuestionarios y listas de cotejo para cada dimensión según la norma ISO 27001, obteniendo resultados que el 58% de fuga de documentación especializada es de manuales, procedimientos, documentación técnica, por debajo con el 33% otra de la fuga de documentación es por las incidencias en información de carácter personal. En conclusión, luego de realizar dicha investigación se

propuso elaborar la propuesta técnica, en la que incluyen los controles de seguridad basada en la norma ISO 27001, acorde con los procesos implementados por el estándar ISO 9001.

2.2. Bases teóricas

2.2.1. Información de la empresa

2.2.1.1. Definición municipalidad

Según Pantoja y Muñoz (11), Las municipalidades son corporaciones autónomas de derecho público, con personalidad jurídica y patrimonio propio, cuya finalidad es satisfacer las necesidades de la comunidad local y asegurar su participación en el proceso económico, social y cultural de las respectivas comunas.

Las municipalidades forman parte del sector público, en calidad de servicios descentralizados. Las municipalidades son una rama de la Administración del Estado. Las municipalidades son servicios públicos territorialmente descentralizados, dotados de personalidad jurídica y patrimonio propios (11).

Municipalidades y desarrollo económico local

Un primer abordaje proviene de los enfoques o modelos económicos que se discuten para el desarrollo latinoamericano y que se pueden aplicar en el ámbito local. Esta entrada nos remite a una pregunta: ¿debe o no

intervenir el gobierno municipal en el desarrollo económico local? Quiénes adopten la postura neoclásica, neoliberal ortodoxa, sostendrán que no, que el municipio –en tanto parte del Estado- debe intervenir lo menos posible en el desarrollo económico y dejar que las fuerzas del mercado estimulen el desarrollo (12).

La otra posición –tradicional en la economía de la política latinoamericana –plantea que las fuerzas liberadas del mercado generan fuertes desequilibrios económicos y sociales, y que el Estado debe intervenir en este proceso. Por lo tanto, el municipio también debe participar en el desarrollo económico local, crear empresas municipales y regular el desarrollo económico; es decir, intervencionismo. Esas son las dos posiciones extremas, pero ello admite mucha discusión. Como en todo, la verdad está en el medio. En efecto, el mercado genera desequilibrio, distorsiones y también progreso; se hace indispensable algún grado de intervención. Para no situarnos en los extremos es importante un punto de equilibrio (12).

La posición de las Naciones Unidas es la concepción del desarrollo. Esta concepción, desarrollada por el programa de las Naciones Unidas para el Desarrollo(PNUD)de Lima, no se contrapone, sino que es bastante similar a la postura que hemos asumido y a la estrategia de competividad. Entre esos dos extremos-dejar funcionar libremente el mercado e intervenir en la economía-, el municipio puede optar por una estrategia de promoción del desarrollo humano. El desarrollo humano, en términos de la propuesta elaborada

por el PNUD, esta medido en un índice. Este índice se publica anualmente en los informes de este organismo, que en su formulación básica incluye tres variables: ingresos reales, esperanza de vida y escolaridad (12).

La combinación de estas tres variables permite formular una estrategia apropiada de desarrollo. Los municipios deberíamos garantizar el desarrollo humano. Esto quiere decir que deberíamos garantizar el acceso a los recursos para generar empleo, ingresos, acceso a la salud para incrementar la esperanza de vida y a la educación, al conocimiento. Para garantizar el acceso a estas tres condiciones el municipio tiene que promover el desarrollo económico. Éste es un enfoque y un tema por discutir cuando analizamos el desarrollo económico local (12).

Las municipalidades y su regulación en la ley peruana

Según Dávila (13), indico que:

De acuerdo a la nueva ley Orgánica de Municipalidades Nº27972, promulgada el 256 de mayo del año 2003, las municipalidades o gobiernos locales son entidades básicas de la organización territorial del Estado y canales inmediatos de participación vecinal en los asuntos públicos, que institucionalizan y gestionan con autonomía los intereses propios de las correspondientes colectividades. Sus elementos esenciales son el territorio, la población y la organización.

Conforme al artículo I del Título Preliminar de la nueva Ley Orgánica de Municipalidades, éstas pueden ser Provinciales y/o Distritales y están encargadas del gobierno local. Asimismo, cuentan con autonomía política, económica y administrativa. En el caso de las Municipalidades Delegadas, este nuevo texto legal difiere del marco establecido en la Constitución Política vigente que en el artículo 191º les otorga el carácter de órgano de gobierno local, así como la autonomía antes referida, lo que en la nueva Ley Orgánica se entiende reservado únicamente a las Provincias y Distritales.

La consecuencia de esta discrepancia normativa tendría efectos concretos en el estatus reservado por la Constitución a las Municipalidades Delegadas, que, según la nueva LOM pasaría a ser una especie de agencia municipal con ciertos privilegios económicos correspondiente a un centro poblado menor (ley 27972) (13).

Por lo tanto, este texto va en contra del espíritu de la Constitución del 93 que busca que poblaciones significativas, poblacional y económicamente hablando puedan regular sus propios servicios, administrar sus recursos, solucionar sus problemas y alcanzar sus propias aspiraciones por medio de la autonomía sin necesidad de ser un Municipio legalmente reconocido. En conclusión, el artículo I del Título Preliminar de la Ley 27972 tendría el carácter de inconstitucionalidad y procedería, por lo tanto, el planteamiento de una acción de inconstitucionalidad

conforme el artículo 200º numeral 4 de la Constitución política vigente (13).

Por su jurisdicción, las Municipalidades se clasifican según la Ley en (13):

a) Municipalidad Provincial, cuya jurisdicción es el territorio de la respectiva provincia y los distritos de la misma.
b) Municipalidad Distrital, cuya jurisdicción es el territorio del distrito.
c) Municipalidad de Centro Poblado, cuya jurisdicción la denomina el respectivo concejo provincial, a propuesta del Consejo Distrital.

Asimismo, por su ámbito las municipalidades pueden ser "Urbanas "y "Rurales".

2.2.2. Municipalidad Investigada

A. Ubicación

Dirección: Jr. Leoncio Prado Nro. S/n

Distrito: Suyo

Provincia: Ayabaca

Teléfono:(073) – 703439

Grafico Nro.1: Ubicación de la municipalidad Distrital de Suyo

Fuente: Municipalidad Distrital de Suyo (14).

B. Historia

La historia organizacional de la Municipalidad Distrital de Suyo (14), se inicia 02 de enero del año 1857 con la creación del distrito de Suyo por el gobierno del presidente Ramón castilla. El 10 de enero del año de 1829, Descansa en SUYO, el Batallón "Callao" al mando de Agustín Gamarra, quien participó en la Gran Colombia por la independencia del Perú. Por ese tiempo llego también el General José De La Mar. 02 de abril de 1895 Nace en el fundo de San José Del Quiroz en SUYO, Manuel Vegas Castillo, destacándose en el campo de la Historia. Es

autor de “Bronces de Históricos”; “Los Ayabaca en la Época Prehistórica”. El 01 septiembre del año 1913 Se reconstruye la Iglesia del Pueblo de Suyo y se adquiere un melódico para ella; según Ley N.º 1877 de esa Fecha. El 30 de abril del año 1968 Se crean las ligas de deportivas de Ayabaca, Frías, Montero y Suyo. En 1987 Apertura del Canal Anchalay Morocho- Suyo.

El Concejo Municipal de Suyo, dentro del proceso de reorganización administrativa y de reestructuración orgánica a que ha sido sometida la Municipalidad en aplicación de la Ley N° 27658, Ley Marco de Modernización de la Gestión del Estado, viene implementando y actualizando los instrumentos normativos de nivel institucional, en concordancia con lo dispuesto por las normas generales de los sistemas administrativos y de control, poniendo en manos de su personal este Manual de Organización y Funciones (MOF), para su aplicación, documento que es susceptible de perfeccionamiento en la medida en que se produzcan cambios en la legislación, y cuando los resultados de su ejecución así lo exijan.

Autoridades 2019-2022:
Alcalde: Edar Troncos Ojeda

Regidores:

Ewduar Soto Chinchay
Santos Ludeña Culquicondor
Ronal Ramirez Estrada
Carlos Gonzales Samaniego
Rosmery Juarez Merino (14).

C. Visión

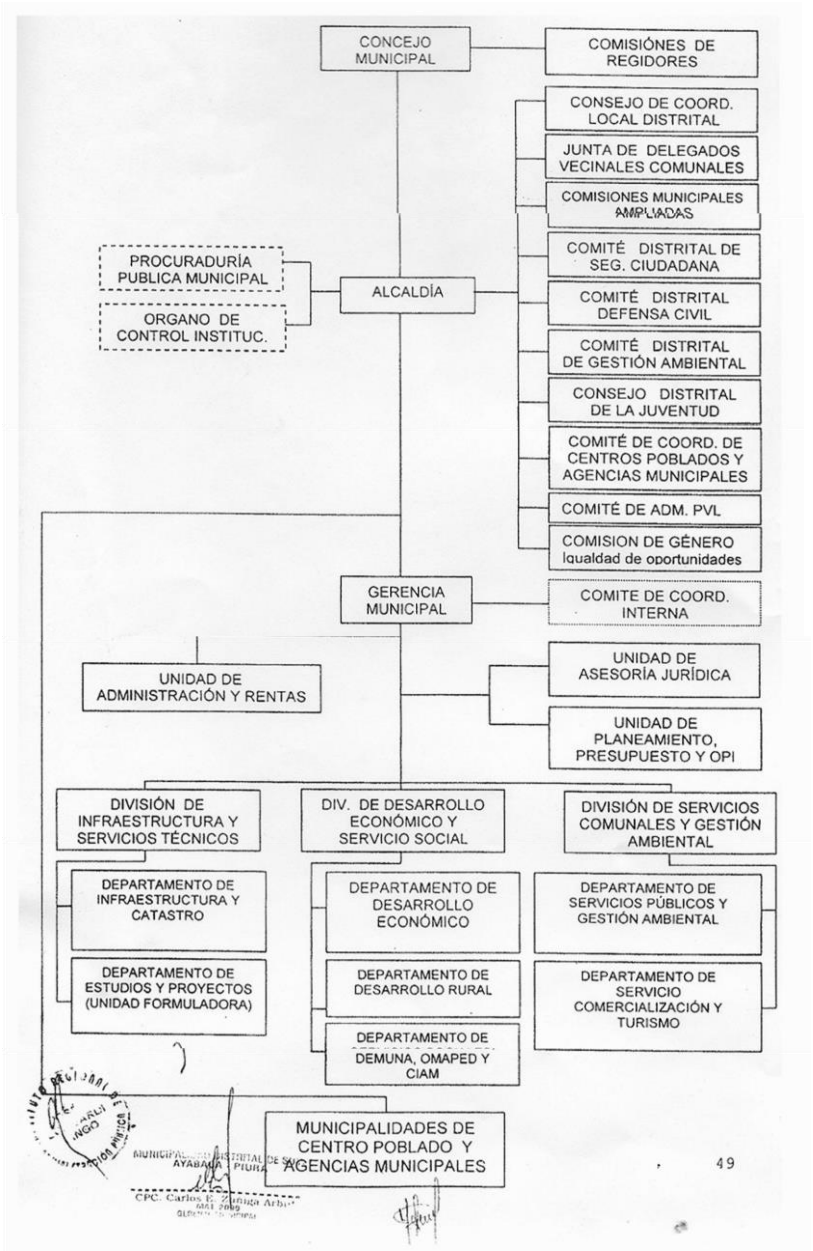
Constituirse en una municipalidad líder del desarrollo distrital y modelo de transparencia, eficiente, eficaz y efectiva en la distribución de su presupuesto, promotora de la participación ciudadana, que contribuye a mejorar los servicios básicos y el nivel de calidad de vida de los vecinos, incidiendo en la difusión de la cultura, así como en la promoción del desarrollo agrario y educativo. Contar con personal capacitado y con áreas equipadas con tecnología adecuada y con ciudadanos organizados participativos y concertadores. En este marco, las autoridades del Gobierno Local actúan con transparencia y generan confianza en la población (14).

D. Misión

La Municipalidad Distrital de Suyo tiene como misión constituirse en una institución pública eficiente y organizada al servicio de la comunidad, que busca contribuir con el desarrollo humano sostenible de nuestro distrito, brindando servicios de mejor calidad, promoviendo la participación de los ciudadanos, ofreciendo una atención inclusiva. Especialmente para los más necesitados y desprotegidos (14).

E. Organigrama

Grafico Nro.2:Organigrama Institucional



Fuente: Municipalidad distrital de suyo (14).

F. Infraestructura Tecnológica

La municipalidad cuenta con la siguiente infraestructura (14):

Tabla Nro. 1: Infraestructura Tecnológica

Tipo de tecnología	**Descripción**
Hadware	20 laptops
	4 servidores
	12 impresoras
	6 routers
	5 switchs
	70 equipos de computo
SOFTWARE	Windows 10, Windows Server 2012 R2, SQL Server, Office 2013.
APLICATIVOS	HI , Eqhali, SIGA, SIAF,SISDEMUNA.
CONECTIVIDAD	Cableada, wifi.

Fuente: Elaboración Propia.

2.2.3. Las TIC

Definición de las Tic

Según Estrada (15),puede enunciar que las tics pueden verse como soportes comunicacionales e informativos de los conocimientos y experiencia humana (acumulada, enriquecida y renovada constantemente), que a través de la electrónica como tecnología base, que sustenta el progreso de las telecomunicaciones, la informática y el audiovisual; potencian la comunicación y la compresión humana, estableciendo una redefinición radical del funcionamiento actual y futuro de la sociedad, de modo interconectado y complementario. La electrónica como base tecnológica y del conocimiento actual, constituye en sí, el sustento de la estructura en red de la comunicación, y posibilita no ya un cambio, sino una renovación constante y acelerada del funcionamiento global de la sociedad en todos sus ámbitos e interconectividades.

Según Azinian (16) Bajo el rotulo de tecnologías de la información y la comunicación (TIC) se engloba a las computadoras y las redes de comunicación. La computadora, desde el punto de vista físico –o sea del hardware-, puede considerarse como un conjunto de componentes eléctricos que deja pasar selectivamente la corriente eléctrica. Es el componente lógico o software -la aplicación- el que permite utilizarla como herramienta y como medio.

En general, las TIC integran los siguientes elementos (17):

- Hardware o Microelectrónica, que es el soporte físico que ayuda al tratamiento de la información.

- Software o conjunto de programas informáticos.
- Infraestructuras de telecomunicaciones, que se encargan de la transmisión de la información.

Los tres se combinan para proporcionar al usuario servicios a través de diversas aplicaciones. La gama de aplicaciones es, por tanto, una integración de tecnologías cuya finalidad es que el acceso y el uso de los servicios sea intuitivo y sencillo para el usuario, evitando cualquier complejidad tecnológica en el servicio.

Las municipalidades y gobiernos provinciales: un nuevo agente política pública de TIC

De manera casi simultánea con el desarrollo de planes nacionales de las TIC (o agendas digitales), un nuevo fenómeno está ocurriendo en el terreno de políticas públicas del sector. Nos referimos a la participación creciente de municipalidades y gobiernos provinciales en la formulación e implantación de planes tecnológicos con un énfasis regional o local (18).

Estos nuevos agentes de política pública han sido a la luz afectando el entorno el entorno en diferentes niveles. En primer lugar, nos referimos a la competencia gobierno central-gobiernos provinciales y municipales. De acuerdo con este concepto, el gobierno central y los correspondientes provinciales y municipales no actúan al unísono de acuerdo con un proceso perfectamente ordenado "arriba para abajo "(top down), donde las directrices del gobierno central son traducidas en planes locales o regionales. Contrariamente a este proceso, los gobiernos locales y regionales comienzan a disputarle el liderazgo en la formulación de agendas tecnológicas a los gobiernos nacionales.

Esto puede estar guiado por diferentes situaciones y contextos (18).

Principales TIC utilizadas en la Municipalidad

Las principales tecnologías de la información y comunicaciones que utiliza una institución son: Internet, telecomunicaciones básicas (19):

a) **Internet:** Ha supuesto una revolución sin precedentes en el mundo de la informática y de las comunicaciones. Desde el punto de vista técnico, se puede definir internet como un inmenso conjunto de redes de ordenadores que se encuentran interconectadas entre sí, dando lugar a la mayor red de redes de ámbito mundial.

b) **Telecomunicaciones básicas:** En nuestro entorno actual es cada vez más frecuente de telecomunicaciones, tanto públicos como privados, que suponen la transmisión de mayor red de redes de ámbito mundial de extremo a extremo de la información facilitada por los clientes. La prestación de los servicios de telecomunicaciones básicas se realiza: mediante el suministro transfronterizo y mediante el establecimiento de empresas extranjeras o de una presencia comercial, incluida la posibilidad de ser propietario y explotar la infraestructura independiente de redes de telecomunicaciones. Son ejemplos de servicios de telecomunicaciones básicas (19):

- Servicios de teléfono.
- Servicios de transmisión de datos con conmutación de paquetes.

- Servicios de transmisión de datos con conmutación de circuitos.
- Servicios de telégrafo.
- Servicios analógicos/digitales de telefonía móvil.

2.2.4 La Tecnología de la Investigación

Auditoria

Según Soy (20), indico la siguiente definición:

El término «auditoría» lo asociamos de forma genérica a diferentes expresiones o conceptos: proceso, misión, función, profesión, informe, balance, diagnóstico, evaluación, etc. Auditar es sinónimo de revisar, inspeccionar, controlar o verificar. Podemos referirnos a tantas clases de auditorías como tipos diferentes de revisiones y objetivos asociados existen: de estados financieros históricos de una sociedad mercantil o administración pública, de una operativa, de una función, etc., si bien la auditoría más conocida y aplicada es la auditoría contable o financiera. Una definición de auditoría que creemos que expresa este espíritu la aporta Jonquières (2010): «La Auditoría no es un examen para aprender a sortear trampas y preguntas molestas, es una herramienta para analizar en profundidad el funcionamiento de la empresa y orientar su actuación a la mejora del desempeño. “Para realizar una auditoría es necesario disponer de información verificable y de algunas normas o criterios sobre cuya base el auditor debe poder evaluarla.

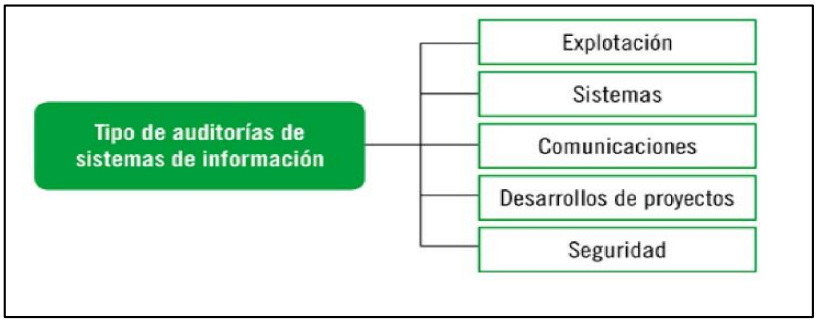
La auditoría es revisar que los hechos, fenómenos y operaciones se den en la forma en que fueron planteados, que las políticas y procedimientos establecidos se han observado y respetado. Es

evaluar la forma en que se administra y opera para aprovechar al máximo los recursos (21).

Tipos de Auditorias dentro de los sistemas de Información

Según Chicano (22), Dentro del área de los sistemas de información, se puede encontrar varias divisiones, descritas en el gráfico:

Grafico Nro.3:Tipo de Auditorias de Sistemas de Información



Fuente: Chicano (22).

Auditoria informática de explotación

La auditoría informática de explotación de se encarga de analizar resultados informáticos de todo tipo: listados impresos, ordenes automatizados de procesos, etc. El análisis consistiría sobre todo en someter los resultados obtenidos a controles de calidad y en analizar si su distribución posterior (al cliente, a otros empleados, a superiores, etc.) se realiza mediante un proceso adecuado. También se auditan las distintas secciones que componen la informática de explotación y las relaciones existentes entre ellos.

Auditoría informática de sistemas

La auditoría informática de sistemas se encarga de analizar las actividades relacionadas en el entorno de sistemas informáticos. Más concretamente, en esta tipología se analizan los siguientes componentes:

- **Sistemas operativos:** se si están actualizados los y, en caso de no estarlo, se averiguan las causas de la desactualización. También se analizan posibles incompatibilidades de software ocasionados por el sistema operativo.

- **Software básico:** se analizan las distintas aplicaciones instaladas para verificar que no agreden ni condicionan al sistema operativo.

- **Tunning:** se evalúan las distintas técnicas y medidas de evaluación de los comportamientos del sistema y de los subsistemas.

- **Optimización de los sistemas y subsistemas:** la auditoria comprobará que las acciones de optimización de sistemas y subsistemas son efectivas y que no se compromete su operatividad.

- **Administración de las bases de datos:** el auditor se asegurará del conocimiento de los distintos procedimientos de la base de datos y comprobará la seguridad, la integridad y la consistencia de los datos.

- **Investigación y desarrollo:** la auditoria se encargará de mantener la actividad de investigación y desarrollo, impidiendo que por estas se dificulten procesos y tareas fundamentales.

Auditoria informática de comunicaciones y redes

La auditoría informática de comunicaciones y redes se encargará de analizar los distintos dispositivos de comunicación que forman parte de las redes de la organización para detectar sus debilidades y proponer medidos que las corrijan. Para ello los auditores deberán conocer la topología de la red de comunicaciones, en las que se describan con detalle las líneas que forman parte de ella, cómo son y su ubicación para comprobar su nivel de operatividad

Auditoria de desarrollo de Proyectos

En la auditoria de desarrollo de proyectos, los auditores informáticos analizan la metodología utilizada para desarrollar los distintos proyectos de la organización, distinguiendo entre cada área de negocio de la empresa. También se analiza el desarrollo de proyectos globales que se extienden al conjunto de la organización, comprobando su correcta ejecución y el mantenimiento de la seguridad a lo largo de todo el proceso.

Auditoria de seguridad informática

La auditoría de seguridad informática analiza todos los procesos referentes a la seguridad informática, tanto física como lógica. La seguridad física es la protección de los componentes hardware, dispositivos, instalaciones y entornos de los distintos sistemas informáticos. Los auditores deberán analizar la correcta protección de los elementos físicos ante posibles catástrofes, incendios, robos, etc.

La seguridad lógica, por el contrario, es la protección del software, los procesos y programas del sistema, y su auditoria

consistirá en analizar la correcta protección y actualización de estos componentes, además de la protección y actualización de estos componentes, además de la protección de los datos que forman parte del sistema.

Seguridad informática

La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable (23).

Tipos de seguridad

Activa

Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema. Ejemplos: impedir el acceso a la información a usuarios no autorizados mediante introducción de nombres de usuario y contraseñas; evitar la entrada de virus instalando un antivirus; impedir, mediante encriptación, la lectura no autorizada de mensajes (23).

Pasiva

Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su percusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos (23).

Mecanismos de seguridad

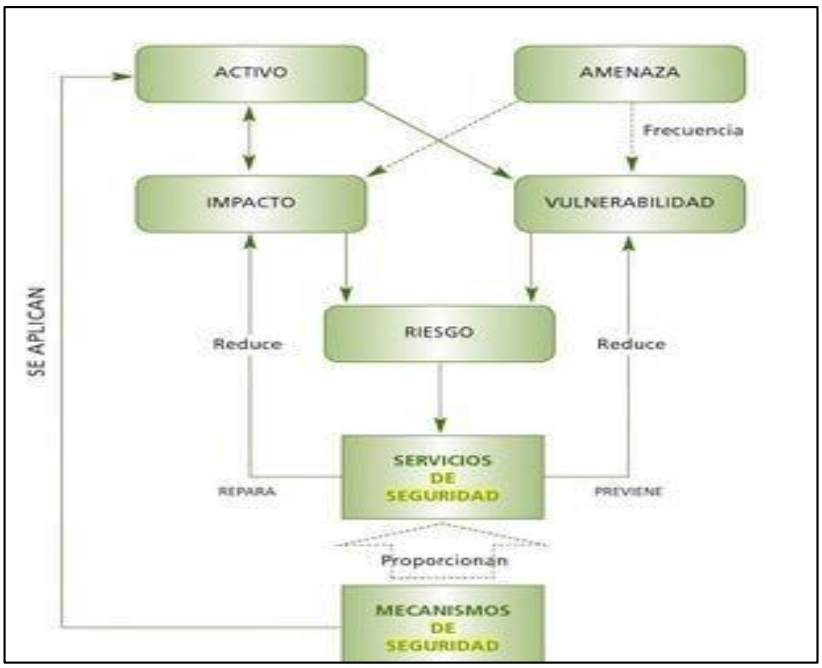
Según la función que desempeñan los mecanismos de seguridad pueden clasificarse en (23):

- **Preventivos.** Actúan antes de que se produzca un ataque. Su misión es evitarlo.

- **Detectores.** Actúan cuando el ataque se ha producido y antes de que cause daño en el sistema.

- **Correctores.** Actúan después que se haya habido un ataque y se hayan producido daños. Su misión es la de corregir las consecuencias del daño.

Grafico Nro.4:Relación entre mecanismos y servicios de seguridad



Fuente: Aguilera (23).

Objetivos

Los objetivos principales de la seguridad informática son proteger el sistema informático, tanto como la información, como los equipos en sí, así como los usuarios del sistema (24):

- **Información:** La información es esencial dentro de cualquier sistema informático, ya sea para defender su integridad como su privacidad. Por integridad entendemos evitar su perdida, y por privacidad el que cualquier persona no autorizada puede acceder a ella y hacer un mal uso de la misma.

- **Equipos físicos:** Aquí se hace referencia a que la parte física del sistema no se estropee, ya sea por un ataque físico, así como por causas accidentales.
- **Usuarios:** Dentro del sistema informático y de su seguridad una parte primordial es asegurar los usuarios, como los usuarios no autorizados, para para lo que se utilizan perfiles de usuario, restricciones físicas de acceso a ciertos lugares.

La Norma UNE-ISO/IEC 27001

Origen de la Norma

Para Gómez y Andrés (25), ISO (Organización Internacional de Normalización) e IEC (Comisión Electrotécnica Internacional) constituyen el sistema especializado para la normalización a nivel mundial. Los organismos nacionales que son miembros de ISO o IEC participan en el desarrollo de las normas internacionales a través de comités técnicos establecidos por las organizaciones

respectivas para realizar acuerdos en campos específicos de la actividad técnica. Los comités técnicos de ISO e IEC colaboran en los campos de interés mutuo.En el campo de la tecnología de la información, ISO e IEC han establecido un comité técnico conjunto, el denominado ISO/IEC JTC 1 (Joint Technical Committee 1). Los borradores de estas normas internacionales, adoptadas por la unión de este comité técnico, son enviados a los organismos de las diferentes naciones para su votación. La publicación como norma internacional requiere la aprobación de, por lo menos, el 75% de los organismos nacionales que emiten su voto.

Una vez que fue publicada la Norma ISO/IEC 17799-1 (actualmente se corresponde con la Norma ISO/IEC 27002), Reino Unido (BSI) y España (AENOR) elevaron al comité internacional sus normas nacionales sobre las especificaciones de los sistemas de gestión de la seguridad de la información (SGSI), BS 7799-2 y UNE 71502 respectivamente, siendo estas normas el origen de lo que finalmente acabo publicándose como norma internacional ISO/IEC 27001 en el año 2005, que fue adoptada como norma Española UNE-ISO/IEC 27001 en el año 2007, tras un periodo de convivencia con la norma anteriormente mencionada (25).

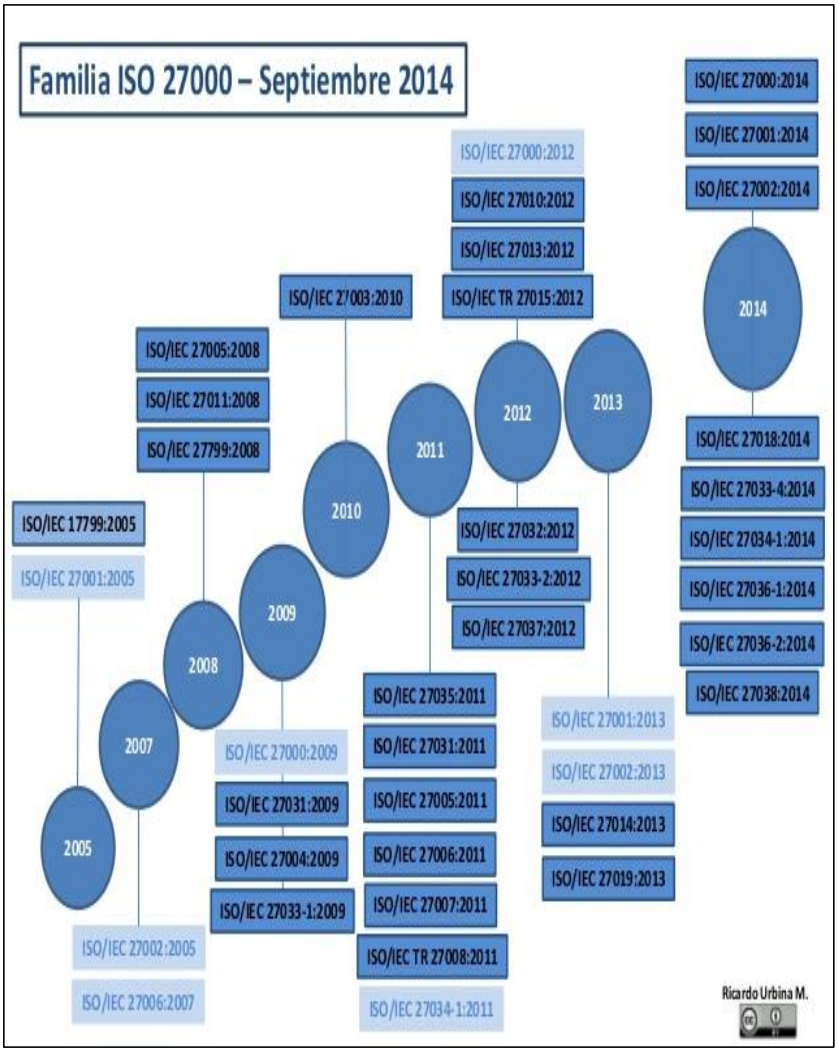
NTP-ISO/IEC 27001:2014

La presente norma Técnica Peruana ha sido elaborada por el comité técnico de normalización de codificación e intercambio electrónico de datos, mediante el sistema 1 o de adopción, durante los meses de Abril a junio del 2014,utilizando como

antecedente a la norma ISO/IEC 27001:2013 Information Technology-Security techniques-Information security management systems-Requeriments y la ISO/IEC 27001:2013/COR 1 2013 Information Technology-Security techniques –Information security management systems-Requirements. El comité Técnico de Normalización de Codificación e intercambio electrónico de datos presento a la comisión de Normalización y de Fiscalización de Barreras Comerciales no Arancelarias -CNB-, con fecha 2014-08-19,el PNTP-ISO/IEC 27001:2014,para su revisión y aprobación, siendo sometido a la etapa de discusión pública el 2014-10-18.No habiéndose presentado observaciones fue oficializada como Norma Técnica Peruana NTP-ISO/IEC 27001:2014 Tecnología de la Información .Técnicas de Seguridad. Sistemas de gestión de seguridad de la información. Requisitos, 2ª Edición, el 01 de diciembre de 2014 (26).

Esta Norma Técnica Peruana reemplaza a la NTP-ISO/IEC 27001:2018(revisada el 2013) y es una adopción de la norma ISO/IEC 27001:2013 y de la ISO/IEC 27001:2013/COR 1.La presente Norma Técnica Peruana presenta cambios editoriales referidos principalmente a terminología empleada propia del idioma español y ha sido estructurada en concordancia a las Guias Peruanas GP 001:1995 Y GP 002:1995 (26).

Grafico Nro.5:Evolución de la norma



Fuente: Urbina (27).

Comprender la Norma UNE-ISO/IEC 27001

La seguridad no es el resultado de un proceso, es un proceso en sí mismo. Se conseguirá un nivel de seguridad aceptable en la medida en que este proceso funcione y progrese adecuadamente (25).

No es de extrañar, por tanto, que la Norma UNE-ISO/IEC 27001 exija que se adopte un proceso para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI en una organización. Es decir, hay que diseñarlo, ponerlo en marcha, comprobar que se obtienen los resultados esperados y, en función de esa evaluación, tomar acciones para corregir las desviaciones detectadas o intentar mejorar la situación, en este caso, la seguridad de la información. Y todo ello de una manera ordenada y metódica, mediante un proceso (25).

El ISO /IEC 27001 va acompañado, además, de una serie de documentos que lo complementan, siendo alguno de los más significativos los siguientes (28):

- **ISO /IEC 27000:** Un vocabulario estándar para las normas de un SGSI, el único documento gratuito de la familia.

- **ISO /IEC 27002:** Un código de buenas prácticas para la gestión de la seguridad de la información. Ayuda a poner en marcha las practicas necesarias para cumplir los requisitos exigidos para la certificación ISO /IEC 27001.

- **ISO /IEC 27004:** Un nuevo estándar sobre métricas de gestión de seguridad de la información.

- **ISO /IEC 27005:** El estándar propuesto para gestión de riesgos.

- **ISO /IEC 27006:** Una guía para el proceso de registro y certificación.

- **ISO /IEC 27007:** Una guía para hacer auditoria de un SGSI.

PROCESO DE CERTIFICACIÓN

Según Gómez (29), El proceso de certificación debe ser realizado por una entidad y competente capaz de determinar si un determinado SGSI es correcto, y lo confirma mediante el correspondiente certificado por escrito.

La certificación constituye un reconocimiento al trabajo bien hecho, una garantía de "calidad de la seguridad", que aporta beneficios para la propia organización, sus clientes, inversores y empleados. Sin embargo, la adaptación a la norma no garantizada la inmunidad total de la organización frente a problemas de seguridad, pero permite reducir el riesgo. Conviene recordar, una vez más, que la seguridad total no existe. El proceso de certificación consta de dos grandes etapas (29):

- **Consultoría:** un equipo de consultores con experiencia en la norma ayuda a la organización a cumplir con los requisitos de certificación: Políticas de Seguridad, procedimientos, selección e implantación de controles, etcétera. En esta etapa será necesario determinar las acciones correctivas (que eliminan la causa de las no conformidades en la implantación, operación y uso del SGSI) y las acciones preventivas (que permiten eliminar la causa de no conformidades potenciales, previniendo su ocurrencia).

- **Auditoria:** un organismo acreditado, como AENOR en España, España, se encarga de revisar los distintos procesos y procedimientos de gestión de seguridad exigidos por la norma, así como de revisar la implantación de los distintos controles seleccionados. Una de las instituciones de referencia a nivel internacional en auditoria de los sistemas de Información es ISACA (Information systems Audit and Control

AssociationAsociacion para el control y la Auditoria de los Sistemas de Información-).

Requisitos de la Norma UNE-ISO/IEC 27001

Contexto de la organización

Sistemas de gestión de seguridad de la información

Según Gómez y Fernández (30)**,** manifiestan, Aunque podría pensarse que un sistema de gestión está orientado a grandes empresas, precisamente son las pequeñas organizaciones las que más pueden beneficiarse de los mismos, ya que aportan un conjunto de conocimiento y normas que de otra no estarían a su alcance. No obstante, es importante conocer la organización y su contexto, de manera que la definición del sistema de gestión tenga en cuenta los propios objetivos de negocio de la organización, con los que debería alinearse la gestión de la seguridad de la información.

Cuando una organización quiere cumplir los requisitos de la norma UNE-ISO/IEC 27001, debe demostrar la efectiva implantación de los apartados 4 al 10, que son los que conforman el cuerpo principal de la norma (30):

a. Contexto de la organización

b. Liderazgo.

c. Planificación.

d. Soporte.

e. Operación.

f.Evaluación del desempeño.

g. Mejora.

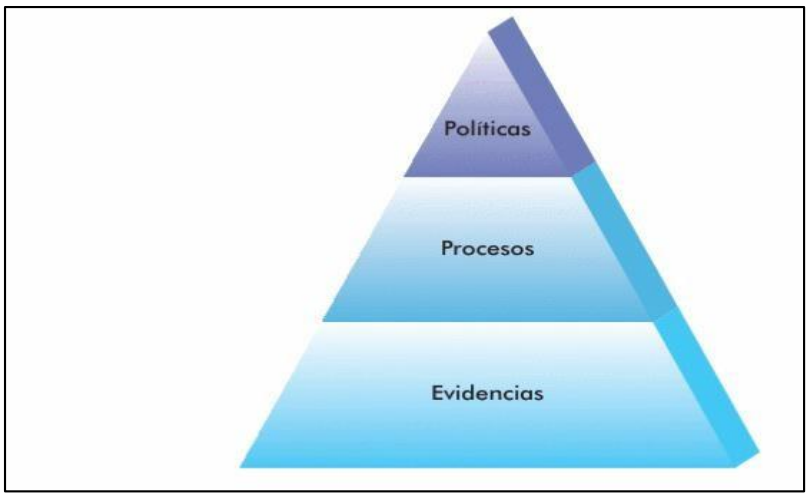
El sistema constará de información documentada en varios niveles (30):

- Políticas, que proporcionan las líneas generales de actuación en cada caso.

- Información documentada sobre procesos (generalmente denominados procedimientos), que proporcionan la descripción de las actividades a ejecutar.

- Información documentada sobre evidencias (anteriormente denominados registros), que permiten demostrar que se han llevado a cabo las actividades previstas.

Grafico Nro.6: Niveles de Organización Documentada



Fuente: Gómez & Fernández (30)**.**

Conocer la organización

Cuando se lleva a cabo la implantación de un sistema de gestión en una organización, es fundamental conocer sus objetivos de negocio y todas aquellas cuestiones externas e internas que pueden favorecer o perjudicar a la obtención de los mismos (30).

El objetivo es que el sistema de gestión favorezca el desempeño de la organización y para eso debe estar alineada con sus objetivos de negocio. En pocas palabras, se debe conocer la organización. Como cuestiones internas se debe considerar, por ejemplo, los recursos financieros o humanos y sus competencias.

Como cuestiones externas se pueden considerar los aspectos políticos, culturales o socioeconómicos que rodean a la organización en su campo de acción, así como las partes interesadas (proveedores, usuarios, competidores, organismos reguladores…) que podrán fijar, legal o contractualmente, los requisitos que afecten al sistema de gestión de seguridad de la información en el que vamos a trabajar (30).

En algunos casos las organizaciones conocen el nivel de seguridad que necesitan, pero estos se encuentran formalizados. Estas necesidades deben establecerse antes de comenzar el diseño del SGSI ya que, con ello, se podrán valorar alternativas y tomar decisiones sobre las más adecuadas (30).

Definición del alcance del SGSI

Se trata de identificar aquellos procesos sobre los que el SGSI va a actuar, no siendo necesario aplicarlo sobre toda la actividad de la organización. A la hora de definir el alcance, se deben tener en cuenta los recursos de los que se dispone, siendo generalmente más practico limitarlo a aquellos procesos o servicios más importantes para la organización y, en posteriores ciclos de mejora continua, ir incorporando el resto. En cualquier caso, es fundamental dimensionar adecuadamente el proyecto para que este tenga éxito (30).

Estructura del modelo

Según Atehortúa, Bustamante y Valencia de los Ríos (31) , El modelo del sistema de gestión de la seguridad de la información ISO 27001 sigue la estructura del PHVA. La planificación inicia con la definición del alcance del SGSI, determinando las áreas o procesos de la organización en los que se va a aplicar el sistema. Generalmente se eligen las áreas más críticas o vulnerables en materia de gestión de la información. Luego de definido el alcance, se debe formular y divulgar una política de gestión de la seguridad de la información, que establezca los lineamientos generales que la organización debe tener en cuenta frente a los riesgos de la información, considerando en ello los requisitos legales, contractuales y propios de la empresa.

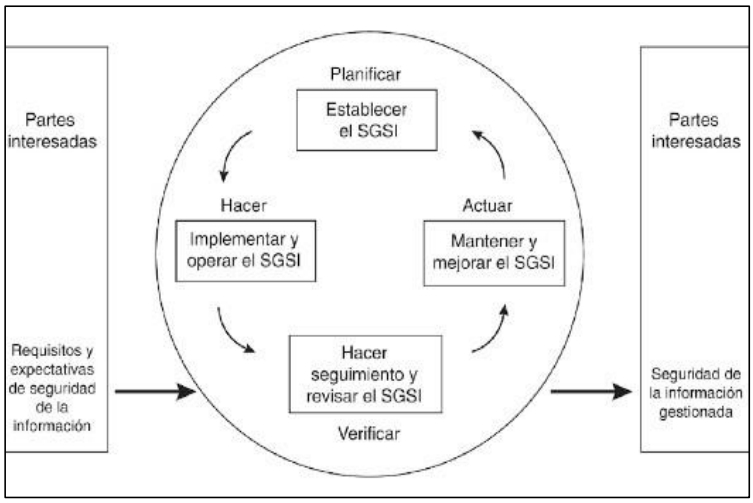
El eje central de la planificación del SGSI consiste en identificar los riesgos de la información, en relación con las posibles

amenazas y los puntos vulnerables de la organización en cuanto a la confiabilidad, seguridad y disponibilidad de la información.

A partir de la identificación de estos riesgos, y de su análisis y valoración, se definirán los planes de control o tratamiento del riesgo, que pretende llevarlo hasta un nivel aceptable o manejable por la entidad. La implementación se fundamenta en poner en práctica estos planes de control o tratamiento del riesgo. Incluye también la documentación y la aplicación de los procedimientos necesarios para aplicar tales controles, así como la formación y la conciencia de los empleados respecto a la seguridad de la información y los controles que se han de aplicar. Un elemento importante es el de definir e implementar planes de detección y respuesta ante incidentes de seguridad de la información, para reducir el impacto que tales incidentes puedan tener en la operación de la organización.

La fase de verificación incluye la medición del desempeño del SGSI, la evaluación de los riesgos y la eficacia de los controles implementados, la realización de auditorías internas al sistema y la revisión del mismo por parte de la dirección. De estas acciones se desprende el mejoramiento, que incluye la actualización de los planes de seguridad y la definición e implementación de las acciones correctivas y preventivas a que haya lugar.

Grafico Nro.7: Modelo del SGSI de la Norma ISO 27001



Fuente: Según Atehortúa& Bustamante& Valencia de los Rios (31).

Existen diferentes metodologías para implementar un SGSI. Veamos algunas (32) :

MAGERIT

Es la sigla de Metodología de Análisis y Gestión de Riesgos de las Administraciones públicas. Es un método formal para investigar los riesgos que soportan los Sistemas de Información, y para recomendar las medidas correspondientes que se deberán tomar para controlar estos riesgos. Es una metodología pública desarrollada por el Ministerio de Administraciones Públicas.

MAGERIT consta de cuatro fases (32):

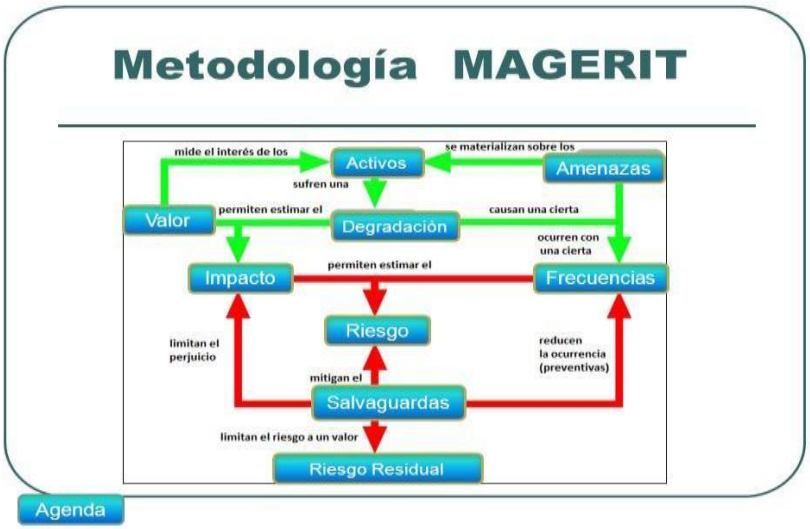
- **Planificación de análisis y gestión de riesgos**: Estimaciones iniciales de los riesgos que pueden afectar al sistema de información y el tiempo y recursos necesarios para su tratamiento.

- **Análisis de riesgos**: realiza una estimación del impacto que tendrán los riesgos de la organización. Esta área es muy importante porque un uso desproporcionado puede afectar negativamente al rendimiento. Es necesario establecer un umbral de riesgo deseable (tolerable) que hay que superar para ser objeto de tratamiento.

- **Gestión del riesgo**: seleccionar posibles soluciones para cada riesgo. Son fundamentales los ejercicios de simulación.

- **Selección de salvaguardas**: Elegir los mecanismos que implementaran las soluciones elegidas en la fase anterior.

Grafico Nro. 8: Metodología Magerit



Fuente: Guagalango & Moscoso (33).

ISO/IEC 27001

La ISO/IEC considera la organización como una totalidad y tiene en cuenta todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que se pueden producir. La mencionada norma está estructurada en once dominios de control que cubren completamente la Gestión de la Seguridad de la Información, donde cada uno de ellos se refiere a un aspecto de la seguridad de la información (32).

- Política de seguridad.
- Aspectos organizativos para la seguridad.
- Clasificación y control de activos.
- Seguridad del personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Gestión de incidentes de seguridad de la información
- Gestión de continuidad del negocio.
- Conformidad legal (32).

En la siguiente figura, puede verse como el objetivo final de la norma ISO 27001 es preservar la disponibilidad, la confidencialidad, la integridad, y el no repudio de la información (34).

Grafico Nro. 9:Enfoque de los controles de la Norma ISO 27001

Fuente: Mantilla (34).

A continuación, por la importancia que tienen estas 11 áreas de control, se detalla a que se refieren cada una de ellas (34):

Política de seguridad

Se necesita una política que refleje las expectativas de la organización en materia de seguridad con el fin subministrar administración con dirección y soporte, la cual también se puede utilizar como base para el estudio y evaluación en curso.

Organización de la seguridad de la organización

Sugiere diseñar una estructura de administración que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

Gestión de activos

Muestra la necesidad de un inventario de los recursos de información de la organización y con base en este conocimiento, asegurar que se brinde un nivel adecuado de protección.

Seguridad de los recursos humanos

Establece la necesidad de educar e informar a los empleados actuales y potenciales sobre lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También determina cómo incide el papel que desempeñan los empleados en materia de seguridad en el funcionamiento general de la CAC o se debe implementar un plan para reportar los incidentes.

Seguridad física y del entorno

Responde a la necesidad de proteger las áreas, el equipo y los controles generales.

Gestión de las comunicaciones y operaciones

Los objetivos de esta sección son:

-Asegurar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información.

-Minimizar el riesgo de falla de los sistemas.

-Proteger la integridad del software y la información.

-Conservar la integridad y disponibilidad del procesamiento y la comunicación de la información.

-Garantizar la protección de la información en las redes y de la infraestructura de soporte.

-Evitar daños a los recursos de información e interrupciones en las actividades de la compañía.

-Evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones.

Control de accesos

Establece la importancia de monitorear y controlar el acceso a la red y los recursos de aplicación para proteger contra los abusos internos e intrusos externos.

Adquisición, desarrollo y mantenimiento de sistemas de información

Recuerda que, en toda labor de la tecnología de la información, se debe implementar y mantener la seguridad mediante el uso de controles de seguridad en todas las etapas del proceso.

Gestión de incidentes de seguridad

Asegura que los eventos y debilidades de seguridad de la información asociadas con los sistemas de información sean comunicados de una manera tal que permita que la acción correctiva sea tomada oportunamente.

Gestión de continuidad del negocio

Aconseja estar preparado para contrarrestar las interrupciones en las actividades de la empresa y para proteger los procesos importantes, en caso de una falla grave o desastre.

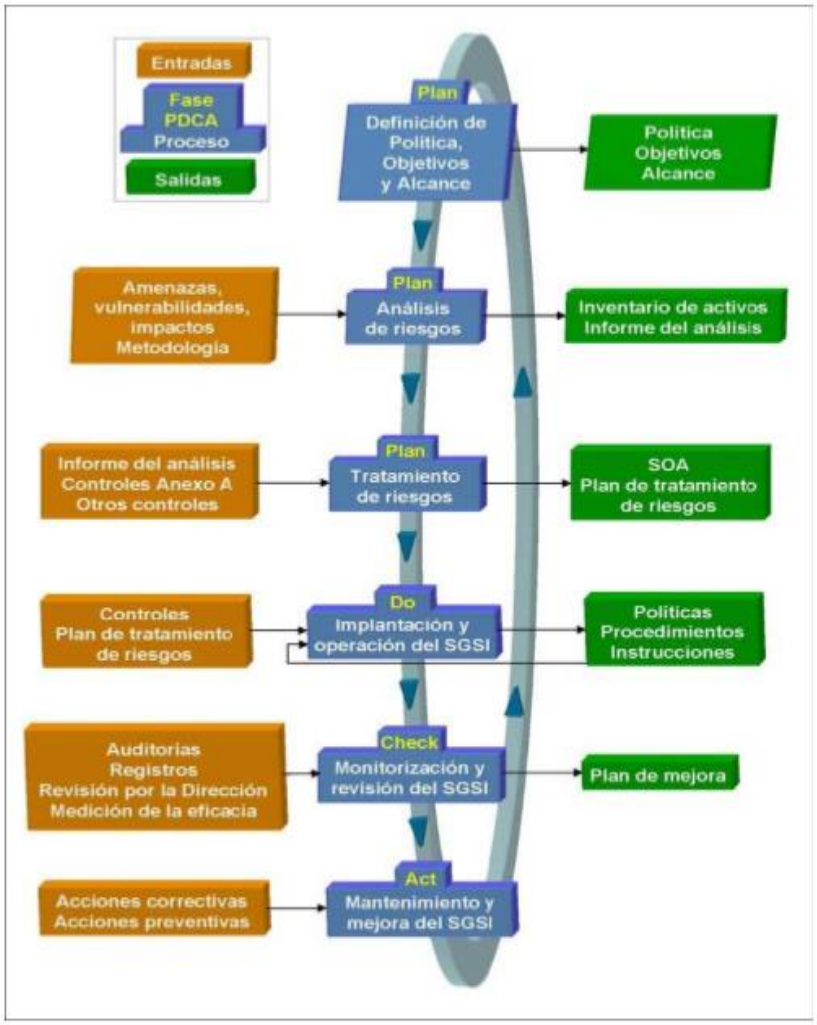
Cumplimiento Normativo (legal, de estándares, técnicas y auditorias)

Imparte instrucciones para que se verifique si el cumplimiento con la norma técnica ISO 27001 concuerda con otros requisitos jurídicos. Esta sección también requiere una revisión a las políticas de seguridad, al cumplimiento y consideraciones técnicas que se deben hacer en relación con el proceso de auditoría del sistema a fin de garantizar que las empresas obtengan el máximo beneficio.

Actividades para alcanzar certificación ISO 27001

Para alcanzar la certificación internacional, las organizaciones deben realizar una serie de actividades, para posteriormente tener un historial de funcionamiento demostrable de al menos tres meses antes de solicitar el proceso formal de auditoria para su primera certificación. El proceso para la certificación debería efectuarse de la manera que indica en la siguiente figura:

Grafico Nro.10: Actividades para alcanzar la certificación ISO 27001 del SGSI



Fuente: Mantilla (34).

III. HIPÓTESIS

La Implementación de Auditoria Informática con la ISO 27001 en la municipalidad Distrital de suyo-Piura, mejorará la seguridad de la información.

IV. METODOLOGÍA

Según Cortés& Iglesias (35), la metodología es la ciencia que nos enseña a dirigir determinado proceso de manera eficiente y eficaz para alcanzar los resultados deseados y tiene como objetivo darnos la estrategia a seguir en el proceso.

Para Sabino (36), la metodología del proyecto incluye el tipo o tipos de investigación, las técnicas los procedimientos que serán utilizados para llevar acabo la indagación. Es el "como" se realizará el estudio para responder al problema planteado.

4.1. Tipo y nivel de la investigación

4.1.1. Tipo de Investigación

El tipo es cuantitativo, según Barragán (37), la investigación cuantitativa es perteneciente o relativo a la cantidad, y de su análisis se determina las porciones de cada elemento analizado.

Uno de los rangos más importantes de la investigación cuantitativa es que opera fundamentalmente con cantidades y que su propósito final es establecer semejanzas y diferencias en términos de proporciones. Esta inquietud, en sus orígenes, ha dado paso al desarrollo de la estadística y dentro de ello la teoría del muestreo (37).

La investigación cuantitativa demanda y/o está obligada a la construcción de una base de datos que generalmente requiere mucho cuidado y disciplina al momento de identificar, levantar, registrar la información.

La validez y confiabilidad de la investigación cuantitativa depende, casi siempre, del método de acercamiento a la fuente de información, de la actitud del investigado frente a la investigación y, definitivamente, del tipo de variables que se hayan definido (37).

4.1.2 Nivel de Investigación

El nivel es descriptivo, para Naghi (38), 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. Se usa un diseño descriptivo para hacer una investigación, cuando el objetivo es:

- Describir las características de ciertos grupos. Por ejemplo, con base en los datos obtenidos de los usuarios de ciertos servicios públicos se quiere desarrollar el perfil de usuarios, "porcentaje de usuarios", respecto a factores demográficos y socioeconómicos.

- Calcular la proporción de gente en una población especifica que tiene ciertas características. Por ejemplo, se requiere calcular la proporción de indígenas del grupo otomí que trabajarán en la industria automotriz.

- Pronosticar, por ejemplo, la venta para los próximos cinco años y usarla como base en la planificación.

4.2. Diseño de la Investigación

El diseño que se utilizó en esta investigación tiene un tipo no experimental, de corte transversal.

Para Sáez (39) , el diseño no experimental hace referencia al proceso de indagación en el que se recogen datos sin intentar inducir ningún cambio. También se le conoce como investigación expost-facto, pues los hechos y variables ya ocurrieron y se observan las variables en su contexto. A partir del objeto del estudio y se procede a la observación de los datos sin la manipulación de variables.

En definitiva, la investigación no experimental se realizas sin manipular las variables independientes, es retrospectiva debido a que se basa en variables de hechos que ya ocurrieron. Se distinguen entre diseños transaccionales (transversales y longitudinales). En la investigación con diseño no experimental a través de diseños transaccionales el estudio se centra en un momento determinado. Pueden ser descriptivos cuando miden y destacan las variables de modo individual y correlaciónales si establecen relaciones entre variables. Estos últimos pueden aportar casualidad entre las variables, en este caso serían correlaciónales/casuales. Por otra parte, los diseños longitudinales, centran el estudio y se llevan a cabo en varios momentos a lo largo del tiempo (39).

Donde:

M=Muestra

O=Observación

4.3. Población y Muestra

4.3.1. Población

Para Tamayo (40), la población "totalidad de un fenómeno de estudio, incluye la totalidad de unidades de análisis o entidades de población que integran dicho fenómeno y que debe cuantificarse para un determinado estudio integrando un conjunto N de entidades que participan de una determinada característica, y se le denomina población por constituir la totalidad del fenómeno adscrito a un estudio o investigación.

La población para esta investigación será un total de 40 trabajadores de la municipalidad de Suyo.

4.3.2. Muestra

Para Gómez (41), la muestra debe ser, en esencia, un subgrupo representativo de la población.

Es un subconjunto de elementos que pertenece a ese conjunto definido por sus características al que llamamos población. Todas las muestras bajo el enfoque cuantitativo deben ser representativas; por lo tanto, los términos "al azar" y "aleatorio "denotan u tipo de procedimiento mecánico para seleccionar unidades de análisis en la población (muestrear), fundamentado en la teoría de las probabilidades, que dará cierta seguridad de que la muestra será representativo de la población.

Tipos de muestra

Básicamente categorizamos las muestras en dos grandes ramas (41):

Las muestras no probabilísticas y las muestras probabilísticas. En estas últimas todos los elementos de la población tienen las mismas posibilidades de ser escogidas. Estas se obtienen a través de una selección aleatoria y mecánica de las unidades de análisis.

En las muestras no probabilísticas, la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o de quien hace la muestra. Aquí el procedimiento no es mecánico, ni con base en fórmulas de probabilidad. Elegir entre una muestra probabilística o una no probabilística depende de los objetos del estudio, del diseño de investigación y de la contribución que se piensa hacer con ella.

Muestras probabilísticas

En las muestras probabilísticas, quizá la principal ventaja sea que puede medirse el error en nuestras predicciones, utilizando la estadística. Se dice incluso que el principal objetivo en el diseño de una muestra probabilística es reducir al mínimo este error, al que se le llama error estándar.

Los elementos muéstrales tendrán valores muy parecidos a los de la población, de manera que las mediciones en el subconjunto nos darán estimaciones precisas del conjunto

mayor. La precisión de dichas estimaciones depende del error en el muestreo.

Para un amuestra probabilística necesitamos principalmente dos cosas: determinar el tamaño de la muestra (n), y seleccionar los elementos muéstrales (unidades de análisis), de manera que todos tengan la misma posibilidad de ser elegidos. Debe destacarse para hacer un muestreo probabilístico, es necesario conocer el listado completo de la población, o universo.

La muestra serán los trabajadores que laboran en el área de informática, definidos de la población, es decir 40 trabajadores ya especificados.

Tabla Nro.2: División de trabajadores de la Municipalidad de Suyo

Personal	Áreas	Cantidad
Nombrados	Registros públicos	5
	Oficina De Control Interno (OCI)	5
	Oficina de OMAPEP	2
Contratados	Of. Procuraduría Pública Municipal	5
	Secretaría General	3
	Oficina De Control Interno (OCI)	5
	Of. De Comunicaciones E Imagen Institucional	4

	Oficina De Desarrollo Económico Rural (Oder)	4
Practicantes	Administrativos, contabilidad, documentarios	6
Total		**40**

Fuente: Elaboración propia**.**

4.4 Definición Operacional de las Variables en Estudio

Tabla Nro.3: Definición Operacional

Variable	Definición Conceptual	Dimensiones	Indicadores	Definición Operacional
Implementación de una auditoria informática con la ISO 27001.	**Seguridad de la Información** Es la protección de la información ante una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo, maximizar el retorno de inversiones y oportunidades de negocio (42) **27001:**	Nivel de conocimiento de la información.	- Sistemas de información. - Norma de Seguridad. - Políticas de seguridad.	En la municipalidad distrital de suyo hay una deficiencia por parte de los trabajadores para cumplir las normas de seguridad informática.
		Seguridad de la información .	- Método para reducir el mal uso de los sistemas.	

	ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización (43)		- Copias de seguridad. - Seguridad en el comercio electrónico.	

Fuente: Elaboración Propia.

4.5. Técnicas e Instrumentos

4.4.1. Técnica

En la presente investigación se aplicaron las siguientes técnicas:

a) Observación Directa: Una de las técnicas más populares, de mayor impacto y más utilizadas para examinar los diferentes aspectos que repercuten en el funcionamiento del área, es la aplicación de diversas técnicas y métodos de observación que permiten recolectar directamente la información necesaria sobre el comportamiento del sistema, del área de sistemas, de las funciones, actividades y operaciones del equipo procesador o de cualquier otro hecho, acción o fenómeno del ámbito de sistemas (44).

b) Encuesta: Según Zapata (45), La encuesta puede definirse como un conjunto de técnicas destinadas a reunir, de manera sistemática, datos sobre determinado tema o temas relativos a una población, a través de contactos directos o indirectos con los individuos o grupo de individuos que integran la población estudiada.

c) Revisión Documental: Esta técnica se utilizó, para la realización del proyecto de investigación, como el apoyo de la información necesaria, por otros autores, es decir tesis, libros, manuales y normativas de empresas, revistas, folletos, Internet, metodologías, con el propósito de obtener una base teórica amplia y citada por sus respectivos autores.

4.4.2. Instrumento

Como instrumento se realizó un cuestionario con sus respectivas preguntas para obtener resultados de dicha investigación.

a) Cuestionario: Para corral (46), este instrumento consiste en aplicar a un universo definido de individuos una serie de preguntas o ítems sobre un determinado problema de investigación del que deseamos conocer algo" puede tratar sobre: un programa, una forma de entrevista o un instrumento de medición. Aunque el cuestionario usualmente es un procedimiento escrito para recabar datos, es posible aplicarlo verbalmente.

Todo cuestionario tiene tres objetivos específicos:

- Traducir la información necesaria a un conjunto de preguntas específicas que los participantes puedan contestar.

- Motivar y alentar al informante para que colabore, coopere y termine de contestar el cuestionario completo, por ello, debe buscar minimizar el tedio y la fatiga.

- Minimizar el error de respuesta, adaptando las preguntas al informante y en un formato o escala que no se preste a confusión al responder.

4.4.3 Procedimiento de recolección de datos

Para realizar este procedimiento de recolección de datos, se realizó una visita al lugar donde se llevaría a cabo el trabajo de investigación, donde se explicó el propósito de la

investigación, para obtener el permiso y realizar una encuesta en este caso sería a los trabajadores de la municipalidad de Suyo, una vez realizada la encuesta se obtiene los resultados del mismo para poder hacer la respectiva tabulación e interpretación de datos.

4.6. Plan de análisis de datos

A partir de los datos que se obtuvieron, se creará una tabulación en el programa Microsoft Excel 2016-hoja de cálculo. El caso describirá el análisis situacional de los procesos, se obtendrán los cuadros y gráficos de las variables de estudio, para establecer las frecuencias y el análisis de distribución de las mismas.

4.7. Matriz de consistencia

Tabla Nro. 4: Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPÓTESIS	METODOLOGÍA
¿La implementación de una auditoria informática con la ISO 27001; mejora la seguridad de información en la Municipalidad Distrital de Suyo-Piura?	**OBJETIVO GENERAL:** Implementar una Auditoria Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura; para mejorar la seguridad de la información. **ESPECÍFICOS:** 1. Identificar los activos de información de los procesos implementados basados en la norma ISO 27001.	La Implementación de una Auditoria Informática con la ISO 27001 en la municipalidad Distrital de suyo-Piura, mejorará la seguridad de la información	- El tipo es cuantitativo. - El nivel es descriptivo. - El diseño de la investigación es no experimental de corte transversal.

	2. Evaluar los riesgos a dichos activos en la municipalidad. 3. Elaborar los controles adecuados de acuerdo a los riesgos identificados.		

Fuente: Elaboración Propia

4.8. Principios éticos

Durante el desarrollo de la presente investigación denominada "Implementación de una Auditoria Informática con la ISO 27001 en la Municipalidad Distrital de Suyo –Piura; 2020" .Han tenido en cuenta el código de ética para la investigación, versión 002 del 2019, el cual tiene por finalidad establecer los principios y valores éticos, de la misma forma del reglamento de sanción por infracción al ejercicio de la investigación Científica y se ha considerado en forma estricta el cumplimiento de los principios éticos que permitan asegurar la originalidad de la Investigación. También se ha considerado respetar los derechos de propiedad intelectual, de los autores de los libros de texto, tesis y de las fuentes electrónicas consultadas, que nos facilitó la información necesaria para estructurar el marco teórico.

De igual manera se ha considerado que gran parte de los datos utilizados son de carácter público, y pueden ser conocidos y aplicados por cualquier investigador sin ningún inconveniente.

Se conserva intacto el contenido de las respuestas, manifestaciones y opiniones recibidas de los trabajadores que han colaborado contestando los cuestionarios. Por último, se ha creído conveniente mantener en reserva la identidad de los mismos con la finalidad de lograr objetividad en los resultados.

V. RESULTADOS

5.1. Resultados

5.1.1. Dimensión 01: Nivel de conocimiento

Tabla Nro. 5: Sistemas de información

Distribución de frecuencia y respuestas relacionadas con un responsable encargado de evaluar la adquisición y cambios de los sistemas de información; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de SuyoPiura;2020.

Respuesta	n	%
Si	24	60
No	16	40
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cuentan la municipalidad con un responsable encargado de evaluar la adquisición y cambios de los sistemas de información?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

Tabla Nro.5 se observa que el 60% de los trabajadores encuestados expresaron que SI cuentan con un responsable encargado de evaluar los sistemas de información, mientras que el 40% indica que NO cuentan con un responsable.

Tabla Nro. 6:Norma de Seguridad

Distribución de frecuencia y respuestas relacionadas con alguna norma relativa para la seguridad de los sistemas de información; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	16	40
No	24	60
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe alguna norma relativa a la seguridad de sistemas de Información?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.6 se observa que el 60% de los trabajadores encuestados opinaron que NO existe una norma relativa de seguridad en la municipalidad, mientras que el 40% dijeron que SI.

Tabla Nro. 7: Políticas de seguridad

Distribución de frecuencia y respuestas relacionadas con políticas de seguridad Informática; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de SuyoPiura;2020.

Respuesta	n	%
Si	18	45
No	22	55
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen políticas de seguridad informática en la municipalidad?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.7 se determina que el 55% de los trabajadores encuestados expresaron que NO existen políticas de seguridad en la municipalidad, mientras que el 45% dijeron que SI.

Tabla Nro. 8: Mecanismos para la comunicación a los trabajadores

Distribución de frecuencia y respuestas relacionadas con mecanismos para la comunicación a los usuarios acerca de las normas de seguridad; para la Implementación de Auditoria Informática con la ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	14	35
No	26	65
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿En la municipalidad existen mecanismos para la comunicación a los trabajadores acerca de las normas de seguridad?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.8 se divisa que el 65% de los trabajadores encuestados dijeron que NO existen mecanismos para la comunicación a los trabajadores acerca de las normas, mientras que el 35% indican que SI.

Tabla Nro. 9: Programas de formación en seguridad

Distribución de frecuencia y respuestas relacionadas con programas de formación en seguridad; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo Piura;2020.

Respuesta	n	%
Si	22	55
No	18	45
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen programas de formación en seguridad para los trabajadores de dicha municipalidad?**,** en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.9 se manifiesta que el 55% de los trabajadores encuestados nos indica que SI existen programas de formación en seguridad, mientras que el 45% nos dice que NO.

Tabla Nro.10: Roles y responsabilidades

Distribución de frecuencia y respuestas relacionadas con roles y responsabilidades definidas para las personas comprometidas en seguridad; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	20	50
No	20	50
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen roles y responsabilidades definidas para las personas comprometidas en la seguridad?**,** en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.10 se muestra que el 50% de los trabajadores encuestados indican que SI existen roles y responsabilidades definidas para las personas comprometidas en la seguridad, mientras que el otro 50% nos indican que NO.

Tabla Nro.11: Confidencialidad de la información

Distribución de frecuencia y respuestas relacionadas de confidencialidad la información; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	N	%
Si	24	60
No	16	40
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿En la municipalidad figuran un acuerdo de confidencialidad de la información a la que accede?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.11 se deduce que el 60% de los trabajadores encuestados expresaron que SI figuran un acuerdo de confidencialidad de la información en la municipalidad, mientras que el 40% indican que NO.

Tabla Nro.12: Proceso Disciplinario

Distribución de frecuencia y respuestas relacionadas de un proceso disciplinario de la seguridad de la información; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	N	%
Si	16	40
No	24	60
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Consta la municipalidad de un proceso disciplinario de la seguridad de la información?**,** en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.12 se deduce que el 60% de los trabajadores encuestados indican que NO constan la municipalidad de un proceso disciplinario de la seguridad de la información, mientras que el otro 40% nos indican que SI consta la municipalidad con un proceso disciplinario.

Tabla Nro.13: Áreas restringidas

Distribución de frecuencia y respuestas relacionadas de áreas restringidas a las cuales solo puede acceder el personal autorizado; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	12	30
No	28	70
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Conoce usted si en la municipalidad existen áreas restringidas a las cuales solo puede acceder el personal autorizado?, en la municipalidad distrital de Suyo Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.13 se interpreta que el 70% de los trabajadores encuestados expresaron que NO existen áreas restringidas en la municipalidad, mientras que el 30% nos indican que SI.

Tabla Nro. 14: Incidente de seguridad

Distribución de frecuencia y respuestas relacionadas de un canal y procedimientos a seguir en caso de incidente de seguridad; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	16	40
No	24	60
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe en la municipalidad un canal y procedimientos claros a seguir en caso de incidente de seguridad?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro. 14 se manifiesta que el 60% de los trabajadores encuestados dijeron que NO existe en la municipalidad un canal y procedimientos a seguir en caso de incidente de seguridad, mientras que el 40% nos dicen que SI.

Tabla Nro. 15: Resumen de la dimensión 01-Nivel de conocimiento de la información

Distribución de frecuencias y respuestas relacionadas con la dimensión 01 nivel de conocimiento de la información; para la Implementación de Auditoria Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	20	50
No	20	50
Total	40	100

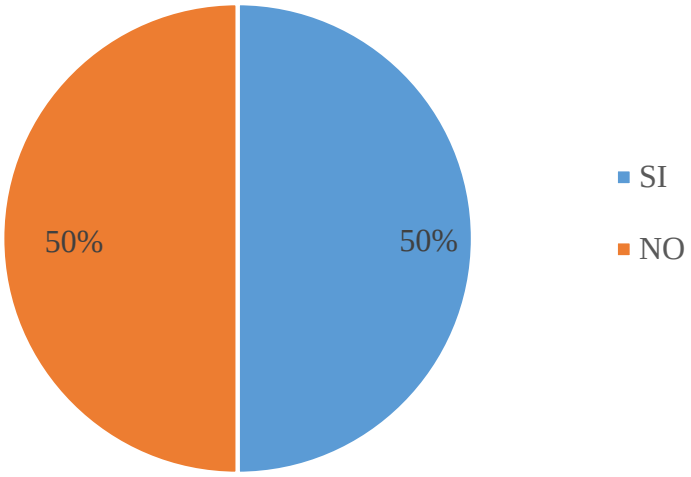
Fuente: Aplicación del instrumento para medir el nivel de conocimiento, basado en 10 preguntas aplicadas a los trabajadores de la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro. 15 se puede interpretar en esta dimensión el 50 % de los trabajadores encuestados contestaron que SI tienen conocimiento acerca de seguridad de la información, mientras que el otro 50% NO tienen conocimiento.

Grafico Nro.11:Resultados de la Dimensión 01

Distribución porcentual de las frecuencias y respuestas relacionadas con la dimensión 01: Nivel de conocimiento; para la Implementación de Auditoria Informática con la ISO 27001 en la Municipalidad distrital de Suyo-Piura; 2020.



Fuente: Tabla Nro.15

5.1.2. Dimensión 02: Seguridad de la información

Tabla Nro.16: Método para reducir el mal uso de los sistemas

Distribución de frecuencia y respuestas relacionadas de un método para reducir el mal uso deliberado de los sistemas; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	18	45
No	22	55
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cuenta la municipalidad con algún método para reducir el mal uso occidental deliberado de los sistemas?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.16 se indica que el 55% de los trabajadores encuestados indicaron que NO cuenta la municipalidad con un método para reducir el mal uso deliberado de los sistemas, mientras que el 45% nos indican que SI.

Tabla Nro.17: Asentadores para la gestión de los sistemas de Información

Distribución de frecuencia y respuestas relacionadas de asentadores externos para a gestión de los sistemas de información; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	16	40
No	24	60
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe asentadores externos para la gestión de los sistemas de información?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro. 17 se enuncia que el 60% de los trabajadores encuestados indicaron que NO existen asentadores externos para la gestión de los sistemas de información, mientras que el 40% nos indican que SI.

Tabla Nro.18: Copias de seguridad

Distribución de frecuencia y respuestas relacionadas de copias de backup para resguardar la información; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	22	55
No	18	45
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Elaboran copias de backup para resguardar la información esencial de la municipalidad?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.18 se manifiesta que el 55% de los trabajadores encuestados expresan que SI elaboran copias de backup para resguardar la información, mientras que el 45% nos indican que NO elaboran.

Tabla Nro.19: Documentación de los sistemas de información

Distribución de frecuencia y respuestas relacionadas de seguridad en la documentación de los sistemas de información; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	20	50
No	20	50
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe seguridad en la documentación de los sistemas de información?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.19 se observa que el 50% de los trabajadores encuestados dijeron que, SI existe seguridad en la documentación de los sistemas de información, mientras que el 50% nos indican que NO existen.

Tabla Nro. 20: Seguridad en el comercio electrónico

Distribución de frecuencia y respuestas relacionadas de medidas de seguridad en el comercio electrónico; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	18	45
No	22	55
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Disponen de medidas de seguridad en el comercio electrónico?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.20 se determina que el 55% de los trabajadores encuestados manifestaron que NO disponen de medidas de seguridad en el comercio electrónico, mientras que el 45% manifiesta que SI.

Tabla Nro. 21: Encriptación de password

Distribución de frecuencia y respuestas relacionadas de encriptación de password de acceso al sistema que utiliza; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	20	50
No	20	50
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existe algún sistema de encriptación de password de acceso al sistema que utiliza?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.21 se determina que el 50% de los trabajadores encuestados indican que, SI existen algún sistema de encriptación de password, mientras que el 50% indican que NO.

Tabla Nro. 22: Capacidad de proceso y almacenamiento de la Información

Distribución de frecuencia y respuestas relacionadas de un plan de capacidad para asegurar adecuada capacidad de proceso y almacenamiento de la información; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	16	40
No	24	60
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Cuenta la municipalidad un plan de capacidad para asegurar la adecuada capacidad de proceso y almacenamiento de la información?, en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.22 se examina que el 60% de los trabajadores encuestados dijeron que NO cuenta la municipalidad de un plan de capacidad para asegurar proceso y almacenamiento de la información, mientras que el 40% indican que SI.

Tabla Nro. 23: Logs

Distribución de frecuencia y respuestas relacionadas de un logs para las actividades realizadas por los operadores y administradores; para la Implementación de Auditoria Informática con las ISO 27001 en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	20	50
No	20	50
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen logs para las actividades realizadas por los operadores y administradores de la municipalidad?**,** en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.23 se deduce que el 50% de los trabajadores encuestados dijeron que SI existen logs para las actividades realizadas, mientras que el 50% indican que NO.

Tabla Nro.24: Control de accesos

Distribución de frecuencia y respuestas relacionadas de una política de control de accesos; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de SuyoPiura;2020.

Respuesta	n	%
Si	16	40
No	24	60
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿En la municipalidad existe una política de control de accesos? en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.24 se manifiesta que el 60% de los trabajadores encuestados indican que NO existe una política de control de accesos, mientras que el 40% indican que SI.

Tabla Nro.25:Controles criptográficos

Distribución de frecuencia y respuestas relacionadas de controles criptográficos; para la Implementación de Auditoria Informática con las ISO 27001en la Municipalidad Distrital de Suyo-Piura;2020.

Respuesta	n	%
Si	12	30
No	28	70
Total	40	100

Fuente: Aplicación del instrumento para medir el conocimiento de los trabajadores encuestados respecto a la pregunta: ¿Existen controles criptográficos en dicha municipalidad?**,** en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.25 se examina que el 70% de los trabajadores encuestados indican que NO existen controles criptográficos, mientras que el 30% indican que SI.

Tabla Nro.26: Resumen de la dimensión 02-Seguridad de la información

Distribución de frecuencias y respuestas relacionadas con la dimensión 02 seguridad de la información; para la Implementación de Auditoria Informática con la ISO 27001 en la Municipalidad Distrital de Suyo-Piura; 2020.

Respuesta	n	%
Si	18	45
No	22	55
Total	40	100

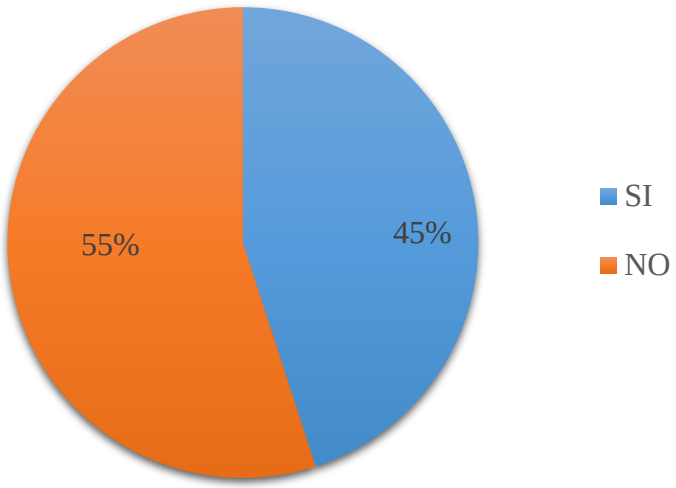
Fuente: Aplicación del instrumento para medir el nivel de conocimiento, basado en 10 preguntas aplicadas a los trabajadores de la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.26 se puede examinar que el 55 % de los trabajadores encuestados contestaron que NO cuentan en la municipalidad con seguridad de la información, mientras que el otro 45% indican que SI existe en la municipalidad seguridad de la información.

Grafico Nro.12: Resultados de la Dimensión 02

Distribución porcentual de las frecuencias y respuestas relacionadas con la dimensión 02: seguridad de la información; para la Implementación de Auditoria Informática con la ISO 27001 en la Municipalidad distrital de Suyo-Piura; 2020.



Fuente: Tabla Nro.26.

Tabla Nro.27: Resumen General de las Dimensiones

Distribución de frecuencias y respuestas relacionadas con las 02 dimensiones definidas para determinar los niveles de conocimiento y seguridad de la información; para la Implementación de Auditoria Informática con las ISO 27001 en la municipalidad distrital de Suyo-Piura; 2020.

DIMENSIONES	SI		NO		TOTAL	
	n	%	n	%	n	%
Nivel de conocimiento	20	50	20	50	40	100
Seguridad de la información	18	45	22	55	40	100

Fuente: Aplicación del instrumento para el conocimiento de los trabajadores encuestados acerca del conocimiento y seguridad de la información de las 02 dimensiones definidas para la interpretación; en la municipalidad distrital de Suyo-Piura; 2020.

Aplicado por: Cosios, T.; 2020.

En la Tabla Nro.27 se observa que en las dos dimensiones el mayor porcentaje de los trabajadores encuestados dijeron que No hay seguridad de la información en la municipalidad.

Grafico Nro. 13:Resumen General de las Dimensiones

Dimensión porcentual de las frecuencias y respuestas relacionadas con las 02 dimensiones definidas para determinar los niveles de conocimiento y seguridad de la información; para la implementación de Auditoria informática con la ISO 27001 - Piura; 2020.

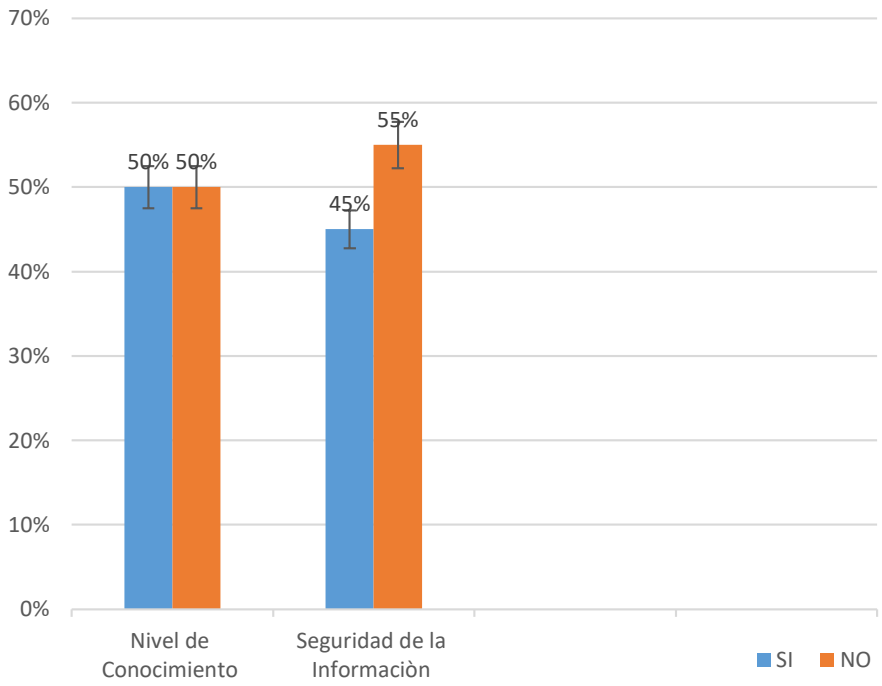


Tabla Nro.27

5.2. Análisis de Resultados

La presente investigación tuvo como objetivo general : Realizar una Implementación de Auditoria Informática con las ISO 27001 en la municipalidad distrital de Suyo, con el fin de mejorar el sistema de información; en este sentido para poder cumplir con este objetivo es necesario realizar una evaluación de esta situación actual a fin de que esta implementación identifique claramente los requisitos y pueda cubrir las exigencias de la entidad a través de una propuesta de mejora seria y técnica.

Para realizar esta sección de análisis de resultados se diseñó un cuestionario agrupado en 02 dimensiones y, luego de los resultados obtenidos e interpretados en la sección, se realizará el siguiente análisis:

1) En lo que respecta a la dimensión 01: Nivel de conocimiento, en Tabla Nro.15 se puede interpretar en esta dimensión el 50 % de los trabajadores encuestados contestaron que No tienen conocimiento acerca de seguridad de la información. Este resultado tiene similitud con lo obtenido por Agurto (10) en su investigación para una dimensión similar a la presente , obteniendo resultados que el 58% de fuga de documentación especializada es de manuales, procedimientos, documentación técnica, por debajo con el 33% otra de la fuga de documentación es por las incidencias en información de carácter personal. Esta similitud en los resultados justifica que los trabajadores de ambas empresas no conocen sobre la norma ISO 27001 para poder implementarla, por lo tanto, la municipalidad no brinda protección necesaria, porque su información está expuesta a los peligros que hay al tener toda su documentación en forma manual en consecuencia el riesgo que existe en la información de ambas empresas conlleva la falta de confidencialidad.

2) Con respecto a la dimensión 02: Seguridad de la información, en la Tabla Nro.26 nos muestra los resultados donde se puede interpretar que el 55% de los trabajadores indican que NO existe en la municipalidad seguridad de la información, este resultado es similar al resultado obtenido Lara (9) en su investigación donde obtuvo como resultado para una dimensión similar a la presente, 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.Esta similitud en los resultados se justifica que la implementación de auditoria informática con las ISO 27001 mejorara la seguridad de la información en la municipalidad.

5.3. Propuesta de mejora

Luego de haber analizado los resultados obtenidos en la presente investigación, se plantea la siguiente propuesta de mejora:

Se desarrollará la documentación exigida por la norma ISO/IEC 27001 para la Municipalidad distrital de Suyo-Piura.

La norma ISO 27001 fue elijada para realizar el sistema de gestión de seguridad de información, la cual permitirá ver a la información tanto interna y externa de la municipalidad como un activo valioso, que debe tener una gestión adecuada, para que los trabajadores puedan trabajar con confianza. Así mismo al implementar esta norma permitirá minimizar los riesgos, al asegurar que se identifican, valoran los activos y sus riesgos, por otro lado, se podrá evaluar los diferentes riesgos y establecer una serie de estrategias, controles oportunos para asegurar la protección y salvaguardar la información.

CONTROLES DE SEGURIDAD BASADO A LA NORMA ISO 27001

Referencias Normativas

Los siguientes documentos, en parte o en su totalidad, se referencian normativamente en este documento y son indispensables para su aplicación.

5.3.1. ANÁLISIS DIFERENCIAL DEL ESTADO ACTUAL VERSUS ISO/IEC 27001 Y 27002 :2013

En esta sección se realizará el análisis diferencial con respecto a la ISO/IEC 27002, en o cual este análisis nos permite conocer el estado actual de la organización, teniendo como base la norma ISO27001:2013, este trabajo de investigación estará enfocado en analizar todos los controles y requerimientos de seguridad detallados en el Anexo **A** son directamente derivados y alineados con los listados en ISO/IEC 27001 – 27002:2013" y alineados con los procesos de la municipalidad. Lo cual se mirará en detalle cada uno de los capítulos empezando por el numeral 5-politicas de seguridad de la información y terminando con el número 18-cumplimiento, dentro de cada capítulo existen controles que también deben implementarse.

Los hallazgos a continuación son resultados del análisis de las medidas de seguridad y la normativa que tiene la organización en relación con la seguridad de la información. Este análisis nos permitirá conocer de manera global el estado actual de la municipalidad en relación de la seguridad de la información.

Se agrega un valor a cada control en base al estado en el que se encuentra:

0- No esta implementado.

1- Esta parcialmente implementado.

2- Completamente implementado.

Tabla Nro. 28: Evaluación de los controles de la Normativa ISO/IEC 27002:2013Control de la normativa ISO/IEC 27001:2013

A5.POLÍTICAS DE SEGURIDAD			
OBJETIVO DE CONTROL	**CONTROL**	**DESCRIPCIÓN**	**VALOR**
5.1 DIRECTRICES DE LA DIRECCIÓN EN SEGURIDAD DE LA INFORMACIÓN	5.1.1.Políticas para la Seguridad de la Información.	-Existe un documento de políticas. -No se evidencia los entrenamientos realizados a los trabajadores acerca de las políticas en la seguridad de la información. -Se sugiere establecer y publicar una Política General de Seguridad de la información y comunicar a todos los niveles, trabajadores y terceras partes que lo requieran.	1

	5.1.2.Revisión de las Políticas para la Seguridad de la Información	-Se evidencia que no hay ningún tipo de revisión de políticas de seguridad y están desactualizadas. -Se recomienda la revisión la revisión periódica de las políticas de seguridad (idealmente cada año) para asegurar el cumplimiento de las modificaciones o nuevas normas legales que involucren a la institución.	0
A6.ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
6.1 ORGANIZACIÓN INTERNA	6.1.1.Asignación de Responsabilidades para la Seguridad de la Información.	-No se tiene un rol apropiado para el responsable del SGSI. -Ordenar y documentar todas las responsabilidades sobre la seguridad de información por	1

		cada uno de los activos y procesos de seguridad.	
	6.1.2 Segregación de tareas	-No existen funciones específicas para cada trabajador. -Especificar y documentar la separación de funciones.	0
	6.1.3.Contacto con las autoridades	-Se mantiene contacto con autoridades.	2
	6.1.4 Contacto con grupos de interés especial	-se debe mantener contacto con un especialista e en seguridad de la información.	0
	6.1.5 Seguridad de la información en la gestión de proyectos.	-Utilizan una metodología en la gestión de proyectos.	2
	6.2.1 Política de uso de dispositivos para movilidad	-No existe políticas, ni controles para analizar los riesgos en dispositivos móviles.	

6.2 DISPOSITIVOS MÓVILES Y TELETRABAJO		-Se debe implementar políticas para para proteger la información de terceros en los dispositivos móviles.	0
	6.2.2 Teletrabajo	-No se considera, por lo que no hay el servicio de teletrabajo en la municipalidad.	0
A7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS			
7.1 ANTES DE ASUMIR EL EMPLEO	7.1.1 Selección	-Como parte del proceso de selección y reclutamiento se revisan los antecedentes Penales y policiales de cada uno de los candidatos a un puesto laboral.	2
		-Existen contratos en donde se incluye una cláusula de	1

	7.1.2 Términos y condiciones del empleo	confidencialidad de la información. -Se debe concientizar acerca de seguridad de la información.	
7.2 DURANTE LA CONTRATACIÓN	7.2.1.Responsabilidades de gestión.	-No se tienen acuerdos de confidencialidad donde se definan las recomendaciones de seguridad sobre el tratamiento de la Información.	0
	7.2.2. Concienciación, educación y capacitación en seguridad de la información.	-Establecer un plan de entrenamiento o capacitación que se inicie con la inducción y que introduzca conocimiento de las	0

		políticas de seguridad de la municipalidad antes que los servicios o información se ponga a disposición del empleado, contratistas o terceras partes.	
	7.2.3.Proceso disciplinario.	Implementar un procedimiento para la ejecución de procesos disciplinarios	0
7.3 TERMINACIÓN Y CAMBIO DE EMPLEO	7.3.1 La terminación o el cambio o cambio de responsabilidades de empleo	No se tiene un proceso documentado para el retiro del trabajador.	0
A8. GESTIÓN DE ACTIVOS			
8.1 RESPONSABILIDAD SOBRE LOS ACTIVOS	8.1.1 Inventario de activos	La municipalidad tiene un inventario de activos. Sin embargo se sugiere clasificar de acuerdo a su sensibilidad y criticidad, para tener un control	0

		permanente de los más representativos para la municipalidad.	
	8.1.2 Propiedad de los activos.	Se firman documentos, donde se detalla la asignación y responsable del activo. Este documento debe contener: Nombre del activo: Tipo de Activo, propietario. código de barras para su identificación. ubicación(Área, proceso, etc).	0
	8.1.3 Uso aceptable de los activos.	- Especificar y documentar las reglas para el uso aceptable de la información y los activos de la municipalidad mediante una política o procedimiento que debe ser conocido por el personal del área.	0

	8.1.4 Devolución de activos.	Actualmente, la municipalidad tiene un formato para la devolución de equipos asignados; sin embargo se debe establecer un procedimiento detallado para la devolución de activos en toda la institución	1
8.2 CLASIFICACIÓN DE LA INFORMACIÓN	8.2.1 Directrices de clasificación.	-Realizar la clasificación de activos de acuerdo a su confidencialidad y criticidad.	0
	8.2.2 Etiquetado y manipulado de la información.	-Desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información.	0
	8.2.3 Manipulación de activos.	-Desarrollar e implementar procedimientos para la manipulación de activos.	0

8.3 MANEJO DE LOS SOPORTES DE ALMACENAMIENTO	8.3.1 Gestión de soportes extraíbles.	-Establecer un formato de asignación de propietario de medios removibles tales como, correo electrónico laboral, servicios de mensajería, USB, CD, entre otros además de un formato para la entrega o custodia y destrucción de tales medios o dispositivos.	0
	8.3.2 Eliminación de soportes	-Se hace una disposición adecuada de los activos a dar de baja y se elimina todo tipo de información. -No existe un proceso donde se definan los pasos a seguir en caso de la eliminación segura de equipos, eliminación de información y datos.	1

	8.3.3 Soportes físicos en tránsito	-Se debe llevar a cabo un procedimiento en el manejo y almacenamiento de la información, para asegurar la que se eviten eventos como divulgación,	0
A9. CONTROL DE ACCESOS			
9.1 REQUISITOS DE NEGOCIO PARA EL CONTROL DE ACCESOS	9.1.1 Política de control de accesos	-La municipalidad día a día genera y desarrolla activos de información lo cuales deben estar salvaguardados o custodiados de acuerdo a su importancia o clasificación por lo que se debe controlar el acceso a la información. Por lo tanto, se debe: - Desarrollar e implementar una política de control de acceso, documentada, revisada y basada en los requerimientos de	1

		seguridad y objetivos institucionales.	
	9.1.2 Control de acceso a las redes y servicios asociados.	- Se tiene un proceso de solicitud de ingreso de usuario donde se especifica los servicios. - Se debe tener un proceso de seguridad en red y actividades de revisiones permisos de acceso, Se debe centralizar las revisiones documentadas.	1
9.2 GESTIÓN DE ACCESO DE USUARIO	9.2.1 Gestión de altas/bajas en el registro de usuarios	La municipalidad está aplicando este control. Sin embargo, se debería implementar las siguientes directrices para mejorar el control actual. -Implementar un procedimiento formal por escrito de alta del usuario al sistema, que regule y exija el ingreso de los siguientes	1

		datos: - Usuario. - Tipo o nivel de usuario al que pertenece. - Password(requerimientos mínimos) - Nombre y apellidos completo - Contador de intentos fallidos - Permisos mínimos y necesarios de acuerdo a su nivel o tipo de usuario para que desempeñe su tarea.	
	9.2.2 Gestión de los derechos de acceso asignados a usuarios.	Existe un proceso de ingreso, actualización y retiros a los usuarios de los servicios informáticos, para empleados. -No se tiene un sistema de control de acceso para los espacios físicos, se debe actualizar el procedimiento.	1

	9.2.3 Gestión de los derechos de acceso con privilegios especiales.	Identificar y documentar los privilegios asociados a cada producto del sistema (sistema operativo, sistema de administración de bases de datos y aplicaciones), y las categorías de personal a las cuales deben asignarse los productos.	0
	9.2.4 Gestión de información confidencial de autenticación de usuarios.	Todos los trabajadores de la municipalidad tienen un ID como identificador de usuario, solamente para su uso personal.	2

	9.2.5 Revisión de los derechos de acceso de los usuario	-En la municipalidad no hay una revisión periódica en el sistema de información. Se recomienda realizar una revisión periódica semestralmente, después de cualquier cambio ya sea por finalización de empleo, para asegurar que cada trabajador tenga acceso a la información que requiere sus funciones.	0
	9.2.6 Retirada o adaptación de los derechos de acceso	-Desarrollar e implementar una política donde se exija el retiro de todos los derechos de acceso al empleado o tercero, que deje de laborar en la municipalidad.	0

9.3 RESPONSABILIDADES DEL USUARIO	9.3.1 Uso de información confidencial para la autenticación	-Se debería exigir y promover a los trabajadores que cumplan las buenas prácticas de la municipalidad para el uso de información de autenticación.	0
9.4 CONTROL DE ACCESO A SISTEMAS Y APLICACIONES	9.4.1 Restricción del acceso a la información.	-Dar acceso a la información y a las funciones del sistema de aplicaciones solo a los usuarios de éste, incluido el personal de apoyo de acuerdo con una política de control de accesos definida.	0
	9.4.2 Procedimientos seguros de inicio de sesión.	-La municipalidad ha implementado procedimientos básicos de inicio de sesión. Sin embargo, se debe incluir las siguientes directrices para mejor el nivel de seguridad: -Implementar un política de control de accesos para controlar	1

		el acceso a los sistemas y aplicaciones mediante un procedimiento seguro de log-in.	
	9.4.3 Gestión de contraseñas de usuario	En la municipalidad existen sistemas los cuales tienen contraseñas, pero no es de uso personal. -Se debería realizar una evaluación a los sistemas de gestión de contraseñas ya que estas deberían ser seguras y asegurar la calidad de las contraseñas.	1

	9.4.4 Uso de herramientas de administración de sistema	Es necesario realizar un procedimiento documentado, en el cual se indique que cada jefe de área, debe solicitar los permisos adecuados para cada personal que se le autorice. -Restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.	0
	9.4.5 Control de acceso al código fuente de los programas	En la municipalidad no existe alguna política de seguridad o procedimiento documentado de acceso al código fuente de los sistemas informáticos. -Implementar a los controles ya establecidos lo cual deben comprender:	0

		- Un registro de personas autorizadas y funciones. - La fecha de ingreso y salida. - El motivo de acceso. -	
A.10.CIFRADO			
10.1 CONTROLES CRIPTOGRÁFICOS	10.1.1 Políticas sobre el uso de controles criptográficos	-No se tiene una política sobre el uso de controles criptográficos, puesto que son necesarios para discos externos que sale con información de la empresa.	0

		-Implementar una política documentada con respecto al uso del correo electrónico e internet.	
	10.1.1 Gestión de llaves	Debemos desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas ,durante todo su ciclo de vida.	0
A11.SEGURIDAD FÍSICA Y DEL ENTONO			

11.1 ÁREAS SEGURAS	11.1.1 Perímetro de seguridad física	- Se tiene controles a nivel de hardware como a nivel de personas los procesos están documentados y existen registros que lo evidencian	2
	11.1.2 Controles de entrada Físicas	Los archivos físicos que tienen información sensible e historia de la compañía no tienen control de acceso por carnet ni cámara cercana, el centro de cómputo no tiene control de acceso ni cámara de seguridad.	1
	11.1.3 Asegurar oficinas, salas e instalaciones	No se menciona en el proceso seguridad física el manejo del control .	0

	11.1.4 La protección contra amenazas externas y ambientales	No se menciona ningún proceso paran la seguridad contra las amenazas externas y ambientales.	0
	11.1.5 Trabajar en zonas seguras	-No existe en la municipalidad procedimientos para trabajos en zona segura.	0
	11.1.6 Áreas de carga, despacho y acceso publico	-No se tiene un control de seguridad para restringir en ingreso de personas no autorizadas.	0

11.2 EQUIPOS	11.2.1 Ubicación y protección de los equipos	-No existen procesos ni alineados que existen análisis de riesgos ambientales documentados.	0
	11.2.2 Servicios de suministro	-Se tiene incorporado una documentación con las UPS y una vez por año el proceso de mantenimiento con proveedor externo El área de instrumentación electricidad tiene controles para revisiones periódicas de la energía, mantenimientos a equipos, acciones durante un apagón. -No se tiene un registro de los mantenimientos de UPS en el proceso, No se menciona en el proceso de instrumentación y electricidad el sistema del centro	1

		de cómputo, sus revisiones y mantenimiento	
	11.2.3 Seguridad en el cableado	-No hay cableado certificado en la empresa. Se detectó falta de canaletas y separación de cables eléctricos y de datos -No existe un documento o plano de la compañía que apoye las rutas de cableado estructurado. No se cumple el estándar en la terminación de cableado	

	11.2.4 Mantenimiento de los equipos	En la municipalidad existe un programa de mantenimiento de equipos tanto lógico como físico Se tiene un indicador de mantenimiento que se evidencia cada mes. -El proceso de mantenimiento preventivos esta desactualizado. hace falta incorporar el indicador de mantenimiento.	1
	11.2.5 Retiro de activos	-Se tiene agregado un proceso de registro de dar de baja un equipo. Se tiene incorporado un proceso de desecho tecnológico. -El proceso de desecho tecnológico no está documentado.	1

	11.2.6 Seguridad de equipos y activos fuera de las instalaciones	-Se debe aplicas medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la municipalidad	0
	11.2.7 Disposición segura o reutilización de equipos.	-Se hace una disposición adecuada de los activos de información y se elimina todo tipo de información corporativa. -En el proceso "Actualización de usuarios - Ingreso o Retiro" se debe especificar el borrado de la información segura En el formato de Retiro es necesario agregar un ítem para el borrado de información	1

	11.2.8 Equipos de usuario desentendido	.Se recomienda implementar una política de equipo desentendido .se debe implementar un control para el tiempo de inactividad del equipo de cómputo.	0
	11.2.9 Política de escritorio y pantalla limpia	Se debe adoptar una política de escritorio limpio para los papeles y medios de alamcenamiento,removibles,y una política de pantalla en las instalaciones de procesamiento de la información.	0
A12 .SEGURIDAD DE LAS OPERACIONES			

A 12.1 PROCEDIMIENTOS OPERACIONALES Y RESPONSABILIDADES	12.1.1 Procedimientos de operación documentados	-Se tienen procesos diarios, semanales, mensuales, de todo el sistema de información que soportan la operación. -Se debe actualizar de manera constante el manual de seguridad colocando las tareas operativas.	1
	12.1.2 Gestión de cambios	-Existe un proceso de gestión de cambios para desarrollo de software. Existe proceso de gestión de cambios para infraestructura. Existe un proceso incorporado en manejo de versiones de aplicaciones de software. -No existe una estandarización y políticas de seguridad que la respalden.	1

	12.1.3 Gestión de capacidad	A nivel de desarrollo de software tienen procesos establecidos que les permiten manejar indicadores de calidad y reporte de defectos. Se hacen pruebas de rendimiento bajo demanda de la infraestructura. Se debe en el proceso de desarrollo de software detallar el cómo se realiza No se tiene un proceso estandarizado que especifique la gestión de capacidades	1
	12.1.4 Separación de los ambientes de desarrollo, pruebas y operación	-Se hacen entrenamiento sobre las buenas prácticas de desarrollo. -No se evidencia el seguimiento del proceso en cuento los controles de calidad.	1

A12.2 PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS	12.2.1 Controles contra malware	Actualmente la municipalidad tiene herramientas de detección y protección de código malicioso, sin embargo, no están documentadas. Para lo cual se debe: -Capacitar al usuario sobre el uso de los antivirus y cuando haya una infección.	0
12.3 COPIAS DE SEGURIDAD	. 12.3.1 Copia de seguridad de la información	-Implementar y documentar un procedimiento para la copias de seguridad y recuperación de la información.	0
12.4 REGISTRO Y SEGUIMIENTO	12.4.1 El registro de evento	Implementar un control para el registro de logs, fallas, excepciones o eventos de seguridad.	0

	12.4.2 Protección de la información de registro	Implementar un control para registrar las actividades del administrador y del operador del sistema.	0
	12.4.3 Registros de administrador y operado	-Se tiene un proceso incorporado de monitoreo diario, semanal por parte del administrador y el operador de los servicios críticos de la compañía.	2
	12.4.4 Sincronización de reloj	-Se tiene un proceso incorporado para la sincronización de la hora de todos los equipos.	1

12.5 CONTROL DE SOFTWARE OPERACIONAL	12.5.1 La instalación del software en los sistemas operativos	-En dicha municipalidad existe la instalación de software en los sistemas operativos. -No se tiene control de instalación de aplicaciones para el área administrativa desde medios extraíbles.	1
12.6 GESTIÓN DE VULNERABILIDAD TÉCNICA	12.6.1 Gestión de vulnerabilidades técnicas	-Implementar un procedimiento para controlar el acceso a los archivos que contengan información crítica sobre los sistemas de información	1
12.7 CONSIDERACIONES SOBRE AUDITORIAS DE SISTEMAS DE INFORMACIÓN	12.7.1 Controles de auditoría de sistemas de información	-Se tiene incorporada la periodicidad de auditoria. -No se tiene documentado el manual del administrador de seguridad la periodicidad de las auditorias.	1

A13 .SEGURIDAD DE LAS COMUNICACIONES			
13.1 GESTIÓN DE LA SEGURIDAD DE LAS REDES	13.1.1 Controles de red	-La municipalidad mantiene asegurada la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte. Se ha desarrollado mecanismos de seguridad, los niveles de servicio y los requisitos de gestión mínimos de todos los servicios de red.	2

	13.1.2 Seguridad de los servicios de red	-Se tiene para los dispositivos de red configurados los roles de acceso a los dispositivos administrador, operador a nivel de dominio se tiene unos grupos creados y determinados accesos para los servicios de plataforma como internet. No se tiene documentado como se configuran las seguridades de switch. No se tiene dentro del grupo de soporte técnico limitación de acceso al directorio.	1
	13.1.3 La segregación en las redes	Los grupos de servicios de información, usuarios y sistemas de información se mantienen separados en las redes para así evitar que el tráfico de una subred afecte a las demás.	2

13.2 TRANSFERENCIA DE INFORMACIÓN	13.2.1 Las políticas y los procedimientos de transferencia de información	Se tiene incorporado en los procesos de inducción y entrenamiento del personal nuevo explicar las buenas prácticas para el correcto de sus usuarios(Id)y no ser manipulados por terceros. - Implementar una política documentada concerniente al uso de redes y servicios de red.	1

	13.2.2 Los acuerdos sobre la transferencia de información	-Dentro de los contratos proveedores se tienen cláusulas de confidencialidad. -Se debe establecer acuerdos de confidencialidad y manejo de la información de acuerdo con la ley con los trabajadores .	
	13.2.3 La mensajería electrónica	-Se debe implementar una política de seguridad para brindar un servicio de mensajería instantánea de manera segura y confiable.	
	13.2.4 Los acuerdos de confidencialidad o de no divulgación	Los trabajadores se les explica acerca de la cláusula, donde deberían respetar el área donde trabajan y no divulgar ningún tipo de información. -También se debe documentar todo tipo de información y así no	1

		perder información confidencial que pueda causar daño a la organización	
14 ADQUISICION,MANTENIEMIENTO Y DESARROLLO DE SISTEMAS			
14.1 REQUERIMIENTOS DE SEGURIDAD DE LOS SI	14.1.1 Análisis de los requisitos de seguridad de la información y especificación	-Dentro de la metodología de desarrollo del proyecto de software se estables los requerimientos no funcionales de la seguridad, se elaboran estrategias de tratamiento a los riesgos según la criticidad del proyecto.	2

	14.1.2 Asegurar los servicios de aplicaciones en las redes públicas	-Se tiene a nivel de Firewall protección IDS Las carpetas web server tienen seguridades se deben fortalecer las políticas de firewall contra ataques -Se debe implementar estrategias y protecciones hacia web server a nivel interno.	1
	14.1.3 La protección de las transacciones de servicios de aplicación	-Se debe establecer para las aplicaciones que manejan y trasmiten información sensible el uso de códigos criptográficos, certificados, firmas digitales	0
14.2 SEGURIDAD EN DESARROLLO Y PROCESOS DE SOPORTE	14.2.1 Políticas de desarrollo seguro.	-Se tienen procesos establecidos para el desarrollo de software las personas del área de desarrollo son capacitadas en buenas prácticas de desarrollo seguro.	2

	14.2.2 Procedimientos de control de cambios del sistema	-Existen procedimientos de cambios en las aplicaciones las cuales son documentados en actas de entrega de proyectos. -Se deben realizar análisis de riesgos de aplicaciones de cada proyecto, donde se identifiquen las amenazas.	1
	14.2.3 Revisión técnica de las aplicaciones después de operar cambios de plataforma	-Existe un proceso de actualización de plataforma, para realizar reuniones de planeación donde se establecen las actividades, responsables y pruebas. -Se debe crear un procedimiento para la actualización de plataforma donde describa unos	1

		lineamientos a seguir se debe actualizar el proceso de pruebas.	
	14.2.4 Restricciones en los cambios a los paquetes de software	-En las aplicaciones que son necesaria se establecen restricciones o bloqueos para aplicaciones como antivirus en los equipos de los usuarios y sistema operativo. -Se debe establecer un proceso estándar donde se controle los lineamientos para elegir las aplicaciones que deben tener bloqueos, activación de logs, seguimientos.	1

	14.2.5 Uso de principios de ingeniería en protección de sistemas	-Se tiene para la etapa de implementación entregables que ayudan en la etapa desarrollo de requerimiento. - Se deben establecer ,documentar y mantener principios para la construcción de sistemas seguros.	1
	14.2.6 Seguridad en entornos de desarrollo	-Se están incorporado prácticas de revisión de seguridad de micros para el área de informática y desarrollo. -Se debe tener una estrategia de seguridad para los entornos de desarrollo y estaciones de trabajo para proteger la información de estos equipos	1

	14.2.7 Desarrollo Outsourced	No aplica.	0
	14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas	-Se tiene dentro de la metodología de desarrollo de software una etapa de pruebas funcionales para una buena implementación. -Se debe incorporar dentro del proceso de pruebas, pruebas de seguridad.	1

	14.2.9 Pruebas de aceptación del sistema	-Durante el proceso de desarrollo, se deben de llevar a cabo pruebas de funcionalidad de la seguridad .	0
14.3 DATOS DE PRUEBA	14.3.1 Protección de los datos de prueba	Se debe realizar nuevas actualizaciones a los sistemas de información, establecer programas de prueba para aceptación y criterios de aceptación relacionados.	0
A 15. RELACIONES CON LOS PROVEEDORES			

15.1 SEGURIDAD DE LA INFORMACIÓN EN LA RELACIÓN CON LOS PROVEEDORES	15.1.1 Política de seguridad de la información para las relaciones con proveedores	-Teniendo el acceso de los proveedores en la organización, se deben documentar los activos para una seguridad de información optima .	0
	15.1.2 Abordar la seguridad dentro de los acuerdos con proveedores	-Existen un proceso de para la compra de servicios con proveedores, y se establecen los requerimientos del servicio brindado. -Se deben establecer acuerdos de confidencialidad donde se estipulen la forma para el tratamiento de la información, con los proveedores.	1

15.2 GESTIÓN DE LA PRESTACIÓN DE SERVICIOS DEL PROVEEDOR	15.2.1 El seguimiento y la revisión de los servicios de proveedores	-Se debe hacer seguimiento constante, revisar y auditar con regularidad la prestación de los servicios de los proveedores.	0
	15.2.2 Gestión de cambios en los servicios de proveedores	-Se hacen un proceso de selección de proveedor y se evidencia en estudio de las cotizaciones y el análisis costo beneficio al final de cada contrato se hace evaluación de servicio a los proveedores.	2
A 16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN			

16.1 GESTIÓN DE INCIDENTES Y MEJORAS EN LA SI	16.1.1Responsabilidades y procedimientos	Se tiene un informe físico donde se ingresan todos los incidentes que afectan la disponibilidad, integridad y confidencialidad de la información. Dentro de los roles se tiene especificado la función de quienes ingresan y clasifican los incidentes de seguridad.	2
	16.1.2 Informar sobre los eventos de seguridad de información	-Se comunica a los trabajadores, como evaluar y identificar un incidente que afecta la seguridad de la información.	2

	16.1.3 Presentación de informes de información debilidades de seguridad	-Se tiene un proceso de reporte de incidentes tanto para trabajadores como proveedores. -Los proveedores externos no conocen el procedimiento y pueden reportar incidentes	1
	16.1.4. Valoración de eventos de seguridad de la información y toma de decisiones	-Se tiene incorporado en los grupos primarios de informática mensuales el análisis de resultados de las solicitudes atendidas y los reproceso a través de indicadores. -No se tiene clasificación en el sistema de ingreso de incidentes para seguridad, ni la criticidad.	1
	16.1.5 Respuesta a incidentes de seguridad de la información	-Se tienen informes de gestión sobre incidentes de seguridad, los cuales son reportados a la dirección mensualmente.	1

		-No se tiene una respuesta de los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	
	16.1.6 Aprendiendo de los incidentes de seguridad de la información	-Se tiene conocimiento de los incidentes de seguridad de la información, pero no se realiza un procedimiento adecuado para reducir la posibilidad o impacto de incidentes a futuro.	1
	16.1.7 El acopio de pruebas	-No se tiene establecido un proceso para la recolección de evidencia formal	0

A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO			
17.1 CONTINUIDAD DE SEGURIDAD DE LA INFORMACIÓN	17.1.1 Información de planificación de continuidad de seguridad	-Los documentos del plan de continuidad de negocios se encuentran desactualizado, no se tiene un documento donde se estipulen los tiempos aceptables de recuperación de cada proceso crítico.	0
	17.1.2 Implantación de la continuidad de la seguridad de la información	No se tiene establecido en la municipalidad, un procedimiento documentado y controles para asegurar el nivel de continuidad requerido para la seguridad de información durante cualquier situación adversa	0

	17.1.3 Verificar, revisar y evaluar la información de seguridad de continuidad	-El departamento realiza una vez al año como mínimo un simulacro para verificar que los procesos si sean efectivos en la información. -Se debe verificar a intervalos los controles de continuidad de la seguridad de la información establecidos e implementados ,con el fin de asegurar que son válidos y eficaces durante una situación adversa	1
17.2 REDUNDANCIAS	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información	-No se tiene documentado en el plan de continuidad de negocios los servidores redundantes y su tiempo de activación en caso de incidentes.	0

A18 CUMPLIMIENTO			
18.1 CUMPLIMIENTO DE REQUISITOS LEGALES Y CONTRACTUALES	18.1.1 Identificación de la legislación aplicable y los requisitos contractuales	-Existe clausula confidencial; términos legales entre las partes tanto para trabajadores, como para proveedores se tiene clausulas en los contratos para el cuidado de la propiedad intelectual. -No se tiene un documento especifico donde se definan y estipulen las leyes aplicables en tema de seguridad informática en dicha municipalidad.	1

	18.1.2 Derechos de propiedad intelectual	-Se tiene conocimiento que en los contratos existe una cláusula hacia la propiedad intelectual, cláusula de confidencialidad y manejo de la información. Dentro de las políticas existen secciones para la instalación de software. -No se tiene un documento donde se defina la periodicidad del monitoreo de software.	1
	18.1.3 Protección de los registros	-Se tiene controles de acceso a la información que garantizan la confidencialidad, integridad y disponibilidad de la información. -La información no tiene ninguna clasificación. no se	1

		tiene documentación de los procesos de clasificación de y tipos de protección y cuidados que se tiene para cada tipo de información.	
	18.1.4 Privacidad y protección de datos personales	- para cada trabajador un login y password, pero se desconoce los riesgos y amenazas que están expuestos.	1
	18.1.5 Regulación de los controles criptográficos	-Se tiene controles criptográficos establecidos para los servicios de comunicación y -No se tiene documentados los procesos criptográficos transferencia de información.	1

18.2 REVISIONES DE SI	18.2.1 Revisión independiente de la seguridad de la información	-Se tienen procesos de revisiones diarias, semanales y mensuales en cuanto a seguridad y servicio de la plataforma; se tiene dentro del proceso de plataforma auditorías internas a los procesos de seguridad, 1 veces al año. Se hacen auditorías externas las áreas de informática a los diferentes procesos de plataforma se tiene planes de auditorías a los procesos. Se debe incorporar en la programación de auditorías internas el sistema de gestión de seguridad de la información se debe actualizar el procedimiento de revisiones de seguridad agregando los reportes de	1

		servicios y vulnerabilidades técnicas y demás generalidades de SGSI.	
	18.2.2 El cumplimiento de las políticas y normas de seguridad	-Se debe establecer una política de seguridad donde defina el tratamiento de la información segura y buenas prácticas se deben establecer controles para monitorizar y reportar todo uso indebido de los sistemas de información.	0
	18.2.3 Revisión de cumplimiento técnico	-No se tiene definido el proceso formal para la revisión de actividades diarias de los servicios de infraestructura.	0

Fuente: Elaboración propia

Tras el análisis completo de los diferentes dominios se encontró que, de un total de 98 ítems, 47 de estos no se cumplen, 38se cumplen parcialmente y 13 se cumplen satisfactoriamente.

En lo que respecta a las políticas de seguridad no se cuenta con la documentación necesaria a los procedimientos y controles que ayuden a garantizar la seguridad de información, por otro lado, se realizó el análisis de la seguridad de la información en la municipalidad, se cuenta con acuerdos de confidencialidad, sin embargo, no tiene la documentación adecuada y clara en los roles para el control adecuado de la operación de la seguridad.

Por otro lado, se observa que la seguridad de los recursos humanos no cuenta con un control adecuado para los procesos referentes a la terminación de contratos, tampoco tiene un control de los equipos que serán devueltos a la culminación del contrato de los empleados. Por otro lado, en la gestión de activos se puede visualizar que, aunque se ha trabajado en el inventario de activos, este no se encuentra actualizado en su totalidad, así mismo no se tiene procedimientos para las clasificaciones de la información.

En el control de accesos se cuenta con el uso de contraseñas, sin embargo, no se cuenta con documentación formal, mientras que en lo que respecta a la criptografía se verifica que no existe procedimientos en todo lo relacionado al uso de las llaves criptográficas.

En la seguridad física y ambiental no se cuenta con una protección completa en la alimentación eléctrica, lo que evidencia falta de seguridad en el cableado y la restricción en el uso de los equipos móviles: así mismo se detectan errores en la seguridad en las operaciones, puesto que no se cuenta con logs y/o contraseñas en la gestión de medios informativos.

En relación con los proveedores no se cuentan con un control adecuado referente a los requisitos de seguridad, tiendo en cuenta toda la comunicación, para el aseguramiento de la protección de los activos; así como en la gestión de incidentes de seguridad no hay una correcta gestión, para la recolección de evidencia.

Según el análisis realizado, se observa a nivel general, que se requiere una intervención inmediata a nivel de los dominios relacionados con políticas de seguridad, continuidad del negocio, control de accesos, criptografía y relación con los proveedores, puesto que son los que tiene mayor índice de incumplimiento con la norma y afectan la seguridad de la información que se requiere en dicha municipalidad.

5.3.2. Gestión de riesgos

La realización del análisis de riesgos tiene como fin identificar de manera clara los riesgos a los cuales está expuesta la organización, y basados en esta identificación de los riesgos determinar cuáles son las medidas de seguridad adecuadas para los diferentes activos de seguridad de la información, de igual manera permite establecer los planes de contingencia, para este caso realizaremos un análisis de riesgo, que es un tipo de análisis que se realiza teniendo en cuentas las medidas de seguridad que la municipalidad ya tienen planteadas.

Por otro lado, describe la metodología a utilizar para la gestión de riesgos, derivados de las tecnologías de la información, así como el inventario de los activos de la municipalidad y la valorización de estos. Se tendrá en cuenta la confidencialidad, integridad y disponibilidad de la información, realizando de esta manera el análisis de amenazas y la valorización de los riesgos.

La metodología para realizar para la gestión de riesgos es MARGERIT la cual permitirá la implementación en el proceso de gestión de riesgos dentro de un marco de trabajo.

Por otro lado ayudara a los responsables de la municipalidad a tener conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos y la necesidad de gestionarlos, así mismo permitirá a analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones, por otro lados ayudara a descubrir y planificar el tratamiento oportuno para los riegos bajo control y finalmente ayudará a preparar a la municipalidad con los procesos de evaluación, auditorio y certificación o acreditación según corresponde en cada caso.

Inventario de activos

Un análisis de riesgos generará el inventario de activos que deberá ser administrado y controlado todos los activos serán etiquetados de acuerdo con su nivel de confidencialidad.

Tabla Nro. 29: Inventario de los activos

Tipo de Activo Descripción	**Activo**
Instalaciones	Sala eléctrica, ups, telecomunicaciones
	Ubicación local de infraestructura y comunicaciones
Hadware	Servidores
	Router Inalámbrico
	Equipos de escritorio, portátiles
	Equipos de comunicaciones
Software	Windows server 2012
	Office 2013
	Sistema operativo widows 10
	Antivirus: ESET NOD32

	Asistencia
Datos	Base de datos Administrativos
	Base de datos proveedores, empresarios
	Base de datos correo institucionales
	Backus generados de base de datos
Redes de comunicaciones	Acceso a Internet
	Red de telefonía
	Acceso inalámbrico
Servicios	Internet (navegador Chrome)
	Servicio de internet, telefonía y cable de Movistar.
	Correo electrónico Institucional
Equipamiento Auxiliar	Aire acondicionado
	Sistema eléctrico general
	Sistemas primeros auxilios
	Cableado estructurado
	Fibra óptica
Personal	Gerente
	Personal Administrativo
	Jefe de Informática

Fuente: Elaboración Propia

Valoración de activos

Siguiendo la metodología se define una tabla de valoración de activos con el fin de utilizarla para la evaluación de los activos de información.

Las escalas de valoración de los activos son las siguientes categorías muy bajo, bajo, medio, alto y Muy alto.

Tabla Nro. 30:Valor de los activos

MA	Muy alta
A	Alta
M	Media
B	Baja
MB	Muy baja

Fuente: Libro de Magerit (47).

En esta tabla quedan establecidas las abreviaturas que se utilizaran para la valoración de los activos de información. Desde el punto de vista de la seguridad, junto a la valoración en sí de los activos debe indicarse cuál es el aspecto de la seguridad más crítico.

Identificados los activos se realiza entonces la valoración ACIDA de los mismos. Dicha valoración viene a medir la criticidad en las cinco dimensiones de la seguridad de la información manejada por el proceso de negocio. Esta valoración valorar el impacto que tendrá la materialización de una amenaza sobre la parte de activo expuestos.

Cada activo de información puede poseer un valor diferente en cada una de las diferentes dimensiones para la organización que deseemos analizar. En este caso utilizaremos una escala de valoración de diez valores siguiendo los siguientes criterios:

Tabla Nro.31:Escala de valoración

Valor	Criterio
10	Daño muy grave de la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Fuente: Libro de Magerit (47)

A continuación, la valoración de las dimensiones de seguridad de los activos que incluyen aspectos críticos como: Autenticidad, Criticidad, Integridad, Disponibilidad y trazabilidad.

Tabla Nro.32: Valoración de seguridad de los activos

Valoración Dimensiones de Seguridad de los Activos							
Tipo de Activo Descripción	Activo	Valor	Aspectos críticos				
			A	C	I	D	T
Instalaciones	Sala eléctrica, ups, telecomunicaciones	Alto				7	
	Ubicación local de infraestructura y comunicaciones	Muy Alto				10	
Hardware	Servidores	Muy alto	10	10	10	8	10
	Router Inalámbrico	Alto	9	9	9	8	9
	Equipos de escritorio, portátiles	Alto	8	6	7	7	7

	Equipos de comunicaciones	Muy Alto	10	9	9	10	9
Software	Windows server 2012	Muy Alto	10	9	8	10	10
	Office 2013	Medio	5	6	6	7	7
	Sistema operativo widows 10	Muy Alto	10	9	8	10	10
	Antivirus: ESET NOD32	Alto	9	6	8	6	8
	Asistencia	Alto	9	8	8	7	8
Datos	Base de datos Administrativos	Muy Alto	10	10	10	10	10
	Base de datos proveedores, empresarios	Muy Alto	10	10	10	9	9
	Base de datos correo institucionales	Alto	9	8	8	7	8
	Backus generados de base de datos	Alto	9	9	8	6	8
Redes de comunicaciones	Acceso a Internet	Alto				9	
	Red de telefonía	Medio				7	
	Acceso inalámbrico	Ato				9	
Servicios	Internet (navegador Chrome)	Alto				9	
	Servicio de internet, telefonía y cable de Movistar.	Medio				7	
	Correo electrónico Institucional	Muy Alto				10	
Equipamiento auxiliar	Aire acondicionado	Alto				9	
	Sistema eléctrico general	Muy Alto				10	
	Sistemas primeros auxilios	Medio				8	
	Cableado estructurado	Alto				6	
	Fibra óptica	Alto				6	
Personal	Gerente	Muy Alto		10		10	
	Personal Administrativo	Muy Alto		10		10	

	Jefe de Informática	Alto		9		9	

Fuente: Elaboración Propia

5.3.3. Análisis de Amenazas

Después de haber definidos los activos y su valor en la municipalidad, se debe realizar un análisis que muestre cuales son los activos que están expuestos a amenazas y pueden afectar a los distintos aspectos de la seguridad de la información, para posteriormente conocer lo vulnerable que es el activo para dicha amenaza.

De acuerdo con lo anterior, se procedió a realizar la clasificación de las amenazas utilizando las tablas existentes en el libro 2: catálogo de elementos de Margerit, el cual seguiré la agrupación de las amenazas en cuatro grupos:

Desastres naturales, de origen industrial, errores y fallos no interconectados, y amenazas intencionales presenciales. Realizándose la siguiente tabla de amenazas:

Tabla Nro.33: AMENAZAS

	Amenazas	Dimensión afectada					Activos Afectados							
		D	I	C	T	A	Hardware	Redes de comunicaciones	Instalaciones	Software	Equipamiento Auxiliar	Datos	Servicios	Personal
Desastres Naturales	Fuego	X					X	X	X		X			
	Daños por agua	X					X	X	X		X			
	Inundación	X					X	X	X		X			
	Siniestro mayor	X					X	X	X		X			
	Fenómeno sísmico	X					X	X	X		X			
	Fenómeno meteorológico	X					X	X	X		X			
Accidentes de origen industrial	Fuego	X					X	X	X		X			
	Daños por agua	X					X	X	X		X			
	Sobrecarga eléctrica	X					X	X	X		X			
	Fluctuación eléctrica	X	X				X	X		X	X			
	Contaminación mecánica	X					X							

	Contaminación electromagnética	X					X		X					

	Avería de origen físico o lógico	X	X				X			X				
	Corte del suministro eléctrico	X					X	X	X					
	Condiciones inadecuadas de temperatura o humedad	X	X				X		X		X			
	Fallos de servicios de comunicaciones	X						X						
	Interrupción de otros servicios y suministros esenciales	X					X							
	Degradación de los soportes de almacenamiento de la información	X									X			
	Emanaciones electromagnéticas			X			X		X	X				
	Errores de los usuarios	X	X							X	X	X	X	
	Errores del administrador	X	X	X			X	X		X	X	X	X	
	Errores de monitorización		X		X						X			
	Errores de configuración		X								X			

Errores y fallas no intencionados	Deficiencias en la organización	X												X
	Difusión de software dañino	X	X	X	X	X				X				
	Errores de re-encaminamiento			X				X		X			X	
	Errores de secuencia		X					X		X			X	
	Escapes de información			X							X			

	Destrucción de información	X	X					X	X	X		X	X	
	Fugas de información			X						X	X	X	X	X
	Vulnerabilidades de los programas	X	X	X						X				
	Errores de mantenimiento/ actualizaciones de programas (software)	X	X							X				
	Errores de mantenimiento/ actualizaciones de equipos (hardware)	X					X	X						

	Caída del sistema por agotamiento de recursos	X					X	X					X	
	Pérdidas de equipos	X		X			X							
	Indisponibilidad del personal	X												X
Amenazas intencionales presenciales	Manipulación de los registros en actividad		X		X									
	Suplantación de la identidad del usuario		X	X		X		X		X		X	X	
	Abusos de privilegios de acceso	X	X	X						X				
	Re-encaminamiento de mensajes			X				X		X			X	
	Alteración de secuencias		X					X		X			X	
	Acceso no autorizado		X	X		X	X	X	X	X	X	X	X	
	Análisis de tráfico			X				X						X
	Repudio		X				X							
	Interceptación de información (Escucha)			X				X						
	Modificación deliberada de la información		X					X	X	X	X	X	X	
	Destrucción de información	X							X	X		X	X	
	Divulgación de información		X						X	X	X	X	X	

	Manipulación de programas	X	X	X						X				
	Manipulación de los equipos	X		X			X							
	Denegación de servicio	X					X	X					X	
	Robo	X		X			X							
	Ataque destructivo	X					X		X		X			
	Indisponibilidad del personal	X												X
	Extorsión	X	X	X										X
	Ingeniería social	X	X	X										X

Fuente: Elaboración propia

Después de analizar los activos los más relevantes para la unidad son: la información y la infraestructura. Así mismo los datos, recursos humanos y respaldos (copias de seguridad), se constituyen en los activos que dan el valor agregado a la municipalidad.

Después de hacer el análisis de las posibles amenazas se ubicaron las siguientes sobre los sistemas información:

Todas las relacionados con desastres naturales sobre las instalaciones, encontrándose que el impacto en caso de materializarse dejaría inoperativa la unidad.

Las amenazas de difusión de software dañino y destrucción de información se contribuyen en las que impactan más a los activos, teniendo un valor muy alto.

Esto es debido a que los procesos dentro de la municipalidad no tienen una adecuada protección para el canal de datos, los equipos y las aplicaciones de manera apropiada, se puede tener una caída a la municipalidad, dejándola así inoperativo durante cierto tiempo, y creando destrucción en todos los procesos de municipalidad.

5.3.4. Propuesta de proyectos

Introducción

Al llegar a este punto, ya se tiene conocimiento acerca del estado actual de la municipalidad distrital de suyo, los riesgos que afrontan los activos, por lo cual deben plantearse proyectos que ayuden a mejorar los niveles de seguridad que se necesitan.

Los proyectos a trabajar que se plantean a continuación son resultados del análisis de riego en la municipalidad de suyo para mejorar todos sus procesos. A continuación, se presentarán proyectos los cuales consisten en el plan de capacitación y de continuidad del negocio, también se formulará un plan de concientización en seguridad de información para los trabajadores de la municipalidad.

Objetivo

Plan de capacitación

- Constituir y mejorar el manejo en los procesos de seguridad de la información en la municipalidad.

Plan de continuidad

- Asegurar la continuidad de la municipalidad ante diversas situaciones que se presentan.
- Sobrellevar los riesgos a un nivel aceptable.

Plan de mitigación de riesgos

- Implementar acciones que ayuden a mitigar los riesgos en la seguridad de la información.

En la siguiente tabla muestra la relación de los proyectos con los riesgos identificados para mitigar, y las dimensiones que se ven impactadas por los riegos.

Tabla Nro.34: Relación de proyectos

Proyectos	Amenazas identificadas	Dimensiones	Acciones	Impacto	Prioridad del desarrollo
Plan de capacitación	Errores de los usuarios	Integridad	Cursos de capacitación	Alto	Medio
	Errores del administrador	Integridad	Cursos de capacitación	Alto	Medio
	Deficiencias en la organización	Disponibilidad	Campaña publicitaria	Alto	Medio
	Destrucción de la información	Integridad	Concienciación	Alto	Alto
	Fugas de información	Confidencialidad	Concienciación	Alto	Alto
Plan de Continuidad	Fuego (Problemas industriales)	Disponibilidad	Generar un plan de acción	Alto	Alto
	Avería de origen físico o lógico	Disponibilidad	Generar un plan de acción	Alto	Alto
	Corte del suministro eléctrico	Disponibilidad	Establecer grupos de respuesta	Medio	Medio
	Sobrecarga eléctrica	Disponibilidad	Establecer grupos de respuesta	Medio	Medio
	Fluctuación eléctrica	Disponibilidad	Establecer grupos de respuesta	Medio	Medio
	Fuego	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Daños por agua	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Inundación	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto

	Siniestro mayor	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Fenómeno sísmico	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Ataque destructivo	Disponibilidad	Implementación de un centro de datos alterno	Alto	Alto
	Interceptación de información	Integridad y disponibilidad	Bloqueo de puertos de comunicación para empleados	Alto	Alto
	Destrucción de información	Disponibilidad e integridad	Bloqueo de puertos de comunicación para empleados	Alto	Alto
	Difusión de software dañino	Disponibilidad e integridad	Establecer políticas de uso de software, políticas de intercambio de información y actualización de políticas de uso de TIC.	Medio	Medio

Fuente: Elaboración propia.

A continuación, se describen los proyectos planteados anteriormente.

Plan de continuidad del negocio

Alcance:

El plan de continuidad del negocio busca diseñar un formato que permita el control para reducir los posibles efectos que se puedan generar en la organización y poder recuperarse de pérdidas de activos de información, también verificar procesos y procedimientos que cumplan.

Los procedimientos planteados en este documento son las acciones a ejecutar en relación con el software, hardware y equipos activos involucrados en los procesos críticos determinados en este plan.

El plan de continuidad de la municipalidad busca reducir el riesgo de las amenazas de fluctuación eléctrica, avería de origen físico o lógico, fuego, daños por agua, inundación, siniestro mayor, fenómeno sísmico, fuego, sobrecarga eléctrica, corte del suministro eléctrico, destrucción de información, ataque destructivo, con respecto a la disponibilidad en el área de informática.

Fases:

Análisis de negocio y evaluación de riesgos: Se optó por realizar un análisis de gestión de riesgo para identificar los activos en la municipalidad, ya que estos deben ser claramente identificados, se deben elaborar y mantener un inventario de todos los activos importantes y evitar incidentes que afecte a los activos asociados a la seguridad de la información.

Estrategia de respaldo: La municipalidad deberá establecer un centro de datos que permita la seguridad de los activos de información. Así mismo evaluar los recursos técnicos y humanos para dicha operación.

Desarrollo del plan: En esta etapa se definirán los equipos necesarios para un desarrollo apropiado del plan, además de sus responsabilidades y funciones, También se hará una descripción de los procedimientos y actuación ante los eventos que pueden llegar a activar el plan.

Pruebas: Se ejecutarán las pruebas pertinentes para verificar que el plan funciona correctamente.

Capacitación: Se realizará la capacitación a los trabajadores de la municipalidad acerca de la importancia de la seguridad de la información para el uso de los recursos y activos a los que tienen acceso en el desempeño de sus funciones.

Puesta en marcha del plan, adicionalmente se consideran los riesgos y soluciones del ambiente físico, relacionados con la operación de los procesos del área de informática para implementar el centro de datos.

Plan de capacitación

Alcance

El plan de capacitación involucra al gerente y los trabajadores de la municipalidad, así mismo se debería implantar un plan de formación para concientizar a los trabajadores de la importancia de la seguridad de la información para el correcto funcionamiento en los procesos en los que estén involucrados.

El plan de capacitación está orientado a disminuir el nivel de riesgo en los activos de la información y así evitar la interrupción de las actividades en la organización.

Fases:

Diseño del plan de sensibilización: En esta etapa se diseñarán estrategias para sensibilizar a todos los trabajadores de la municipalidad. Para ello se utilizarán diferentes estrategias.

Diseño del plan de capacitación: En esta fase se revisará y diseñará los cursos relacionados con seguridad de la información para personal, así como talleres prácticos para todo el personal.

Consecución de recursos: En esta etapa se realizará la gestión de recurso financiero y de los trabajadores que se necesitan para poner en funcionamiento el plan de sensibilización y capacitación.

Plan de mitigación de riesgos

Alcance:

El plan de mitigación de riesgos busca establecer acciones y recursos que ayuden a reducir la probabilidad de ocurrencia del riesgo o reducir el impacto que pueda causar en la seguridad de la información de dicha municipalidad. Así mismo se busca con este plan restringir el acceso a la información contenida en los discos duros de los equipos de cómputo, de acuerdo con los niveles de acceso de los trabajadores.

Objetivos:

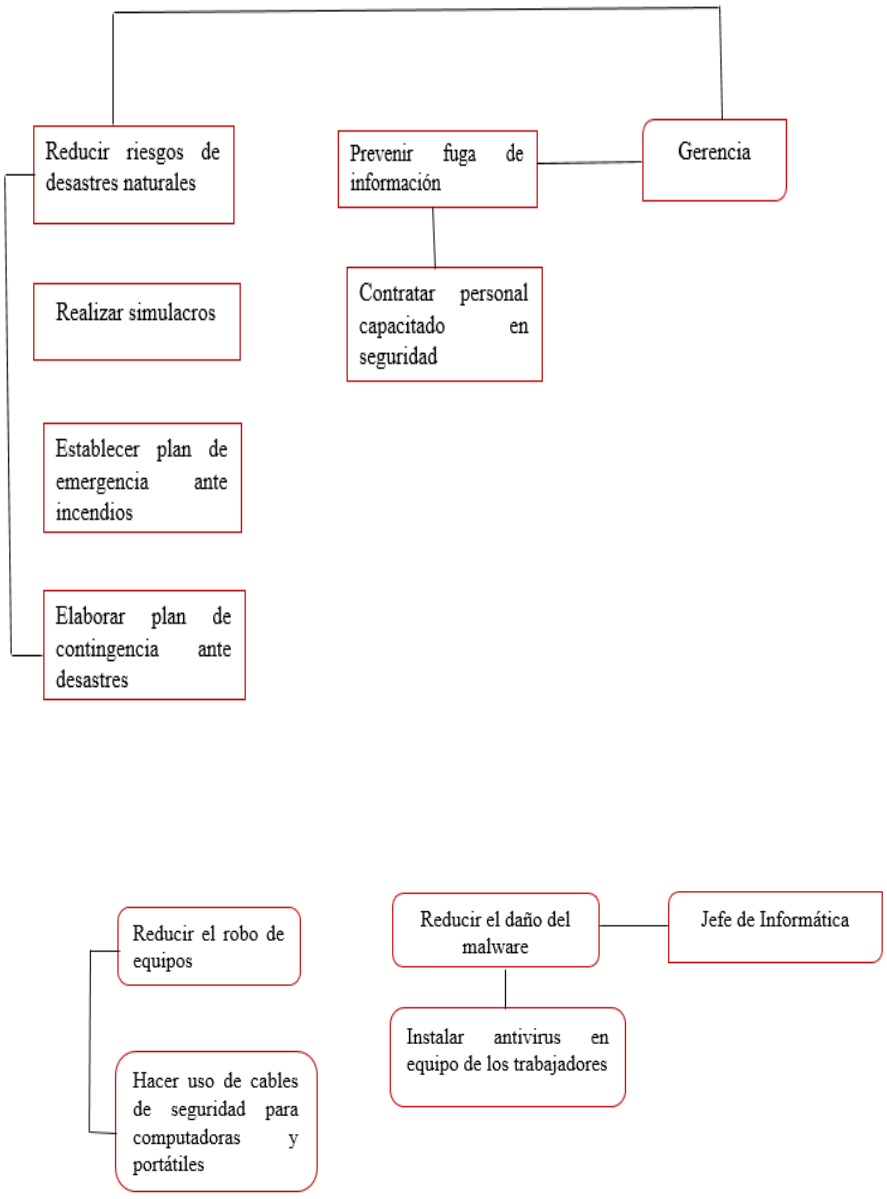
Establecer las acciones enfocadas a mitigar los riesgos más relevantes en el análisis de riesgos ante alguna eventualidad de toda acción que lo pueda paralizar, ya sea de forma parcial o total.

Plan de ejecución

A continuación, se aplicarán salvaguardas para implementar el plan de gestión de los riesgos existentes. En primera instancia se deberá aplicar las salvaguardas en niveles con prioridad mayor es decir medidas preventivas. Se requieren procedimientos tanto para la operación de las salvaguardas preventivas como para la gestión de incidencias y la recuperación tras las mismas.

Entre las salvaguardas de mayor prioridad se encuentran la prevención contra incendios y terremotos, prevención de la fuga de información, prevención de perdida de almacenamiento y la prevención de acceso no autorizado.

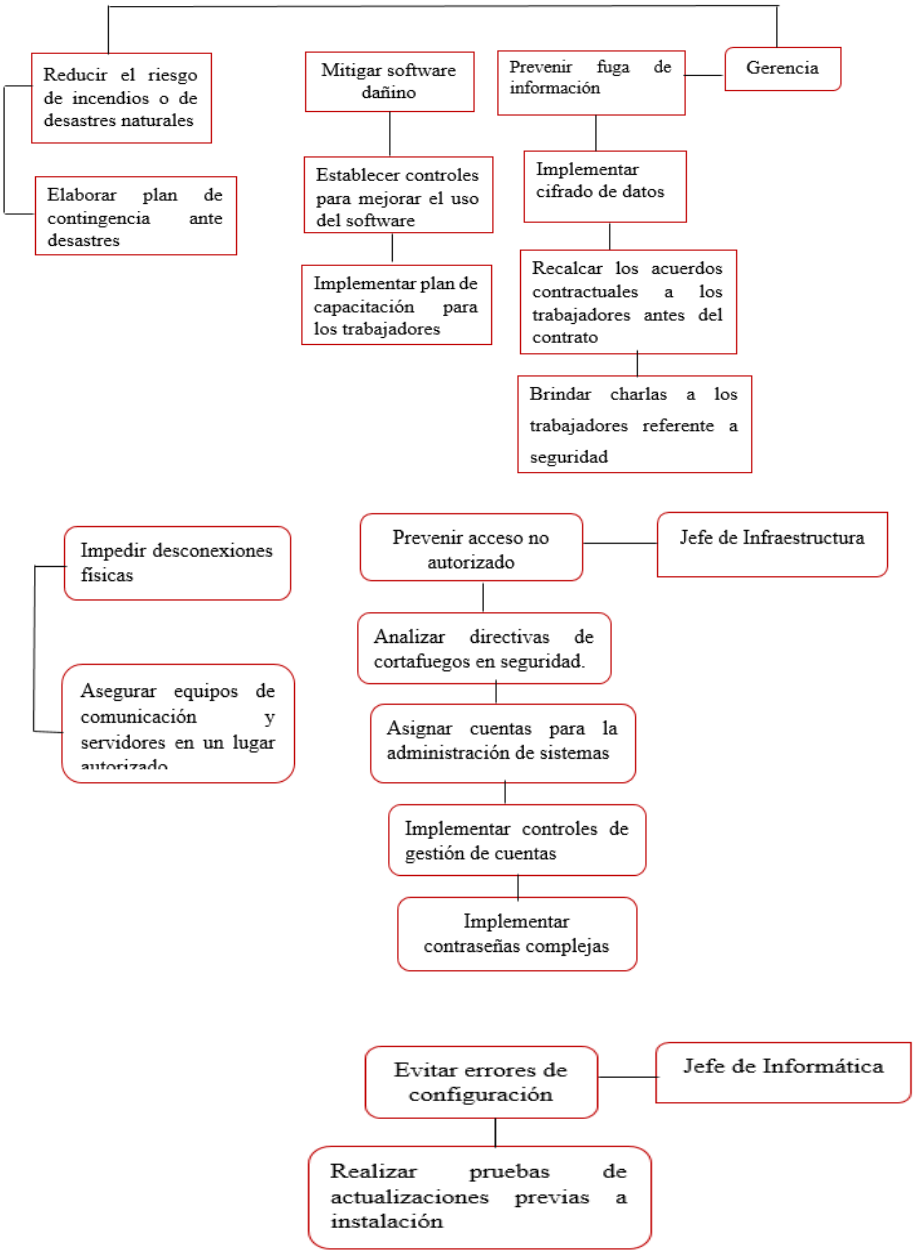
Grafico Nro. 14:Salvaguardas en primer nivel



Fuente: Elaboración propia

Se muestra cómo aplicar las salvaguardas para los procesos que requieren de mejoras en la gestión.

Grafico Nro15:Salvaguardas de mejoras en la gestión



Fuente: Elaboración propia

Luego de haber definido e implementado los diversos procesos a realizar dentro del plan de seguridad es necesario volver a realizar un nuevo análisis de riesgo para conocer el nivel de riesgo obtenido y así tratar de mejorar las medidas de seguridad necesarias para mantener la seguridad de información.

Por otro lado, estas normas generales permitirán disminuir los riesgos en la municipalidad:

1. Ofrecer un mejor servicio a la ciudadanía, garantizando que se aplique los controles necesarios para asegurar su información.

2. Brindar confidencialidad a los trabajadores y proveedores por la información que tiene la municipalidad, así mismo los trabajadores deberán asumir una responsabilidad individual respecto a los criterios de confidencialidad, integridad y disponibilidad de la información, así como del uso de información privilegiada

3. Cumplir con los requerimientos legales en cuento a la protección de la información de los trabajadores.

4. Brindar información a los trabajadores sobre la importancia del SGSI, así como su responsabilidad sobre el cumplimiento de los dispuestos por el SGSI.

5. La información y los recursos de vital importancia como activos en la municipalidad, debe ser utilizados con responsabilidad, bajo los principios de ética y moral, para protegerlos.

El tiempo de implantar el plan de seguridad no ha sido considero porque depende de una serie de factores como financieros y administrativos.

Finalmente se ha desarrollado un plan de ejecución que conlleva la participación de los trabajadores de varias áreas e implementación a mejorar los procesos aplicando medidas preventivas correctoras para reducir los niveles de riesgo existentes.

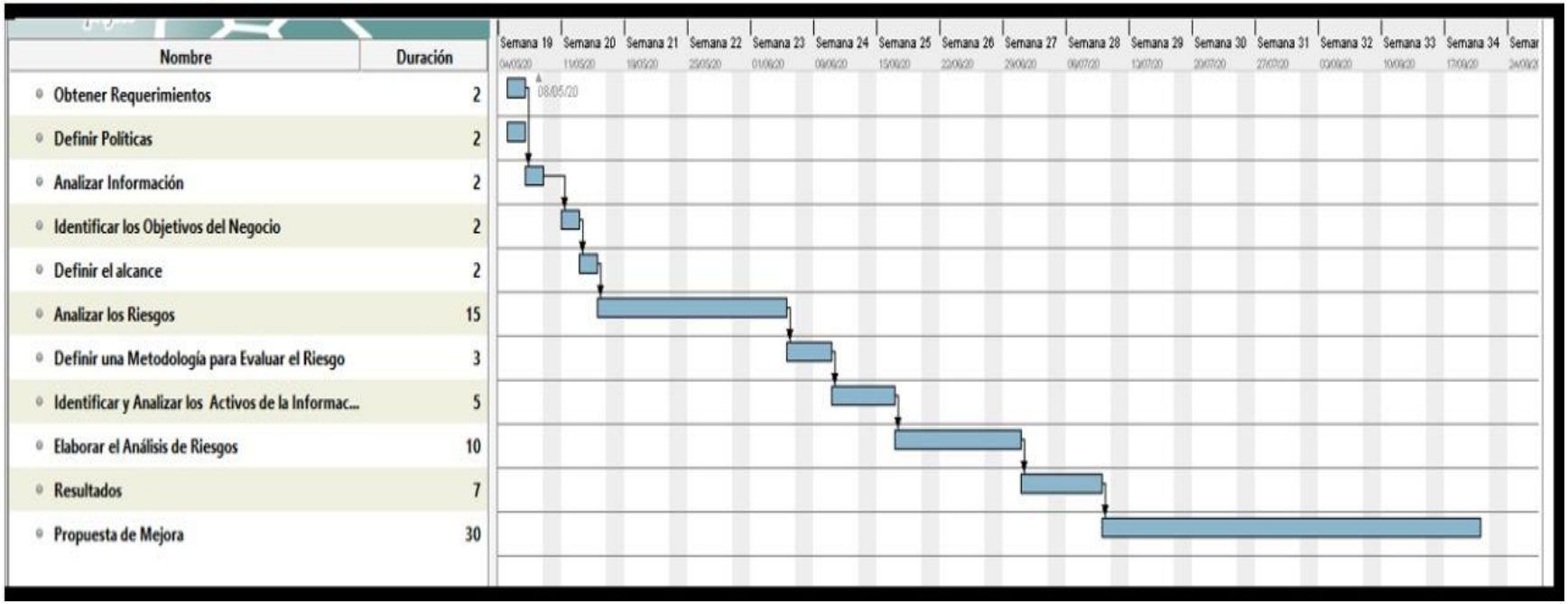
Es importante mencionar que las salvaguardas sugieren permitir minimizar los riesgos, pero cada una tiene un costo por lo que en cada caso en particular se debe evaluar el valor de la información a proteger y los costos que implicaría la pérdida o el sufrimiento de un ataque y en este sentido planificar las acciones pertinentes para la protección de la información.

Los resultados ayudaran a la organización a reconocer la necesidad de iniciar la implementación de un plan de gestión de riesgos que permiten mitigar los riesgos más críticos, hasta que decidan desarrollar un plan de tratamiento de riesgo en el que se considera la contratación del personal especializado en seguridad, análisis de documentos y registros de incidentes.

5.3.5. Plazo de ejecución

La implementación del sistema se llevará a cabo en un plazo no mayor de 80 días.

Grafico Nro.16:Tiempo de realización



Fuente: Elaboración Propia

V. CONCLUSIONES

1. En lo que respecta a la dimensión 01: Nivel de conocimiento. En la Tabla Nro. 15 se puede interpretar que el 50 % de los trabajadores encuestados contestaron que no tienen conocimiento acerca de seguridad de la información. Este resultado tiene una similitud con lo indicado en la hipótesis para esta dimensión, por lo tanto, se concluye que la hipótesis es aceptada.

2. Con respecto a la dimensión 02: Seguridad de la información, en la Tabla Nro.26 se puede examinar que el 55 % de los trabajadores encuestados contestaron que NO existe en la municipalidad seguridad de la información, por lo tanto, no cuenta con la seguridad adecuada para los activos de la municipalidad. Este resultado tiene una similitud con lo indicado en la hipótesis para esta dimensión, por lo tanto, se concluye que la hipótesis es aceptada.

RECOMENDACIONES

1. Conseguir los servicios de un especialista que pueda guiar una implementación exitosa de la norma, adoptando las políticas de seguridad de información señaladas en la investigación, debido a que estas se alinean a lo que establece la norma ISO/IEC 27001, que es un estándar reconocido dentro del ámbito de la seguridad de información.

2. Establecer un rol de "Oficial de Seguridad de Información" dentro de la municipalidad para el monitoreo y cumplimiento de las políticas y controles establecidos.

3. Capacitar a todo el personal de manera periódica con respecto a la seguridad de la información, para lograr que todos los involucrados tengan los mecanismos o procedimientos claros frente a las amenazas o riesgos de seguridad y así poder salvaguardar la información.

4. Actualizar de manera habitual el Sistema de Gestión de Seguridad de la Información, debido a la posible modificación de las actividades de los procesos, aparición de activos de información y aparición de nuevas amenazas, riesgos.

REFERENCIAS BIBLIOGRÁFICAS

1. Chicano E. Gestión de Incidentes de Seguridad Informática. IFCT0109. primera edición ed. Editorial I, editor. Málaga; 2015.

2. Aguilar M. Plan de Seguridad Informática Basado en Estándar ISO-IEC 27001 para Proteger la Información y Activos del Gad Cantonal de Pastaza. Tesis Grado Académico De Magister En Informática Empresarial. Ecuador: Universidad Regional Autónoma De Los Andes "UNIANDES", Sistemas Mercantiles; 2017.

3. Bermúdez K , Bailón E. Análisis en Seguridad Informática y Seguridad de la Información Basado en la Norma ISO/IEC 27001-Sistemas de Gestión de Seguridad de la Información Dirigido a una Empresa de Servicios Financieros. Tesis para obtener el título de Ingeniero de Sistemas. Guayaquil: Universidad Politécnica Salesiana, Departamento de Ingeniería; 2015.

4. Landázuri Y. Auditoría a la Seguridad del Sistema de Información Sivigila de la Alcaldía de San Andrés de Tumaco Basado en el Estándar Iso 27001. Tesis para obtener el título de Ingeniera de Sistemas. San Juan de pasto: Universidad de Nariño, Departamento de Ingeniería; 2015.

5. Celis L. Plan de Seguridad de la Información Aplicado a la Central Hidroeléctrica Carhuaquero. Tesis para Optar el Título de Ingeniero de Sistemas Y Computación. Chiclayo: Universidad Católica Santo Toribio de Mogrovejo, Ingeniería; 2018.

6. Ccesa M. "Diseño de un Sistema de Gestión de Seguridad de la Información Bajo la NTP ISO/IEC 27001:2014 Para la Municipalidad Provincial de Huamanga, 2016". Para optar el título profesional de: Ingeniero Informático. Ayacucho: Universidad Nacional de San Cristóbal De Huamanga, Ingeniería; 2017.

7. García A. Implementacion de un Sistema de Gestión de Seguridad de la Información,Aplicado a los Riesgos Asociados a los Activos de Información en la Empresa Net-Consultores S.A.C. Tesis para Optar el título de Ingeniero de Sistemas

e Informática. Tarapoto: Universidad Nacional de San Martín , Departamento de Ingeniería de Sistemas e Informática ; 2016.

8. 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 Para Optar el Título Profesional de Ingeniero Informático. Piura: Universidad Nacional de Piura , Ingeniería Informática ; 2019.

9. Lara K. Propuesta para la Seguridad Informática Basado en La Norma ISO/IEC 27001 en la Clínica Simedic Diagnóstica S.A.C – Piura; 2018. Tesis para optar el tìtulo profesional de Ingeniero de Sistemas. Piura: Universidad Católica los Ángeles de Chimbote, Ingeniería;2018.

10. Agurto M. Diagnóstico de los activos de información de los procesos implementados por el estándar ISO 9001 en el área QHSE de la empresa PISER S.A.C Talara, basado en la norma ISO 27001. Tesis para Optar el Título Profesional de Ingeniero de Sistemas. Piura: Universidad Cesar Vallejo, Ingeniería; 2017.

11. Pantoja R, Muñoz J. Leyes administrativas sobre municipalidades. Primera Edición ed. Chile EJd, editor. Chile; 1994.

12. Practicas S, editor. Las Municipalidades y su papel en la Democratización y el Desarrollo del País: Asociación Servicios Educativos Rurales; 1998.

13. Davila J. Perú, gobiernos locales y pueblos indígenas IWGIA IWGIA , editor.; 2005.

14. Municipalidad Distrital Suyo. [Online].; 2015 [cited 2017 Febrero. Available from: http://www.munisuyo.gob.pe/portal/.

15. Estrada J. Modelo para la gestión de tecnologías de información y comunicación en la gestión empresarial. Santiago de Cuba : Universidad Oriente ; 2014.

16. Azinian H. Las tecnologías de la información y la comunicación en las prácticas pedagógicas. Primera ed. CEP , editor. Buenos Aires; 2009.

17. De R . Negocio electrónico Madrid: UNED; 2009.

18. Katz R. El Papel de las TIC en el Desarrollo. Segunda Edición ed. Katz R, editor. España; 2009.

19. Palacios Y. Nivel de gestíon del Dominio Planificación y Organización de las Tecnologías de Información y Comunicaciones (TIC)en la Municipalidad Provincial de Piura. Tesis para optar el Tìtulo Profesional de Ingeniero de Sistemas. Piura: Universidad Católica los Ángeles Chimbote , Departamento de Ingenierìa ; 2016.

20. Soy C. Auditoría de la Información:Identificar y Explotar la Información en las Organizaciones: UOC; 2014.

21. Tapia C , Salomón L , Guevara E , Castillo S , Rojas M. Fundamentos de Auditoría:Aplicación Práctica de las Normas Internacionales de Auditoría IMCP , editor.; 2016.

22. Chicano E. Auditoría de Seguridad Informática. IFCT0109 IC , editor. Málaga; 2019.

23. Aguilera P. Seguridad Informática: EDITEX; 2010.

24. Alegre M, . Cervigón A.Seguridad Informática Paraninfo E, editor.; 2011.

25. Gómez L, Andrés A. Guía de aplicación de la Norma UNEISO/IEC 27001 sobre seguridad en sistemas de información para pymes. Segunda ed. AENOR , editor. España; 2012.

26. Tecnología de la Informacion.Tecnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. Comisión de normalización y de fiscalización de barreras comerciales no Arancelarias-INDECOPI. 2014 Noviembre;(45).

27. Urbina R. slideshare.net. [Online].; 2014 [cited 2020 Marzo 14. Available from: https://es.slideshare.net/mobile/RicardoUrbinaM/iso-40313086.

28. Castro M, Díaz G, Alzorriz I, SanCristóbal E. Procesos y Herramientas para la Seguridad de Redes UNED E, editor. Madrid ; 2014.

29. Gómez Á. Enciclopedia de la Seguridad Informática. 2ª edición. Segunda edición ed. España: RA-MA; 2011.

30. Gómez L, Fernández P. Cómo Implantar un SGSI Según UNEISO/IEC 27001:2014 y su Aplicación en el Esquema Nacional de Seguridad España: AENOR; 2015.

31. Atehortúa F, Bustamante R, Valencia J. Sistema de gestión integral. Una sola gestión, un solo equipo Antioquia Ud, editor. Antioquia; 2008.

32. Colobran M , Arques J, Marco E. Administración de sistemas operativos en red. primera ed. UOC E, editor.; 2008.

33. Guagalango R , Moscoso P. Evaluación Técnica de la Seguridad Informática Del Data Center de la Escuela Politécnica del Ejército. [Online].; 2020 [cited 2020 Marzo 13. Available from: http://slideplayer.es/slide/1644740/.

34. Mantilla A. Diseño de un Sistema de Gestión de Seguridad de la Información para Cooperativas de Ahorro y Crédito en Base a la Norma Iso 27001. Tesis Previa a la Obtención del Grado de Máster,en Gestión de las Comunicaciones y Tecnologías de la Información,MSC. Quito : Escuela Politécnica Nacional , Departamento de Ingeniería ; 2009.

35. Cortés M, Iglesias M. Generalidades Sobre Metodología de Investigación. Trabajo de Investigación. México : Universidad Autónoma del Carmen ; 2004. Report No.: ISBN.

36. Sabino C. El Proyecto de Investigación. Tercera Edición ed. Carlos , editor. Caracas : Episteme; 1999.

37. Barragàn R, Ayllón V, Sanjinés J, Langer E, Córdova J, Rojas R. Guía para la Formulación y Ejecución de Proyectos de Investigación. Tercera Edición ed. Bolivia: Offser Boliviana Ltda; 2003.

38. Naghi M. Metología de la Investigación Limusa E, editor. Mexico ; 2005.

39. Sáez J. Investigación Educativa.Fundamentos teóricos,Procesos y Elementos Prácticos.Enfoque Práctico con Ejemplos ,esencial para TFG,TFM y Tesis. 2017th ed. Madrid: UNED; 2017.

40. Tamayo M. El proceso de la Investigación Cientifífica. Cuarta Edición ed. Noriega G, editor. México: Limusa ; 2004.

41. Gómez M. Introducción a la Metología de la Investigación Científica. primera Edición ed. Marcelo , editor. Argentina: Brujas ; 2005.

42. Alberto M. "Plan de seguridad de la Información Basado en la Norma Técnica Peruana NTP-ISO/IEC 27001:2014 para el Centro de salud Mental Comunitario San Gabriel Alto". Ingeniero de Sistemas. Lima: Universidad Nacional Tecnológica de Lima Sur, Ingeniería ; 2016.

43. Segovia A. Iso 27001. [Online].; 2017 [cited 2020 Marzo 15. Available from: https://advisera.com/27001academy/es/herramientas/.

44. Yan F, Zavala C. "Plan de mejora de la Seguridad de Información y Continuidad del Centro de Datos de la Gerencia Regional de Educación La Libertad aplicando lineamientos ISO 27001 y buenas prácticas COBIT ". Tesis Para Obtener el Título Profesional de Ingeniero de Computación y Sistemas. Trujillo : Universidad Privada Antenor Orrego, Deparatmento de Ingeniería ; 2013.

45. Zapata O. Herramientas para Elaborar Tesis e Investigaciones SocioEducativas. Primera Edición ed. México: Pax México; 2005.

46. Corral Y. Diseño de Cuestionarios para Recolección de Datos. Revista Ciencias de la Educación. 2010 Diciembre; 20(17).

ANEXOS

Anexo Nº 1: Cronograma de actividades

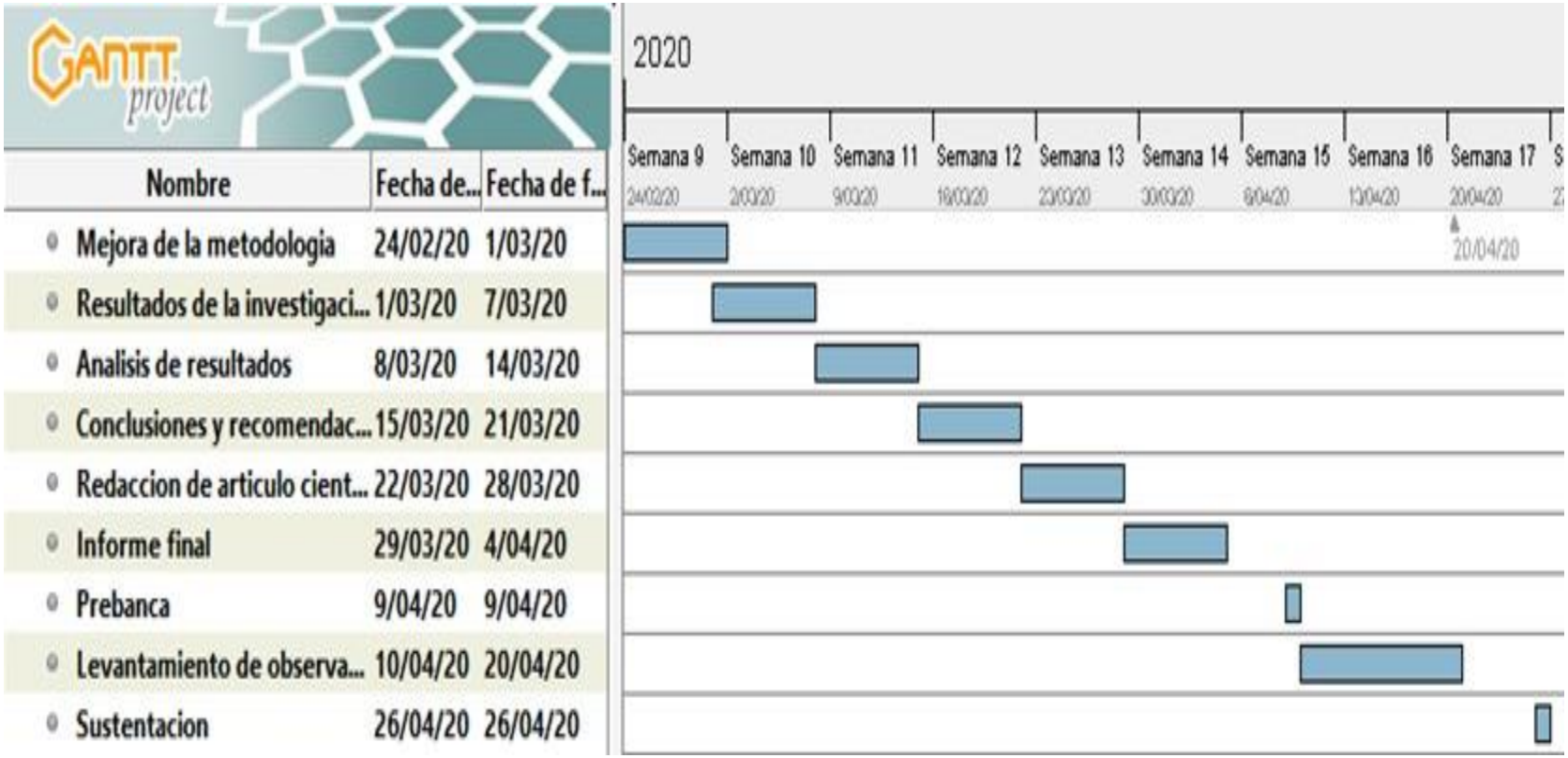


Imagen Elaborada con Software licenciado “Gantt Proyect”.

Anexo Nº 2: Presupuesto

DESCRIPCIÓN	CANTIDAD	COSTO UNITARIO	TOTAL PARCIAL	TOTAL
1. REMUNERACIONES				
1.1. Asesor	01	1500.00	1500.00	
1.2. Estadístico	01	200.00	200.00	
			1,700.00	1,700.00
2. BIENES DE INVERSIÓN				
2.1. Impresora	01	230.00	230.00	
			230.00	230.00
3. BIENES DE CONSUMO				
3.1. Papel bond A-4 80	01 m	25.00	25.00	
3.2. Tóner para impresora	01	50.00	50.00	
3.3. CD	02	2.00	2.00	
3.4. Lapiceros	02	1.00	1.00	
3.5. Lápices	02	2.00	2.00	
			80.00	80.00
4. SERVICIOS				
4.1. Fotocopias	50 hoja	25.00	25.00	
4.2. Anillados	3	20.00	20.00	
4.2. Servicios de Internet	90hrs	90.00	90.00	
4.3. Pasajes locales		240.00	240.00	
			375.00	375.00
TOTAL				**2,385.00**

Fuente: Elaboración Propia

Anexo Nº 3: Cuestionario

El presente instrumento forma parte del trabajo de investigación titulada: "Implementación de Auditoría Informática con la ISO 27001 en la Municipalidad Distrital De Suyo-Piura; 2020." Por lo que se solicita su participación, respondiendo a cada pregunta de manera objetiva y veraz. La información por proporcionar es de carácter confidencial y reservado; y los resultados de la misma serán utilizados solo para la presente investigación.

INSTRUCCIONES: A continuación, se le presenta 20 preguntas que deberá responder, marcando con un aspa ("X") en el recuadro correspondiente (SI o NO) según considere la alternativa correcta.

NIVEL 1: NIVEL DE CONOCIMIENTO DE LA INFORMACIÓN			
Nro.	Pregunta	SI	NO
1	¿Cuentan la municipalidad con un responsable encargado de evaluar la adquisición y cambios de los sistemas de información?		
2	¿Existe alguna norma relativa a la seguridad de sistemas de Información?		
3	¿En la municipalidad existen documentos de políticas de seguridad Informática?		
4	¿En la municipalidad existen mecanismos para la comunicación a los trabajadores acerca de las normas de seguridad?		
5	¿Existen programas de formación en seguridad para los trabajadores de dicha municipalidad?		
6	¿Existen roles y responsabilidades definidas para las personas comprometidas en la seguridad?		
7	¿En la municipalidad figuran un acuerdo de confidencialidad de la información a la que accede?		
8	¿Consta la municipalidad de un proceso disciplinario de la seguridad de la información?		
9	¿Conoce usted si en la municipalidad existen áreas restringidas a las cuales solo puede acceder el personal autorizado?		
10	¿Existe en la municipalidad un canal y procedimientos claros a seguir en caso de incidente de seguridad?		

NIVEL 2: SEGURIDAD DE LA INFORMACIÓN			
Nro.	Pregunta	SI	NO
1	¿Cuenta la municipalidad con algún método para reducir el mal uso occidental deliberado de los sistemas?		
2	¿Existe asentadores externos para la gestión de los sistemas de información?		
3	¿Elaboran copias de backup para resguardar la información esencial de la municipalidad?		
4	¿Existe seguridad en la documentación de los sistemas de información?		
5	¿Disponen de medidas de seguridad en el comercio electrónico?		
6	¿Existe algún sistema de encriptación de password de acceso al sistema que utiliza?		
7	¿Cuenta la municipalidad un plan de capacidad para asegurar la adecuada capacidad de proceso y almacenamiento de la información?		
8	¿Existen logs para las actividades realizadas por los operadores y administradores de la municipalidad?		
9	¿En la municipalidad existe una política de control de accesos?		
10	¿Existen controles criptográficos en dicha municipalidad?		