UNIVERSIDAD PERUANA UNIÓN

FACULTAD DE INGENIERÍA Y ARQUITECTURA

Escuela Profesional de Ingeniería de Sistemas

Una Institución Adventista

Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazona

Por:
Henry Percy Cabrera Cubas

Asesor:
Mg. Miguel Ángel Valles Coral

Tarapoto, noviembre de 2018

DECLARACIÓN JURADA

DE AUTORÍA DEL INFORME DE TESIS

Mg, Miguel Ángel Valles Coral asesor de investigación de la Facultad de Ingeniería y Arquitectura de la Universidad Peruana Unión Filial Tarapoto.

DECLARO:

Que el presente informe de investigación titulado: "DISEÑO DE UN MODELO DE POLÍTICAS BASADO EN LA NORMA ISO 27001, PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE FLORIDA – BONGARÁ – AMAZONAS" constituye la memoria que presenta el Bachiller Henry Percy Cabrera Cubas, para aspirar al título Profesional de Ingeniero de Sistemas, cuya tesis ha sido realizada en la Universidad Peruana Unión Filial Tarapoto, bajo mi dirección.

Las opiniones y declaraciones en este informe son de entera responsabilidad del autor, sin comprometer a la institución.

Y estando de acuerdo, firmo la presente declaración en Tarapoto, a los 06 días del mes de noviembre del año 2018.

Mg, Miguel Ángel Valles Coral

Asesor

Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

TESIS

Presentada para optar el título profesional de Ingeniero de Sistemas

JURADO CALIFICADOR

Mg. Danny Lévano Rodríguez
Presidente

Ing. Joel Pérez Suárez
Secretario

Ing. Jenson Daniel Chambi Aguilar
Vocal

Mg. Miguel Angel Valles Coral
Asesor

Tarapoto, 29 de agosto del 2018

Dedicatoria

A mis padres José Demetrio Cabrera Quintana y Dina Cubas Becerra, quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía, de no temer las adversidades porque Dios está conmigo siempre.

A mis hermanas, que con sus consejos me han ayudado a afrontar los retos que se me han presentado a lo largo de la mi vida.

Agradecimientos

A Dios por ser mi guía durante todo el proceso de mi investigación, por darme la sabiduría y entendimiento en el desarrollo de la investigación.

A mis padres por todo el sacrificio incondicional realizados a lo largo de todos estos años para lograr alcanzar mi meta planeada.

A los docentes de la Universidad Peruana Unión que me brindaron su sabiduría durante cada clase para poder alcanzar mi meta.

Al Mg. Miguel Ángel Valles Coral por toda la colaboración brindada, durante la elaboración de este proyecto.

A mis amigos por su amistad y motivación, que de una y otra manera me ayudaron a realizar mis metas.

A todos, mis respetos.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

Símbolos y términos

TI: “Tecnología de la información (TI, o más conocida como IT por su significado en inglés: information technology) es la aplicación de ordenadores y equipos de telecomunicación para almacenar, recuperar, transmitir y manipular datos, con frecuencia utilizado en el contexto de los negocios u otras empresas”.

TIC: “El término tecnologías de la información y la comunicación (TIC) tiene dos acepciones. Por un lado, a menudo se usa tecnologías de la información para referirse a cualquier forma de hacer cómputo. Por el otro, como nombre de un programa de licenciatura, se refiere a la preparación que tienen estudiantes para satisfacer las necesidades de tecnologías en cómputo y comunicación de gobiernos, seguridad social, escuelas y cualquier tipo de organización”.

CONTROL: “Políticas, procedimientos, prácticas y estructuras organizacionales, diseñados para proporcionar una seguridad razonable de que los objetivos del negocio serán alcanzados y que eventos no deseados serán prevenidos o detectados o corregidos”.

ISACA: “Asociación para la Auditoría y Control de Sistemas de Información. (Information Systems Audit and Control Foundation)”.

ISO: “Organización de Estándares Internacionales. (International Standards Organisation) (con oficinas en Génova, Suiza)”.

UTILIDAD: “Capacidad que tiene una cosa de servir o de ser aprovechada para un fin determinado”.

USABILIDAD: “Es la medida de la calidad de la experiencia que tiene un usuario cuando interactúa con un producto o sistema”.

CREDIBILIDAD: “Capacidad de ser creído es decir esto debe generar confianza”.

ACCESIBILIDAD: “Posibilidad de acceder a cierta cosa o facilidad para hacerlo”.

SEGURIDAD: “Sensación de total confianza que se tiene en algo o alguien o ausencia de peligro o riesgo”.

METODOLOGÍA: “Conjunto de métodos que se siguen en una investigación científica, un estudio o una exposición doctrinal”.

CONFIABILIDAD DE LA INFORMACIÓN: “Se refiere al suministro de información apropiada para la administración de las operaciones del negocio y para ejercer sus responsabilidades de reportes financieros y de cumplimiento”.

EFECTIVIDAD: “Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consístete, y de manera utilizable”.

EFICACIA: “Es la provisión de información a través de la utilización óptima de recursos”.

CONFIDENCIALIDAD: “Es la protección de información sensible contra divulgación no autorizada”.

INTEGRIDAD: “Es la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio”.

DISPONIBILIDAD: “Se refiere a la disponibilidad de la información cuando esta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas”.

CUMPLIMIENTO: “Se refiere a al cumplimiento de aquellas leyes, regulaciones y acuerdos y acuerdos contractuales a los que el proceso de negocio está sujeto, por ejemplo, criterios de negocio impuestos externamente”.

TECNOLOGÍA: “La tecnología cubre hardware sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc”.

PERSONAL:” Habilidades del personal, conocimiento, sensibilización y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información”.

MONITOREO: “Es la constante evaluación a través del tiempo para verificar su calidad y suficiencia en cuanto a su calidad y suficiencia de control”.

ENTREGA Y SOPORTE: “Se refiere a la entrega o distribución de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por la seguridad en los sistemas y la seguridad de las operaciones, así como aspectos sobre entrenamiento. Con el fin de proveer servicio, deberán establecer los procesos de soporte necesarios”.

RESUMEN

El presente trabajo de investigación tiene como objetivo implantar el diseño de un modelo de políticas basado en la norma ISO 27001 para la gestión de la seguridad de la información en la Municipalidad Distrital de Florida, Bongará – Amazonas, 2018, donde han incrementado mejoras en la seguridad de la información. Por tal motivo el estudio tiene un diseño “Pre-experimental” y una población conformado por el personal administrativo; como el Alcalde, Gerente, Tesorero, etc. que en su conjunto suman 13 trabajadores. Los resultados que se obtuvieron en el post test fueron satisfactorios ya que los trabajadores que laboran en dicha entidad están comprometidos y capacitados con temas relacionados con la seguridad de la información, eso quiere decir que la información que posee dicha entidad se encuentra protegida y segura. La investigación se dio por medio de cuatro dimensiones como: Políticas, Servicio, Riesgo y Consistencia; de estas dimensiones se muestra que la significancia bilateral (valor de P) es 0,717, 0,732, 0,394, 0,886 la cual es mayor a 0.05.

Palabras clave: Norma ISO 27001, seguridad de la información, políticas, gestión, seguridad, consistencia.

ABSTRACT

The present research work aims to implement a model policy design based on the ISO 27001 standard for management of information security in the District Municipality of Florida, Bongará, Amazonas - Peru, 2018, where improvements have been made in information security. For this reason, the study has a "Pre-experimental" design and a population consisting of administrative staff such as the Mayor, Manager, Treasurer, etc. all together making up a total of 13 workers. The results obtained in the post test were satisfactory since workers working in this entity are committed and trained with issues related to information security, that means that the information held by this entity is protected and safe. The research was done through four dimensions such as: Policies, Service, Risk, and Consistency; from these dimensions it is shown that the bilateral significance (P value) is 0,717, 0,732, 0,394, 0,886 which is greater than 0.05.

Keywords: ISO 27001 standard, information security, policies, management, security, consistency.

CAPÍTULO I: INTRODUCCIÓN

Hablar hoy en día sobre el tema de seguridad de la información y el rol que cumplen los servicios críticos en la Municipalidad Distrital de Florida es un tema muy importante. En ello contamos con varios recursos de información como; sistemas de información, redes, archivos, proyectos, etc. Esto nos sirve como apoyo para los, trabajadores, esto debería estar bien planteado en el estudio y trabajo, pero no debe ser permitida para la utilización con fines comerciales. Es por eso que la siguiente investigación brinda información valiosa que servirá como un apoyo para que analicen los resultados sobre la calidad y eficacia de servicio y también plantear políticas de seguridad de la información.

"Hoy en día la pérdida de información en las organizaciones es un punto muy importante en la cual uno debe estar a la preventiva de ella para que no haya sabotaje, violación de la privacidad, intrusos terceros" (Standardization, 2015).

Es por esta razón que, la presente investigación se orienta a demostrar que una gestión de seguridad de la información basada en políticas de seguridad resultara exitosa; esto si se toma en cuenta todas sus necesidades de las diferentes áreas de la Municipalidad Distrital de Florida, y que contribuya con la eficacia y la calidad en los servicios críticos como son los servicios de, Cartas, Licitaciones, Ordenanzas, Informes, Proyectos, etc. Estos servicios recopilan información valiosa y confidencial tales como: registros de postulantes a las licitaciones, registros de postulantes a los proyectos, registro de archivos, documentación de certificaciones, base de datos financieros, base de datos económicos, registro de direcciones de correos electrónicos.

La investigación propuesta muestra conceptos, teorías de información dentro del contexto de seguridad de la información como son los sistemas de información, análisis, riesgos, seguridad, lo que busca es encontrar explicaciones muy claras para contribuir con calidad y eficacia de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas, para el desarrollo de la investigación contamos con una revisión

de la literatura, materiales y métodos, conclusiones y recomendaciones, anexos y biografías.

En la investigación propuesta, hablamos de seguridad de la información; pero no de seguridad informática que es totalmente diferente, se habla de seguridad de información porque lo que importa está representada de diversas formas como: impresa, escrita, almacenada en forma electrónica. Es por ello que nuestro objetivo está referido principalmente a temas relacionados con la información, la forma que posee la información debe usarse y protegerse de manera adecuada.

El objetivo de la investigación es la implantación de un modelo de políticas basado en la norma ISO 27001, para la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas, 2017, y para el cumplimiento de este objetivo tenemos que llevar acabo la recolección de información para definir el alcance, objetivos y políticas del desarrollar el SGSI para velar por la confidencialidad, integridad y disponibilidad de la información de la Municipalidad Distrital de Florida, analizar las probabilidades e impactos y niveles de riesgos con la implantación de SGSI, y establecer políticas de seguridad de información en la Municipalidad Distrital de Florida.

La investigación está desarrollada en cinco capítulos; en el primer capítulo se presentan los aspectos metodológicos de la investigación, desarrollándose dentro de ella; identificación del problema, formulación del problema, los objetivos de la investigación, la justificación y su preposición filosófica.

En el segundo capítulo se desarrolla la revisión de la literatura que sustenta la investigación. En este capítulo se estudia el origen de la información y los atributos principales de la seguridad de la información como la confidencialidad, integridad y disponibilidad, todo eso está desarrollado referido a la norma ISO 27001.

En el tercer capítulo se presenta los materiales y métodos que se utilizó en el desarrollo de la investigación como: El tipo de investigación, descripción del lugar de ejecución, población y muestra, diseño de la investigación, formulación de hipótesis,

identificación de variables, operacionalización de variables, instrumentó de recolección de datos, y el procesamiento y análisis de datos.

En el cuarto capítulo se presenta el desarrollo de la solución, donde se muestra el Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

En el quinto capítulo se precisan los resultados y discusiones de la propuesta presentada, para mejorar la seguridad de la información de la Municipalidad Distrital de Florida.

En el sexto y último capítulo se muestran las conclusiones recopiladas con la presente investigación y las recomendaciones que de ellas se generan, como una forma de contribuir con la gestión de seguridad de la información en la Municipalidad Distrital de Florida

Para llegar a cumplir los objetivos de la investigación, se acude a las técnicas de la investigación, y para el procesamiento de la información se utilizó las herramientas de Microsoft Office, SPSS.

De esta forma, teniendo en cuenta los lineamientos con la Facultad de Ingeniería y Arquitectura, con esta investigación espero contribuir con los postulados de la universidad y el desarrollo de las organizaciones que nos rodean.

CAPÍTULO II: REVISIÓN DE LA LITERATURA

Antecedentes

Según los autores Dos, Santos y Alves, (2014) con el tema de investigación: “Sistema de Gestión de Seguridad de la Información en el club militar con la norma ISO 27001:2005, El objetivo de este proyecto de investigación es implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para la protección de los inventarios de activos de datos las cuales no estaban actualizados siendo estos de mayor importancia, pues son lo que contiene los registros que se generan en las operaciones misionales. En consecuencia, al club Militar le faltaba implementar el Sistema de Gestión de Seguridad de la Información ya que el acceso, administración y protección a la información presentaba una gran debilidad al no poseer un sistema de administración de seguridad de la información aplicable a toda la infraestructura informática”.

“El mencionado antecedente se relaciona con la investigación en la parte que referencia a los Sistemas de Gestión y Guías de implementación en la seguridad en este en particular se utiliza una metodología específica conocida la de Piattini” (Tavalera, 2015).

Según Tavalera (2015), muestra, En su tema de investigación: “Sistema de Gestión de Seguridad de la Información para una entidad estatal de salud ex maternidad Lima utilizando como normativa la ISO 27001-2013”.

Donde sostiene que: “En la mencionada entidad estatal especializada en brindar servicios de salud a mujeres gestantes y neonatos. Como entidad prestadora de salud manejaba información sobre sus pacientes que permite mantener un historial las atenciones y diagnósticos de los mismos por lo cual en estos historiales clínicos que contienen información personal que identifican al paciente y debe ser protegida ya se para poder garantizar la correcta atención evitar la fuga de información que pueda ser utilizada de manera maliciosa por alguna persona o institución externa al flujo de información el objetivo es idéntico a dicha investigación por la cual está relacionada en implementar un SGSI con la normativa ISO/IEC 27001:2013, Los resultados esperados es de tener una

documentación exigida por la norma ISO/IEC 27001:2013,Mapa de procesos del alcance, Metodología de análisis de riesgos, Metodología de valoración de activos , Mapa de riesgos , Declaración de aplicabilidad" (Tavalera, 2015).

Justino Salinas (2015), pretende. "Con el tema de investigación: Diseño de un Sistema de Gestión de Seguridad de Información para una empresa inmobiliaria alineado a la norma ISO/IEC 27001:2013 afirma dar soluciones mediante la administración de la seguridad de información en una empresa del sector inmobiliario ,cuyo objetivo será gestionar de manera eficiente la información y desde el punto de vista de la alta dirección , permitir obtener una visión global del estado de los sistemas de información sin caer en detalles técnicos , además de observar las medidas de seguridad aplicadas y los resultados obtenidos, para finalmente tomar las mejores decisiones estratégicas para la organización".

Marco Conceptual

"A continuidad, se muestran los principales conceptos necesarios para el complemento entendimiento del desarrollo del presente proyecto, así como el Sistema de Gestión de Seguridad de la Información que se pretende alcanzar en el mismo" (ISSA, 2011).

1.1. Seguridad de la Información

Qualitas Consultores (2012), menciona. "La seguridad de información se caracteriza por la preservación de la confidencialidad, asegurando que la información sea accesible sólo por aquellos que están autorizados; la integridad, salvaguardando la exactitud de la información en su procesamiento; y finalmente su disponibilidad, asegurando que los usuarios tengan acceso a la información y a los activos asociados cuando sean requeridos".

Algunas características de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas.

- **Confidencialidad**, "es la garantía y protección de la información confidencial del acceso o divulgación por parte de entidades" (ISSA, 2011).

- **Integridad**, “la información debe mantenerse permanentemente protegida frente a la modificación o eliminación sin la autorización o accesos necesarios y es necesario garantizar la información sea la correcta en todo momento” (ISSA, 2011).
- **Disponibilidad**, “la información debe estar disponible para su uso en todo momento, cuando se lo requiera. También se considera como parte de la disponibilidad, la rapidez con que se puede ofrecer servicios o realizar operaciones” (ISSA, 2011).
- **Autenticación**, “permite identificar a la persona o personas que han generado la información que se está verificando, permite una validación en autoría de la información por parte de un usuario especifico” (ISSA, 2011).
- **No repudio**, “permite que la información se validada a través de algún mecanismo que compruebe su integridad y contenido, declarándola como genuina” (ISSA, 2011).

  “Estas propiedades son las mínimas que un SGSI debe proteger para asegurar la información de la organización según” (Indecopi, 2008).

1.2. Sistema de Gestión de Seguridad de la Información (SGSI)

Según INDECOPI (2011), describe que. “Este sistema se fundamenta en la norma UNE-ISO/IEC 27001:2007, es parte del sistema gerencial general, está basado en un enfoque de riesgo comercial para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de información; sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o ciclo Deming, o más conocido como PDCA (Plan-Do-Check-Act), asimismo se tiene su fundamento en la norma UNE-ISO/IEC 27002:2009 que recoge una lista de controles necesarios para lograr los objetivos de seguridad de información”.

“El Sistema de Gestión de Seguridad de la Información (SGSI) está diseñado para asegurar una selección de controles de seguridad que protejan los activos de información

y den confianza a las partes interesadas; El diseño e implementación del Sistema de Gestión de Seguridad de la Información (SGSI) de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad , procesos, tamaño y estructura de la organización" (García, 2012).

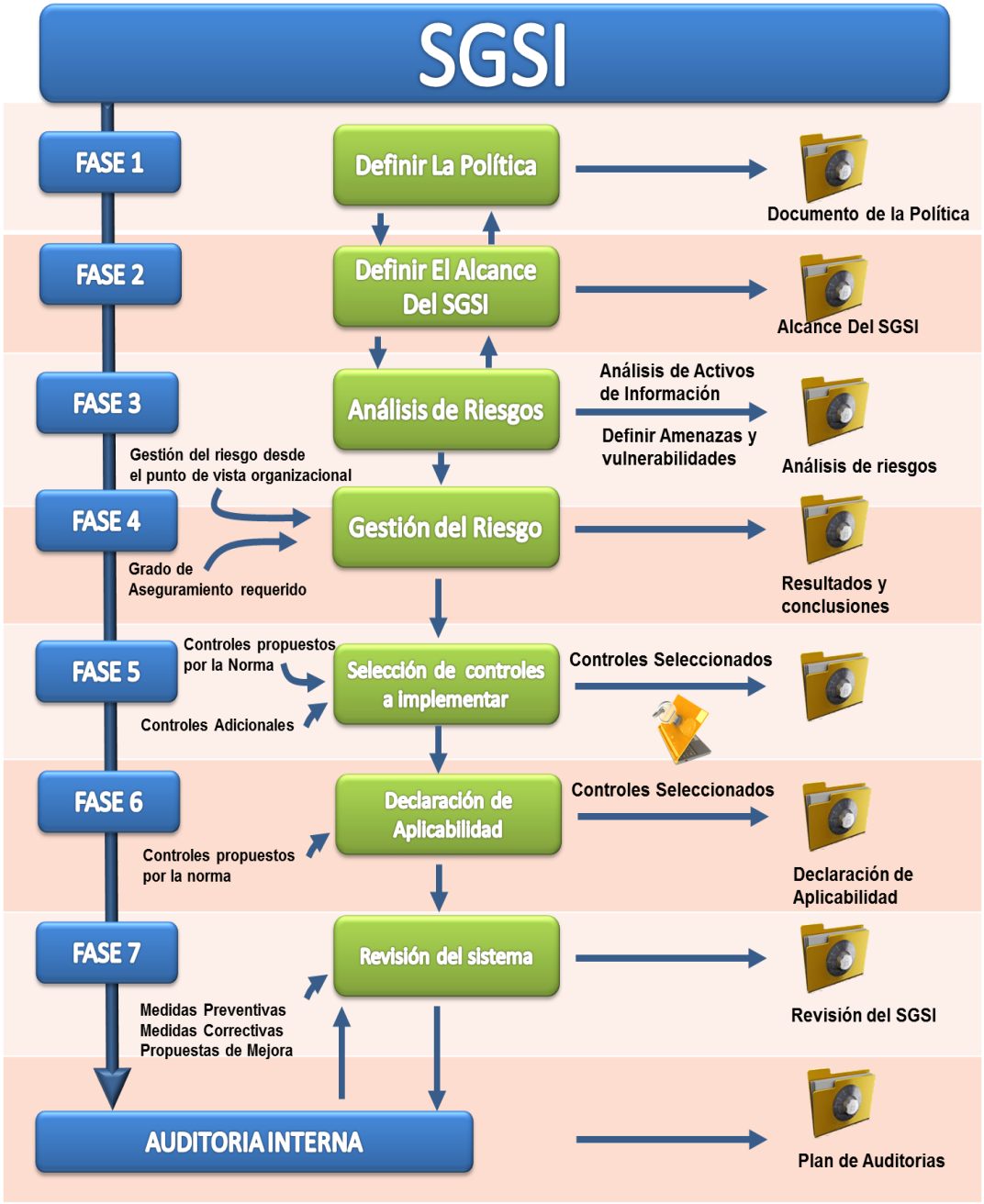


Figura 1: Fases del sistema de gestión de seguridad de la información.

Fuente: Norma ISO 27001: http://www.normas-iso.com/iso-27001/

1.3. Gestión de Seguridad de la Información

"La Gestión de Seguridad de la Información, es un proceso continuo que consiste en garantizar que los riesgos de la seguridad de la información sean identificados, valorados, gestionados y tratados por todos los miembros de la organización de una forma documentada, sistemática, estructura, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías" (Standardization, 2015).

"La GSI, instancia la participación activa de toda la organización con relación a la planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de la información, así como el debido control de acceso a los recursos y activos de información" (Standardization, 2015).

INDECOPI, (2011), alude, "La gestión de la seguridad de la información, implica que las organizaciones clasifican sus activos de información en términos de su valor, requerimientos legales, sensibilidad y criticidad. Con el propósito de identificar los riesgos que pueden afectar su seguridad y determinar las medidas de prevención, detección, retardo y reacción que se requieran implementar para controlar al acceder no autorizado a las instalaciones, recursos, sistema e información de la organización, o cualquier amenaza proveniente del entorno, la naturaleza y las acciones del hombre que pueda llegar a comprometer el normal funcionamiento y operación del negocio".

1.4. BMIS (Business Model Information security)

"Esta guía tiene un enfoque integral y orientado a los negocios de gestión de seguridad de la información. Establece un lenguaje común para referirse a la protección de la información y permite a los profesionales examinar la seguridad desde la perspectiva de los sistemas, creando un entorno donde la seguridad se puede gestionar de manera integral, permitiendo que los riesgos reales sean abordados" (INDECOPI, 2011).

"El Busines Model Information Security, está conformado de cuatro elementos y seis interconexiones dinámicas, asimismo puede ser visto como un modelo tridimensional, mejor visualizada como pirámide" (Isaca, 2013)

Elementos:

- Organización
- Personas
- Procesos
- Tecnologías

Interconexiones dinámicas:

- Cultura
- Arquitectura
- Gobierno
- Penetración
- Habilitación y soporte
- Factores humanos

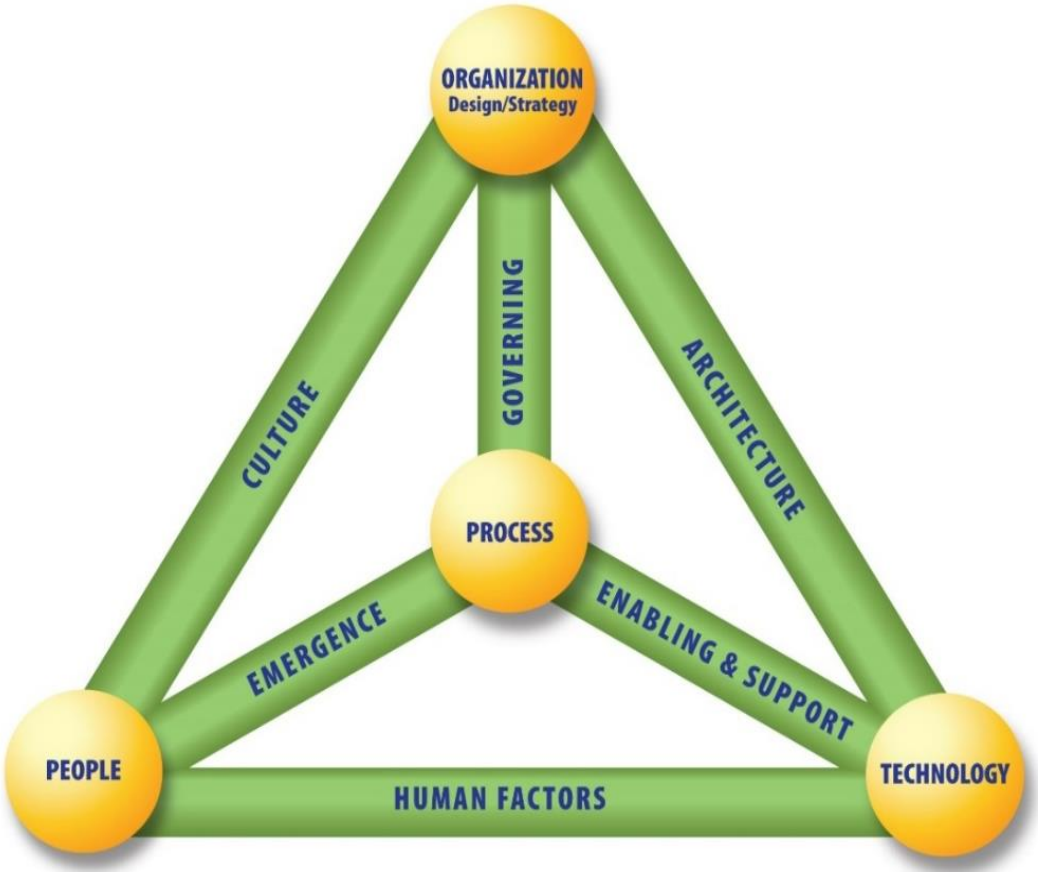


Figura 2: Ciclo de vida del modelo de negocio de la Seguridad de la Información.

Fuente: Isaca, 2013.

1.5. Activo de Información

INTERNATIONAL STANDARD, (2007), menciona, “La definición primordial de activo es cualquier cosa que tenga valor para la organización, ya sean activos tangibles – equipos, muebles de oficina, vehículos, edificios, terrenos, etc. – como intangibles – software, datos, patentes, etc”.

“Así mismo para el diseño de un sistema de seguridad de la información, se debe realizar un estudio de todos los activos críticos para el funcionamiento de la organización, centrándose en aquellos que generen, contengan o procesen información” (Indecopi, 2008).

1.6. Riesgo

“Es definido de una manera muy simple como una situación que expone a un objeto a que pueda se afectado o dañado. Extendiendo más el concepto de riesgos se puede determinar que esta situación tiene cierto grado de probabilidad de generar un incidente en el cual el objeto de estudio – en el caso de un proyecto de SGSI sería el activo de información pueda resultar afectado (Indecopi, 2008), (Tavalera, 2015), por ello la situación en la cual existe probabilidades que son distintas para los riesgos como parte de definición inicial se puede reconocer los siguientes componentes del riesgo, los cuales están relacionados con los términos utilizados en dicha definición”.

1.6.1. Evento o incidente (situación)

INDECOPI, (2007), afirma. “Que es alusivo a un evento futuro, del cual no se tiene certeza de que ocurrirá o no y que tiene una gran influencia en las consecuencias que puedan determinarse para el riesgo. La identificación de los eventos posibles es crítica en el estudio relacionado con el control de riesgos”.

1.6.2. Activo (objeto)

Según Tapia Manuel (2011), afirma. “Determinado como algo que tiene un valor para la organización, es el objetivo directo o indirecto de un evento y como tal, se verá afectado por las consecuencias que se generen como materialización de este evento”.

1.6.3. Consecuencia (daño)

Tapia Manuel (2011), afirma. “Es el impacto que tiene sobre el activo, la ocurrencia de uno de los eventos que constituyan un riesgo para el mismo. Como tal supone un daño o potencial pérdida ya sea parcial o total del activo relacionado”.

1.6.4. Probabilidad

Tapia Manuel (2011),afirma. “Es la medición o valuación que se realiza sobre el riesgo, y que tiene como resultado un valor que permita determinar una métrica que sirva para catalogar y priorizar los riesgos, y así definir para cuáles es crítico establecer controles o cuales pueden ser aceptados”.

NOTA: García, Alfonso & Maria (2011), mencionan. “La existencia del riesgo en conjunto con la incertidumbre que se generan como consecuencia del uso de probabilidades sumada a la gran cantidad de información que se maneja una organización, requiere que se proceda a proteger los activos de información críticos – puesto que la protección de todos los activos supondría un gran trabajo y costo operativo”.

Para este fin se realiza un Análisis de Riesgos, el cual comprende las siguientes etapas

1. **Identificación que dio de la valoración de activos**

“Es el responsable del estudio de los procesos de negocio que comprende las actividades de la organización objetivos para poder definir el alcance el cual debería ser uno o más procesos críticos de negocio que tendrá el presente análisis. Para realizar el levantamiento de información que lleve a la definición del alcance y activos críticos se puede utilizar herramientas como entrevistas, encuesta, documentación existente, etc. Como resultado de esta etapa se debería tener la documentación que especifique los procesos y activos sobre los que se centrará el Análisis de Riesgo” (INDECOPI, 2007).

2. **Identificación y valoración de riesgos**

“En base al alcance que se definió en la etapa anterior, se realiza un análisis de los riesgos y amenazas existentes. Dado que los riesgos pueden categorizarse en diferentes grupos dependiendo de su origen (naturales, humanos o del entorno), es importante que

se utilicen herramientas que puedan cubrir la mayor cantidad de posibilidades. Para este fin, se pueden utilizar checklist, revisión de la información histórica de los eventos e incidente ocurrido y lluvia de ideas" (INDECOPI, 2007).

"Una vez determinadas las amenazas existentes, se procede a establecer la probabilidad de ocurrencia de cada uno, así como el impacto que generaría su materialización sobre los activos de información. Por último, paso nos permitirá establecer una priorización de los riesgos según su criticidad o impacto en el negocio, sin embargo, como resultado de este análisis puede escogerse aceptar algunos de ellos y no establecer controles para los mismos, ya sea por su bajo impacto o su poca probabilidad de ocurrencia" (INDECOPI, 2007).

3. Establecimiento de controles a implementar

"Es establecer controles que minimicen el impacto del riesgo, o disminuyan la probabilidad de ocurrencia del mismo. Mientras más controles se identifiquen para un riesgo la mitigación del mismo será mayor, sin embargo, es importante evaluar si los controles que se tienen pensados serán efectivos o no. Para este fin se debe realizar nuevamente un análisis del riesgo, pero teniendo en cuenta los controles que se desee implementar como parte del contexto del mismo. De esta forma se podrá tener una medición de cuanto limitada el riesgo cada control implementando" (ISSA, 2011).

1.7. Ley de Protección de Datos Personales

La Ley N° 29733 de Protección de datos personales publicada en julio del 2011 y siendo aprobada su aplicación en marzo del 2013, "Nace como respuesta a la necesidad de tener un documento que regule la manera en la que se hace uso de la información personal en los procesos de negocio de todas las organizaciones que realicen operaciones en Perú. Anteriormente se crearon diferentes normas que hablaban acerca de las limitaciones que se debería tener en cuenta para el manejo de la información personal de los clientes o interesados. Sin embargo, la falta de especificación en los casos, así como el carácter un tanto abierto de las sanciones que dichos documentos especificaban requirieron que se

cree una norma más específica que sirva como ente reglamentario sobre la información personal" (ISSA, 2011).

Según especifica la ley, "Se considera dato personal a cualquier dato que pueda ser utilizado para identificar a una persona natural, de esta forma se puede considerar como datos personales el nombre de una persona, su dirección, su sexo, etc. Profundizando más en este concepto, se define además como dato sensible a aquellos que comprendan los datos biométricos, origen racial, religión, etc. Si bien es cierto que dichos datos casi siempre son necesarios para poder acceder a algún servicio – ya sea financiero, educativo o de salud – la ley detalla que el titular de dichos datos tiene los siguientes derechos respecto de esta información" (ISSA, 2011):

- "Solicitar información sobre el uso que se dará a la información que facilite".
- "Solicitar acceso a la información que la organización posee sobre él".
- "Solicitar la actualización, rectificación, adición o supresión de datos".
- "Solicitar que su información personal no sea suministrada a terceros".

Congreso de la Republica, (2011), menciona. "El principal objetivo de la norma es que las personas naturales puedan tener conocimiento de quién tiene acceso a su información personal, además de conocer el tipo de uso que se le dará. De esta forma establece como garantía principal que el uso de datos personales debe estar sujeto al conocimiento – previo, informado, expreso e inequívoco – por parte del titular de dicha información. Sin embargo, dicha garantía puede quedar invalidada en el caso que el ejercicio de este derecho afecte, por ejemplo, intereses de terceros o investigaciones judiciales".

1.8. Familia de Normas ISO/IEC 27000

"La Organización Internacional para la Estandarización ISO por sus siglas en inglés se encarga de publicar estándares sobre diferentes temas que tienen una gran importancia en diferentes aspectos relacionados con el comercio, fabricación, etc. Siguiendo el constante crecimiento que ha tenido el desarrollo del campo de las Tecnologías de

Información, dicho ente ha emitido varios estándares que regulan el ciclo de vida del software, estándares de calidad, sistemas de información y seguridad de la información" (Isaca, 2013).

"Proporcionada a este último grupo, se ejecutó la publicación de la familia de normas de la serie 27000, enfocadas directamente a la estandarización de los aspectos relacionados con la gestión de la seguridad de la información en las empresas y organizaciones que requieran contar con sistemas de gestión para este fin" (Isaca, 2013).

Se muestran las principales normas que sirven de soporte para realizar procesos requeridos para completar un proyecto o investigación.

ISO/IEC 27000. "Esta norma suministra una visión general de los sistemas de gestión de seguridad dela información y contiene los términos y definiciones que se utilizan en las diferentes normas de la 27000" (Isaca, 2013).

ISO/IEC 27001. "La última versión de esta norma fue publicada finales de 2013, y corresponde a la principal norma de la serie 27000 debido a que contiene los diferentes requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en las organizaciones independiente de su tipo, tamaño o naturaleza. Esta norma también incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adoptadas a las necesidades de la organización" (Isaca, 2013).

"Para el desarrollo de un SGSI, la versión 2013, muestra una serie de lineamientos en donde dichos lineamientos están descriptivos en forma detallada en 10 capítulos. En los primeros tres capítulos se define el alcance que tiene la normativa para poder certificar, centrándose en los requisitos cubiertos en los capítulos 4 a 10" (Isaca, 2013).

Tabla 1: Capítulos de los lineamientos de la versión 2013 de la ISO/IEC 27001

Capítulo	Tema
0	Introducción
1	Alcance y campo de aplicación
2	Referencias normativas
3	Términos y definiciones
4	Contexto de la organización
5	Liderazgo
6	Planificación
7	Apoyo
8	Operación
9	Evaluación de desempeño
10	Mejora

Fuente: Elaboración propia

En la tabla 1 muestra detalladamente los capítulos de los lineamientos de la versión 2013 de la ISO/IEC 27001.

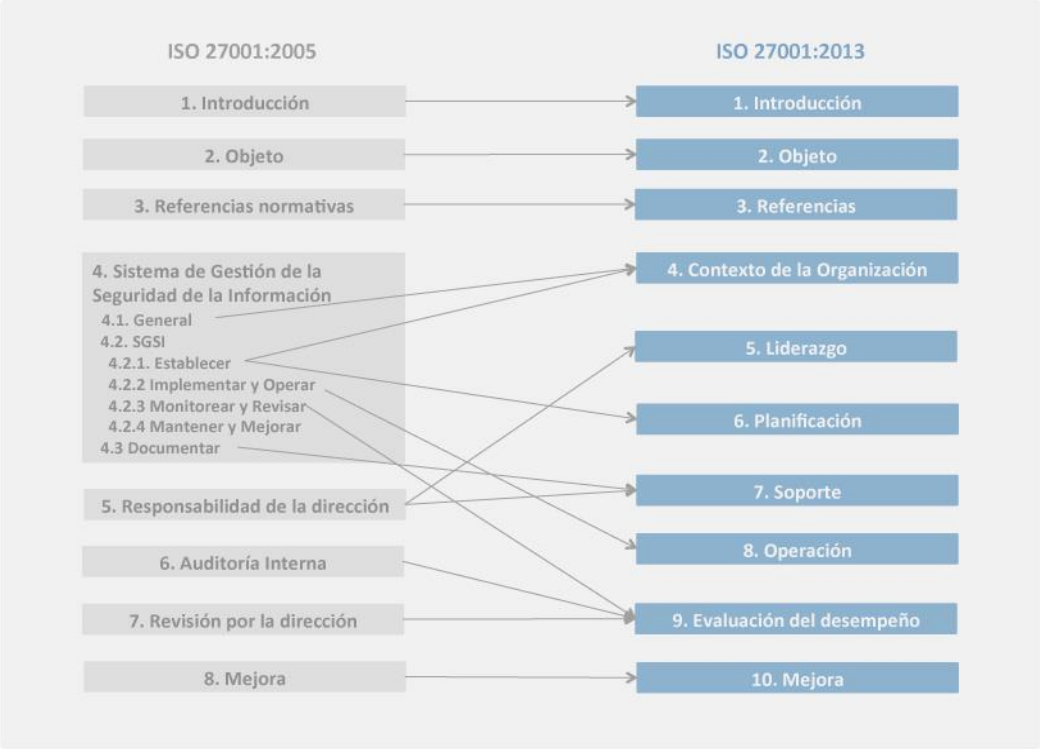


Figura 3: Diferencia entre las Norma ISO 27001:2005 y 27001:2013

Fuente: SGSI (Sistemas de Gestión de Seguridad de la Información), 2013.

1.8.1. Generalidades

"La elaboración de esta norma internacional es con el fin de proporcionar un modelo para establecer, implementar, operar, revisar, mantener y mejora continua de un Sistema de Gestión de Seguridad de la Información" (ICONTEC, 20013) .

"La adopción de un SGSI es una decisión estratégica para una organización. El diseño y la implementación del Sistema de Gestión de Seguridad de la Información de una organización están influenciados por sus necesidades y objetivos, los requisitos de seguridad, los procesos organizacionales empleados y el tamaño y estructura de la organización. Se espera que éstos y sus sistemas de apoyo cambien con el tiempo. Se espera que la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) se ajuste de acuerdo con las necesidades de la organización" (ICONTEC, 20013).

"El Sistema de Gestión de Seguridad de la Información preserva la confiabilidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente" (Isaca, 2013).

1.8.2. Compatibilidad con otras normas de sistemas de gestión

"Esta norma técnica aplica la estructura de alto nivel, títulos de sub-Clausulas idénticos, texto idéntico, términos comunes, y definiciones básicas proporcionadas en el anexo SL de las Directivas ISO/IEC, suplemento ISO consolidado, y por lo tanto mantiene compatibilidad con otras normas de sistemas de gestión que han adoptado del anexo SL" (INDECOPI, 2014).

"Este enfoque común definido en el Anexo SL será útil para aquellas organizaciones que decidan poner en funcionamiento un único sistema de gestión que cumpla los requisitos de dos o más normas de sistema de gestión" (INDECOPI, 2014).

1.8.3. Objeto y campo de aplicación

"Esta norma específica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI dentro del contexto de la organización. La presente norma

incluye también los requisitos para la valoración y el tratamiento de riegos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos establecidos en esta norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza". (INDECOPI, 2014).

"Cuando una organización declara conformidad con esta norma, no es aceptable excluir cualquiera de los requisitos específicos de los numerales 4 al 10" (INDECOPI, 2014).

1.8.4. Referencias normativas

Los siguientes documentos, en parte o en su totalidad, se refieren normativamente en este documento y son indispensables para su aplicación. "Para referencias fechadas sola se aplica la edición citada. Para referencias no fechadas de aplica la edición más reciente del documentó referenciado (Incluyendo cualquier modificación)" (ICONTEC, 20013).

"ISO/IEC 27000, Tecnología de la información— Técnicas de seguridad — Código de práctica para la gestión de seguridad de la información" (ICONTEC, 20013).

1.8.5. Términos y definiciones

Se muestra los siguientes términos

1.8.5.1. Activo

"Es toda cosa que tenga valor para la organización" (INDECOPI, 2014).

1.8.5.2. Disponibilidad

"Propiedad de ser accesible y utilizable cuando lo requiera una entidad autorizada" (INDECOPI, 2014).

1.8.5.3. Confidencialidad

"Propiedad por la cual no se pone a disposición o revela información a personas, entidades o procesos no autorizados" (INDECOPI, 2014).

1.8.5.4. Seguridad de la información

"Conservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, rendición de cuentas, no repudio y confiabilidad también pueden estar implicadas" (INDECOPI, 2014).

1.8.5.5. Hecho de seguridad de la información

"Ocurrencia identificada del estado de un sistema, servicio o red que indica un posible incumplimiento de la política de seguridad de la información o falla de las protecciones, o situación previamente desconocida que puede estar relacionada con la seguridad" (INDECOPI, 2014).

1.8.5.6. Incidente de seguridad de la información

"Hecho único o serie de hechos no deseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información" (INDECOPI, 2014).

1.8.5.7. Sistema de gestión de seguridad de la información SGSI

"Parte del sistema de gestión general, basada en un enfoque de riesgos del negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la" (INDECOPI, 2014).

1.8.5.8. Seguridad de la información.

NOTA: "El sistema de gestión incluye la estructura organizativa, políticas, actividades de planificación, responsabilidades, prácticas, procedimientos, procesos y recursos". (INDECOPI, 2014).

1.8.5.9. Integridad

"Propiedad de proteger la exactitud e integridad de los activos" (INDECOPI, 2014).

1.8.5.10. Riesgo residual

"Riesgo que se mantiene después del tratamiento de los riesgos" (INDECOPI, 2014).

1.8.5.11. Aceptación del riesgo

"Decisión de aceptar un riesgo" (INDECOPI, 2014).

1.8.5.12. Análisis del riesgo

"Uso sistemático de información para identificar fuentes y estimar el riesgo" (INDECOPI, 2014).

1.8.5.13. Evaluación del riesgo

"Proceso general de análisis y evaluación del riesgo" (INDECOPI, 2014).

1.8.5.14. Valoración del riesgo

"Proceso de comparación del riesgo estimado con determinados criterios de riesgo para determinar la importancia del riesgo" (INDECOPI, 2014).

1.8.5.15. Gestión del riesgo

"Actividades coordinadas para orientar y controlar una organización con respecto al riesgo" (INDECOPI, 2014).

1.8.5.16. Tratamiento del riesgo

"Proceso de selección e implementación de medidas para modificar el riesgo" (INDECOPI, 2014).

NOTA: En esta Norma Internacional, el término "control" se utiliza como sinónimo de "medida" (INDECOPI, 2014).

1.8.5.17. Declaración de aplicabilidad

"Declaración documentada que describe los objetivos de control y controles que son pertinentes y aplicables al SGSI de la organización" (INDECOPI, 2014)

NOTA: "Los objetivos de control y controles se basan en los resultados y conclusiones de los procesos de evaluación y tratamiento del riesgo, los requisitos legales o reglamentarios, las obligaciones contractuales y los requisitos del negocio de la organización para la seguridad de la información" (INDECOPI, 2014).

1.8.6. Contexto de la organización

"Se resalta la necesidad de hacer un análisis para identificar los problemas externos e internos que rodean a la organización. De esta forma se puede establecer el contexto del

SGSI incluyendo las partes interesadas que deben estar dentro del alcance del SGSI" (ISO/IEC 27001, 2013).

1.8.6.1. Conocimientos de la organización y de su contexto

"La organización debe determinar las cuestiones externas e internas que son pertinentes para su propio propósito y que afectan su capacidad para lograr los resultados previstos de su sistema de gestión de la seguridad de la información" (ISO 27000, 2013).

1.8.6.2. Comprensión de las necesidades y expectativas de las partes interesadas

La organización debe determinar:

- "Las partes interesadas que son pertinentes al sistema de gestión de la seguridad de la información" (ICONTEC, 20013).
- "Los requisitos de estas partes interesadas pertinentes a seguridad de la información" (ICONTEC, 20013).

1.8.6.3. Determinación del alcance del sistema de gestión de la seguridad de la información

"La organización debe determinar los límites y la aplicabilidad del sistema de gestión de la seguridad de la información para establecer su alcance, y cuando esta ya esté terminada su alcance entonces la organización debe considerar lo siguiente" (ICONTEC, 20013).

- "Las cuestiones externas e internas referidas a la enumeración 6.1.6.1" (ICONTEC, 20013).
- "Los requisitos referidos a la enumeración 6.1.6.2" (ICONTEC, 20013).
- "Las interfaces y dependencias entre las actividades realizadas por la organización. Y las que realizan otras organizaciones" (ICONTEC, 20013).

1.8.6.4. Sistemas de gestión de seguridad

"La organización debe establecer, implementar, mantener y mejorar continuamente un sistema de gestión de la seguridad de la información, de acuerdo con los requisitos de esta norma" (ICONTEC, 20013).

1.8.7. Liderazgo

"Se define las responsabilidades de la alta dirección respecto al SGSI. Por ejemplo, sus responsabilidades en la definición de la política de seguridad de la información alineada a los objetivos del negocio y asignación de los recursos necesarios para la implementación del SGSI" (Isaca, 2013).

1.8.7.1. Liderazgo y compromiso

La ata dirección debe demostrar liderazgo y compromiso respecto al SGSI.

- "Asegurando que se establezcan la política de la seguridad de la información y los objetivos de la seguridad de la información, y que estos sean compatibles con la dirección estratégica de la organización" (ICONTEC, 20013).
- "Asegurando la integridad de los requisitos del SGSI en los procesos de la organización" (ICONTEC, 20013).
- "Asegurando que los recursos necesarios para el SGSI estén disponibles" (ICONTEC, 20013).
- "Comunicando la importancia de una gestión de la seguridad de la información eficaz y de la conformidad con los requisitos del SGSI" (ICONTEC, 20013)
- "Asegurando que el SGSI logre los resultados previstos" (ICONTEC, 20013)
- "Dirigiendo y apoyando a las personas, para contribuir a la eficacia del SGSI" (ICONTEC, 20013).
- "Promoviendo la mejora continua" (ICONTEC, 20013)
- "Apoyando otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a sus áreas de responsabilidades" (ICONTEC, 20013).

1.8.7.2. Políticas

La alta dirección debe establecer una política de seguridad de la información que:

- “Es apropiada al propósito de la organización” (ICONTEC, 20013).
- “Incluye objetivos de seguridad de la información o proporciona el marco de referencia para fijar los objetivos de seguridad de la información” (ICONTEC, 20013).
- “Incluye un compromiso de satisfacer requisitos aplicables relacionados a la seguridad de la información” (ICONTEC, 20013).
- “Incluye un compromiso de mejora continua del SGSI” (ICONTEC, 20013).

La política de seguridad de la información debe:

- “Estar disponible como información documentada” (ICONTEC, 20013).
- “Estar comunicada dentro de la organización” (ICONTEC, 20013).
- “Estar disponible a las partes interesadas, según sea apropiado” (ICONTEC, 20013).

1.8.7.3. Roles, responsabilidades y autoridades organizacionales

ICONTEC, (20013), menciona. “La alta dirección debe asegurar que las responsabilidades y la autoridad para los roles relevantes a la seguridad de la información estén asignadas y comunicadas”. Es por ello que la alta dirección debe asignar la responsabilidad y la autoridad para:

- “Asegurar que el SGSI este conforme a los requisitos de esta Norma” (ICONTEC, 20013)
- “Reportar sobre el desempeño del SGSI a la alta dirección” (ICONTEC, 20013)

1.8.8. Planificación

“Se desarrolla la definición de objetivos de seguridad claros que permitan elaborar planes específicos para su cumplimiento. En esta planificación debe también considerarse

la identificación de aquellos riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información” (Isaca, 2013).

1.8.8.1. Acciones para tratar los riesgos y las oportunidades

1.8.8.1.1. Generalidades

“Cuando se planifica para el SGSI, la organización debe considerar los asuntos referidos en la enumeración 6.1.6.1 y determinar los riegos y oportunidad que necesitan ser tratados para: Asegurar que el SGSI pueda lograr su(s) resultado(s) esperado(s); prevenir, o reducir, efectos indeseados y lograr la mejora continua” (ICONTEC, 20013).

“La organización debe planificar, acciones que traten riesgos y oportunidades y como integrar e implementar estas acciones en sus procesos del SGSI y evaluar la efectividad de estas acciones” (ICONTEC, 20013).

1.8.9. Soporte

“Se describen los requerimientos para implementar el SGSI incluyendo recurso, personas y elementos de comunicación para las partes interesadas en el sistema” (Isaca, 2013).

1.8.9.1. Recursos

“La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI” (ICONTEC, 20013).

1.8.9.2. Competencia

“La organización debe determinar la competencia necesaria de la(s) persona(s) que trabajan bajo su control que afecta su desempeño en seguridad de la información, asegurar que estas personas son competentes sobre la base de educación, capacitación, o experiencia adecuados; cuando sea aplicable, tomar acciones para adquirir la competencia necesaria y avaluar la efectividad de las acciones tomadas y retener información documentada apropiada como evidencia de competencia” (ISO/IEC 27001, 2013).

1.8.10. Operación

"Establece los mecanismos para planear y controlar las operaciones y requerimientos de seguridad. Las evaluaciones periódicas de riesgos constituyen el enfoque central para la gestión del SGSI. Las vulnerabilidades y las amenazas a la información se utilizan para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad" (Isaca, 2013).

1.8.10.1. Planificación y control operacional

"La organización debe planificar, implementar y controlar los procesos necesarios para cumplir con los requisitos de seguridad de la información e implementar las acciones determinadas en 6.1.8.1. (Acciones para tratar los riesgos y las oportunidades). La organización debe también implementar planes para lograr los objetivos de seguridad de la información determinados en 6.1.8.2" (ISO/IEC 27001, 2013).

"La organización debe mantener información documentada en la medida necesaria para estar segura de que los procesos de han llevado a cabo tal como fueron planificados" (ISO/IEC 27001, 2013).

"La organización debe controlar los cambios planeados y revisar las consecuencias de cambios no intencionados, actuando para mitigar cualquier efecto adverso, según sea necesario" (ISO/IEC 27001, 2013).

"La organización debe garantizar que los procesos tercerizados son determinados y controlados" (ISO/IEC 27001, 2013).

1.8.10.2. Avaluación de riesgos de seguridad de la información

"La organización debe realizar evaluaciones de riesgo de seguridad de la información en los intervalos planificados o cuando cambios significativos se propagan u ocurran" (ISO/IEC 27001, 2013).

"La organización debe retener información documentada de los resultados de las evaluaciones de riesgo de seguridad de la información" (ISO/IEC 27001, 2013).

1.8.10.3. Tratamiento de riesgos de la seguridad de la información

"La organización debe implantar el plan de tratamiento de riesgos de seguridad de la información" (ISO/IEC 27001, 2013).

"La organización debe retener información documentada de los resultados del tratamiento de riesgos de seguridad de la información" (ISO/IEC 27001, 2013).

1.8.11. Evaluación del desempeño

"Se definen las bases para medir la efectividad y desempeño del SGSI. Dichas mediciones se realizan usualmente a través de auditorías internas" (Isaca, 2013).

1.8.11.1. Seguimiento, medición, análisis y avaluación

"La organización debe evaluar el desempeño de la información y la eficacia del sistema de gestión de la seguridad de la información" (ISO/IEC 27001, 2013).

Según ISO/IEC 27001, (2013). La organización debe determinar lo siguiente:

- "A que es necesario hacer seguimientos y que es necesario medir, incluidos los procesos y controles de la seguridad de la información"
- "Los métodos de seguimiento, medición, análisis y avaluación, según sea aplicable, para asegurar resultados válidos".
- "Cuando se debe llevar a cabo el seguimiento y la medición".
- "Quien debe llevar a cabo el seguimiento ya la medición".
- "Cuanto se debe analizar y evaluar los resultados del seguimiento y de la medición".
- "Quien debe analizar y evaluar estos resultados".

"Eso quiere decir que la organización debe conservar información documentada apropiada como evidencia de los resultados del monitoreo y de la medición"(ISO/IEC 27001, 2013).

1.8.11.2. Auditoria interna

"La organización debe llevar a cabo auditorías a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información" (ISO/IEC 27001, 2013).

"Es conforme con: Los propios requisitos de la organización para su SGSI; y los requisitos de esta Norma" (ISO/IEC 27001, 2013).

"Esta implementado y mantenido eficazmente" (ISO/IEC 27001, 2013).

"La organización debe planificar, establecer, implementar y mantener uno o varios programas de auditorías que incluyan la frecuencia, el método, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoria debe tener en cuenta la importancia de los procesos involucrados y los resultados de las auditorias previas" (ISO/IEC 27001, 2013).

1.8.11.3. Revisión por la gerencia

1.8.12. Mejora

"Propone, a partir de las no conformidades identificadas en el SGSI, establecer las acciones correctivas más efectivas para solucionarlas" (Isaca, 2013).

1.8.13. No conformidades y acción correctiva

Según ISO/IEC 27001, (2013). "Cuando sucede una no conformidad, la organización debe":

- "Reaccionar a la no conformidad y, según sea posible. Tomar acción para controlarla y corregirla; y ocuparse de las consecuencias".
- "Evaluar las necesidades de la acción para eliminar las causas de la no conformidad con el fin de que no recurra u ocurra en otro lugar de las siguientes maneras: Revisando la no conformidad, determinando las causas de la conformidad; y determinando si existen no conformidades similares o si podrían ocurrir potencialmente".
- "Implementar cualquier acción necesaria".

- “Revisar la efectividad de cualquier acción correcta tomada”.
- “Hacer cambios al SGSI, si fuera necesario”.

Según ISO/IEC 27001, (2013). “La organización debe retener información documentada como evidencia de”:

- “La naturaleza de las no conformidades y cualquier acción subsiguiente tomada”.
- “Los resultados de cualquier acción correctiva”.

1.8.14. Mejora continua

“La organización debe mejorar continuamente la convivencia, educación, y efectividad del sistema de gestión de seguridad de la información” (ISO/IEC 27001, 2013).

ISO/IEC 27002. “Guía de buenas prácticas en seguridad de la información que describe de forma detallada la acciones que se deben tener en cuenta para el establecimiento en implementación delos objetivo de control y controles descritos de una forma general de la norma ISO 2700” (Isaca, 2013).

Según Méndez & Aguilar, (20013), mencionan. “Las organizaciones de todos los tipos y tamaños (sector público y privado, comercial y sin fines de lucro) recopilan, procesan y transmiten información de varias formas incluidas las electrónicas, físicas y verbales (es decir, conversaciones y presentaciones). Los procesos, los sistemas, y el personal involucrado en la operación, manipulación y protección de dicha información son activos que, al igual que otros activos comerciales de importancia, resultan valiosos para la organización y, por lo tanto, merecen o requieren protección contra diversos peligros”.

“La seguridad de la información se logra implementando un conjunto adecuado de controles de seguridad, que incluyen políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Estos controles se deberían establecer, implementar, monitorear, revisar y mejorar para garantizar que se cumplen los objetivos comerciales y de seguridad de las organizaciones” (Méndez & Aguilar, 20013).

ICONTEC, (2013), menciona. “El estándar ISO/IEC 27002:2013 es una norma que describe controles de seguridad que pueden ser implementados dentro de una organización. Este estándar es una guía de buenas prácticas que constituyen un conjunto de controles recomendables en cuanto a seguridad de la información. Esta norma sigue las directrices de la norma ISO/IEC 27001:2013. Está diseñada para que la utilicen las organizaciones que tienen la intención de: (a) seleccionar controles de seguridad dentro del proceso de implementación de un SGSI basado en ISO/IEC 27001:2013, (b) implementar controles de seguridad de la información de aceptación común, y (c) desarrollar sus propias pautas de gestión de seguridad de la información”.

La ISO/IEC 27002:2013 contiene 35 categorías de seguridad agrupados en 14 cláusulas de control. Por ejemplo, “la cláusula Control de Acceso tiene 4 categorías de seguridad: (1) requerimientos de negocio de control de acceso, (2) gestión de acceso de usuarios, (3) responsabilidades de los usuarios, y (4) control de acceso al sistema”.

“Para cada categoría de seguridad, la norma ISO/IEC 27002:2013 detalla un conjunto de controles específicos que las organizaciones deberían implementar. El total de controles específicos presentados por la norma ISO/IEC 27002:2013 es de 114 controles de seguridad. No es la intención de la norma que todos estos controles sean implementados para lograr una certificación. Cada organización debería aplicar los controles adecuados para sus necesidades específicas” (Méndez & Aguilar, 20013).

ISO/IEC 27003. “Guía que contiene aspecto necesario para el diseño e implementación de un Sistema de Gestión de Seguridad de la Información de acuerdo a los requerimientos establecidos en la norma ISO/IEC 27001, donde se describe el proceso desde la planeación hasta la puesta en marcha de planes de implementación” (INTERNATIONAL ORGANIZATION FOR STANDARIZATION, 2014).

ISO/IEC 27004. “Guía para el desarrollo y utilizando de métricas y técnicas de medida aplicables para determinar a la eficacia de un Sistema de Gestión de Seguridad de la

Información y de los objetivos de control y controles implementando de acuerdo a la norma ISO 27001" (INTERNATIONAL ORGANIZATION FOR STANDARIZATION, 2014).

ISO/IEC 27005. "Esta norma establece los lineamientos para la gestión de riesgos de seguridad de la información y está diseñada para ayudar a la organización en la implementación de un Sistema de Gestión de Seguridad de la Información basada es un enfoque de gestión de riesgos. Entre otros aspectos, establecer lo requerido que se deben tener en cuenta para el proceso y valoración de riesgos, relaciones con la identificación, análisis, evaluación y tratamiento en los riesgos en la seguridad de la información" (INTERNATIONAL ORGANIZATION FOR STANDARIZATION, 2014).

ISO/IEC 27006. "Establece los requisitos relacionados en la norma ISO 27001 que deben cumplir las organizaciones para la acreditación entidades de auditoria y certificación de Sistema de Gestión de Seguridad de la información" (INTERNATIONAL ORGANIZATION FOR STANDARIZATION, 2014).

ISO/IEC 27035. Proporciona una guía sobre la gestión de incidentes de seguridad en la información (INTERNATIONAL ORGANIZATION FOR STANDARIZATION, 2014).

CAPÍTULO III: MATERIALES Y MÉTODOS

3.1. Tipo de investigación

1.1 3.1.1. Tipo

Según Bunge (1979), es aplicada, y según Hernández, Fernández, &; Baptista, (2010) tiene enfoque cuantitativo, por que usa la recolección de datos para probar hipótesis, como base en la medición numérica y el análisis estadístico, para establecer patrones de comportamiento y probar teorías.

Según Hernandez, Fernandez,& Baptista (2010), menciona. Que parte de una idea, que va acotándose y, una vez delimitada, se derivan objetivos y preguntas de investigación, se revisa la literatura y se construye un marco o una perspectiva teórica. De las preguntas se establecen hipótesis y determinan variables; se desarrolla un plan para probarlas (diseño); se miden las variables en un determinado contexto; se analizan las mediciones obtenidas (con frecuencia utilizando métodos estadísticos), y se establece una serie de conclusiones respecto de las hipótesis.

Según Cano, Basabe, Perdomo, Mosquera, & Fuentes (2015), inducen. "Que el tipo cuantitativo es aquello que permite examinar los datos de manera numérica especialmente en el campo de la estadística, se requiere que el elemento del problema de la investigación exista una relación lineal (que sea posible definirlo) y saber exactamente donde inicia el problema, en qué dirección va, asume una postura objetiva y qué tipo de incidencia existe entre sus elementos".

3.2. Descripción del lugar de ejecución

3.3. Población y muestra

3.3.1. Población

"La población es el conjunto de todos los casos que concuerdan con una serie de especificaciones" (Hernandez , Fernandez, & Baptista, 2010). A través de esta investigación la población está conformada por todo el personal administrativo; como, el Alcalde, Gerente, Tesorería, Abastecimientos, que en su total son 13 trabajadores.

3.3.2. Muestra

Hernández, Fernández, & Baptista (2010), expresan la ventaja de una muestra no probabilística es su utilidad para un determinado diseño de estudio, que requiere no tanto de una "representatividad de elementos de una población, sino de una cuidadosa y controlada elección de sujetos con ciertas características especificadas previamente en el planteamiento del problema".

3.4. Diseño de la investigación

Según Hernandez, Fernandez,& Baptista (2010), Consiste en administrar un estímulo o tratamiento a un grupo y después aplicar una medición de una o más variables para observar cual es el nivel del grupo en estas. Es por eso que el diseño de la investigación es pre experimental con pre-test y post-test.

El proceso de la investigación se ha desarrollado de acuerdo al diagrama mostrado en la figura 4.

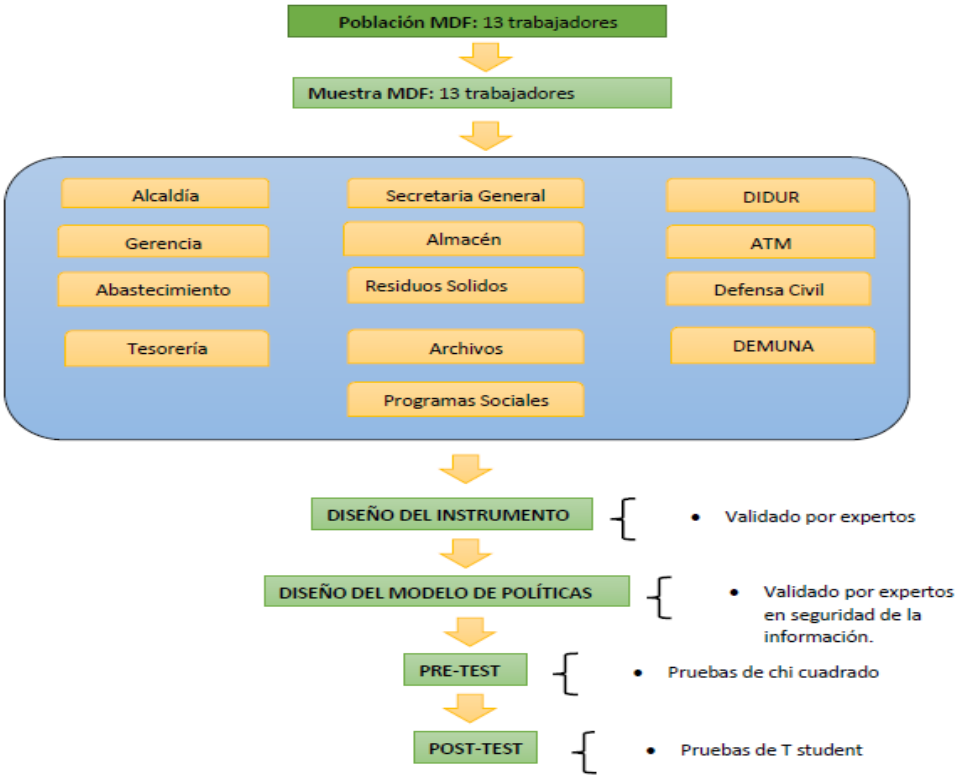


Figura 4: Diseño de la investigación.

Fuente: Elaboración propia.

3.5. Formulación de hipótesis

Con el diseño del modelo de políticas basado en la norma ISO 27001, mejorará la gestión de la seguridad de la información en las diferentes áreas de la Municipalidad Distrital de Florida – Bongará – Amazonas.

3.5.1. Hipótesis Nula

Con el diseño del modelo de políticas basado en la norma ISO 27001, no mejorará la gestión de la seguridad de la información en las diferentes áreas de la Municipalidad Distrital de Florida – Bongará – Amazonas.

3.5.2. Hipótesis Alterna

Con el diseño del modelo de políticas basado en la norma ISO 27001, si mejorará la gestión de la seguridad de la información en las diferentes áreas de la Municipalidad Distrital de Florida – Bongará – Amazonas.

3.6. Identificación de variables

3.6.1. Variable independiente

Diseño de un modelo de políticas basado en la norma ISO 27001.

3.6.2. Variable dependiente

Gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

CAPÍTULO IV: DESARROLLO DE LA SOLUCIÓN

En este capítulo de muestra el desarrollo en el cual contiene el Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

4.1. Procesamiento y presentación de datos

4.1.1. Procesamiento de datos

En la investigación presente se realizó el análisis cuantitativo, a través de la estadística. Los resultados se presentan mediante cuadros y gráficos. Los procedimientos estadísticos mediante los cuales se realizó el procesamiento de datos y el análisis de resultados fueron la distribución de frecuencias, la determinación del promedio, para la comprobación de hipótesis se utilizó “T-Student”.

4.1.2. Presentación de resultados

Se realizó pruebas estadísticas para mejorar la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

Se realizó encuestas para ver las mejoras que se obtuvo mediante la implantación de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

4.2. Análisis e interpretación de datos y resultados

El presente capitulo muestra el desarrollo del modelo de políticas de seguridad implementado en la Municipalidad Distrital de Florida – Bongará – Amazonas.

4.2.1. Estrategias de difusión

La última fase de un SGSI consiste en la concientización y formación del personal administrativo, con el fin de crear en la organización una cultura de seguridad mostrando la importancia de sus actividades y como ellos pueden contribuir al logro de los objetivos de sus actividades y como ellos pueden contribuir al logro de los objetivos establecidos en el sistema.

La concientización y divulgación consiguen que el personal conozca qué actividades se están llevando a cabo y por qué se están realizando. Con ello se concede transparencia al proceso y se involucra a todo el personal administrativo de la Municipalidad Distrital de Florida – Bongará - Amazonas.

Para llegar a utilizar esta estrategia se da mediante programas de capacitación en seguridad de la información.

4.2.2. Políticas de seguridad

Estas políticas que mostrare más adelante representan conductas (Reglas) que deben ser adoptadas por el personal de la Municipalidad Distrital de Florida – Bongará - Amazonas.

4.2.2.1. Políticas de seguridad generales

- El ingreso de las personas a cualquier área de la municipalidad será restringido, eso quiere decir que solo pueden ingresar personas registradas en el área de mesa de partes.
- Los usuarios o personal responsable de cada área solo deben tener acceso a los servicios según están establecidos en dicho contrato.
- Se debe utilizar métodos de autentificación para controlar el acceso de usuarios remotos.
- Los servicios de información, usuarios y sistemas de información de deben segregar en las redes.
- Las contraseñas se seguridad de las pc, laptops, contendrán al menos tres referencias de los siguientes caracteres: letras mayúsculas, letras minúsculas, símbolos, números; además que tenga mínimo 8 caracteres de longitud.
- Se debe mantener el escritorio del computador (Windows) limpio de información confidencial para dicha área administrativa.

- Cuando el personal quiere retirarse o alejarse del computador por cualquier motivo inmediatamente debe, bloquear la sesión activa, para cuando retorne nuevamente inicie sesión.
- Todos los archivos creados deberán ser almacenados en el disco “D” en la carpeta “MDF” la cual mantiene una copia sincronizada en “MDF” del servidor de área de la Municipalidad Distrital de Florida.
- Se debe usar un protector de pantalla ante inactividad del computador, el mismo que se establecerá para activarse luego de 2 minutos de inactividad.

4.2.2.2. Políticas de seguridad a nivel lógico

- Todos los equipos con Windows deben contar con software antivirus.
- Todo equipo con sistema operativo Windows tiene activo el firewall de comunicaciones para evitar infección y posibles ataques al computador.
- Verificar que la base de datos del software antivirus esté actualizada.
- Todo archivo de dudosa procedencia se debe rechazar.
- No se debe conectar a redes inalámbricas inseguras, solo a las que la Municipalidad le da acceso ya que se trabaja con información confidencial.
- Las contraseñas contendrán al menos 3 referencias de los siguientes caracteres: números, letras mayúsculas, letras minúsculas, símbolos; además que tenga mínimo 8 caracteres de longitud.
- Al finalizar cada fin de contrato se debe realizar el cambio de contraseñas del acceso al computador.
- No abrir el case del equipo. Esta actividad está reservada solo al personal de Soporte Técnico de la Municipalidad.
- El personal no debe utilizar las contraseñas de su correo electrónico, Facebook, etc. a las que usa para la administración o acceso a equipos del área correspondiente de la Municipalidad.

4.2.2.3. Políticas de seguridad a nivel físico

- El ingreso de las personas a cualquier área de la municipalidad será restringido, eso quiere decir que solo pueden ingresar personas registradas en el área de mesa de partes.
- El personal debe contar con su respectiva tarjeta o fotochecks de identificación, donde estas tarjetas o fotochecks deben ser autorizadas por gerencia o alcaldía.
- El personal externo deberá ser registrado en mesa de partes y esperar el orden de ingreso a la oficina solicitada, para cuando requiere ingresar a la oficina. En este registro debe estar anotado el porqué de su visita y mencionar la política de seguridad de la información y mecanismo para reportar incidentes de seguridad.
- Al ingresar o salir de la oficina, todo el personal deberá registrarse en un portal asignado por la Municipalidad. Cuando personas extrañas o invitadas ingresen o salgan de la oficina, cada uno de ellos deberá registrar individualmente su ingreso o salida.
- Se deberá mantener extintores contra fuego cerca de la oficina de mesa de partes, y esto debe ser revisado solo por el personal de mantenimiento de la Municipalidad.
- Se prohíbe el consumo de cigarrillos dentro de las áreas de trabajo de la oficina.
- Se prohíbe el consumo de comidas y bebidas en los escritorios donde se encuentran equipos de computación y documentos físicos.

4.2.2.4. Políticas de mantenimiento de equipos

- Al iniciar o encender el computador se debe asegurar que inicie correctamente, que todo esté en orden.
- Evitar tocar la pantalla del computador con los dedos u otros objetos.
- Cuando apague el computador o laptops evite colocar objetos o archivos sobre el mismo.

- El equipo deber estar ubicado y protegido para reducir los riesgos de las amenazas y las oportunidades para el acceso no autorizado.
- Se deberá contar con protección ante fallas o interrupciones de energía mediante la utilización de UPS.
- Se debe contar con mantenimiento preventivo físico para los equipos que almacenan información en medio electrónico para permitir su disponibilidad e integridad.
- Se prohíbe el consumo de comidas y bebidas en los escritorios donde se encuentran equipos de computación y documentos físicos
- Los mantenimientos físicos programados a los equipos, se realizarán dentro del área de la municipalidad y bajo supervisión de una persona de soporte técnico.
- Al finalizar la hora de trabajo se debe apagar el sistema solamente haciendo uso de la opción apagar y esperar hasta que el proceso finalice normalmente.

4.2.2.5. Políticas de uso de software

- Está prohibido instalar o desinstalar programas, utilitarios o complementos para navegar por internet. Esta actividad solo está reservada solo para el personal de soporte técnico de la Municipalidad Distrital de Florida.
- Se prohíbe el uso de software que no tenga licencia.
- Todo equipo de computación debe mantener en forma residente un antivirus instalado y las actualizaciones de las nuevas versiones, deben realizarse en línea.

4.2.2.6. Políticas de respaldo y recuperación de información

- Se realizará el respaldo de la información por lo menos una o dos veces al día.
- La información será almacenada en una unidad externa como una copia de seguridad.
- La unidad externa donde contiene la información solo le puede tener el Gerente de la Municipalidad.

- Se debe realizar una recuperación de la información por lo menos 3 veces al año.

CAPÍTULO V: RESULTADOS Y DISCUSIONES

5.1. Resultados

En este capítulo se presenta la síntesis de los principales resultados obtenidos, se muestra la parte descriptiva de las variables de la investigación, ver cuánto varían los datos, así como la consecución de los objetivos propuestos.

"El estadístico de contraste empleado para el análisis de esta investigación fue "T – Student". Este se utiliza para comparar las medias de dos grupos en una variable dependiente y permitirá identificar si la hipótesis nula ("h_0") se puede rechazar o se acepta la hipótesis alterna ("hi"). Para este estudio la prueba de "T-Student" se aplicó sobre muestras relacionadas (es decir en un mismo grupo en tiempos diferentes) y sobre muestras independientes (comparación entre dos grupos) donde mostrará detalladamente sobre los resultados aplicando el pre test y post test, para diferenciar y ver la mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas".

5.2. Prueba de hipótesis

Hipótesis alterna (H1): Con el diseño del modelo de políticas basado en la norma ISO 27001, si mejorará la gestión de la seguridad de la información en las diferentes áreas de la Municipalidad Distrital de Florida – Bongará – Amazonas.

Hipótesis (H0): Con el diseño del modelo de políticas basado en la norma ISO 27001, no mejorará la gestión de la seguridad de la información en las diferentes áreas de la Municipalidad Distrital de Florida – Bongará – Amazonas.

Procedimiento: Se inició con la observación a todo el personal que hace uso de la información para el monitoreo de la gestión, seguido de una encuesta realizada para medir el nivel de la seguridad de la información basado en la norma ISO 27001 en la Municipalidad Distrital de Florida – Bongará – Amazonas como se muestra en el (Anexo 01); con esta encuesta se evaluó a 13 trabajadores antes de la implementación de la solución de políticas basado en la norma ISO 27001, si mejorara la gestión de la seguridad

de la información en las diferentes áreas de la Municipalidad Distrital de Florida – Bongará – Amazonas., con los que se obtuvieron resultados en donde nos da a conocer el desconocimiento de políticas de seguridad de la información, por parte del personal.

"Se utilizó la prueba de "T-Student" por tratarse de una muestra pequeña (n<13), los datos que se utilizaron en la prueba de "T-Student" son los correspondientes al promedio de los 13 trabajadores en los meses de enero a marzo aun sin la aplicación de las políticas de seguridad de la información y de abril a diciembre con la aplicación del modelo de políticas pasado en la norma ISO 27001, como se muestra a continuación en el siguiente cuadro":

Tabla 2 *Resultados de encuestas de conocimiento de las políticas de seguridad de la información.*

Trabajadores	Pre Test	Pos Test
1	0.91	4.40
2	1.62	4.50
3	1.41	4.50
4	1.02	4.62
5	1.76	4.40
6	1.31	4.62
7	1.14	4.50
8	1.40	4.62
9	1.31	4.62
10	1.31	3.67
11	1.62	4.31
12	1.65	4.76
13	1.41	4.76

Fuente: Elaboración propia

En la Tabla 2 nos da a conocer lo siguiente: "El casillero trabajadores representa la cantidad de trabajadores evaluados en este caso se trata de 13 usuarios, luego los resultados de la encuesta de conocimiento de las políticas de seguridad de la información antes de la implementación (Pre Test) y los resultados de la encuesta de conocimiento de las políticas de seguridad de la información después de la implantación de las políticas de seguridad (Pos Test), en la que se puede observar las diferencias entre ambas tal como se muestra el promedio en el siguiente cuadro".

Tabla 3 *Estadística de Grupo*

	Grupo con conocimiento y desconocimiento de las políticas de seguridad.	N	Media	Desviación típ.	Error típ. de la media
Encuesta a los trabajadores	Pre Test	13	1.69	.376	.077
	Post Test	13	4.85	.277	.077

Fuente: SPSS

En la Tabla 3 nos muestra la media de los grupos Pre Test (1.69) y en el Pos Test (4.85) con una muestra de 13 trabajadores de la Municipalidad Distrital de Florida.

5.2.1. Dimensiones

5.2.1.1. Políticas

Hipótesis: El diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

Tabla 4 *Significancia de la solución en indicadores de políticas*

Pruebas de muestras relacionadas			
	T	gl	Sig. (bilateral)
PRETEST-POSTTEST	,954	10	,717

Fuente: SPSS

En la tabla 4 nos muestra la prueba de muestras relacionadas tanto como el PRE TEST y POS TEST de la dimensión políticas.

5.2.1.2. Servicio

Hipótesis: El diseño de un modelo de políticas basado en la norma ISO 27001, mejorará los servicios de Eventos, Licitaciones, Cartas, Memorándum, Ordenanzas, Informes, Proyectos, etc. en la Municipalidad Distrital de Florida – Bongará – Amazonas.

Tabla 5 *Significancia de la solución en indicadores de servicio*

Pruebas de muestras relacionadas

	T	gl	Sig. (bilateral)
PRETEST-POSTTEST	,955	10	,732

Fuente: SPSS

En la tabla 5 nos muestra la prueba de muestras relacionadas tanto como el PRE TEST y POS TEST de la dimensión servicio.

5.2.1.3. Riesgos

Hipótesis: El diseño de un modelo de políticas basado en la norma ISO 27001, mejorará los riesgos de seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

Tabla 6 *Significancia de la solución en indicadores de riesgo*

Pruebas de muestras relacionadas			
	T	gl	Sig. (bilateral)
PRETEST-POSTTEST	,969	10	,886

1.1.1

Fuente: SPSS

En la tabla 6 nos muestra la prueba de muestras relacionadas tanto como el PRE TEST y POS TEST de la dimensión riesgo.

5.2.1.4. Consistencia

Hipótesis: El diseño de un modelo de políticas basado en la norma ISO 27001, mejorará la consistencia de seguridad de información en la Municipalidad Distrital de Florida 2017.

Tabla 7 *Significancia de la solución en indicadores de consistencia*

Pruebas de muestras relacionadas			
	t	gl	Sig. (bilateral)

PRETEST-POSTTEST	,969	10	,886

Fuente: SPSS

En la tabla 7 nos muestra la prueba de muestras relacionadas tanto como el PRE TEST y POS TEST de la dimensión consistencia.

5.3. Prueba de T- Student

Este tipo de prueba es ideal cuando se desea comparar las medidas de dos grupos que tienen una distribución normal con número de observaciones menores a 30 y no se conoce su varianza poblacional σ^2, pero se usa su estimador s^2.

Se utiliza la siguiente fórmula para el caso de número igual de observaciones.

Dónde: *tc= t-student calculado*

$$tc = \frac{\overline{X}a - \overline{X}b}{\sqrt{\frac{s^2a + s^2b}{n}}}$$

$\bar{X}a$ *= Promedio de la muestra a*

$\bar{X}b$*= Promedio de la muestra b*

$s^2\ a$*= Desviación estándar Pre Test*

$s^2\ b$*= Desviación estándar Post Test*

n= Número de elementos

Realizamos las pruebas definiendo la hipótesis nula y alternativa.

H_0; $\mu_a = \mu_d$ (La gestión de la seguridad de la información antes y después no presenta diferencias significativas).

H1; $\mu_a < \mu_d$ (La gestión de la seguridad de la información ANTES es significativamente menor a la gestión de la seguridad de la información DESPUES).

Ahora debemos de calcular T-Student de la tabla (tt) para compararlo con el T-Student calculado (tc), para ello trabajamos con los siguientes paramentos:

Nivel de significancia (α)= 5%

Grado de libertad (n) = 13

Tabla 8 *Pruebas de Muestras Independientes*

		Prueba de Levene para la igualdad de varianzas		Prueba T para la igualdad de medias						
		F	Sig.	T	Gl	Sig. (bilateral)	Diferencia de medias	Error típ. de la diferencia	95% Intervalo de confianza para la diferencia	
									Superior	Inferior
Resultados	Se han asumido varianzas iguales	1.316	0.263	-56.861	24	.000	-46.769	.823	-48.467	-45.072
	No se han asumido varianzas iguales			-56.861	21.383	.000	-46.769	.823	-48.478	-45.061

Fuente: SPSS

Como se puede observar en la Tabla 8. “Los resultados nos dan muchos indicadores estadísticos como la media de cada grupo, su desviación típica o estándar, error típico de la media, grados de libertad entre otras. Lo fundamental es el T-calculado (t_c) y en este caso el valor de t_c = -56.861”.

Este valor lo contrastaremos con el T-tabla (tt); Se busca en la tabla de t-student con 2(n-1) grados de libertad o sea 24 y se encuentra que el valor tabular es de -1.697 al 95% de probabilidad (tc < tt)

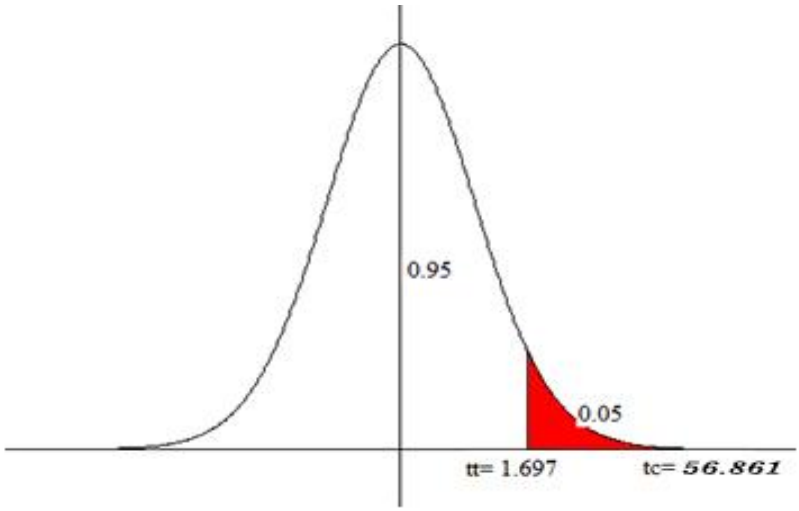


Figura 5: Distribución T-Student según encuesta.

Fuente: Elaboración Propia

Decisión:

Si (tc > tt) 56.861 > 1.697 rechazamos la hipótesis nula.

Como tc =56.861 es mayor que tt=1.697, entonces rechazamos la H0 y por consiguiente aceptamos la hipótesis alternativa.

Procedimiento: Se llevó un registro del tiempo que le toma al personal en realizar un reporte de los indicadores que permiten monitorear la producción por usuario de esta manera se fue llenando el registro de tiempo de incidencia.

Tabla 9 *Tiempo estimado por Usuario ante los reportes más comunes*

Usuario	Pre Test	Pos Test
1	3:43:00	0:16:00
2	4:04:00	0:17:00
3	3:44:00	0:10:00
4	3:59:00	0:13:00
5	3:49:00	0:11:00
6	3:37:00	0:19:00
7	3:50:00	0:24:00
8	3:53:00	0:27:00
9	3:40:00	0:20:00
10	3:50:00	0:21:00
11	3:45:00	0:17:00
12	3:42:00	0:14:00
13	3:51:00	0:08:00

Fuente: Elaboración propia

“En la Tabla 9 nos muestra la cantidad de trabajadores y el tiempo promedio por trabajador en la elaboración de un reporte que permita mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida, antes de la implementación del modelo de políticas (Pre Test) y después de la implementación del modelo de políticas (Post Test)”.

Tabla 10 *Estadísticos de grupo*

	Grupo con PRE TEST Y POS TEST	N	Media	Desviación típ.	Error típ. de la media
Tiempo de creación reportes principales	Pre test	13	3:47:53	0:07:10	0:01:38
	Post test	13	2:18:09	0:05:41	0:01:18

Fuente: SPSS

En la Tabla 10, nos muestra la media del tiempo de resolución de la encuesta antes de la implementación del modelo de políticas (PRE TEST) 3:47:53 horas y después de la implementación del modelo de políticas (POS TES) 0:18:09 horas, se puede observar la diferencia significativa del en la media de los tiempos.

5.3.1. Dimensiones

5.3.1.1. T-Student de la dimensión política

Seguidamente de hacer la normalidad se hizo el T-Student obteniendo el siguiente resultado:

Estadísticos de muestras relacionadas

		Media	N	Desviación típ.	Error típ. de la media
Par 1	D1PRE	6,40	10	1,174	,371
	D1POS	14,40	10	,699	,221

Correlaciones de muestras relacionadas

		N	Correlación	Sig.
Par 1	D1PRE y D1POS	10	-,623	,054

Prueba de muestras relacionadas

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia Inferior	Superior			
Par 1	D1PRE - D1POS	-8,000	1,700	,537	-9,216	-6,784	-14,884	9	,000

Figura 6: T-Student de la dimensión políticas

Fuente: SPSS

En la figura 6 muestra que el T-Student es menor que 0.05, se rechaza la hipótesis nula y se acepta la hipótesis alterna

5.3.1.2. T-Student de la dimensión servicio

Seguidamente de hacer la normalidad se hizo el T-Student obteniendo el siguiente resultado:

Estadísticos de muestras relacionadas

		Media	N	Desviación típ.	Error típ. de la media
Par 1	D2PRE	7,00	10	1,333	,422
	D2POS	14,40	10	,699	,221

Correlaciones de muestras relacionadas

		N	Correlación	Sig.
Par 1	D2PRE y D2POS	10	,119	,743

Prueba de muestras relacionadas

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia				
					Inferior	Superior			
Par 1	D2PRE - D2POS	-7,400	1,430	,452	-8,423	-6,377	-16,366	9	,000

Figura 7: T-Student de la dimensión servicio.

Fuente: SPSS.

En la figura 7 muestra que el T-Student es menor que 0.05, se rechaza la hipótesis nula y se acepta la hipótesis alterna

5.3.1.3. T-Student de la dimensión riesgos

Seguidamente de hacer la normalidad se hizo el T-Student obteniendo el siguiente resultado:

Estadísticos de muestras relacionadas

		Media	N	Desviación típ.	Error típ. de la media
Par 1	D3PRE	9,00	10	1,886	,596
	D3POS	28,50	10	,707	,224

Correlaciones de muestras relacionadas

		N	Correlación	Sig.
Par 1	D3PRE y D3POS	10	,083	,819

Prueba de muestras relacionadas

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia Inferior	Superior			
Par 1	D3PRE - D3POS	-19,500	1,958	,619	-20,901	-18,099	-31,495	9	,000

Figura 8: T-Student de la dimensión riesgos.

Fuente: SPSS.

En la figura 8 muestra que el T-Student es menor que 0.05, se rechaza la hipótesis nula y se acepta la hipótesis alterna

5.3.1.4. T-Student de la dimensión consistencia

Seguidamente de hacer la normalidad se hizo el T-Student obteniendo el siguiente resultado:

Estadísticos de muestras relacionadas

		Media	N	Desviación típ.	Error típ. de la media
Par 1	D4PRE	6,10	10	1,524	,482
	D4POS	14,70	10	,675	,213

Correlaciones de muestras relacionadas

		N	Correlación	Sig.
Par 1	D4PRE y D4POS	10	,248	,489

Prueba de muestras relacionadas

		Diferencias relacionadas					t	gl	Sig. (bilateral)
		Media	Desviación típ.	Error típ. de la media	95% Intervalo de confianza para la diferencia Inferior	Superior			
Par 1	D4PRE - D4POS	-8,600	1,506	,476	-9,677	-7,523	-18,064	9	,000

Figura 9: T-Student de la dimensión consistencia.

Fuente: SPSS.

En la figura 9 muestra que el T-Student es menor que 0.05, se rechaza la hipótesis nula y se acepta la hipótesis alterna

5.4. Discusiones

En el estudio realizado, para poder identificar si los datos tiene una distribución normal o no se realizó mediante la prueba de normalidad Shapiro-Wilk la cual nos muestra que **P** es mayor a 0.05 por lo tanto podemos decir que los datos tienen una distribución normal para la variable gestión de seguridad de la información así mismo se analizó los datos para ver el comportamiento de los mismos para la variable gestión de seguridad de la información la cual el valor de **p** es de 0,540 por lo que también decimos que tienen un comportamiento normal.

Por otro lado, el análisis de los datos recolectados para la dimensión "*Políticas*", se muestra que la significancia bilateral (valor de P) es 0,717 la cual es mayor a 0.05 por lo tanto podemos decir que los datos siguen una distribución normal por lo tanto es paramétrica.

Por otro lado, el análisis de los datos recolectados para la dimensión "*Servicio*", se muestra que la significancia bilateral (valor de P) es 0,732 la cual es mayor a 0.05 por lo tanto podemos decir que los datos siguen una distribución normal por lo tanto es paramétrica.

De igual manera, el análisis de los datos recolectados para la dimensión "*Riesgo*", se muestra que la significancia bilateral (valor de P) es 0,394 la cual es mayor a 0.05 por lo tanto podemos decir que los datos siguen una distribución normal por lo tanto es paramétrica.

Y, por último, el análisis de los datos recolectados para la dimensión "*Consistencia*", se muestra que la significancia bilateral (valor de P) es 0,886 la cual es mayor a 0.05 por lo tanto podemos decir que los datos siguen una distribución normal por lo tanto es paramétrica.

CAPÍTULO VI: CONCLUSIONES Y RECOMENDACIONES

2 6.1. Conclusiones

Tomando como punto de referencia los estudios presentados y los resultados obtenidos en esta investigación sobre la seguridad de la información en la Municipalidad Distrital de Florida, encontramos las siguientes conclusiones.

- La seguridad de la información es una responsabilidad compartida de todas las áreas de la municipalidad, que requiere del apoyo de todos ellos que estén comprometidos con la seguridad, pero esto debe estar dirigida por un plan y con una adecuada coordinación.
- El estudio realizado, para poder identificar si los datos tienes una distribución normal o no, se realizó mediante la prueba de normalidad Shapiro-Wilk la cual nos muestra que **P** es mayor a 0.05 por lo tanto podemos decir que los datos tienen una distribución normal para la variable gestión de seguridad de la información".
- "Con respecto al pre test, los resultados que se obtuvieron, fue que los trabajadores administrativos de las diferentes áreas de la Municipalidad Distrital de Florida no consideran a la seguridad como una prioridad alineada con las estrategias de la Municipalidad. Esto se refleja en las encuestas realizadas al personal.
- Con respecto a la encuesta aplicada en el Pos Test, los resultados fueron satisfactorios ya que los trabajadores que laboran en dicha entidad, están comprometidos, y capacitados con temas relacionados con la seguridad de la información.
- Los sistemas de Gestión de Seguridad de Información bajo la norma ISO 27001, se basan en la prevención, por lo tanto, es muy importante identificar los riesgos a los que están expuestos los activos para así evitar pérdidas económicas u operacionales.
- La elaboración de la investigación, contribuyó a que la Municipalidad, en especial el área de Gerencia y Tesorería, tome conciencia de cuán importante es que la

información sea confiable, ´íntegra y disponible para la organización ya que vieron que si cualquiera de estas características sufriera alteraciones conllevaría a resultados nefastos.

- Con esta investigación deseo fomentar una cultura de seguridad en todas aquellas personas que consulten y sedeen ponerlo en práctica.

3 6.2. Recomendaciones

Al finalizar la investigación se hacen las siguientes recomendaciones.

- Realizar talleres, programas de capacitación de seguridad de la información más seguido, y especialmente al personal nuevo que ingresa; pero primero debemos implementar el programa de seguridad para los administrativos, jefes de cada área administrativa, luego trabajadores, y a todo el personal externo que brinda servicios.
- Se debe buscar el compromiso y soporte gerencial, de manera que el proyecto venga patrocinado desde arriba en la gerencia, y sea esta la primera en dar ejemplo a la hora de aplicar aquellas medidas necesarias para definir, aplicar y mantener la seguridad de la información de la Municipalidad.
- Se deben rediseñar las redes informáticas de la Municipalidad separando el área de gerencia y el área administrativa pues tienen sistemas administrativos críticos. Es necesario consolidar sus redes informáticas aplicando tecnología de prevención y detección de intrusos, que es una buena solución para observar el tráfico de la red, permitir el ingreso del tráfico legítimo y detectar comportamientos maliciosos como los ataques de negación de servicios para evitar interrupciones en la red.
- La Municipalidad debería contar con personal que cumplan las competencias por la norma ISO 27001 para evitar la contratación de consultorías externas, cuyo costo es muy alto.
- La Municipalidad debe implantar una cultura de conciencia de seguridad que fomente la identificación del trabajador con la información que maneja.

Referencias

(ICONTEC), I. C. de N. y C. (20013). ISO 27001 2013 Español .pdf. Retrieved from http://www.iso.org/iso/catalogue_detail?csnumber=54534

27001, I. (2013). Information technology - Security techniques - Information security management systems - Requirements, 32.

Qualitas consultores. (2012). Normas: ISO/ IEC 27001 http://qualitas.com.pe/normas/iso-27001

ISSA. (2011). ISO/ IEC 27004. Lima http://issaperu.org/?p=13

INDECOPI. (2014). NTP ISO/IEC 27001:2014 Tecnología de Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de Información. Requerimientos. Lima, 2014.

INTERNATIONAL STANDARD.(2007). ISO/IEC 27006. Information technology — Security techniques — Requirements for bodies providing audit and certification of information security 68 management systems. First Edition. http://www.pqm-online.com/assets/files/standards/iso_iec_27006- 2007.pdf

INTERNATIONAL STANDARD. (2011). ISO/IEC 27007. Information technology — Security techniques — Guidelines for information security management systems auditing. First Edition.

Enrique Martín Méndez, Miguel Ángel Aguilar. (2012). Proyecto Sanitas: Sistema de Gestión de Seguridad de la Información y certificación UNE 71502 e ISO 27001.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. (2014). ISO/IEC 27000:2014 Tecnología de Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de Información - Descripción y vocabulario. Suiza.

Bunge, M. (1979). La Ciencia. Su método y su fiosofía, 37. Retrieved from http://users.dcc.uchile.cl/~cgutierr/cursos/INV/bunge_ciencia.pdf

Cano Reyes, D., Basabe Sierra, L., Marcela Perdomo, J., Mosquera Mosquera, A. Fuentes

Sarmiento, W. D. (2015). INVESTIGACIÓN, (1), 1–14. Retrieved from http://sisbib.unmsm.edu.pe/bibVirtualData/Tesis para marcación3 (para Informática)/2011/alva_ar/alvar_ar.pdf

Hernandez Sampieri, R., Fernandez Collado, C., & Baptista Lucio, M. del P. (2010). *Metodología de la investigación*. *Metodología de la investigación*. Retrieved from http://www.casadellibro.com/libro-metodologia-de-la-investigacion-5-ed-incluye-cd-rom/9786071502919/1960006

INDECOPI. (2014). PERUANA NTP-ISO / IEC 27001 TECNOLOGÍA DE LA INFORMACIÓN . Técnicas de información . Requisitos, 45. Retrieved from http://www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

ISO 27000. (2013). Iso 27000, 19. Retrieved from http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO/IEC 27001. (2013). Information technology -- Security techniques -- Information security management systems – Requirements.

Anexos

Anexos 1: Encuesta realizada para medir el nivel de la seguridad de la información basado en la norma ISO 27001 en la Municipalidad Distrital de Florida – Bongará – Amazonas.

INSTRUCCIONES: Marque con una x la opción que usted crea conveniente.

VARIABLES				
1	**2**	**3**	**4**	**5**
Nunca	Casi Nunca	A veces	Casi Siempre	Siempre

1. EDAD: ……
2. SEXO: Masculino ( ) Femenino ( )

FACTORES DETERMINANTES	**ALTERATIVAS**				
	1	2	3	4	5
En la municipalidad donde labora cuenta con políticas de seguridad de la información.					
Con que frecuencia se cumplen las políticas de seguridad de la información.					
La calidad en el servicio tanto para los trabajadores y alcalde ha aumentado.					
Se realiza un monitoreo y un reporte mensual de las actividades realizadas en la red.					
La información que posee en la Municipalidad Distrital de Florida es segura.					
La municipalidad cuenta con una buena seguridad de la información.					
Es posible realizar un seguimiento sobre la información.					
Usted cree que las políticas de seguridad aumentan la calidad de servicio para los trabajadores y alcalde.					
Se realiza capacitaciones o talleres sobre seguridad de información.					

Usted cree que existe un orden de la información tanto física como virtual.					
Realiza usted un uso adecuado de las herramientas de seguridad de la información.					
Los softwares o programas que utiliza cuentan con licencia, y antivirus actualizados.					
Usted cree que la divulgación ilícita de la información se da por parte de los empleados o terceros.					
Las contraseñas que utiliza en Facebook, Gmail, Instagram, deben ser diferentes a la pc de trabajo.					
La información que comparte con personas externas, son totalmente diferentes a la de su trabajo.					

Anexos 2: *Documento de autorización para hacer entrega del manual de políticas de seguridad, a las diferentes áreas de la Municipalidad Distrital de Florida.*

MUNICIPALIDAD DISTRITAL DE FLORIDA
BONGARÁ – AMAZONAS
"Año del dialogo y de la reconciliación nacional"

AUTORIZACIÓN MUNICIPAL

CARGO

EL GERENTE DE LA MUNICIPALIDAD DISTRITAL DE FLORIDA, PROVINCIA DE BONGARA, DEPARTAMENTO DE AMAZONAS, OTORGA LA PRESENTE:

AUTORIZACIÓN MUNICIPAL:

Al señor **HENRY PERCY CABRERA CUBAS,** identificado con DNI N°48421156, con domicilio legal en Av. Marginal S/N, Barrio Fichack-Pomacochas; para entregar manual de políticas de seguridad, a las diferentes áreas de la Municipalidad Distrital de Florida.

Habiendo cumplido con los requisitos que establece el texto único de procedimientos Administrativos (TUPA).

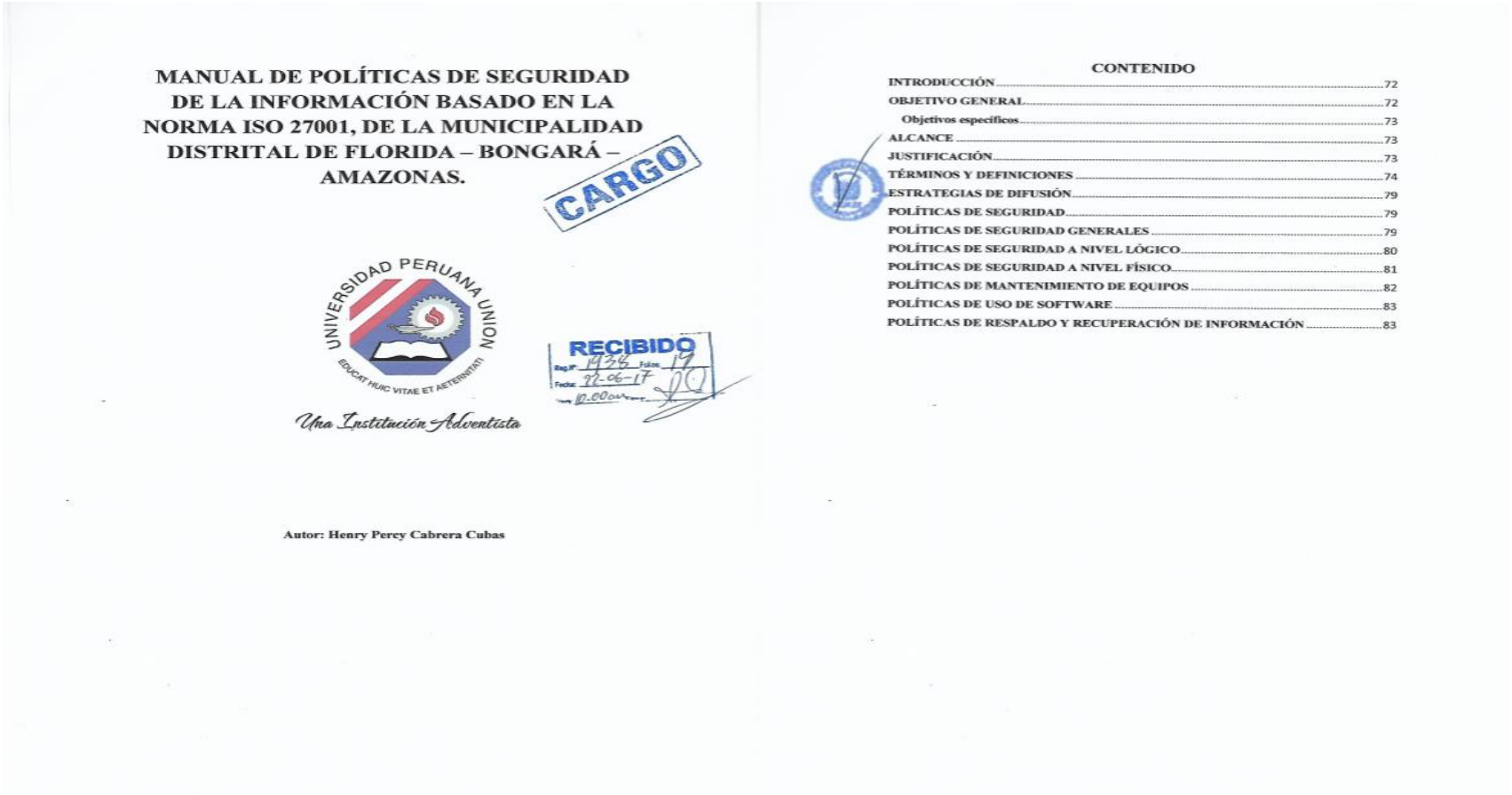
Pomacochas, 26 de junio del 2017.

JR. FLORIDA N° 501 POMACOCHAS – BONGARÁ – AMAZONAS. EMAIL: muniflorida@hotmail.com

Figura 10: autorización para hacer entrega del manual de políticas de seguridad

Fuente: Elaboración Propia

Anexos 3: Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001, de la Municipalidad Distrital de Florida.



MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO 27001, DE LA MUNICIPALIDAD DISTRITAL DE FLORIDA – BONGARÁ – AMAZONAS.

CARGO

UNIVERSIDAD PERUANA UNION

EDUCAT HUIC VITAE ET AETERNITATI

Una Institución Adventista

RECIBIDO

Reg.N° 1936 Folios 19

Fecha 22-06-17

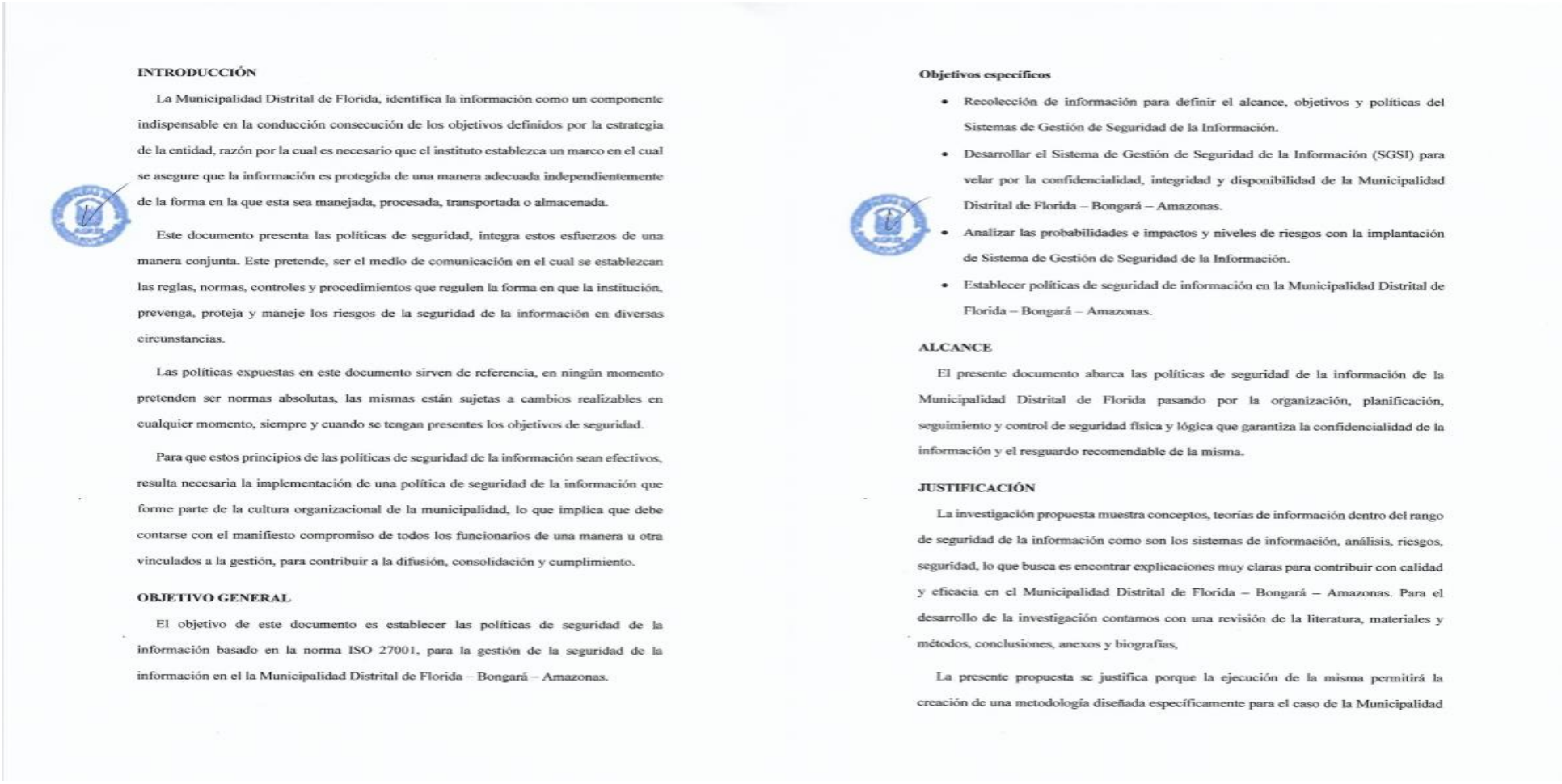
S/. 10.00

Autor: Henry Percy Cabrera Cubas

CONTENIDO

Figura 11: Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001

Fuente: Elaboración propia.



INTRODUCCIÓN

La Municipalidad Distrital de Florida, identifica la información como un componente indispensable en la conducción consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que el instituto establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que esta sea manejada, procesada, transportada o almacenada.

Este documento presenta las políticas de seguridad, integra estos esfuerzos de una manera conjunta. Este pretende, ser el medio de comunicación en el cual se establezcan las reglas, normas, controles y procedimientos que regulen la forma en que la institución, prevenga, proteja y maneje los riesgos de la seguridad de la información en diversas circunstancias.

Las políticas expuestas en este documento sirven de referencia, en ningún momento pretenden ser normas absolutas, las mismas están sujetas a cambios realizables en cualquier momento, siempre y cuando se tengan presentes los objetivos de seguridad.

Para que estos principios de las políticas de seguridad de la información sean efectivos, resulta necesaria la implementación de una política de seguridad de la información que forme parte de la cultura organizacional de la municipalidad, lo que implica que debe contarse con el manifiesto compromiso de todos los funcionarios de una manera u otra vinculados a la gestión, para contribuir a la difusión, consolidación y cumplimiento.

OBJETIVO GENERAL

El objetivo de este documento es establecer las políticas de seguridad de la información basado en la norma ISO 27001, para la gestión de la seguridad de la información en el la Municipalidad Distrital de Florida – Bongará – Amazonas.

Objetivos específicos

- Recolección de información para definir el alcance, objetivos y políticas del Sistemas de Gestión de Seguridad de la Información.
- Desarrollar el Sistema de Gestión de Seguridad de la Información (SGSI) para velar por la confidencialidad, integridad y disponibilidad de la Municipalidad Distrital de Florida – Bongará – Amazonas.
- Analizar las probabilidades e impactos y niveles de riesgos con la implantación de Sistema de Gestión de Seguridad de la Información.
- Establecer políticas de seguridad de información en la Municipalidad Distrital de Florida – Bongará – Amazonas.

ALCANCE

El presente documento abarca las políticas de seguridad de la información de la Municipalidad Distrital de Florida pasando por la organización, planificación, seguimiento y control de seguridad física y lógica que garantiza la confidencialidad de la información y el resguardo recomendable de la misma.

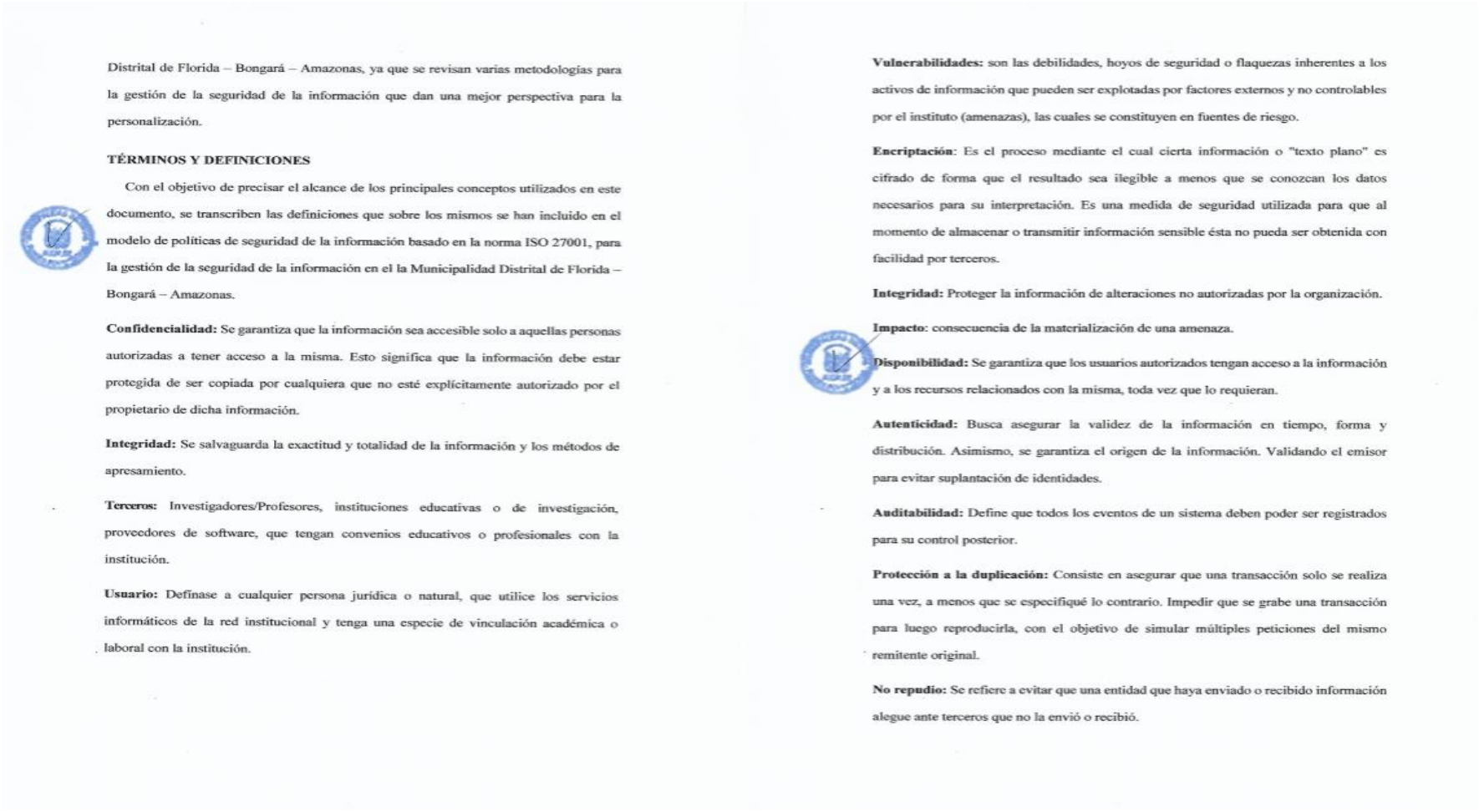
JUSTIFICACIÓN

La investigación propuesta muestra conceptos, teorías de información dentro del rango de seguridad de la información como son los sistemas de información, análisis, riesgos, seguridad, lo que busca es encontrar explicaciones muy claras para contribuir con calidad y eficacia en el Municipalidad Distrital de Florida – Bongará – Amazonas. Para el desarrollo de la investigación contamos con una revisión de la literatura, materiales y métodos, conclusiones, anexos y biografías,

La presente propuesta se justifica porque la ejecución de la misma permitirá la creación de una metodología diseñada específicamente para el caso de la Municipalidad

Figura 12: Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001

Fuente: Elaboración propia



Distrital de Florida – Bongará – Amazonas, ya que se revisan varias metodologías para la gestión de la seguridad de la información que dan una mejor perspectiva para la personalización.

TÉRMINOS Y DEFINICIONES

Con el objetivo de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones que sobre los mismos se han incluido en el modelo de políticas de seguridad de la información basado en la norma ISO 27001, para la gestión de la seguridad de la información en el la Municipalidad Distrital de Florida – Bongará – Amazonas.

Confidencialidad: Se garantiza que la información sea accesible solo a aquellas personas autorizadas a tener acceso a la misma. Esto significa que la información debe estar protegida de ser copiada por cualquiera que no esté explícitamente autorizado por el propietario de dicha información.

Integridad: Se salvaguarda la exactitud y totalidad de la información y los métodos de apresamiento.

Terceros: Investigadores/Profesores, instituciones educativas o de investigación, proveedores de software, que tengan convenios educativos o profesionales con la institución.

Usuario: Defínase a cualquier persona jurídica o natural, que utilice los servicios informáticos de la red institucional y tenga una especie de vinculación académica o laboral con la institución.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el instituto (amenazas), las cuales se constituyen en fuentes de riesgo.

Encriptación: Es el proceso mediante el cual cierta información o "texto plano" es cifrado de forma que el resultado sea ilegible a menos que se conozcan los datos necesarios para su interpretación. Es una medida de seguridad utilizada para que al momento de almacenar o transmitir información sensible ésta no pueda ser obtenida con facilidad por terceros.

Integridad: Proteger la información de alteraciones no autorizadas por la organización.

Impacto: consecuencia de la materialización de una amenaza.

Disponibilidad: Se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Autenticidad: Busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información. Validando el emisor para evitar suplantación de identidades.

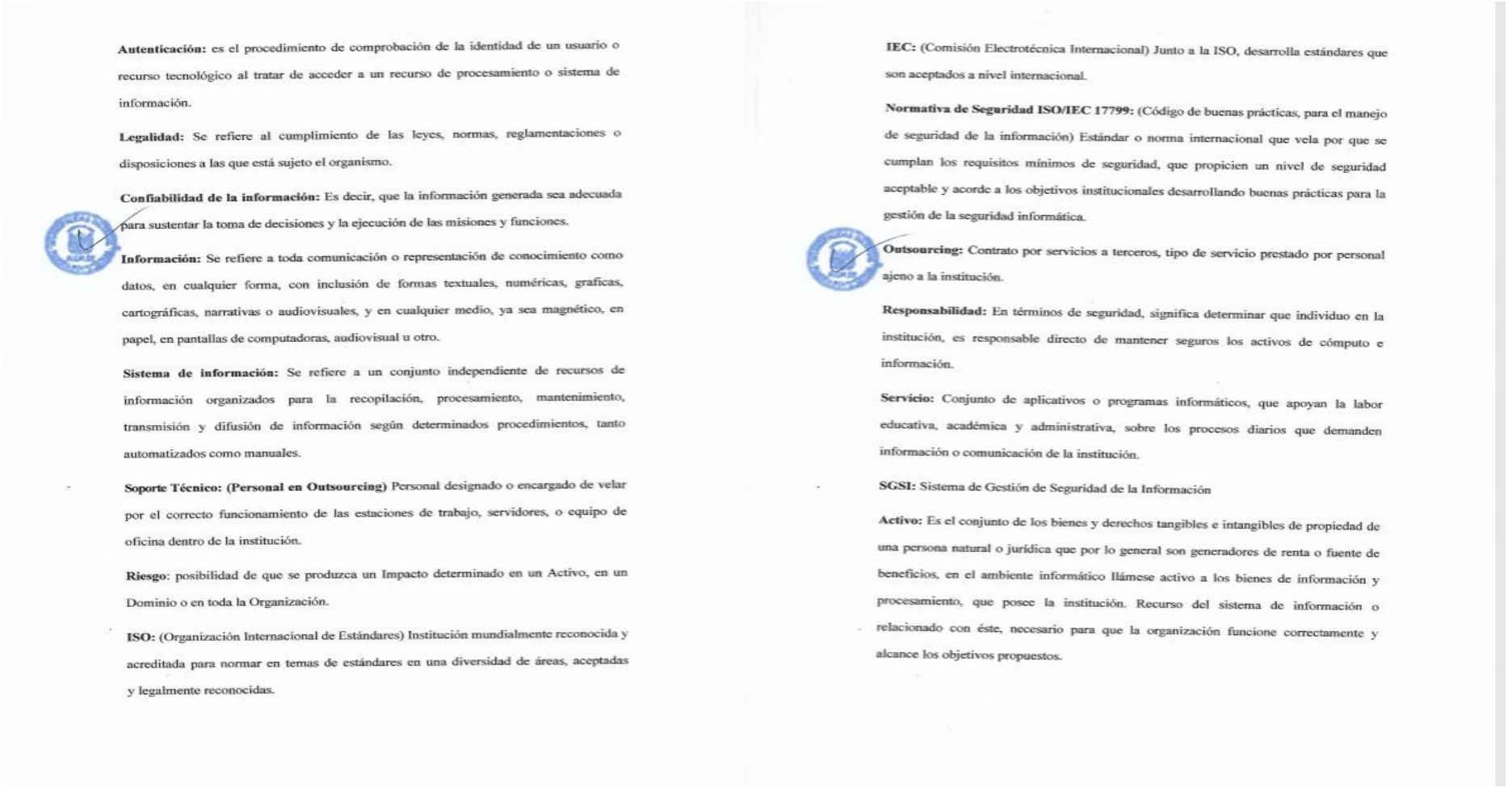
Auditabilidad: Define que todos los eventos de un sistema deben poder ser registrados para su control posterior.

Protección a la duplicación: Consiste en asegurar que una transacción solo se realiza una vez, a menos que se especifiqué lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objetivo de simular múltiples peticiones del mismo remitente original.

No repudio: Se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió.

Figura 13: Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001

Fuente: Elaboración propia



Autenticación: es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Legalidad: Se refiere al cumplimiento de las leyes, normas, reglamentaciones o disposiciones a las que está sujeto el organismo.

Confiabilidad de la información: Es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, graficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Soporte Técnico: (Personal en Outsourcing) Personal designado o encargado de velar por el correcto funcionamiento de las estaciones de trabajo, servidores, o equipo de oficina dentro de la institución.

Riesgo: posibilidad de que se produzca un Impacto determinado en un Activo, en un Dominio o en toda la Organización.

ISO: (Organización Internacional de Estándares) Institución mundialmente reconocida y acreditada para normar en temas de estándares en una diversidad de áreas, aceptadas y legalmente reconocidas.

IEC: (Comisión Electrotécnica Internacional) Junto a la ISO, desarrolla estándares que son aceptados a nivel internacional.

Normativa de Seguridad ISO/IEC 17799: (Código de buenas prácticas, para el manejo de seguridad de la información) Estándar o norma internacional que vela por que se cumplan los requisitos mínimos de seguridad, que propicien un nivel de seguridad aceptable y acorde a los objetivos institucionales desarrollando buenas prácticas para la gestión de la seguridad informática.

Outsourcing: Contrato por servicios a terceros, tipo de servicio prestado por personal ajeno a la institución.

Responsabilidad: En términos de seguridad, significa determinar que individuo en la institución, es responsable directo de mantener seguros los activos de cómputo e información.

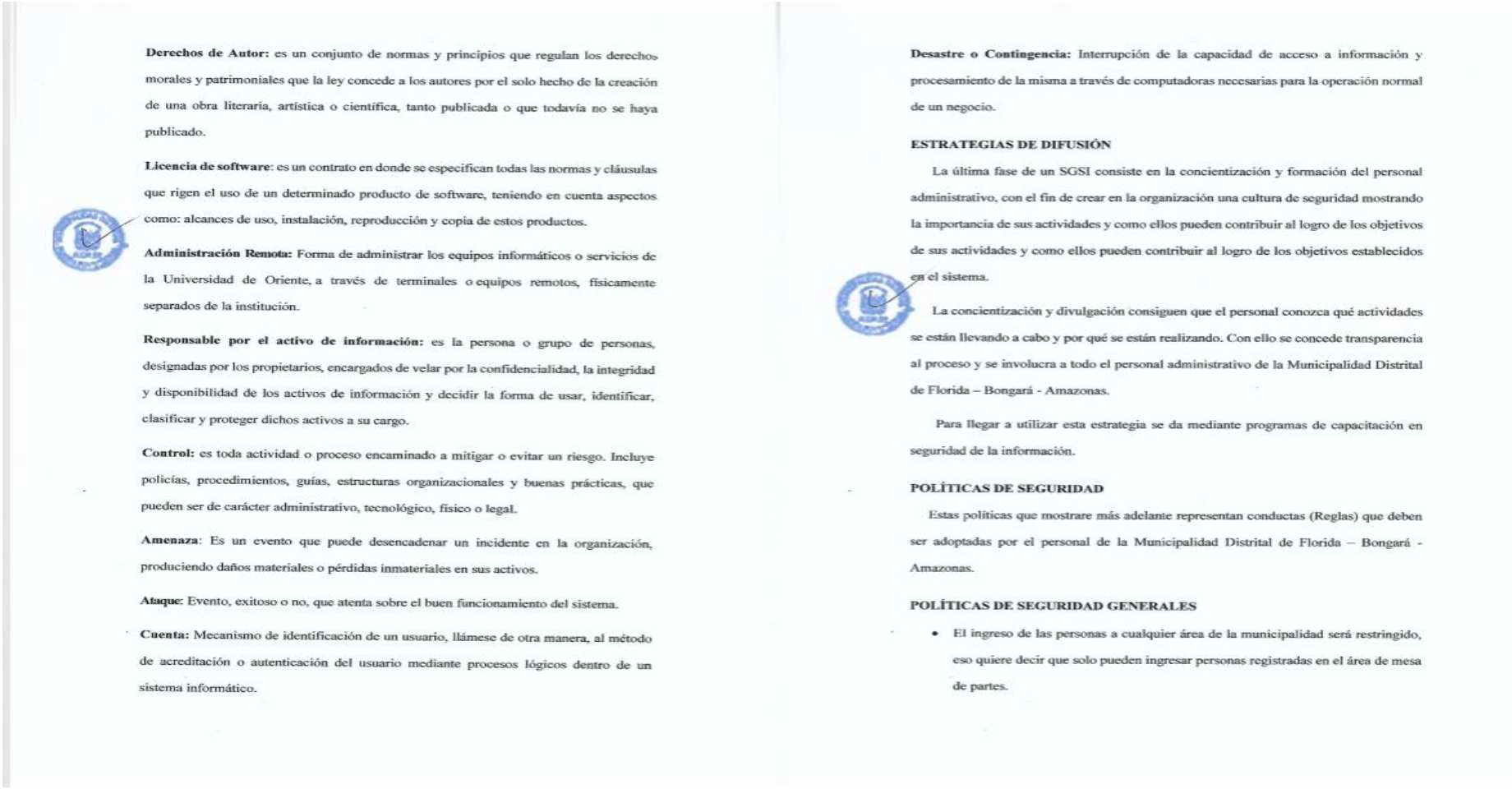
Servicio: Conjunto de aplicativos o programas informáticos, que apoyan la labor educativa, académica y administrativa, sobre los procesos diarios que demanden información o comunicación de la institución.

SGSI: Sistema de Gestión de Seguridad de la Información

Activo: Es el conjunto de los bienes y derechos tangibles e intangibles de propiedad de una persona natural o jurídica que por lo general son generadores de renta o fuente de beneficios, en el ambiente informático llámese activo a los bienes de información y procesamiento, que posee la institución. Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos.

Figura 14: Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001

Fuente: Elaboración propia



Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Administración Remota: Forma de administrar los equipos informáticos o servicios de la Universidad de Oriente, a través de terminales o equipos remotos, físicamente separados de la institución.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Amenaza: Es un evento que puede desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Ataque: Evento, exitoso o no, que atenta sobre el buen funcionamiento del sistema.

Cuenta: Mecanismo de identificación de un usuario, llámese de otra manera, al método de acreditación o autenticación del usuario mediante procesos lógicos dentro de un sistema informático.

Desastre o Contingencia: Interrupción de la capacidad de acceso a información y procesamiento de la misma a través de computadoras necesarias para la operación normal de un negocio.

ESTRATEGIAS DE DIFUSIÓN

La última fase de un SGSI consiste en la concientización y formación del personal administrativo, con el fin de crear en la organización una cultura de seguridad mostrando la importancia de sus actividades y como ellos pueden contribuir al logro de los objetivos de sus actividades y como ellos pueden contribuir al logro de los objetivos establecidos en el sistema.

La concientización y divulgación consiguen que el personal conozca qué actividades se están llevando a cabo y por qué se están realizando. Con ello se concede transparencia al proceso y se involucra a todo el personal administrativo de la Municipalidad Distrital de Florida – Bongará - Amazonas.

Para llegar a utilizar esta estrategia se da mediante programas de capacitación en seguridad de la información.

POLÍTICAS DE SEGURIDAD

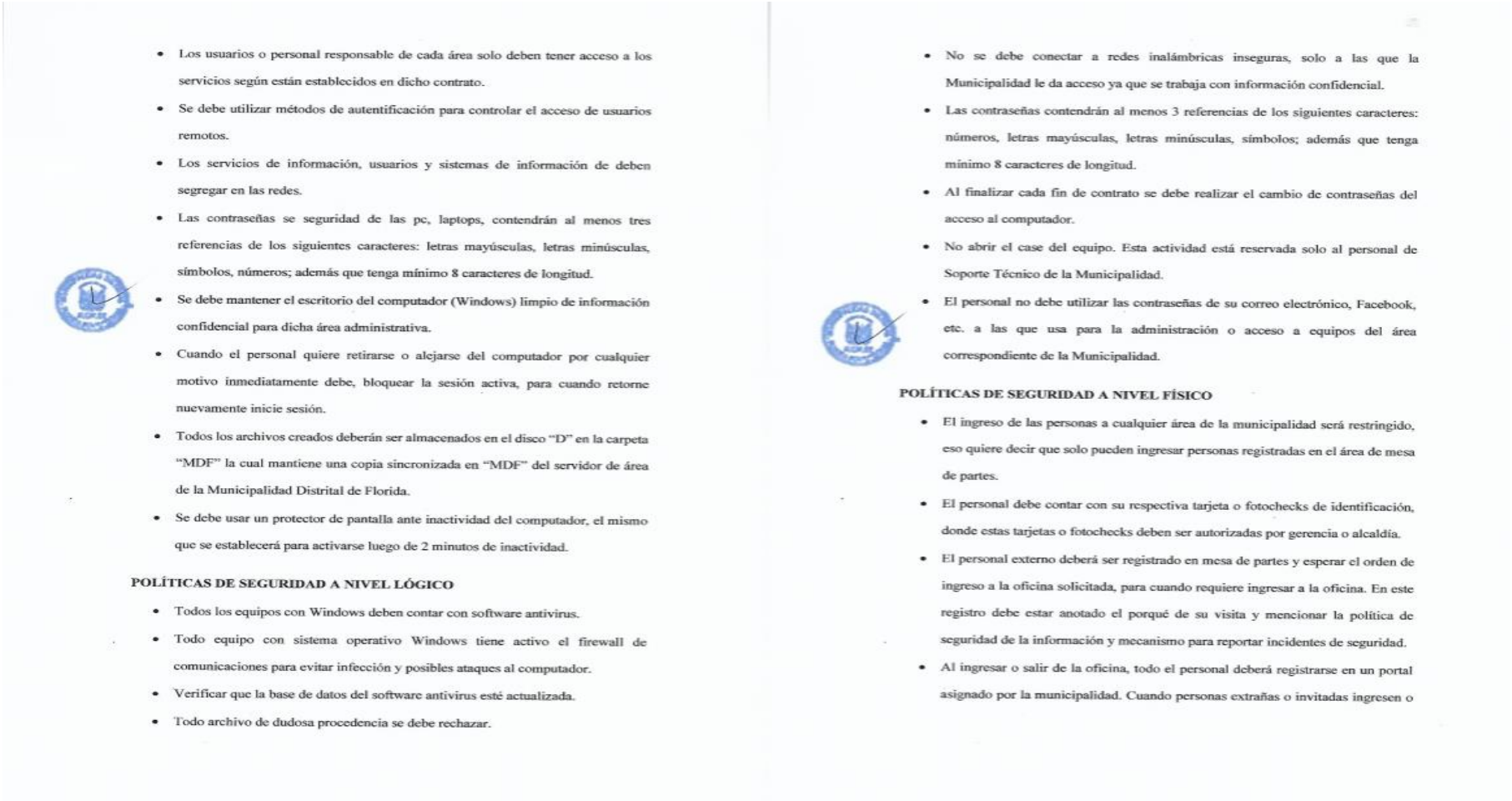
Estas políticas que mostrare más adelante representan conductas (Reglas) que deben ser adoptadas por el personal de la Municipalidad Distrital de Florida – Bongará - Amazonas.

POLÍTICAS DE SEGURIDAD GENERALES

- El ingreso de las personas a cualquier área de la municipalidad será restringido, eso quiere decir que solo pueden ingresar personas registradas en el área de mesa de partes.

Figura 15: Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001

Fuente: Elaboración propia



- Los usuarios o personal responsable de cada área solo deben tener acceso a los servicios según están establecidos en dicho contrato.
- Se debe utilizar métodos de autentificación para controlar el acceso de usuarios remotos.
- Los servicios de información, usuarios y sistemas de información de deben segregar en las redes.
- Las contraseñas se seguridad de las pc, laptops, contendrán al menos tres referencias de los siguientes caracteres: letras mayúsculas, letras minúsculas, símbolos, números; además que tenga mínimo 8 caracteres de longitud.
- Se debe mantener el escritorio del computador (Windows) limpio de información confidencial para dicha área administrativa.
- Cuando el personal quiere retirarse o alejarse del computador por cualquier motivo inmediatamente debe, bloquear la sesión activa, para cuando retorne nuevamente inicie sesión.
- Todos los archivos creados deberán ser almacenados en el disco "D" en la carpeta "MDF" la cual mantiene una copia sincronizada en "MDF" del servidor de área de la Municipalidad Distrital de Florida.
- Se debe usar un protector de pantalla ante inactividad del computador, el mismo que se establecerá para activarse luego de 2 minutos de inactividad.

POLÍTICAS DE SEGURIDAD A NIVEL LÓGICO

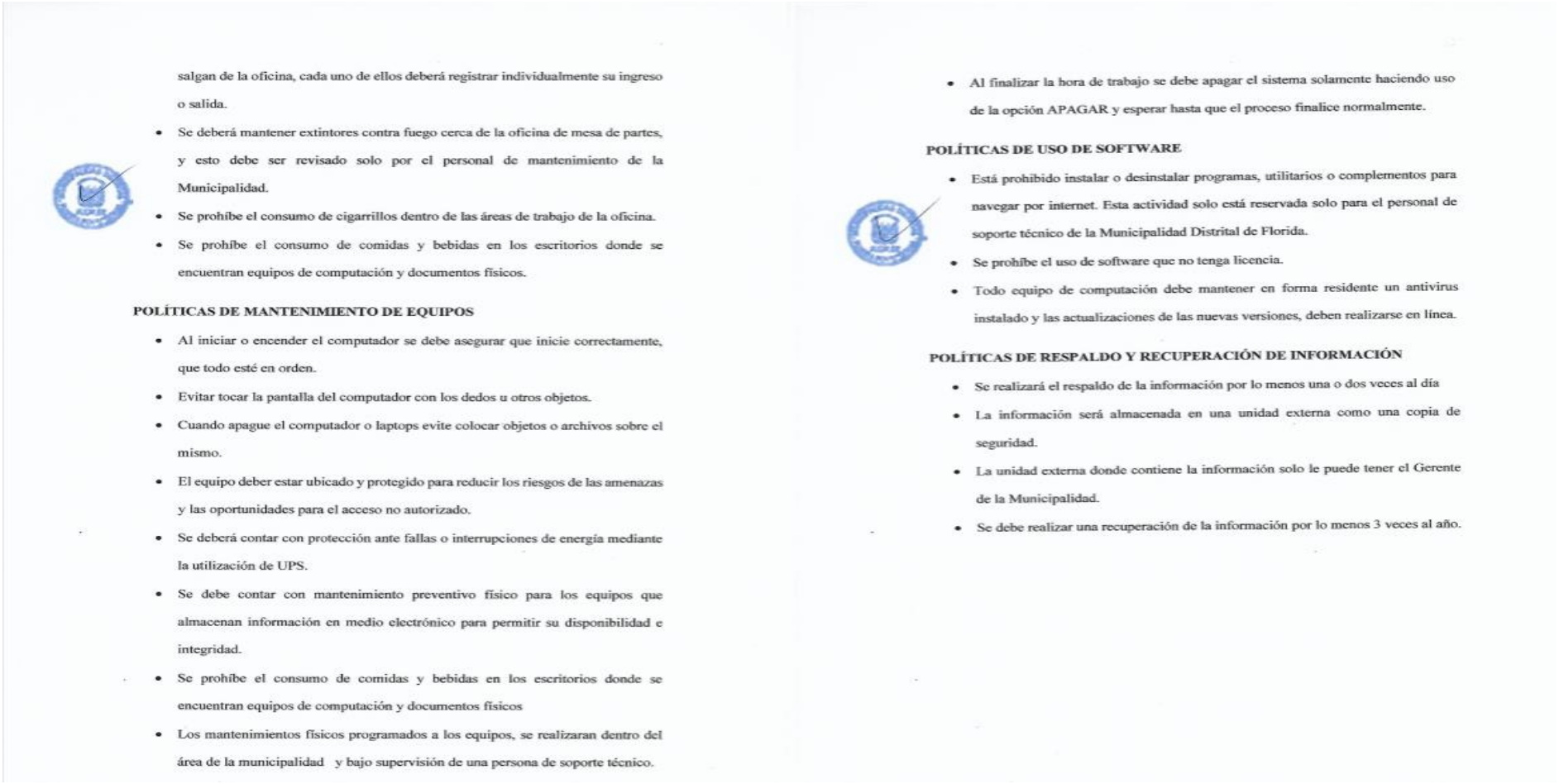
- Todos los equipos con Windows deben contar con software antivirus.
- Todo equipo con sistema operativo Windows tiene activo el firewall de comunicaciones para evitar infección y posibles ataques al computador.
- Verificar que la base de datos del software antivirus esté actualizada.
- Todo archivo de dudosa procedencia se debe rechazar.
- No se debe conectar a redes inalámbricas inseguras, solo a las que la Municipalidad le da acceso ya que se trabaja con información confidencial.
- Las contraseñas contendrán al menos 3 referencias de los siguientes caracteres: números, letras mayúsculas, letras minúsculas, símbolos; además que tenga mínimo 8 caracteres de longitud.
- Al finalizar cada fin de contrato se debe realizar el cambio de contraseñas del acceso al computador.
- No abrir el case del equipo. Esta actividad está reservada solo al personal de Soporte Técnico de la Municipalidad.
- El personal no debe utilizar las contraseñas de su correo electrónico, Facebook, etc. a las que usa para la administración o acceso a equipos del área correspondiente de la Municipalidad.

POLÍTICAS DE SEGURIDAD A NIVEL FÍSICO

- El ingreso de las personas a cualquier área de la municipalidad será restringido, eso quiere decir que solo pueden ingresar personas registradas en el área de mesa de partes.
- El personal debe contar con su respectiva tarjeta o fotochecks de identificación, donde estas tarjetas o fotochecks deben ser autorizadas por gerencia o alcaldía.
- El personal externo deberá ser registrado en mesa de partes y esperar el orden de ingreso a la oficina solicitada, para cuando requiere ingresar a la oficina. En este registro debe estar anotado el porqué de su visita y mencionar la política de seguridad de la información y mecanismo para reportar incidentes de seguridad.
- Al ingresar o salir de la oficina, todo el personal deberá registrarse en un portal asignado por la municipalidad. Cuando personas extrañas o invitadas ingresen o

Figura 16: Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001

Fuente: Elaboración propia



salgan de la oficina, cada uno de ellos deberá registrar individualmente su ingreso o salida.

- Se deberá mantener extintores contra fuego cerca de la oficina de mesa de partes, y esto debe ser revisado solo por el personal de mantenimiento de la Municipalidad.
- Se prohíbe el consumo de cigarrillos dentro de las áreas de trabajo de la oficina.
- Se prohíbe el consumo de comidas y bebidas en los escritorios donde se encuentran equipos de computación y documentos físicos.

POLÍTICAS DE MANTENIMIENTO DE EQUIPOS

- Al iniciar o encender el computador se debe asegurar que inicie correctamente, que todo esté en orden.
- Evitar tocar la pantalla del computador con los dedos u otros objetos.
- Cuando apague el computador o laptops evite colocar objetos o archivos sobre el mismo.
- El equipo deber estar ubicado y protegido para reducir los riesgos de las amenazas y las oportunidades para el acceso no autorizado.
- Se deberá contar con protección ante fallas o interrupciones de energía mediante la utilización de UPS.
- Se debe contar con mantenimiento preventivo físico para los equipos que almacenan información en medio electrónico para permitir su disponibilidad e integridad.
- Se prohíbe el consumo de comidas y bebidas en los escritorios donde se encuentran equipos de computación y documentos físicos
- Los mantenimientos físicos programados a los equipos, se realizaran dentro del área de la municipalidad y bajo supervisión de una persona de soporte técnico.

- Al finalizar la hora de trabajo se debe apagar el sistema solamente haciendo uso de la opción APAGAR y esperar hasta que el proceso finalice normalmente.

POLÍTICAS DE USO DE SOFTWARE

- Está prohibido instalar o desinstalar programas, utilitarios o complementos para navegar por internet. Esta actividad solo está reservada solo para el personal de soporte técnico de la Municipalidad Distrital de Florida.
- Se prohíbe el uso de software que no tenga licencia.
- Todo equipo de computación debe mantener en forma residente un antivirus instalado y las actualizaciones de las nuevas versiones, deben realizarse en línea.

POLÍTICAS DE RESPALDO Y RECUPERACIÓN DE INFORMACIÓN

- Se realizará el respaldo de la información por lo menos una o dos veces al día
- La información será almacenada en una unidad externa como una copia de seguridad.
- La unidad externa donde contiene la información solo le puede tener el Gerente de la Municipalidad.
- Se debe realizar una recuperación de la información por lo menos 3 veces al año.

Figura 17: Manual de Políticas de Seguridad de la Información basado en la norma ISO 27001

Fuente: Elaboración propia.

Anexos 4: *Constancia de revisión lingüística.*

"Año del Diálogo y la Reconciliación Nacional"

CONSTANCIA DE REVISIÓN LINGÜÍSTICA DE LA TESIS DE PREGRADO

El que suscribe, Mg. Alberto Corimayhua Condori – docente de Capacidades Comunicativas de la Universidad Peruana Unión, Filial Tarapoto,

HACE CONSTAR QUE:

El proyecto de la tesis titulada: **"Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida-Bongará-Amazonas"**, correspondiente al alumno: **Henry Percy Cabrera Cubas, con código 201220471;** ha pasado satisfactoriamente la revisión lingüística del contenido de la tesis.

Se expide la presente, para fines pertinentes.

Morales, 30 de octubre de 2018

Mg. Alberto Corimayhua Condori
DOCENTE DEL ÁREA DE COMUNICACIONES

Figura 18: Constancia de revisión lingüística

Fuente: Elaboración propia

Anexos 5: Constancia de traducción

"Año del Diálogo y la Reconciliación Nacional"

CONSTANCIA DE TRADUCCIÓN

El que suscribe, Director del Centro de Idiomas de la Universidad Peruana Unión – Filial Tarapoto,

HACE CONSTAR QUE;

Realizó la traducción de español a inglés del resumen de tesis titulada: Diseño de un modelo de políticas basado en la norma ISO 27001, para mejorar la gestión de la seguridad de la información en la Municipalidad Distrital de Florida – Bongará – Amazonas, correspondiente al alumno:

Henry Percy Cabrera Cubas, con código 201220471

Se expide la presente, para fines pertinentes.

Morales, 30 de octubre de 2018

Lic. Freddy Chávez Moleros
Director de Centro de Idiomas

Figura 19 Constancia de traducción.

Fuente: Elaboración propia