UNIVERSIDAD NACIONAL

SANTIAGO ANTÚNEZ DE MAYOLO

FACULTAD DE CIENCIAS

ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

"DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MINIMIZAR RIESGOS EN LOS ACTIVOS DE INFORMACIÓN EN LA SUB GERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA 2016"

TESIS

PARA OPTAR EL TÍTULO DE
INGENIERO DE SISTEMAS E INFORMÁTICA

AUTORES

Bach. Angelica Madeleine ARMAS HUAMÁN

Bach. Flor Rosmery PEREZ ROMERO

ASESOR

Ing. Alberto Martin MEDINA VILLACORTA

HUARAZ – PERU

2018

DEDICATORIA

A Dios, *por haberme dado la vida, las fuerzas necesarias para seguir adelante y permitirme llegar a este momento tan importante de mi carrera profesional.*

A mis padres, *por demostrarme siempre su cariño, su apoyo incondicional, sus consejos siempre sabios, su comprensión, su ayuda en los momentos difíciles y por ser un pilar importante en nuestra familia, que me han dado todo lo que soy como persona para conseguir mis objetivos y metas planteadas.*

A mis hermanos*, por compartir momentos significativos conmigo y siempre estar dispuestos a escucharme y apoyarme en cualquier momento.*

Al asesor de Tesis y a nuestro docente guía *porque hasta el final de este proyecto nos apoyaron en el desarrollo de la misma, brindándonos los consejos necesarios para su realización.*

Finalmente, a los docentes, *que nos inculcaron los conocimientos, los cuales permitieron el desarrollo del presente proyecto*

.

Angelica Madeleine ARMAS HUAMÁN

DEDICATORIA

A Dios, *por darme la oportunidad de llegar hasta este punto y por haberme dado salud para poder lograr mis objetivos, por la fuerza y la fe para culminar este proyecto importante en mi vida, además de su infinita bondad y amor.*

A mis padres, *por ser el pilar fundamental en todo, por la paciencia, confianza, apoyo incondicional y por demostrarme cada día que la vida está llena de retos y que no hay mejor satisfacción en el mundo que poder cumplirlos con el apoyo de la familia. A mis hermanas, por su amor y por impulsarme cada día las ganas de ser mejor como persona y como profesional.*

Al asesor de Tesis y a nuestro docente guía *porque hasta el final de este proyecto nos ayudaron a ser minucioso en cada detalle, así como también en la vida profesional.*

Finalmente, a los docentes, *que son la fuente de conocimientos, los cuales marcaron cada etapa en la vida universitaria, quienes nos ayudaron en asesorías y dudas presentadas en la elaboración de este proyecto.*

Flor Rosmery PEREZ ROMERO

AGRADECIMIENTOS

En primer lugar, a Dios, que nos ofrece día a día el privilegio de vivir, disfrutar de las cosas sencillas de ella y aprovechar nuevas oportunidades que se nos presente a lo largo del camino.

A nuestros padres, que siempre nos han dado su apoyo incondicional y su amor, a quienes le debemos la vida, por todo su trabajo, empeño y dedicación para brindarnos una formación académica, humanista y sobre todo espiritual; y a nuestros hermanos por demostrarme que siempre hay tiempo para cumplir las tareas y metas de la vida. A ellos les debemos todo nuestro agradecimiento.

A nuestra alma mater, UNIVERSIDAD NACIONAL SANTIAGO ANTÚNEZ DE MAYOLO, por ser quien nos acogió y nos dio la oportunidad de seguir nuestra formación académica y profesional.

Al asesor de tesis, Ing. Alberto Medina Villacorta, por su esfuerzo, empeño, dedicación e impulso brindado, pues hasta el final confió en que esta tesis sería un proyecto por el que valdría la pena esperar y apostar, así como también el tiempo y paciencia dedicados para elaborar un excelente trabajo.

PRESENTACIÓN

Señores miembros del Jurado:

Cumpliendo con las disposiciones del Reglamento de Grados y Títulos de la Escuela Profesional de Ingeniería de Sistemas e Informática, de la Facultad de Ciencias de la Universidad Nacional Santiago Antúnez de Mayolo, presentamos ante su ilustrado criterio la tesis, que lleva por título "DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MINIMIZAR RIESGOS EN LOS ACTIVOS DE INFORMACIÓN EN LA SUB GERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA 2016".

La Sub Gerencia de Informática y Telecomunicaciones es uno de los órganos de apoyo que cumple un papel importante en la Municipalidad Distrital de Independencia, ya que esta área tiene bajo su control el archivo, mantenimiento y almacenamiento de equipos e información en general, luego de realizar la investigación se pudo apreciar que la información que se maneja está expuesta a riesgos y amenazas. Es aquí donde empezamos a hablar de seguridad de la información, ya que ésta nos ayuda a resguardar y proteger la información manteniendo su confidencialidad, disponibilidad e integridad de la misma, todos estos criterios son importantes porque nos ayudaran a identificar los controles que se deben aplicar. Por otro lado, esta área tiene implicancia en algunos procesos de las demás gerencias de la Municipalidad Distrital de Independencia, es por ello por lo que optamos por elegir el Área de Registro Civil para realizar un estudio piloto respecto a los procesos en el que está implicado la Sub Gerencia de Informática y Telecomunicaciones. Además, siendo este requisito obligatorio para obtener el Título Profesional de Ingeniero de Sistemas e Informática.

Las autoras

MIEMBROS DEL JURADO

Ing. Cesar Augusto NARRO CACHAY
Reg. CIP N° 169491
PRESIDENTE

Ing. Erick Giovanny FLORES CHACÓN
Reg. CIP N° 89540
SECRETARIO

Ing. Alberto Martin MEDINA VILLACORTA
Reg. C.I.P. N° 143211
VOCAL

RESUMEN

El presente proyecto tiene como producto final el Desarrollo de un Sistema de Gestión de Seguridad de la Información para la Sub Gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia, el que se describe en el Documento de aplicabilidad que al ser ejecutado tendrá como resultado un adecuado aseguramiento de la información, manteniéndolo al margen o fuera de riesgo los activos de información.

En este caso además de realizar el estudio en la Subgerencia de Informática y Telecomunicaciones realizaremos un estudio piloto en el Área de Registro Civil ya que es uno de los procesos más vulnerables y expuesto, de esta manera también se espera llegar a las otras dependencias y crear una cultura organizacional que involucre a la seguridad de la información.

Para este desarrollo el Sistema de Gestión de Seguridad de la Información, se usó normas de la familia ISO/IEC 27000 y a su vez en la metodología MAGERIT, todo ello con el fin de poder identificar y mitigar los riesgos y amenazas a los que están expuestas la información, con las cuales se obtuvo como resultado la Declaración de aplicabilidad.

Palabras Claves: MAGERIT**,** ISO/IEC 27000, Minimizar Riesgos, Activo, Gestión de Seguridad, Documento de aplicabilidad.

ABSTRACT

The present project has as final product the Development of an Information Security Management System for the Information Technology and Telecommunications Sub-Department of the District Municipality of Independencia, which is described in the Applicability Document that, when executed, will perform an adequate assurance of the information keeping it on the margin or out of risk information assets.

In this case, in addition to carrying out the study in the Information Technology and Telecommunications Division, we will conduct a pilot study in the Civil Registry Area since it is one of the most vulnerable and exposed processes, in this way it is also expected to reach the other dependencies and create an organizational culture that involves information security.

For this development the Information Security Management System, ISO / IEC 27000 family standards were used, as well as the MAGERIT methodology, all with the purpose of identifying and mitigating the risks and threats to which they are exposed. the information, with which the Declaration of applicability was obtained as a result.

Key Words: MAGERIT, ISO / IEC 27000, Minimize Risks, Active, Security Management, Applicability Document.

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

CAPÍTULO I

GENERALIDADES

1.1. REALIDAD PROBLEMÁTICA

Luego de realizar la investigación del proyecto y la problemática que engloba, dividimos los problemas que encontramos en los siguientes indicadores:

Agrupación por tipo de problema:

1.1.1. **Tecnología:** Desfase tecnológico

TABLA N° 1.1: PROBLEMA DE TECNOLOGÍA

N°	Problema	Tipo de Problema
1	Las áreas involucradas sienten preocupación en los cambios tecnológicos y los riesgos en tecnologías de información (TI).	Tecnología
2	No realiza un adecuado control en cuanto al hardware y el software de los equipos.	Tecnología

Fuente: *Elaboración Propia*

1.1.2. **Normativa:** No aplicación y uso de normativas

TABLA N° 1.2: PROBLEMA DE NORMATIVA

N°	Problema	Tipo de Problema
3	La aplicación de Sistemas de Gestión de Seguridad de la Información es limitada y se refleja en planes de seguridad básicos, generalmente realizado por similitud con otras entidades y no es específica al entorno real.	Normativa
4	No realizan la aplicación de normativas o estándares de seguridad sobre los activos de información.	Normativa

N°	Problema	Tipo de Problema
5	La investigación también muestra que hay una preocupación de los usuarios hacia los riesgos o pérdidas de información, ya que hoy en día no necesariamente siguen una normativa.	Normativa

Fuente: *Elaboración Propia*

1.1.3. **<u>Conocimiento:</u>** Falta de conocimiento del tema

TABLA N° 1.3: PROBLEMA DE CONOCIMIENTO

N°	Problema	Tipo de Problema
6	El personal que labora en las áreas de estudio no tiene conocimiento sobre el tema de seguridad de la información.	Conocimiento
7	La Gestión de la Seguridad de la Información constituye un tema fundamental, el cual recién está siendo implantado en el medio profesional y las entidades públicas de manera obligatoria.	Conocimiento
8	Los Sistemas de Gestión de Seguridad abarcan un conjunto alto de tratamiento de riesgos como por ejemplo personal poco fiable, falta de experiencia en la gestión, problemas de personal, problemas con la tecnología, cambio de normativas del gobierno.	Conocimiento
9	Se puede apreciar que los trabajadores de las áreas involucradas no tienen el conocimiento adecuado de las herramientas cuantitativas (MAGERIT) de gestión de riesgos, y se apoyan, generalmente, en las herramientas cualitativas (Juicio de expertos).	Conocimiento
10	Se debe puntualizar correctamente cada riesgo, lo cual ayudará a entender mejor el riesgo y nos permitirá identificar el control más adecuada para el tratamiento del riesgo.	Conocimiento

Fuente: *Elaboración Propia*

Con lo mencionado anteriormente vemos que hoy en día los sistemas de información que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de organizaciones de diferentes rubros y la información se ha convertido en un activo que al igual que otros activos importantes de las entidades públicas representa un valor significativo. De esta forma se tiene que existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes entidades en las que trabajan.

Adicionalmente a este riesgo interno, siempre se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante algún mecanismo de ataque. Independientemente de la forma que tome la información o el medio por el que se distribuya, debe protegerse. [ISO 27002]

Si bien es cierto la Municipalidad Distrital de Independencia y específicamente la Sub Gerencia de Informática y Telecomunicaciones, no se encuentran ajenos a lo descrito anteriormente, ya que en la actualidad esta no cuenta con ningún sistema de gestión de seguridad y mucho menos iniciativas de planes de desarrollo de estas, a pesar de que hoy en día se cuenta con una serie de normas estándar internacionales, publicadas por la Organización Internacional de Normalización (ISO), en el Perú se han definido leyes alineadas a éstos para que puedan ser aplicadas al contexto de las entidades existentes en el país en cuanto a la gestión de la información utilizada por las entidades públicas. Es así que en el marco de la NTP ISO/IEC 27001:2014 con la RM-129-2012-PCM que aprueban el uso obligatorio de la Norma en todas las entidades integrantes del Sistema Nacional de Informática, NTP ISO/IEC 17799:2007 y la RM-129-2012-PCM la que define el código de buenas prácticas de la seguridad de la información en ciertas entidades del estado peruano1. Teniendo dichas instituciones que realizar las diferentes fases detalladas en el plan de implementación Incremental publicada por la Oficina Nacional de Gobierno Electrónico e Informática (ONGEI).

1 Perú Gobierno Digital, RESOLUCION MINISTERIAL 129-2012-PCM, Seguridad de la Información, http://www.ongei.gob.pe/entidad/ongei_tematicos.asp?cod_tema=4552 (Consultada el 15 de febrero de 2016).

Es por ello que las entidades públicas tienen la necesidad de contar con un análisis que les permita realizar el diseño de un SGSI, en conjunto con los controles correspondientes al mismo como respuesta a la exigencia legal establecida por las normas previamente mencionadas, lo cual en conjunto constituyen la problemática que el proyecto, pretende resolver siguiendo las buenas prácticas y estándares internacionales correspondientes que permitan realizar una identificación de la información crítica con la que trabaja la entidad y en consecuencia definir los riesgos a los que se encuentra expuesta y los controles que deberían implementarse para garantizar su seguridad.

Esta es una breve descripción de la realidad problemática que atraviesa actualmente la Sub Gerencia de Informática y Telecomunicaciones, vemos que presenta dificultades en el manejo de información y la seguridad de la misma, estos problemas deben de tener un tratamiento de manera rápida.

Para hacer esto posible, la Municipalidad Distrital de Independencia debe de tomar en consideración la importancia de la seguridad de la información y los riesgos a los cuales están expuestos, con el objetivo de impulsar de una manera conjunta y coherente los diferentes elementos que ayudarán a su crecimiento y desarrollo institucional y tecnológico, de esta manera dar un tratamiento adecuado a los riesgos de información presentes en los procesos más importantes de la institución pública.

1.2. ENUNCIADO DEL PROBLEMA

¿De qué manera el desarrollo de un Sistema de Gestión de Seguridad de la Información minimizara los riesgos en los activos de información[2] de la Sub Gerencia de Informática y Telecomunicaciones?

1.3. HIPÓTESIS

El desarrollo de un sistema de seguridad de la información implementa controles de seguridad que minimizan los riesgos en los activos de información de la Municipalidad Distrital de Independencia Huaraz.

1.4. OBJETIVOS

1.4.1. OBJETIVO GENERAL:

Desarrollar un sistema de gestión de seguridad de la información, para minimizar riesgos en los activos de información de la Sub Gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia.

1.4.2. OBJETIVOS ESPECÍFICOS:

1) Diagnosticar la situación actual y elaborar la documentación requerida por las normas adoptadas para el SGSI.
2) Elaborar la matriz de amenazas y vulnerabilidades de los procesos del alcance.
3) Identificar y realizar la valorización de los activos de información de los procesos de negocio que conforman el alcance.

[2] Entiéndase por activos de información: los activos de información incluyen la información estructurada y no estructurada que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo, incluyendo datos contenidos en registros, archivos y bases de datos, https://www.finagro.com.co/qui%C3%A9nes-somos/sig (Consultada el 15 de febrero de 2016).

4) Identificar, analizar y evaluar los riesgos a los cuales están expuestos los activos identificados en el punto anterior.
5) Seleccionar sistemas de control para el tratamiento de los riesgos identificados y así establecer políticas de seguridad.
6) Diseñar la declaración de aplicabilidad que permita implementar estrategias de mitigación de los riesgos identificados.
7) Elaborar la documentación requerida por las normas adoptadas para el SGSI

1.5. JUSTIFICACIÓN

Se realizó el Desarrollo y propuesta de mejora para la gestión de riesgos basado en la ISO/IEC 27001:2013 para la Subgerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia y a su vez se propuso mejoras en base a los lineamientos de las buenas prácticas, cuyos beneficios se verán reflejados en la calidad de la información y en la seguridad para su manipulación. Esto beneficia a la comunidad de colaboradores, ya que tienen la certeza de que la información se encuentra segura y libre de riesgos informáticos. Cabe recalcar que el proyecto es viable y de gran utilidad no sólo para la Subgerencia de Informática y Telecomunicaciones, sino también para la Municipalidad Distrital de Independencia.

1.5.1. JUSTIFICACIÓN OPERATIVA

La Subgerencia de Informática y Telecomunicaciones es la unidad que se encarga de brindar los servicios a toda la Municipalidad siendo ellos los encargados del manejo de la información y mantenimiento de los recursos (activos) de los colaboradores, ya que es aquí donde se administra la información y se vela por el correcto funcionamiento de los

sistemas. Este ente cuenta con el personal calificado, el cual fácilmente puede ser capacitado para garantizar el cumplimiento de los lineamientos que se establezcan en cuanto a la seguridad informática, no presentando mayores inconvenientes si se hace de manera oportuna.

1.5.2. JUSTIFICACIÓN TECNOLÓGICA

Tecnológicamente el presente proyecto es factible puesto que con el pasar de los años han ido mejorando los equipos necesarios para el proyecto y además se cuenta con dichos recursos, ya que además contamos con el conocimiento de la protección de la información ya sea en formato digital o físico. El correcto uso de la TI nos permite brindar una mejor seguridad a los usuarios, permitiendo que la información llegue de manera oportuna y segura.

Pero aun así hay deficiencias pendientes a corregir y mejorar, lo cual a futuro traerá beneficios para la institución.

1.5.3. JUSTIFICACIÓN ECONÓMICA

El presente proyecto es económicamente viable porque llega hasta la fase de desarrollo, obteniendo al final una propuesta (Declaración de Aplicabilidad) que dependerá de las autoridades la aplicación y puesta en marcha del misma.

1.5.4. JUSTIFICACIÓN SOCIAL

Se justifica socialmente ya que dentro del desarrollo de un Sistema de Gestión de la Seguridad de la Información; la identificación, el análisis y tratamiento de riesgos es uno de los temas centrales y críticos, por lo tanto, buscamos concientizar a la población profesional que laborar en la Municipalidad Distrital de Independencia acerca de tecnologías de la información de la importancia de tener un SGSI para poder Identificar, analizar y

evaluar los riesgos a los cuales están expuestos los activos identificados, por lo tanto puedan brindar un servicio eficiente a la población, y que la población se sienta segura y satisfecha al momento de realizar cualquier tipo de trámite.

1.5.5. JUSTIFICACIÓN NORMATIVA

El presente proyecto tiene su justificación legal en la ISO/IEC 27001, un estándar para la seguridad de la información, para que sean seleccionadas por las organizaciones en el desarrollo de sus SGSI. Este fue aprobado y publicado como estándar internacional en octubre de 2005 por International ISO (*"Organization for Standardization")* y por la comisión IEC (*"International Electrotechnical Commission")*. Que, mediante Resolución Ministerial Nº 246-2007-PCM se aprobó el uso de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI".

Posteriormente, mediante Resolución Ministerial Nº 129-2012-PCM se estableció un nuevo cronograma y la incorporación del rol del oficial de seguridad para el proceso de implementación de la Norma Técnica Peruana "NTP-ISO /IEC 27001:2008", además teniendo en cuenta la Resolución Ministerial N° 004-2016-PCM, donde aprueban el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014, en todas las entidades integrantes del Sistema Nacional de Informática.

Por otra parte, para optar el título de Ingeniero de Sistemas, en la Universidad Nacional Santiago Antúnez de Mayolo en la modalidad de Tesis es necesario para las tesistas presentar, sustentar y aprobar la Tesis de investigación en Ingeniería de Sistemas e Informática ante un jurado. Esto está normado bajo el Reglamento de Grados y Títulos de la escuela de Ingeniería

de Sistemas e Informática, aprobado bajo Resolución N.º 091-2011-UNASAM-FC/D del 01 de Agosto del 2011.

1.6. LIMITACIONES Y ALCANCE

1.6.1. LIMITACIONES

Las limitaciones que presenta la tesis se detallan a continuación:

- La presente tesis consiste en el diagnóstico, análisis, diseño y desarrollo del Sistema de Gestión de Seguridad de la Información para la Sub Gerencia de Informática y Telecomunicaciones, basado en la norma ISO/IEC 27001:2013, pero no abarca las fases de implementación, revisión y mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información.
- No se aplicó la propuesta de declaración de aplicabilidad ya que es decisión de la alta gerencia poner en marcha y la disposición de este.
- La presente tesis plantea algunos controles, que serán indispensables para proteger los activos de información más importantes de la Sub Gerencia de Informática y Telecomunicaciones, pero si cambia alguna regulación a nivel nacional e incluso internacional, la cual le exija a la oficina muchos controles extras, la propuesta que se plantea no podrá abarcar esa necesidad contractual.

1.6.2. ALCANCE

- Está orientado a cubrir la primera fase de la implementación de un Sistema de Gestión de Seguridad de la Información, que corresponde a la etapa de planeación.
- El alcance de la tesis abarca solo la Sub Gerencia de Informática y Telecomunicaciones, por lo tanto, el proceso de clasificación de activos de información y valoración de

riesgos solo se realizará para la Sub Gerencia y al enfoque piloto de Registro Civil.

- Dentro del desarrollo del Sistema de Gestión de Seguridad de la información para la Subgerencia de Informática y Telecomunicaciones, se realizará un estudio piloto en los procesos involucrados en el Área de Registro Civil el cual puede ser adaptado a las demás áreas, con la que se podrá crear una cultura organizacional que involucre a la seguridad de la información como punto clave.

1.7. DESCRIPCIÓN Y SUSTENTACIÓN DE LA SOLUCIÓN

El desarrollo del Sistema de Gestión de Seguridad de la Información (SGSI) se orientó a gestionar los riesgos en cuanto a seguridad de la información se refiere para la Sub Gerencia de Informática y Telecomunicaciones, llevando a cabo un diagnóstico previo de su situación actual. Todo ello será posible ya que se proporcionará la información necesaria por parte de los encargados del manejo de la información, conociendo cada uno de sus procesos y actividades verificaremos en qué nivel de seguridad se encuentra esta área. Del mismo modo a continuación se presenta en la Tabla N°1-4 especificando la metodología a utilizar, las características técnicas de los resultados esperados:

TABLA N° 1.4: DESCRIPCIÓN DE LA SOLUCIÓN

ETAPA	ACCIONES		RESULTADOS	
	SGSI	PROYECTO	Entregable	Herramientas
PLANEAR	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.	Definir el problema a resolver, la forma en que se buscara resolverlo, definir el objetivo general y objetivos específicos, definir el alcance y las limitaciones que tendrá el proyecto de tesis, realizar la planificación temporal del proyecto y elegir los métodos y procedimientos que se emplearan.	Manual de seguridad	Norma ISO 27001 Business Process Management (BPM 2.0)
HACER	Implementar y operar la política, controles, procesos y procedimientos SGSI.	Desarrollo del proyecto, documentar y controlar las acciones realizadas, levantar información, implementación del SGSI para el tipo de empresa seleccionada, etc.	Procedimientos (declaración de aplicabilidad)	Norma ISO 31000
CHEQUEAR	Valorar donde sea aplicable y medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.	Después del desarrollado e implementado el SGSI, volver a revisar los datos obtenidos y analizarlos, comparándolos con los objetivos específicos iniciales, para evaluar si se han obtenido los resultados esperados.	Instrucciones Checklists Formularios	Norma ISO 27002
ACTUAR	Realizar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.	Modificar y corregir algunos aspectos errados encontrados en la etapa anterior, con el fin de garantizar que se obtengan los resultados esperados del proyecto, aplicar mejoras y terminar de documentar todo el proyecto.	Registros	Norma ISO 27799

Fuente: *Elaboración Propia*

Como el presente proyecto de fin de carrera solo abarca el análisis y diseño del SGSI, solo se tomó en cuenta las etapas de “Planear” y “Hacer” (Plan – Do) de la metodología, para las otras dos fases se estableció solo pautas a seguir, como base el proyecto.

CAPÍTULO II
MARCO TEÓRICO.

2.1. ANTECEDENTES

Luego de la extensa recopilación de datos de diferentes estudios ya sean internacionales, naciones y locales tomamos como referencia lo siguiente:

2.1.1. ANTECEDENTE LOCAL

Mory, (2014) en su tesis *"Diagnóstico y Diseño de un Sistema de Gestión de Seguridad de Información aplicado a la empresa HM Contratistas S.A."* El tesista tiene como objetivo principal Diseñar un Sistema de Gestión de Seguridad de Información (SGSI) siguiendo las normas internacionales ISO/IEC 27001:2005 e ISO/IEC 27002:2005 en la empresa HM CONTRATISTAS S.A. de la ciudad de Huaraz, ya que a partir de su realidad problemática tiene el fin de proteger sus activos de información ante las amenazas a las cuales están expuestos, cumpliendo con los objetivos especificos de dicho proyecto. A partir de lo expuesto previamente, el autor en el presente proyecto realizo el diseño un Sistema de Gestión de Seguridad de Información (SGSI) según el estándar internacional ISO/IEC 27001:2005 en dicha constructora así de esta manera dando y/o exponiendo los controles adecuados para proteger sus activos de información ante las amenazas a las cuales están expuestos, dándole un tratamiento adecuado a los riesgos de información presentes en los procesos más importantes de la empresa.

Este proyecto de tesis aporta al nuestro en la manera de identificar y evaluar los riesgos apoyándonos en la familia de la norma ISO 27000 lo cual nos permitirá, a la institución, gestionar la seguridad de la información que maneja, de manera que se pueda cumplir con la preservación de la confidencialidad, integridad y disponibilidad de la información.

2.1.2. ANTECEDENTES NACIONALES

Talavera Álvarez (2015) en su trabajo de fin de carrera desarrolla el "*Análisis y Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud*" – el Instituto Nacional Materno Perinatal – en la cual el tesista tiene como objetivo pincipal del proyecto el de *"Diseñar un sistema de gestión de seguridad de la información para una institución estatal de salud, de acuerdo a la norma ISO/IEC 27001:2013",* obteniendo como resultado el diseño desarrollado en el presente documento en la cual presenta la aplicación de estándares aplicados a un entorno de una institución del sector salud específica, sin embargo esto no limita su replicación en otras entidades públicas que brinden servicios de salud.

Para lograr esto, es necesario contar con los modelos de los procesos de negocio de la nueva institución, además se debe realizar una revisión de la metodología de riesgos desarrollada puesto que para distintas entidades la misma puede variar dependiendo de su apetito por el riesgo, así como la forma en que perciben los riesgos existentes.

Este proyecto apoya al nuestro ya que nos da las pautas que se debe ajustar en el análisis de riesgos aplicándolo a la realidad de la institución, de modo que se pueda desarrollar una lista de

controles debidamente adecuada a la nueva entidad, realizando un análisis actual y rediseño de la red institucional, que se enfoque a mejorar los aspectos de seguridad informática así como la implementación de algunos de los controles definidos en la Declaración de Aplicabilidad del mismo modo este nos debe facilitar la digitalización y manejo de la información contenida en la Municipalidad Distrital de Independencia.

Camacho y Ramos (2010), en su tesis "Metodología táctica para la implantación de sistemas de información basado en métrica y COBIT", Universidad Nacional Mayor de San Marcos – Lima - Perú, los tesistas lograron el siguiente objetivo: Elaborar una metodología a nivel táctico, orientada a satisfacer las necesidades gerenciales y/o de jefe de proyectos a fin de implementar sistemas de información. Tipo: Descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: El proceso de puesta en marcha de un sistema de información será realizado con mayor fluidez y ordenamiento. Con el previo análisis de las metodologías existentes, se ha logrado obtener un producto capaz de mantener estándares de auditoria. La simplicidad que refleja permitirá realizar el proceso de toma de decisiones gerenciales de una manera eficaz y eficiente. En base a este proyecto nos apoyaremos en el uso adecuado de las metodologías para el desarrollo del presente, la cual nos permita tener un control de los estándares aplicados y usados para así llevarlos a cabo en la Municipalidad Distrital de Independencia exponiendo este plan para la toma de decisiones de la alta gerencia.

Villena M. (2011), en su tesis "Sistema de Gestión de Seguridad de Información para una institución financiera", Pontificia Universidad Católica del Perú – Lima – Perú, el tesista logra el siguiente objetivo: establecer los principales lineamientos para poder implementar de manera exitosa, un adecuado modelo de sistema de gestión de seguridad de información (SGSI) en una institución financiera en el Perú. Tipo: aplicado. Nivel: experimental. Diseño: aplicativo. Conclusión: Para implantar una adecuada gestión de seguridad de información en una institución financiera, el primer paso es obtener el apoyo y soporte de la alta gerencia, haciéndolos participes activos de lo que significa mantener adecuadamente protegida la información de la institución financiera.

Nos apoyamos en este proyecto para realizar la parte logística del proyecto como es el de realizar la entrevista personal a los trabajadores de dicha área, para así tener acceso a los activos de la institución y de esta manera haciéndolos participes del proyecto a realizar.

Este proyecto nos brinda las pautas a seguir para realizar una adecuada gestión de la seguridad de la información, basándola en nuestra institución ya que en este caso estamos hablando de una institución estatal en la cual vamos a hacer partícipes a los colaboradores para que nos permitan el acceso a los activos.

Ampuero (2011), en su tesis "Diseño de un sistema de gestión de seguridad de información para una compañía de seguros", Pontificia Universidad Católica del Perú – Lima – Perú, logra el siguiente objetivo: utilizar estándares y buenas prácticas reconocidos mundialmente para poder desarrollar cada una de las etapas del diseño del Sistema de Gestión de

Seguridad de Información (SGSI) y así poder tener una base que se pueda implementar en cualquier compañía de seguros. Tipo: aplicado. Nivel: experimental. Diseño: aplicado. Conclusión: En la actualidad, con el desarrollo de la tecnología, la información ha tomado mayor fuerza en las empresas, convirtiéndose en la mayoría de los casos en el activo más importante que tienen. Es por esta razón que tienen la obligación de proteger aquella información que es importante para ellas y que tiene relación ya sea con el negocio o con los clientes.
Este proyecto nos brinda el conocimiento de cómo realizar el diseño y gestión de la seguridad de la información ya que es muy importante su aplicación y/o desarrollo en las instituciones tanto publicas y privadas.

Espinoza (2013), en su tesis "Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo", Pontificia Universidad Católica del Perú – Lima – Perú, logra el siguiente objetivo: tomar en cuenta los aspectos más importantes de la norma ISO/IEC 27001:2005, a partir de los cuales se buscará poder desarrollar cada una de las etapas del diseño de un sistema de gestión de seguridad de información. Tipo: aplicado. Nivel: experimental. Diseño: aplicado. Conclusión: En los últimos 20 años la información se ha convertido en un activo muy importante y crucial dentro de las organizaciones, es por ello que tiene la necesidad de protegerla si es que la información tiene relación ya sea con el negocio o con sus clientes.

De la tesis mencionada tomaremos los conocimientos aplicados en la misma para apoyarnos de las definiciones y la teoría de la

norma ISO 27001:2005, en la cual se mencionan como desarrollar paso a paso el sistema de gestión de seguridad de la información ya que, si bien se menciona en el mismo, los activos se han convertido en el ente más importante de cada institución.

2.1.3. ANTECEDENTES INTERNACIONALES

Ferrero (2009), en su proyecto de fin de carrera *"Análisis y Gestión de Riesgos del Servicio Imat del Sistema de Información de I.C.A.I",* Universidad Pontificia Comillas – Madrid – España, el tesista logró el siguiente objetivo: Realizar la definición concreta del sistema y el alcance que este posee, la importancia que tiene para la organización para plantear los objetivos y estrategias que se van a adoptar para la seguridad del sistema de TI. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: la importancia de este proyecto radica en la posibilidad de ver que un sistema de información no se queda en la superficie del código o el diseño de hardware o las comunicaciones; hay toda una estructura detrás que ha de funcionar para que el sistema no sufra una amenaza frente a la cual no está preparado.

El presente proyecta aporta al nuestro de la manera siguiente ya que radica en la posibilidad de implementar un sistema de seguridad de la información teniendo en cuenta la preservación de los activos ya que las protegeremos de las amenazas posible o ya existentes.

Ramírez (2014), en su trabajo final de Master *"Actualización del Sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001:2013"*, UNIVERSITAT OBERTA DE CATALUNYA (UOC de Barcelona España. El presente trabajo considera la reciente actualización de la norma

ISO/IEC 27001 de su versión 2005 a su versión 2013, y la presencia de diferencias relevantes entre las dos versiones, así como los requerimientos de actualización a la nueva versión que tendrán que afrontar las organizaciones certificadas en la antigua versión contando como plazo máximo para esto hasta Septiembre de 2015; el presente proyecto aborda realizar la transición del sistema de gestión de seguridad de la información de una empresa dedicada al transporte de energía basado en ISO/IEC 27001:2005 (No certificado) al nuevo estándar ISO/IEC 27001:2013. Para abordar el proyecto se realizó las siguientes fases:

Fase 1 Situación actual: Contextualización, objetivos y análisis diferencial

Fase 2 Sistema de Gestión Documental

Fase 3 Análisis de riesgos

Fase 4 Propuesta de Proyectos

Fase 5 Auditoría de Cumplimiento de la ISO/IEC 27002:2013

Tomando base el siguiente proyecto nos servirá como referencia para cada etapa o fase del desarrollo del mismo ya que el tesista en este trabajo nos da las fases a desarrollar para realizar un SGSI. Ya que este es de mucho aporte para llevar acabo el nuestro.

Pallas (2009), en su tesis magistral *"Metodología de Implantación de un SGSI en un grupo empresarial jerárquico"*, Universidad de la República – Montevideo – Uruguay, el tesista logró el siguiente objetivo: dar lineamientos metodológicos, de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de

un SGSI según la norma ISO 27001, para una empresa perteneciente a un grupo empresarial. Tipo: aplicado. Nivel: experimental. Diseño: aplicativo. Conclusión: En referencia a la estrategia de análisis y gestión de riesgos, así como de planificación, implementación y seguimiento del SGSI, proponemos un enfoque mixto, de dirección centralizada, pero con la autonomía necesaria a nivel de cada dominio y cada empresa, fundamentalmente en la gestión de controles y en la percepción del impacto de los riesgos locales.

En base a este proyecto tomaremos y haremos uso de la norma ISO 27001, la cual nos ayudara a realizar el análisis y gestión de los riesgos de los activos con lo que cuenta la institución, ya que también nos brinda un enfoque mixto para optimizar los controles.

Duque (2010), en su estudio *"Metodologías de Gestión de Riesgos (Octave, MAGERIT, DAFP)"*, Universidad de Caldas – Caldas – Colombia, la tesista logró el siguiente objetivo: dar a conocer algunas metodologías existentes en cuanto a la Gestión de Riesgos. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: En toda organización se requiere la creación de una "cultura de seguridad" que, emanando de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia. Son dos los pilares fundamentales para la creación de esta cultura: una política de seguridad corporativa y una formación continua, a todos los niveles.

Nos apoyamos en este estudio para crear una cultura de seguridad entro de la institución y de esta manera haciendo el reconocimiento de las metodologías existentes en cuanto a la gestión y valorización de los riesgos y su minimización.

Álvarez (2010), en su tesis magistral de *"Seguridad en informática (Auditoría de Sistemas)"*, Universidad Iberoamericana – México D.F – México, el tesista logró el siguiente objetivo: Proponer lineamientos que se deben tomar en cuenta en cuanto a la seguridad informática, así como también ver la importancia de realizar auditoría de sistemas en las organizaciones. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades.

Como bien se menciona en la teoría nuestro proyecto realizara el uso de las normas ISO 27000 y en base al proyecto indicado tomaremos los lineamientos que debemos tener en cuenta para realizar la seguridad informática de los activos ya que es de vital importancia para la institución.

Martínez (2010), en su tesis magistral *"Concienciación en Seguridad de la Información, la estrategia para fortalecer el eslabón más débil de la cadena",* Fundación Universitaria Iberoamericana – Cartagena de Indias – Colombia, el tesista logró el siguiente objetivo: proponer una solución a los problemas de seguridad de la información de una compañía, con la implantación de un programa de concienciación y sensibilización en Seguridad que incorpore buenas prácticas para que los usuarios en sus actividades diarias. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: La seguridad de la Información es para muchas organizaciones la asignatura pendiente, porque consideran prioritario invertir en

estrategias de mercadeo y ventas, o quien sabe en qué. El hecho, es que la Seguridad de la Información es una estrategia tan necesaria como otras.

Basándonos en este proyecto planteamos los indicadores existentes en la municipalidad Distrital de independencia con el cual concientizaremos al personal que labora en el área y hacer un énfasis en el tema de seguridad ya que nos es parte estratégica de la institución y no toma ninguna prioridad en la misma.

Ripoll (2012), en su estudio *"Seguridad en los Sistemas de Información (SSI)"*, Universidad Politécnica de Valencia – Valencia – España, el tesista logró el siguiente objetivo: proporcionar apuntes y el material de apoyo de la asignatura de "Seguridad en los Sistemas Informáticos" que se imparte en la Escuela Técnica Superior de Ingeniería Informática de la Universidad Politécnica de Valencia. Tipo: descriptivo. Nivel: descriptivo. Diseño: descriptivo. Conclusión: estos apuntes se han elaborado con la intención de servir de apoyo a la impartición de las clases. Puede que algunos temas o conceptos no se expliquen con la extensión y detalle necesarios; siendo necesario consultar otras fuentes para completar la formación.

El presente estudio nos sirve de apoyo para unificar nuestras ideas respecto al sistema de gestión de seguridad de la información aportando de esta manera con conceptos y definiciones claras y precisas, ya que se muestran detalladamente.

2.2. TEORÍAS QUE SUSTENTAN EL TRABAJO

2.2.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Este concepto, también nombrado SGSI, o ISMS ("*Information Security Management System*") nace como respuesta a la necesidad de las empresas de proteger la información que es crítica para sus operaciones, tanto del acceso por personas no autorizadas como de daños producidos por las consecuencias de la materialización de los riesgos a los cuales esta se encuentra expuesta. Se encuentra muy relacionado con el plan de continuidad de negocios que se encarga de definir las acciones a seguir en caso un evento produzca una interrupción en las operaciones normales de la compañía.

A grandes rasgos el SGSI contiene la identificación de los activos de información que deban ser protegidos, el motivo por el que se deban proteger – es decir, la criticidad que éstos representan para la organización – los riesgos y amenazas ante los que se encuentran expuestos y los controles que se apliquen para asegurar la preservación de dichos activos. Al ser de vital importancia para las operaciones de la organización, se define también como "la parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información" (ALEXANDER, 2007).

Al requerir una identificación de los objetivos que se deban proteger, así como de todas las amenazas a las cuales se encuentran expuestos, y los controles que deban implementarse, la implementación de un SGSI se realiza

utilizando los resultados que se obtengan del Análisis de Riesgos. (ALEXANDER, 2007) (ORMELLA, 2013)

i. SEGURIDAD INFORMÁTICA:

Seguridad Informática, es la disciplina que se encarga de las implementaciones técnicas de la protección de la información, el despliegue de las tecnologías antivirus, firewalls, detección de intrusos, detección de anomalías, correlación de eventos, atención de incidentes, entre otros elementos, que articulados con prácticas de gobierno de tecnología de información establecen la forma de actuar y asegurar las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo. [Jeimy J. Cano, Ph.D., CFE.]

ii. SEGURIDAD DE LA INFORMACIÓN

Se denomina así al conjunto de políticas, estándares y controles que se implementan en la organización con la finalidad de asegurar la preservación de las siguientes propiedades de la información:

- **Confidencialidad:** Protección de la información confidencial del acceso o divulgación por parte de entidades – personas jurídicas o naturales – no autorizadas al mismo, tanto por parte del originario de la información como por parte de la entidad que maneja la misma.
- **Integridad:** Protección de la información frente a la modificación o eliminación sin la autorización o accesos necesarios. De esta forma se garantiza que la información sea la correcta en todo momento.

- **Disponibilidad:** La información se encuentra accesible en todo momento, bajo demanda de todo usuario que se encuentre autorizado a poder acceder a la misma.
- **Autenticación:** Mediante esta propiedad, se permite identificar a la persona o personas que han generado la información que se está verificando, permite una validación en la autoría de la información por parte de un usuario específico.
- **No repudio:** Permite que la información sea validada a través de algún mecanismo que compruebe su integridad y contenido, declarándola como genuina.

La Seguridad de la Información es la disciplina que se encarga de garantizar la confidencialidad, integridad y disponibilidad de la información. Para alcanzar el objetivo se apoya en la Seguridad Informática (que estaría gobernada por las directrices de la Seguridad de la Información), es decir, a pesar de ser disciplinas diferentes, la una no puede "ir" sin la otra. De modo que la Seguridad de la Información será la encargada de "regular" y establecer las pautas a seguir para la protección de la información.

Pues bien, ahora que sabemos la diferencia entre seguridad informática y seguridad de la información podemos saber lo que es un Sistema de Gestión de la Seguridad de la Información. Conocemos por Sistema de Gestión de Seguridad de la Información o SGSI, a las directrices, procedimientos y controles de seguridad que se utilizan para gestionar la información.

De una manera más estricta, un Sistema de Gestión de Seguridad de la Información es aquella parte del sistema general de gestión de una organización que comprende de lo siguiente para implantar la gestión de la seguridad de la información.

- La política.
- La estructura organizativa.
- Los procedimientos.
- Los procesos y
- Los recursos necesarios.

Con un sistema de gestión de seguridad de la información nos aseguraremos de cubrir todos los aspectos de seguridad tomando medidas encaminadas a reducir paulatinamente los riesgos a los que la organización se enfrente.

Como cualquier sistema de gestión, el SGSI debe ayudar a conseguir los objetivos de la organización, no convertirse en un impedimento para ello.

Por tanto, definiremos un Sistema de Gestión de Seguridad de la información (SGSI) como la manera en la que una organización conoce los riesgos a los que está sometida su información y los gestiona mediante una sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente.

Estas propiedades son las mínimas que un SGSI debe proteger para asegurar la información de la organización. (CNB - INDECOPI, 2008) (ISACA, 2012).

iii. ACTIVO DE INFORMACIÓN

Se denomina activo a aquello que tiene algún valor para la organización y por tanto debe protegerse. De manera que un activo de información es aquel elemento que contiene o manipula información.

Activos de información son ficheros y bases de datos, contratos y acuerdos, documentación del sistema, manuales de los usuarios, material de formación, aplicaciones, software del sistema, equipos informáticos, equipo de comunicaciones, servicios informáticos y de comunicaciones, utilidades generales como por ejemplo calefacción, iluminación, energía y aire acondicionado y las personas, que son al fin y al cabo las que en última instancia generan, transmiten y destruyen información, es decir dentro de un organización se han de considerar todos los tipos de activos de información (POVEDA S.F.) (SEGURIDAD 2012).

"El activo es algo a lo que una organización directamente le asigna un Valor y, por lo tanto, la organización debe proteger"

El ISO 17799:2005 clasifica los activos de información en las categorías siguientes: [2]

- Activos de información (datos, manuales de usuario, etc.).
- Activos de software (aplicación, software de sistemas, etc.).
- Activos físicos (computadoras, medios magnéticos, etc.).

- Personal (clientes, personal).
- Imagen de la compañía y reputación.
- Servicios (comunicaciones, etc.).

iv. GESTIÓN DE RIESGO:

La gestión de riesgos implica seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible.

Un resultado del análisis de riesgos habrá sido el criterio para determinar cuáles van a ser los niveles de riesgo aceptables y, en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados.

La gestión de los riesgos tiene como objetivo reducir los riesgos que estén por encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización.

Una vez que conocemos los riesgos de la organización y decidido el tratamiento que se le va a dar para cada uno de los activos, se deben tomar acciones en consecuencia. En resumen, la Gestión de Riesgo es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo.

Los cuatro tipos de tratamiento requieren de acciones de distinta naturaleza:

- **Mitigar el riesgo.**

  Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.

- **Asumir el riesgo.**

  La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.

- **Transferir el riesgo a un tercero.**

  Como, por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

- **Eliminar el riesgo.**

  Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el

proceso o incluso el área de negocio que es la fuente del riesgo.

No caben más acciones a la hora de gestionar los riesgos para la correcta implantación de un sistema de gestión de la seguridad de la información, ya que una organización que conoce sus riesgos jamás podrá ignorarlos, puesto que, de este modo, no estaría vigilando que no se convirtiesen en riesgos que la organización no es capaz de asumir o que, por no haberlos tenido en cuenta, se materialicen y den lugar a un incidente de seguridad.

Una vez decididas las acciones a tomar, se debe realizar un nuevo análisis de riesgos, teniendo en cuenta la nueva situación considerando que los controles y medidas que se ha decidido implantar van a reducir en mayor o menor medida el riesgo que existía, ya que ese es su objetivo. El nivel de riesgo resultante de este segundo análisis es el riesgo residual. Este se define como el riesgo remanente que existe después de que se hayan tomado las medidas de seguridad apropiadas.

En una organización nunca se podrá eliminar totalmente el riesgo, siempre quedará un cierto nivel de riesgo, por lo que es importante que todos los riesgos residuales sean aceptados por la alta Dirección.

A continuación, se presentan las definiciones de algunos términos importantes que se ven en la gestión de riesgos.

- **Amenazas**

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza es todo aquello, ya sea físico o lógico que puede causar un incidente no deseado, generando daños materiales o inmateriales a la organización y a sus activos, como la perdida de información, o de su privacidad, o bien un fallo en los equipos físicos. [5]

Las amenazas conviene clasificarlas por su naturaleza, para así facilitar su ubicación. Se tienen seis tipos de amenazas: [2]

- ✓ Amenazas naturales (inundaciones, tsunamis o maremotos, tornados, huracanes, sismos, tormentas, incendios forestales).
- ✓ Amenazas a instalaciones (fuego, explosión, caída de energía, daño de agua, perdida de acceso, fallas mecánicas).
- ✓ Amenazas humanas (huelgas, epidemias, materiales peligrosos, problemas de transporte, pérdida de personal clave).
- ✓ Amenazas tecnológicas (virus, hacking, pérdida de datos, fallas de hardware, fallas de software, fallas en la red, fallas en las líneas telefónicas).
- ✓ Amenazas operacionales (crisis financieras, perdida de suplidores, fallas en equipos, aspectos regulatorios, mala publicidad).
- ✓ Amenazas sociales (motines, (motines, protestas, sabotaje, vandalismo, bombas, violencia laboral, terrorismo).

- **Vulnerabilidades**

Las vulnerabilidades son debilidades de seguridad asociadas con los activos de información de una organización. [2]

Las vulnerabilidades pueden clasificarse en las siguientes categorías:

- ✓ Seguridad de los recursos humanos (falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, empleados desmotivados). [4]
- ✓ Control de acceso (Segregación inapropiada de redes, falta de política sobre escritorio y pantalla limpia, falta de protección al equipo de comunicación móvil, política incorrecta para control de acceso, password sin modificarse). [4]
- ✓ Seguridad física y ambiental (control de acceso físico inadecuado a oficinas, salones y edificios, ubicación en áreas sujetas a inundaciones, almacenes desprotegidos, carencia de programas para sustituir equipos, mal cuidado de equipos, susceptibilidad de equipos a variaciones de voltaje). [4]
- ✓ Gestión de operaciones y comunicación (complicadas interfaces para usuarios, control de cambio inadecuado, gestión de red inadecuada, carencia de mecanismos que aseguren el envío y recepción de

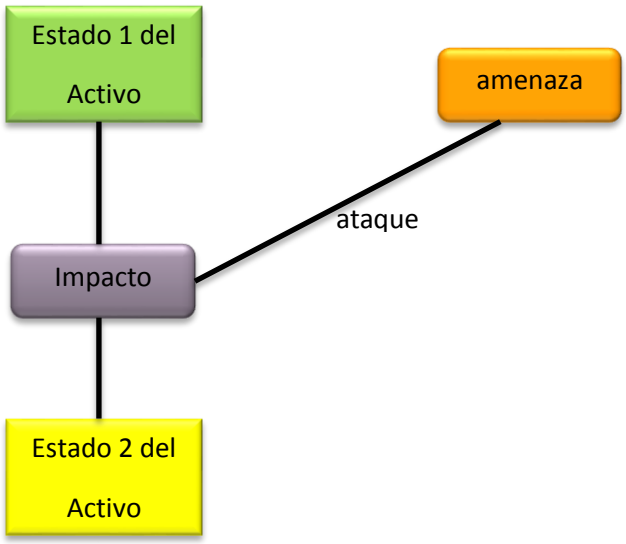
mensajes, carencia de tareas segregadas, carencia de control de copiado, falta de protección en redes públicas de conexión). [4]

- ✓ Mantenimiento, desarrollo y adquisición de sistemas de información (protección inapropiada de llaves criptográficas, políticas incompletas para el uso de criptografía, carencia de validación de datos procesados, carencia de ensayos de software, documentación pobre de software, mala selección de ensayos de datos). [4]

- ➢ **Impacto**

El impacto en un activo es la consecuencia sobre éste de la materialización de una amenaza. De forma dinámica, es la diferencia en las estimaciones del estado de seguridad del activo antes y después de la materialización de la amenaza sobre éste. [3]

GRÁFICO N° 2.1: MUESTRA LA RELACIÓN ENTRE IMPACTO Y AMENAZA.



Fuente: *Elaboración Propia*

- **Riesgos**

El riesgo es la posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización.

En el cálculo del riesgo tiene gran influencia la evaluación del impacto, que es un proceso difícil. El nivel del riesgo depende de la vulnerabilidad y del impacto.

El proceso de identificación y evaluación de riesgos y el de clasificación de activos, permite determinar qué tan expuestos se encuentran los activos de información a ataques por la presencia de vulnerabilidades propias o inherentes a la actividad de la organización.

También podemos decir que es una situación que expone a un objeto a que pueda ser afectado o dañado. Extendiendo más el concepto de riesgo, 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. De esta forma, en un sentido más amplio, se puede definir al riesgo como la combinación de la probabilidad de que ocurra un incidente con las consecuencias que generaría el mismo en el caso de que se materialice. (CNB - INDECOPI, 2008) (ISO 27799, 2008) (TALABIS & Martin, 2012) (ISACA, 2012) (PELTIER, 2005) (ISO 31000, 2013)

Existen muchas clasificaciones para tipificar los riesgos, una de ellas es la que aparece en [ISACA, 2011]:

- ✓ Riesgo inherente: existencia de un error material o significativo sin un control compensatorio.
- ✓ Riesgos de control: existencia de un error que no pueda ser detectado por el sistema de controles establecido.
- ✓ Riesgos de detección: mal uso de procedimientos de detección de errores por parte de un auditor, que lleven a indicar que no existen errores donde si los haya.
- ✓ Riesgos de negocio.
- ✓ Otros riesgos generales propios de la naturaleza de la auditoría.

- ➢ **Controles**

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzaran los objetivos del negocio.

Existen varias formas de establecer controles sobre riesgos organizacionales. La siguiente es la presentada por [ISACA, 2011]:

- ✓ Disuasivos: su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto. Por ejemplo: cámaras de vigilancia.
- ✓ Preventivos: detectan problemas antes que ocurran por medio de monitoreo constante. Por ejemplo: políticas de contratación.

- ✓ Defectivos: detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren. Por ejemplo: Uso de antivirus.
- ✓ Correctivos: minimizan el impacto de una amenaza ya consumada. Por ejemplo: Planes de contingencia. Propios

v. ANÁLISIS Y VALORACIÓN DE LOS RIESGOS

En primer lugar, conviene clarificar qué se entiende por riesgo. Dentro del contexto de un análisis de riesgos, es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

Antes de saber qué es un análisis de riesgos y lo que conlleva es importante conocer qué son otro tipo de conceptos muy relacionados con los Análisis de Riesgos y la seguridad de la información. Estos son los más importantes:

Amenaza: es la causa potencial de un daño a un activo.

Vulnerabilidad: debilidad de un activo que puede ser aprovechada por una amenaza.

Impacto: consecuencias de que la amenaza ocurra.

Riesgo intrínseco: cálculo del daño probable a un activo si se encontrara desprotegido.

Salvaguarda: medida técnica u organizativa que ayuda a paliar el riesgo.

Riesgo residual: riesgo remanente tras la aplicación de salvaguardas.

El análisis de riesgos se define como la utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

A la hora de diseñar un SGSI, es primordial ajustarse a las necesidades y los recursos de la organización para que se puedan cubrir las expectativas, llegando al nivel de seguridad requerido con los medios disponibles. Es relativamente sencillo calcular con cuántos recursos se cuenta (económicos, humanos, técnicos, etc.) pero no es tan fácil saber a ciencia cierta cuales son las necesidades de seguridad.

Hacer un análisis de riesgos permite averiguar cuáles son los peligros a los que se enfrenta la organización y la importancia de cada uno de ellos. Con esta información ya será posible tomar decisiones bien fundamentadas acerca de qué medidas de seguridad deben implantarse.

2.2.2. METODOLOGÍA DEL DESARROLLO DEL PROYECTO

NORMATIVIDAD Y MODELOS

i. 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 DEMING del software, estándares de calidad, sistemas de información y seguridad de la información.

Correspondiente a este último grupo, se realizó 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. A continuación, se detallan las principales normas pertenecientes a esta serie, algunas de las cuales servirán de soporte para realizar los procesos requeridos para completar el presente proyecto.

- *ISO 27001:2013, Information security management systems Requirements*

Especifica los requisitos a cumplir para poder establecer el Sistema de Gestión de Seguridad de la Información.

- *ISO 27002:2013, Code of practice for information security controls*

Presenta una guía de recomendaciones y buenas prácticas a seguir en la gestión de seguridad de la información.

- *ISO 27003:2010, Information security management system implementation guidance*

Establece una guía de implementación para las normas de la serie.

- *ISO 27005:2009, Information security risk management*

Centrada en presentar una metodología para el análisis de riesgos.

- *ISO 27799:2008, Health informatics – Information security management in health using ISO/IEC 27002*

Es una guía que extiende los conceptos y aspectos presentados en ISO 27002 aplicándolos al contexto específico de las entidades de salud.

Dado el alcance del presente proyecto, se utilizarán las normas ISO 27001 como soporte de la implementación de lo indicado por la Norma Técnica Peruana 27001, la cual se detalla en la siguiente sección ISO 27005 como herramienta para cubrir el análisis de riesgos necesario para establecer el SGSI e ISO 27799 dada su especificación de conceptos en el contexto sobre el cual se desarrollará el proyecto. (ORMELLA, 2013) (ISO 27001, 2013) (ISO 27002, 2013) (ISO 27799, 2008).

ii. NORMA TÉCNICA PERUANA NTP ISO/IEC 27001

Es una norma elaborada por el Comité Técnico Permanente de Codificación e Intercambio Electrónico de Datos, publicada en el año 2009 y establecida como de uso obligatorio mediante la Resolución Ministerial N° 129-2012-PCM el año 2012, se encuentra alineada al estándar ISO/IEC 27001 - estándar internacional publicado en el año 2005 que provee un modelo a seguir para el establecimiento y mantenimiento de un SGSI. El objetivo principal de esta norma es establecer los requisitos que se deben cumplir para la implementación del SGSI utilizando un enfoque a

procesos, lo cual requiere que se tenga disponible la mayor cantidad de documentación respecto a los mismos.

La norma utiliza la metodología Plan-Do-Check-Act, también llamado ciclo de Deming para definir las fases de vida y mejora continua del SGSI a través de un seguimiento de este que asegura el mantenimiento de los controles y los cambios necesarios para poder mitigar los posibles nuevos riesgos que aparezcan luego de la implementación del sistema. A continuación, se presenta un diagrama que detalla las etapas de esta metodología.

El diseño del SGSI siguiendo las fases del ciclo de Deming comprende las siguientes etapas:

- **Establecimiento**

  Se dan las recomendaciones a seguir para establecer el alcance que tendrá el sistema sobre la organización sobre la que se está trabajando. A continuación, se realiza un análisis de identificación de activos de información en conjunto con los riesgos y amenazas a los que se encuentran expuestos, además de realizar la valoración tanto de los activos como de los riesgos asociados y los posibles controles que podrían implementarse para mitigar los mismos.

- **Implementación**

  En esta fase se implementan las políticas y planes de mitigación que se requieren para poder tratar el riesgo identificado en el alcance del sistema. Como parte de esta etapa se detallan las acciones específicas que se deben realizar como parte del plan de mitigación.

- **Monitoreo y revisión**

  El establecimiento de políticas que rijan los procesos desde el punto de vista de la seguridad de los activos de información que los mismos utilizan, requiere que se establezcan también métricas y procedimientos con los cuales se pueda evaluar su eficiencia y determinar si es necesario realizar algún cambio para mejorar su desempeño, el cual es el objetivo principal de esta etapa.

- **Mantenimiento y mejora continúa**

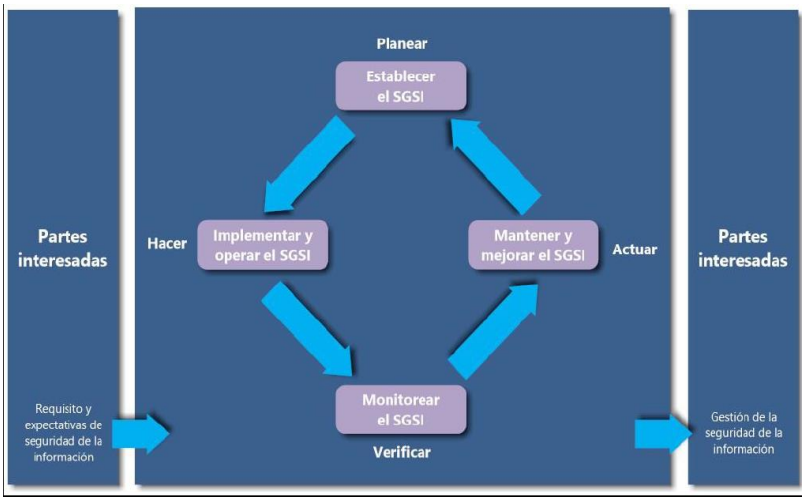
  Luego de realizar las evaluaciones de desempeño del SGSI en la etapa anterior, se puede identificar cambios que son necesarios para reajustar el alcance o mejorar su eficacia en el control de riesgos.

  Esto, sumado a que el SGSI es una entidad que continua vigente a lo largo del tiempo de vida de la organización, hace que el mantenimiento de este sea una tarea crítica como parte de su ciclo de DEMING.

  Recientemente, mediante la Resolución Ministerial N°129-2012/PCM (PRESIDENCIA DEL CONSEJO DE MINISTROS, 2012), fue aprobado el uso obligatorio de esta norma para todas las entidades que pertenezcan al Sistema Nacional de Informática entre ellas el Ministerio de Salud y todas sus dependencias – siguiendo el cronograma de implementación incremental determinado por la Oficina Nacional de Gobierno Electrónico e Informática, el cual determina las fases y duración del desarrollo de estas.

Para el presente proyecto de fin de carrera, además de seguir los requisitos establecidos por la presente norma. Debido a su carácter de obligatoriedad, está estrechamente relacionada con la problemática que ataca este proyecto y representa uno de los documentos más importantes a seguir durante el desarrollo del Sistema de Gestión de Seguridad de la Información. 2008 (CNB - INDECOPI, 2008) (ISO 27001, 2013) (ALEXANDER, 2007).

GRÁFICO N° 2.2: ESTRATEGIA DE MEJORA CONTINUA DEL SGSI, CICLO DE DEMING



Fuente: *Elaboración basado en NTP ISO/IEC 27001:2008 (CNB - INDECOPI, 2008)*

iii. LA NORMA ISO 27002

La ISO 27002 es una guía de buenas prácticas de seguridad de la información que presenta una extensa serie de controles de seguridad. Es la única norma que no sólo cubre la problemática de la seguridad de las tecnologías de información, sino que hace una aproximación holística a la seguridad de la información corporativa, abarcando todas las funcionalidades de una organización en cuanto a la

seguridad de la información que maneja. La norma considera también los riesgos organizacionales, operacionales y físicos de una empresa, con todo lo que esto implica. (AltoSec Blog).

Desde el 1 de julio de 2007, la ISO 27002 es el nuevo nombre de ISO 17799:2005. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable, sólo hace recomendaciones sobre el uso de 133 controles de seguridad diferentes aplicados en 11 áreas de control o dominios.

La ISO 27002, también nos hace mención de ciertas cláusulas entre ellas la Evaluación y Tratamiento del Riesgo, la cual es punto clave para el desarrollo de este proyecto, ya que nos proporciona indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información. Este punto se desarrollará teniendo en cuenta la realidad problemática expuesta con anterioridad. Esta cláusula considera dos puntos muy importantes para poder establecer objetivos de control en una organización:

GRÁFICO N° 2.3: EVALUACIÓN Y TRATAMIENTO DE RIESGO – ISO/IEC 27002:2008

Fuente: *Elaboración Propia*

Los objetivos de control contemplados en la Norma son:

- Política de Seguridad: Documento de política de seguridad y su gestión.
- Aspectos Organizativos de la Seguridad de la Información: Organización interna; organización externa.
- Gestión de Activos: Responsabilidad sobre los activos; clasificación de la información.
- Seguridad Ligada a los Recursos Humanos: Anterior al empleo; durante el empleo; finalización o cambio de empleo.
- Seguridad Física del Entorno: Áreas seguras; seguridad de los equipos.
- Gestión de Comunicaciones y Operaciones: procedimientos y responsabilidades de operación; gestión de servicios de terceras partes; planificación y aceptación del sistema; protección contra software

malicioso; backup; gestión de seguridad de redes; utilización de soportes de información; intercambio de información y software; servicios de comercio electrónico; monitorización.

- Control Accesos: Requisitos de negocio para el control de accesos; gestión de acceso de usuario; responsabilidades del usuario; control de acceso en red; control de acceso al sistema operativo; control de acceso a las aplicaciones e informaciones; informática y conexión móvil.
- Adquisición, desarrollo y mantenimiento de sistemas de información: Requisitos de seguridad de los sistemas de información; procesamiento correcto en aplicaciones; controles criptográficos; seguridad de los ficheros del sistema; seguridad en los procesos de desarrollo y soporte; gestión de vulnerabilidades técnicas.
- Gestión de incidentes en la Seguridad de la Información: Comunicación de eventos y puntos débiles de seguridad de la información; gestión de incidentes y mejoras de seguridad de la información.
- Gestión Continuidad de negocio: Aspectos de la seguridad de la información en la gestión de continuidad del negocio.
- Cumplimiento legal: Con los requisitos legales; políticas de seguridad y estándares de conformidad y conformidad técnica; consideraciones sobre la auditoría de sistemas de información.

iv. EVALUANDO LOS RIESGOS DE SEGURIDAD:

Las evaluaciones del riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de la seguridad de la información y para implementar los controles seleccionados para protegerse contra estos riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis del riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación del riesgo).

Las evaluaciones del riesgo también se debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; por ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones del riesgo se debieran realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser

efectiva y debiera incluir las relaciones con las evaluaciones del riesgo en otras áreas, si fuese apropiado.

El alcance de la evaluación del riesgo puede ser la organización en su conjunto, partes de la organización, un sistema de información individual, componentes específicos del sistema o servicios donde esto es practicable, realista y útil. Los ejemplos de las tecnologías de evaluación del riesgo se discuten en ISO/IEC TR 13335-3 (Lineamientos para la Gestión de la Seguridad TI: Técnicas para la Gestión de la Seguridad de Tecnologías de Información)

v. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD:

Antes de considerar el tratamiento del riesgo, la organización debiera decidir el criterio para determinar si se pueden aceptar los riesgos, o no. Los riesgos pueden ser aceptados si, por ejemplo, se ha evaluado que el riesgo es bajo o que el costo del tratamiento no es efectivo en costo para la organización. Estas decisiones debieran ser registradas.

Para cada uno de los riesgos definidos después de una evaluación del riesgo se necesita tomar una decisión de tratamiento del riesgo. Las opciones posibles para el tratamiento del riesgo incluyen:

a) Aplicar los controles apropiados para reducir los riesgos;
b) Aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización de la organización;
c) Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra;

d) Transferir los riesgos asociados a otros grupos; por ejemplo, aseguradores o proveedores.
e) Para aquellos riesgos donde la decisión del tratamiento del riesgo ha sido aplicar los controles apropiados, estos controles debieran ser seleccionados e implementados para satisfacer los requerimientos identificados por la evaluación del riesgo. Los controles debieran asegurar que se reduzcan los riesgos a un nivel aceptable tomando en cuenta:
f) Los requerimientos y restricciones de la legislación y las regulaciones nacionales e internacionales:
g) Objetivos organizacionales;
h) Requerimientos y restricciones operacionales;
i) Costo de implementación y operación en relación a los riesgos que se están reduciendo, y manteniéndolo proporcional a los requerimientos y restricciones de la organización;
j) La necesidad de equilibrar la inversión en implementación y operación de los controles con el daño probable resultado de fallas en la seguridad.

Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas de la organización. Es necesario reconocer que algunos controles pueden no ser aplicables a todo sistema de información o medio ambiente, y podría no ser practicable en todas las organizaciones.

Se debieran considerar los controles de seguridad de la información en los sistemas y la especificación de los requerimientos de proyectos, así como la etapa de diseño.

El no hacerlo puede resultar en costos adicionales y soluciones menos efectivas, y tal vez, en el peor de los casos, la incapacidad de lograr la seguridad adecuada.

Se debiera tener en mente que ningún conjunto de controles puede lograr la seguridad completa, y que se debiera implementar una acción de gestión adicional para monitorear, evaluar y mejorar la eficiencia y efectividad de los controles de seguridad para apoyar los objetivos de la organización.

vi. MAGERIT (VERSIÓN 3)

La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información nace como una iniciativa por parte del Consejo Superior de Informática, entidad perteneciente al Gobierno Español como respuesta a la regulación establecida en el Real Decreto 3/2010 el cual regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Esta metodología de gestión de riesgos tiene los siguientes objetivos: (MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS, 2012)

1. Concientizar a los responsables de las organizaciones sobre la presencia de riesgos y la necesidad e importancia de gestionarlos.
2. Ofrecer un método para analizar los riesgos a los que estén expuestos los activos de información.
3. Descubrir y planificar los controles a implementar para mitigar y controlar los riesgos.

4. Preparar a la organización para los futuros procesos de evaluación, auditoría o certificación que pueda requerir.

El esquema de trabajo que sigue la presente metodología permite cubrir todos los resultados referentes al análisis, documentación y control de los riesgos a los que se encuentra expuesta la información de la organización. Esto se puede ver en los pasos que la metodología establece para realizar el análisis de riesgos:

a. Determinar los activos relevantes para la organización, su interrelación y su valor (entendido como el costo de que éstos se vean afectados como consecuencia de algún riesgo).

b. Determinar las amenazas a las que se encuentran expuestos los activos identificados.

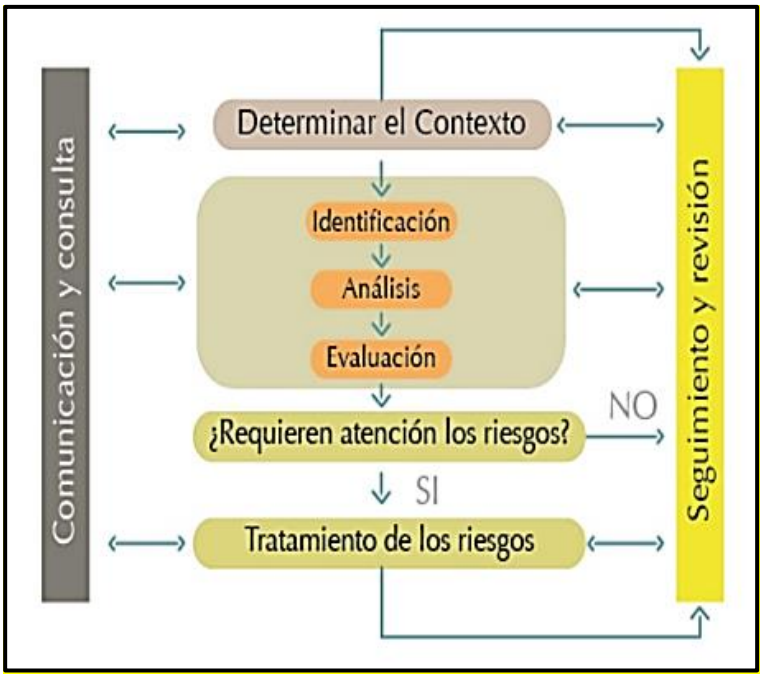
c. Determinar las medidas de protección actuales y la eficacia de estas frente al riesgo.

d. Estimar el impacto, es decir el daño que ocasionaría al activo de información la materialización de una amenaza.

e. Estimar el nivel de riesgo, el cual se calcula utilizando el impacto ponderado con la tasa de ocurrencia que se espera de la amenaza.

Con MAGERIT se persigue una aproximación metódica que no deje lugar a la improvisación, ni dependa de la arbitrariedad del analista. (Ver Graf. N° 2-4).

GRÁFICO N° 2.4: PROCESO DE GESTIÓN DE RIESGOS



***Fuente**: MAGERIT versión 3.0*

2.3. DEFINICIÓN DE TÉRMINOS

1. ***Activo:*** Algo que tenga valor para lo organización. Componente o funcionalidad de un sistema de información susceptible de ser atacado deliberada o accidentalmente con consecuencias para la organización. Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos. [ISO 13335].
2. ***Amenaza:*** Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. Causa potencial de un incidente no deseado que puede resultar en daño al sistema u organización. [ISO 13335]
3. ***Análisis de riesgos:*** Proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.
4. ***ARC:*** Área de Registro Civil.

5. ***Confidencialidad:*** Propiedad o característica consistente en que la información ni se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. [ISO 13335]
6. ***Control:*** Herramienta de la gestión del riesgo, incluido: políticas, pautas, estructuras organizacionales, que pueden ser de naturaleza administrativa, técnica, gerencial o legal. [ISO 27002]
7. ***Disponibilidad:*** Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados [ISO 13335]
8. ***Enunciado de aplicabilidad:*** Enunciado documentado que describe los objetivos de control y los controles que son relevantes y aplicables al SGSI de la organización. [ISO 27001]
9. ***Integridad:*** Propiedad o característica consistente en que el activo no ha sido alterado de manera no autorizada. [ISO 27000]
10. ***Impacto[3]:*** Consecuencia que sobre un activo tiene la materialización de una amenaza.
11. ***Incidente de seguridad de información:*** Es indicado por una o ***varias series de eventos inesperados y no deseados que tienen*** una gran probabilidad de comprometer las operaciones de negocios y de amenazar la seguridad de información. [ISO 18044]
12. ***Investigación:*** Está determinada por la averiguación de datos o la búsqueda de soluciones para ciertos inconvenientes.
13. ***ISO:*** Organización de Estandarización Internacional.
14. ***MAGERIT:*** Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
15. ***MDI:*** Municipalidad Distrital de Independencia.
16. ***Mitigar:*** Disminuir la intensidad, la gravedad o la importancia de algo.

---

3 ISO 27000, Glosario de Términos, Impacto, http://www.iso27000.es/glosario.html (Consultada el 15 de febrero de 2016).

17. ***Muestreo:*** Es la acción de escoger muestras representativas de la calidad o condiciones medidas de un todo.
18. ***Norma:*** Regla o conjunto de reglas que hay que seguir para llevar a cabo una acción, porque está establecido o ha sido ordenado de ese modo.
19. ***OREC:*** Oficinas de Registros de Estado Civiles
20. ***PDCA***: Ciclo de Deming conocido como círculo PDCA que es (planificar-hacer-verificar-actuar) también conocido como espiral de mejora continua
21. ***Riesgo:*** Es un problema potencial que puede ocurrir dentro de una organización.4
22. ***Riesgo Residual:*** Riesgo que se da tras la aplicación de salvaguardas dispuestas en un escenario de simulación o en el mundo real.
23. ***Registro Civil:*** inscribe todos los acontecimientos en la vida de una persona que tienen relación con su estado civil: nacimientos, matrimonios, defunciones y todo lo relacionado a ellos.
24. ***Salvaguarda:*** Procedimiento o mecanismo tecnológico que reduce el riesgo.
25. ***Seguridad de la información:*** Confianza en que los sistemas de información están libres y exentos de todo peligro o daño inaceptables. Preservación de la confidencialidad, integridad y disponibilidad de la información, así mismo, otras propiedades como la autenticidad, no rechazo, contabilidad y confiabilidad también pueden ser consideradas. [ISO 27002]
26. ***SGSI:*** Sistema de Gestión de Seguridad de la Información. Es una herramienta de gestión.
27. ***SGIT:*** Subgerencia de Informática y Telecomunicaciones

4 ISO 27000, Definición de Términos, Riesgo, http://www.iso27000.es/glosario.html (Consultada el 15 de febrero de 2016).

28. ***Vulnerabilidad:*** Defecto o debilidad en el diseño, implementación u operación de un sistema que habilita o facilita la materialización de una amenaza. Propiedades intrínsecas de que algo se produzca como resultado de una sensibilidad a una fuente de riesgo que puede conducir a un suceso con una consecuencia.5

5 ISO 27000, Definición de Términos, Vulnerabilidad, http://www.iso27000.es/glosario.html (Consultada el 15 de febrero de 2016).

CAPÍTULO III

MATERIALES Y MÉTODOS

3.1. MATERIALES

3.1.1. INSTRUMENTO USADO

a. Laboratorios

Las instalaciones de la Facultad de Ciencias, así como también las instalaciones de la Municipalidad Distrital de Independencia en su conjunto, siendo la más importante a tratar la Sub Gerencia de Informática y Telecomunicaciones.

b. Software

TABLA N° 3.1: INSTRUMENTOS USADOS SOFTWARE

T. TRANS	Software	Características	Descripción
2.6.6.1.3	**Sistema Operativo**	Windows 8	Desarrollada por Microsoft para su uso en computadoras personales, incluidas computadoras de escritorio en casa y de negocios, computadoras portátiles, tabletas, servidores.
2.6.6.1.3 2	**Microsoft Office**	Word 2013	Es el procesador de texto que fue usado para generar documentos como tesis, informes, encuestas y entre otros.
		Excel 2013	Es una hoja de cálculo que nos permitió construir Tabla N° estadísticos, tabulaciones de las encuestas, entre otros.
		PowerPoint 2013	Es un software que permite realizar presentaciones a través de diapositivas, este programa nos da la facilidad de utilizar texto, imágenes, música y animaciones.
2.6.6.1.3 2	**Microsoft Ms Project**	Project 2013	Es un software de administración de proyectos el cual se usó para asistir a administradores de proyectos en el desarrollo de planes, asignación de recursos a tareas, dar seguimiento al progreso y analizar cargas de trabajo.

T. TRANS	Software	Características	Descripción
2.6.6.1.3	**Bizagi modeler**	BPMN 2.0	Bizagi Modeler es usado para diagramar y documentar procesos: es un software gratuito y lo seguirá siendo. Esto significa que usted puede descargar el software y utilizarlo gratis sin restricciones de tiempo, para propósitos personales o de negocio.

Fuente: *Elaboración Propia*

c. Hardware

Dos unidades portátiles: 2 laptop con las siguientes características:

TABLA N° 3.2: INSTRUMENTOS USADOS HARDWARE[6]

T. TRANS	Equipo	Características
2.3.1.6.1.2	**Laptop**	Intel Core i3 1.70 GHz
		Windows 8.1 x 64 bits
		4 GB
		689 GB
2.3.2.4.4	**Impresora**	EPSON L300
2.3.1.6.1.2	**Disco duro externo**	TOSHIBA 1TB
2.3.1.6.1.2	**Pen Drive**	HP 8 GB

Fuente: *Elaboración propia*

3.1.2. POBLACIÓN Y MUESTRA

a. Población

La población en la cual se aplicó los instrumentos de recolección de datos es el personal que labora en la Sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia, así como personal

[6] Ministerio de Economía y Finanzas 2017, Clasificador de Gastos de Bienes y Servicios, Anexo 2, http://www.MEF.es/Anexo2.html (Consultada el 28 de febrero de 2016).

que labora en el área de registro civil para realizar el estudio piloto en los procesos involucrados con la subgerencia. El cual lo podemos observar en la Tabla N°3-3.

TABLA N° 3.3: POBLACIÓN TOTAL

PERSONAL DE LA SUB GERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES		
ITEM	**FUNCIÓN**	**CANTIDAD**
1	SUBGERENTE	1
2	OPERADOR	1
3	TECNICO INFORMÁTICO I	1
4	TECNICO INFORMÁTICO II	1
5	ASISTENTE TÉCNICO	2
ÁREA DE REGISTRO CIVIL		
6	REGISTRADOR CIVIL	1
7	TÉCNICO EN REGISTRO CIVIL	1
8	SECRETARIA	1
9	ASISTENTE ADMINISTRATIVO	1
TOTAL		10

Fuente: *Elaboración propia*

b. **Muestra:**

Teniendo en cuenta la población, para la presente investigación la muestra será igual a la población ya que la población objetivo está delimitada a un solo grupo de estudio, en la cual están involucradas las personas que laboran en la Sub gerencia de informática y telecomunicaciones y el Área de Registro Civil, por ello, no se requiere aplicar un muestreo probabilístico.

c. Unidad de análisis

Personal administrativo que labora en la Sub gerencia de informática y telecomunicaciones y el Área de Registro Civil en la Municipalidad Distrital de Independencia de la ciudad

de Huaraz, que hacen uso de los servicios e información que se maneja dentro de ellos,

El objetivo de contar con la información de este personal es analizar la situación actual de la gestión de información y presentar la declaración de aplicabilidad del sistema de gestión de seguridad de la información en la Sub gerencia de informática y telecomunicaciones.

3.2. MÉTODOS

3.2.1. TIPO DE INVESTIGACIÓN

a. De acuerdo a la orientación

La presente investigación es de tipo aplicada, porque se buscó la aplicación o utilización de los conocimientos que hemos adquirido durante el desarrollo y se empleó conocimientos relacionados con este instrumento teórico y metodológico, la cual está basada en el desarrollo de un sistema de gestión de seguridad de la información en la Sub gerencia de informática y telecomunicaciones de la Municipalidad Distrital de Independencia, para minimizar riesgos en los activos de información la cual servirá como un componente de desarrollo en la gestión de la Municipalidad como entidad pública.

b. De acuerdo a la técnica de contrastación

Es descriptiva ya que, se basó en la observación directa de la situación actual de la Municipalidad Distrital de Independencia y se obtuvo datos en relación a las necesidades, problemas u oportunidades de mejora que constituyen el punto de partida para el presente proyecto de

investigación, los investigadores se esforzaron por especificarlos tal como lo identifica; es decir sin alterarlos o modificarlos.

3.2.2. DEFINICIÓN DE VARIABLES

Variable independiente (Vi) = Sistema de Gestión de Seguridad de la Información.
Variable dependiente (Vd) = Activos de información en la Sub gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia

.

3.2.3. OPERACIONALIZACIÓN DE VARIABLES

TABLA N° 3.4: MATRIZ DE OPERACIONALIZACIÓN DE VARIABLES

VARIABLES	TIPO VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ÍTEMS PREGUNTAS ENCUESTA		ITEMS PREGUNTAS ENTREVISTA	ÍTEMS FICHA DE OBSERVACIÓN
						SGIT[7]	AR[8]C	SGIT	SGIT Y ARC
Sistema de Gestión de Seguridad de la Información.	Independiente	Conjunto de políticas, estándares y controles que se implementan en la organización con la finalidad de asegurar la preservación de la información.	Gestión en la implementación de controles de seguridad de la información en la entidad.	Gestión de riesgos	Cantidad de Incidentes reportados	4	14	F1-F7	
					Cantidad de vulnerabilidades y amenazas	5,6	12, 13		IIA
				Gestión de seguridad	Nivel de Conocimiento de RRHH	36,37	15,22	D1	
					Cantidad de capacitaciones de RRHH	38	21,22		
					Cantidad de controles implantados	2,4,7–32 y 41	4,5,6,8,9,10,11,17	B1-B6,C1,H1-H5	IIB

[7] Entiéndase por SGIT: como Sub Gerencia de Informática y Telecomunicaciones
[8] Entiéndase por ARC: como Área de Registro Civil.

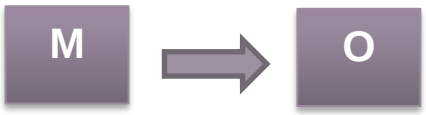
VARIABLES	TIPO VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIÓN	INDICADORES	ÍTEMS PREGUNTAS ENCUESTA		ITEMS PREGUNTAS ENTREVISTA	ÍTEMS FICHA DE OBSERVACIÓN
						SGIT	ARC	SGIT	SGIT Y ARC
Activos de información en la Sub gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia	Dependiente	Es todo aquello que las entidades consideran importante o de alta validez para la misma ya que puede contener importante información.	Gestión de recursos para conservar la confidencialidad, integridad y disponibilidad de la información.	Recursos Tecnológicos	Nivel de confidencialidad de HW y SW	11	18,19	E1-E3	IH
					Nivel de integridad de HW y SW	33	23	E1-E3	IH
					Nivel de disponibilidad de HW y SW	33, 34	16,20		

Fuente: *Elaboración propia*

3.2.4. DISEÑO DE LA INVESTIGACIÓN

Diseño general:

- *Descriptivo*, considerando el tipo y nivel de la investigación, el diseño de la investigación es descriptivo porque se analizó la realidad problemática y se logró comprender de forma íntegra el presente, de una sola casilla y se grafica de la siguiente manera:



Dónde:

M = Muestra,
O = Observación

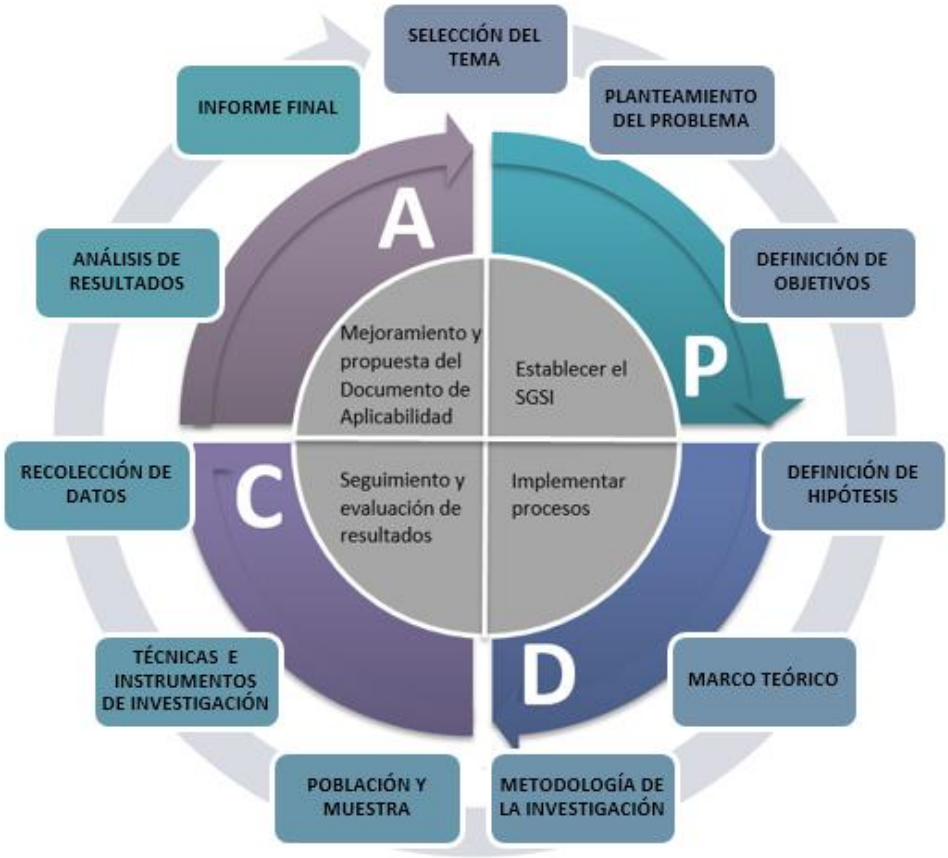
- Bibliográfico, se realizó a través de la información documentada, las cuales fueron el punto de partida para el desarrollo del siguiente proyecto de investigación.

Diseño metodológico:

Para el proyecto se usó un diseño metodológico que nos brinda el “Ciclo de Deming” de Edwards Deming, la cual tiene una mejor afinidad con el tema del presente proyecto.
De acuerdo a Edwards Deming, es también conocido como círculo PDCA esto es: Planificar, Hacer, Verificar y Actuar, es una estrategia de mejora continua de la calidad en cuatro pasos, basada en un concepto ideado por Walter A. Shewhart. Es muy utilizado por los sistemas de gestión de la calidad (SGC) y los sistemas de gestión de la seguridad de la información (SGSI).

En la siguiente investigación, se han utilizado la metodología de Investigación del autor Roberto Hernández Sampieri, relacionando con el ciclo de Deming, basándonos en la estructura del informe de tesis del reglamento de grados y títulos de la escuela académico profesional de ingeniería de sistemas e informática, y en el reglamento del PGT-ISI 2014. Esperamos que este documento de aplicabilidad sirva como punto de partida para su futura ampliación e implementación debidamente autorizada por la alta gerencia de la Municipalidad Distrital de Independencia, con la finalidad de proteger los activos de información del Subgerencia de Informática y Telecomunicaciones de la Municipalidad distrital de independencia.

GRÁFICO N° 3.1: METODOLOGÍA DE LA INVESTIGACIÓN



Fuente: Elaboración propia.

3.3. TÉCNICAS

- **Instrumentos de recolección de datos**

  Para la obtención de información se utilizó las siguientes herramientas como son: entrevista, encuestas y observación (ver Tabla N° 3.5).

TABLA N° 3.5: INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Instrumento	Justificación	Herramientas	Aplicación
Observación	Es el método en la cual enfocamos la perspectiva de los problemas que existen en las áreas a trabajar, ya que nos permite observar los hechos tal cual son y ocurren, y sobre todo aquellos que son de interés y significativos para la investigación.	- Fichas o guías de observaciones - Cámara fotográfica	Trabajadores del área de estudio, secretarias, gerentes y sub gerentes
Entrevista	Nos va a permitir conocer más de cerca los procesos de la Subgerencia de Informática y Telecomunicaciones, sus problemas, objetivos y requerimientos	- Grabador de voz - Entrevistas preparadas con una dinámica de preguntas y respuestas abiertas.	Trabajadores del área de estudio, secretarias, gerentes y sub gerentes
Encuestas	Elaborado especialmente con los ítems y alternativas cerradas con base a las variables e indicadores de estudio. Así mismo comprende las siguientes partes: título, objetivo, instrucción, preguntas y alternativas de respuesta.	- Encuesta estructurada de preguntas abiertas y cerradas	Trabajadores del área de estudio, secretarias, gerentes y sub gerentes

Fuente: *Elaboración propia*

- **Técnicas de procesamiento de información**

  La presente investigación utilizó las siguientes técnicas de recopilación y procesamiento de información:

  - Encuestas dirigidas al personal que labora, procesadas en Microsoft Excel 2013, lo cual nos permitirá obtener un consolidado de los resultados, así como gráficos para su interpretación.
  - Análisis de las entrevistas realizadas (guía de entrevistas), así como también de los documentos, libros y guías (digital e impreso) que se estén empleando para la realización de este proyecto.
  - Análisis de las observaciones realizadas durante la recopilación de información.

En base a estas técnicas de procesamiento de información, se establece la situación actual de la entidad y las necesidades a ser resueltas en base al problema planteado.

3.4. PROCEDIMIENTO

El procedimiento utilizado en esta investigación está separado en diferentes pasos que nos ayudaron a ordenar nuestra investigación:

1. Primer paso: Análisis Bibliográfico.
2. Segundo paso: Análisis de la problemática
3. Tercer paso: Diagnostico de la situación actual (Determinar la fórmula de éxito).
4. Cuarto paso: Desarrollo del Sistema de Gestión de Seguridad de la Información (Comprometer a los actores clave).
5. Quinto paso: Elaboración de la declaración de aplicabilidad.

CAPÍTULO IV

ANÁLISIS

4.1. ANÁLISIS DE LA SITUACIÓN ACTUAL

El análisis presentado a continuación tiene por finalidad hacer una revisión del estado actual de la Municipalidad Distrital de Independencia, identificando los agentes impulsores de cambio, las necesidades que tiene la institución en cuanto a Seguridad de la Información.

La Municipalidad Distrital de Independencia, desde sus inicios tuvo una álgida preocupación por permanecer en constante desarrollo tecnológico, con miras a convertirse en una de las mejores instituciones municipales, brindando una atención adecuada, efectiva y sobre todo de calidad, al público en general de acorde a la realidad. Para lo cual, de manera institucional, esta ha sido conformada por distintas áreas de apoyo que, en conjunto con los altos directivos, se espera que lleven a la municipalidad cumplir sus objetivos como institución regional.

Si bien es cierto la Municipalidad Distrital de Independencia y específicamente la Sub Gerencia de Informática y Telecomunicaciones, no se encuentran ajenos a lo descrito anteriormente, ya que en la actualidad esta no cuenta con ningún Sistema de Gestión de Seguridad y mucho menos iniciativas de planes de desarrollo de estas, a pesar de que hoy en día se cuenta con una serie de normas estándar internacionales, publicadas por la Organización Internacional de Normalización (ISO).

En adición a las disposiciones previas la Subgerencia de Informática y Telecomunicaciones se enfrenta a la necesidad de cumplir con la Norma Técnica Peruana NTP-ISO/IEC 27001:2013 en cuya publicación se establece explícitamente que dicha entidad, como parte de una entidad estatal , debe proceder con el proceso de implementación de un Sistema de Gestión de Seguridad de la Información que garantice la Confidencialidad, Integridad y Disponibilidad de la información que se utilice como parte de sus procesos de negocio, e incluso la relación que esta tiene con los procesos del Área de Registros Civil, el cual es un área del órgano Lineal de la Gerencia de Servicios Públicos y Gestión Ambiental que tiene un objeto esencial que es la de proteger la certeza jurídica y el orden legal al inscribir los hechos y actos del estado civil de las personas, debido a esta atribución mantiene una permanente interrelación con los habitantes del estado, durante el transcurso de su vida física. Con lo dicho anteriormente esta área está encargada de programar, organizar y evaluar la gestión de registros e inscripciones del ciudadano, en las instalaciones de dicha área se manejan una gran cantidad de información la cual es considerada de vital importancia para las autoridades, así como también para los ciudadanos de este Distrito. Para ello y conforme a los objetivos de la Municipalidad Distrital de Independencia, ha ido implementando tecnologías de información para la ayuda y soporte de sus procesos y manejo de información, tal es el caso del sistema de información que maneja conocido como: “OREC”, el cual está almacena la información en los servidores que se encuentran en la Sub Gerencia de Tecnología de Información, para hacer óptimo el manejo de la información.

Actualmente las tecnologías de información con la que cuenta la Subgerencia de Informática y Telecomunicaciones y a la vez que esta brinda los servicios a las demás áreas como el Área de Registro Civil

(ARC), se han podido apreciar ciertas debilidades, vulnerabilidades y deficiencias. Por ejemplo, se puede ver que el “OREC” funciona de manera ineficiente presentando problemas de lentitud al acceder desde la web, esto debido a que la línea de internet de 2 Mb que llega al servidor de la Sub Gerencia de Tecnología de Información la cual recién es distribuida a las demás áreas, la cual no es suficiente ante las solicitudes de los distintos procesos que realizan los usuarios. Además, la base de datos con la que trabaja el “OREC” presenta deficiencia en cuanto a copias de seguridad y mala estructura de esta, debido a que fue desarrollado sin tener en cuenta almacenamiento de la información por cada departamento, perjudicando la velocidad de respuesta a las consultas, todo ello por carecer de un orden. Otro problema que destacar es el cableado de la red, que sufre interferencias por la mala instalación o no tener en cuenta los estándares de este, así como la capacitación para el uso adecuado del sistema.

Dando un salto superficial en cuanto al tema de la seguridad, podemos decir que actualmente un usuario con conocimientos intermedios de informática puede acceder libremente con todos los permisos de la base de datos y por ende a la data (información) que se maneja en el “OREC”, creando un problema de alto índole que se debe de tomar en consideración lo antes posible ya que la información es de carácter confidencial de cada ciudadano. Este problema también se debe a una falta de configuración del servidor proxy, que si se realizara óptimamente solucionaría problemas de seguridad, rendimiento y hasta conectividad. A su vez cabe mencionar que la base de datos del “OREC” no posee un servidor propio, haciendo que este sea vulnerable puesto que está alojado dentro del servidor web.

Lo mencionado anteriormente es el análisis realizado respecto a la situación actual que atraviesa la Subgerencia de Informática y

Telecomunicaciones y su implicancia en el Área de Registro Civil, realidad que se espera cambiar con la ayuda de este proyecto, claro está que todo con la aprobación de la alta dirección.

Como vemos la MDI presenta dificultades en el manejo de información y la seguridad de esta, estos problemas deben de tener un tratamiento de manera rápida. Para hacer esto posible, la MDI debe de tomar en consideración la importancia de la seguridad de la información y los riesgos a los cuales están expuestos y no sólo en la Subgerencia de Informática y Telecomunicaciones y el Área de Registro Civil sino también en todas sus demás áreas, organismos y dependencias con el objetivo de impulsar de una manera conjunta y coherente los diferentes elementos que ayudarán a su crecimiento y desarrollo institucional y tecnológico. Ya que podemos observar que el principal agente impulsor del cambio es el Cumplimiento Normativo aplicado a las nuevas leyes promulgadas, lo cual conlleva a una mejora en la atención del usuario final dado que su información será resguardada, evitando filtraciones o pérdidas que puedan impactar negativamente a sus intereses personales.

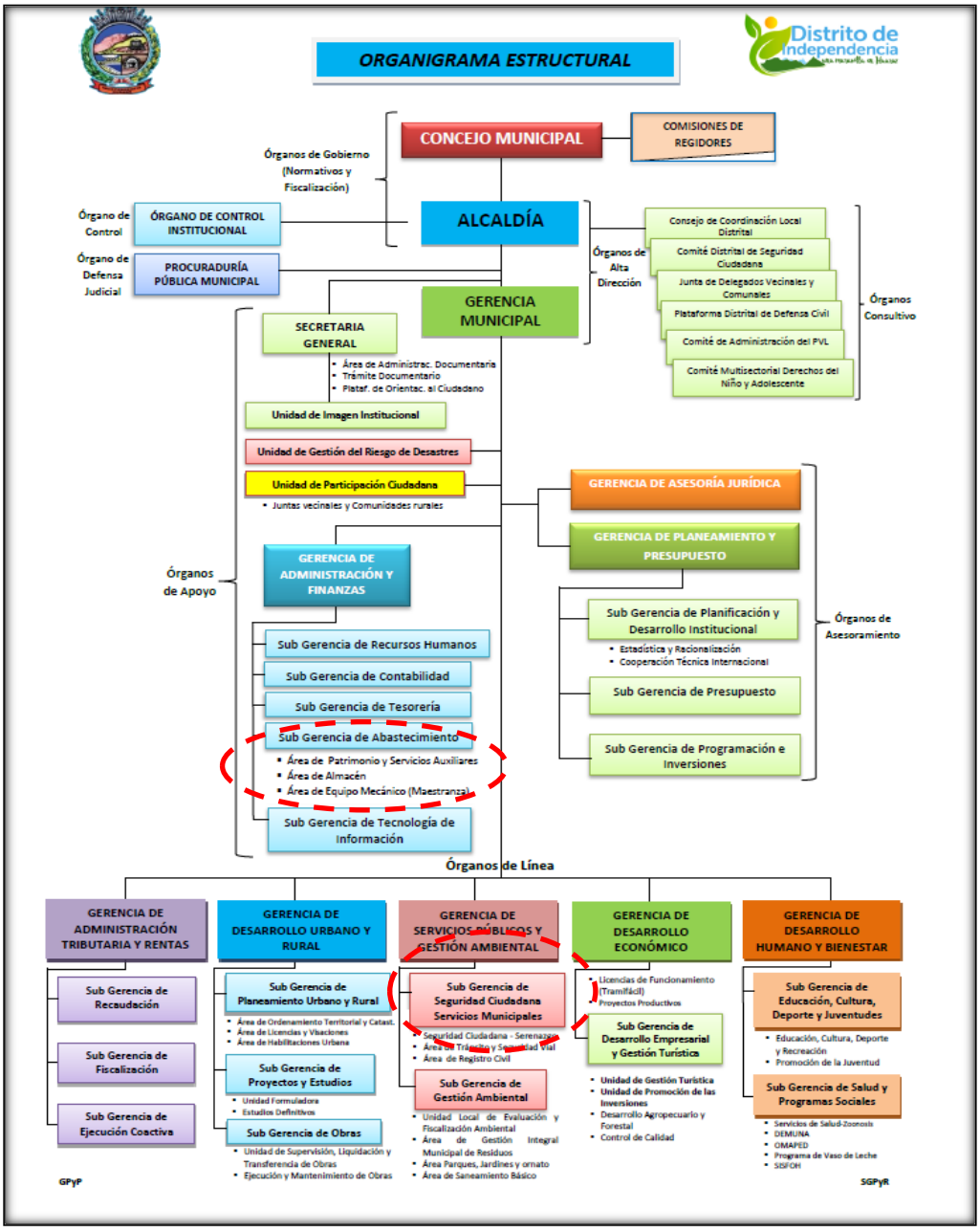
Es sobre este escenario que se presenta el presente proyecto, el cual pretende brindar a la entidad una solución que contara en el desarrollo de un SGSI que cumpla adicionalmente con lo estipulado por las normas.

4.1.1. ANÁLISIS DEL ORGANIGRAMA FUNCIONAL – ESTRATÉGICO

Para realizar un análisis del organigrama funcional, es necesario ubicar la Subgerencia de Informática y Telecomunicaciones y el Área de Registro civil dentro del organigrama estructural de la Municipalidad Distrital de

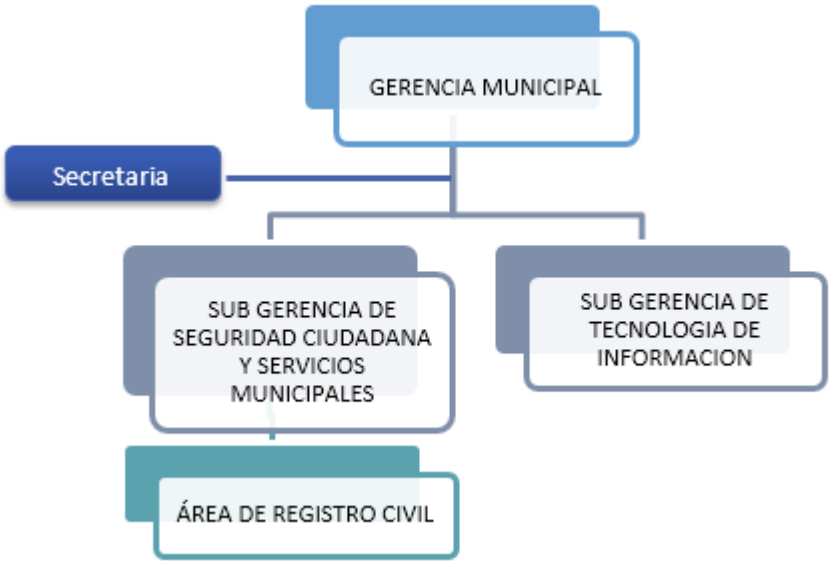
Independencia, como podemos observar a continuación en el siguiente gráfico:

GRÁFICO N° 4.1: ORGANIGRAMA ESTRUCTURAL



***Fuente*:** Manual de Organización y Funciones

GRÁFICO N° 4.2: ORGANIGRAMA ESTRUCTURAL DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES Y EL ÁREA DE REGISTRO CIVIL



***Fuente*:** Manual de Organización y Funciones

La Estructura Orgánica de La Sub Gerencia de Informática y Telecomunicaciones y el Área de Registro Civil son la siguiente:

- **Órgano de Dirección:**
  - Sub Gerente de Seguridad Ciudadana y servicios municipales.
  - Sub Gerente de Tecnología de Información.
- **Órganos de Línea:**
  - Área de registro civil.
- **Órgano de Apoyo:** secretaria

4.1.2. EVALUACIÓN DE LA CAPACIDAD INSTALADA

i. Personal.

El personal que actualmente labora dentro de las instalaciones de la Sub Gerencia de Informática y

Telecomunicaciones y Área de Registro Civil, son los siguientes:

Funciones del personal de Sub Gerencia de Informática y Telecomunicaciones

a. Sub gerente

- Diseñar, organizar, conducir, controlar y evaluar el Sistema Informático, basado en la potenciación de la capacidad instalada de la misma.
- Formular el Plan Operativo Informático de forma anual.
- Monitorear el sistema informático de la entidad compuesto por los recursos de hardware y software (SIAF-SEACE-SNIP, Etc.)
- Realizar el análisis de sistemas para elaborar los programas de cómputo para los órganos de la Municipalidad.
- Distribuir o redistribuir racionalmente los recursos informáticos según las estacionalidades de campaña o labores permanentes de las dependencias.
- Establecer los derechos de usuario, accesos y seguridad a la información institucional procesada en las disposiciones de almacenamiento informático.
- Proponer normas respecto al uso adecuado del hardware y software disponible.
- Realizar el mantenimiento preventivo y correctivo de los equipos de cómputo y accesorios.

- Emitir disposiciones para el correcto uso, protección y mantenimiento de los equipos de cómputo.
- Racionalizar y supervisar el uso institucional de Internet.

b. Operador

- Participar en los procesos de elaboración y evaluación del Plan Estratégico de Tecnología de Información y del Plan Operativo Informático.
- Efectuar estudios técnicos para la asignación y distribución del equipamiento de hardware y software, a las unidades orgánicas De la Municipalidad según sus necesidades.
- Instalar y monitorear la aplicabilidad de software adecuados acorde a las diferentes necesidades administrativas.
- Realizar operaciones técnicas de reparación y mantenimiento de los equipos electrónicos y sus periféricos correspondientes.
- Organizar y ejecutar los servicios de procesamiento de datos, instalación de software y otros asesoría y apoyo técnico a la gestión institucional.
- Participar en los procesos de elaboración y ejecución del Plan Anual de Mantenimiento, Inventario, licenciamiento, estandarización, y distribución del equipamiento de computación de las unidades orgánicas de la Municipalidad.

c. Técnico Informático

- Participar en los procesos de elaboración y evaluación del Plan Estratégico de Tecnología de Información y del Plan Operativo Informático.
- Organizar el proceso de aplicación de tecnologías de Información teniendo como plataforma principal la innovación y el mejoramiento continuo de los procesos de la Municipalidad.
- Diseñar proyectos relacionados con la implementación y funcionamiento del gobierno electrónico que se ejecuta en la Municipalidad e Identificar las necesidades de infraestructura, redes y comunicación.
- Organizar y ejecutar eventos de capacitación continua en temas de mejoras e innovación propiciando el desarrollo de los procesos de Información y Comunicación.

d. Asistente técnico

- Participar en los procesos de elaboración y evaluación del Plan Estratégico de Tecnología de Información y del Plan Operativo Informático.
- Efectuar estudios técnicos para la asignación y distribución del equipamiento de hardware y software, a las unidades orgánicas De la Municipalidad según sus necesidades.
- Instalar y monitorear la aplicabilidad de software adecuados acorde a las diferentes necesidades administrativas y realizar

operaciones técnicas de reparación y mantenimiento de los equipos electrónicos y sus periféricos correspondientes.

- Organizar y ejecutar los servicios de procesamiento de datos, instalación de software y otros asesoría y apoyo técnico a la gestión institucional.

Funciones del personal de Área de registro civil

a. Registrador civil

- Organizar, ejecutar, supervisar y controlar las actividades registrales. Registrar nacimientos ordinarios y extemporáneos; defunciones judiciales, notariales y ordinarias dando cuenta periódicamente a la RENIEC.
- Realizar rectificaciones de actas de nacimiento, matrimonio, defunción de acuerdo con las directivas vigentes y remitir a la RENIEC la información procesada.
- Clasificar y cautelar el archivo central del registro civil para brindar seguridad jurídica y tutela de los intereses colectivos.
- Actualizar el Padrón Electoral para facilitar a la Oficina Nacional de Procesos Electorales ONPE.
- Organizar eventos de capacitación a los registradores civiles de los Centros Poblados para el correcto registro de nacimientos y defunciones.

b. Técnico en Registro Civil

- Efectuar el registro de nacimientos ordinarios y extemporáneos; defunciones judiciales, notariales y ordinarias dando cuenta periódicamente a la RENIEC.
- Participar en las rectificaciones de actas de nacimiento, matrimonio, defunción de acuerdo a las directivas vigentes y remitir a la RENIEC la información procesada.
- Clasificar y cautelar el archivo central del registro civil para brindar seguridad jurídica y tutela de los intereses colectivos.
- Participar en el proceso de actualización del Padrón Electoral para remitirlo a la Oficina Nacional de Procesos Electorales ONPE.

c. Secretaria

- Organizar y preparar la agenda de trabajo y el desarrollo de reuniones de coordinación del Registrador Civil y Organizar y ejecutar el control y seguimiento de los expedientes del Registro Civil.
- Redactar y digitar documentos administrativos del Registro Civil, utilizando un software adecuado.
- Recepcionar, registrar y derivar los expedientes del Registro Civil a las instancias que les corresponde según la naturaleza de estos.
- Elaborar y consolidar el requerimiento de bienes de consumo y otros servicios de conservación y mantenimiento de los enseres del Registro Civil.

- Resguardar y distribuir los materiales de impresión y útiles de escritorio al personal del Registro Civil y Organizar y actualizar el archivo central del Registro Civil.

d. Asistente administrativo

- Organizar y ejecutar el registro de control de acuerdos y ordenanzas.
- Clasificar y cautelar el archivo central del registro civil para brindar seguridad jurídica y tutela de los intereses colectivos. Participar en el proceso de actualización del Padrón Electoral para remitirlo a la Oficina Nacional de Procesos Electorales ONPE.
- Organizar y ejecutar el registro de control de las resoluciones de Alcaldía proyectadas y aprobadas.
- Apoyar en asuntos de elaboración de ordenanzas, acuerdos, resoluciones y redacción de actas.

De acuerdo con esta información, podemos afirmar que los recursos humanos con los que cuenta la Sub Gerencia de Informática y Telecomunicaciones y Área de Registro Civil son suficientes para dar inicio a un mejor control en la información que maneja y realizar una adecuada gestión de riesgos, ya que proporcionará mecanismos de control para evitar incidentes.

ii. Equipos informáticos.

El equipamiento con el que se cuenta son las siguientes:

TABLA N° 4.1: EQUIPOS INFORMÁTICOS

N°	Área	Equipamiento	Cantidad
1	Sub Gerencia De Informática Y Telecomunicaciones	Servidor proliant ml370 g6	3
2		Acumulador de energía - equipo de ups	13
3		Atornillador eléctrico	3
4		Capturador de imagen – scanner	2
5		Compresora de aire	1
6		Computadora personal portátil	2
7		Disco duro externo 1 tb	3
8		Estabilizador	4
9		Impresora a inyección de tinta	3
10		Impresora laser	7
11		Monitor a color	5
12		Monitor plano	24
13		Multimetro-multitester	2
14		Pistola eléctrica para soldar	1
15		Probador de cable de red	1
16		Ruteador de red – router	8
17		Supresor de voltaje transitorio – tvss	3
18		Switch para red	14
19		Teclado - keyboard	8
20		Unidad central de proceso - CPU	27
21	Área De Registro Civil	Monitor de plano	3
22		Capturador de imagen - scanner	3
23		Impresora laser	2
24		Acumulador de energía - equipo de ups	3
25		Fotocopiadora en general	1
26		Monitor plano	1
27		Unidad central de proceso - CPU	2
28		Estabilizador	2
29		Cámara fotográfica digital	1
30		Teclado - keyboard	2

Fuente: *Elaboración propia*

4.2. IDENTIFICACIÓN Y DESCRIPCIÓN DE REQUERIMIENTOS

El área de dirección en nuestro caso es la Sub Gerencia de Informática y telecomunicaciones y como órgano en línea que tenemos en estudio es el Área de Registro Civil, esta última almacena su información en la Subgerencia de Informática y Telecomunicaciones, así como también hace uso de los servicios que

ellos brindan. Ambos órganos de la Municipalidad Distrital de Independencia son las encargadas de llevar un control adecuado de la información que se maneja en sus ambientes y resguardar la información del ciudadano.

4.2.1. IDENTIFICACIÓN DE FUENTES DE INFORMACIÓN

i. ***Encuestas al personal que labora en la*** **Subgerencia de Informática y Telecomunicaciones*, así como personal que labora en el Área de Registro Civil***: Se aplicó una encuesta estructurada brindando las alternativas que nos ayuden a probar la hipótesis. La muestra que se aplico es igual a la población como se muestra en el siguiente Tabla:

TABLA N° 4.2: POBLACIÓN TOTAL

PERSONAL DE LA SUB GERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES		
Item	**Función**	**Cantidad**
1	SUBGERENTE	1
2	OPERADOR	1
3	TECNICO INFORMÁTICO I	1
4	TECNICO INFORMÁTICO II	1
5	ASISTENTE TÉCNICO	2
ÁREA DE REGISTRO CIVIL		
6	REGISTRADOR CIVIL	1
7	TÉCNICO EN REGISTRO CIVIL	1
8	SECRETARIA	1
9	ASISTENTE ADMINISTRATIVO	1
TOTAL		10

Fuente: *Elaboración propia*

De la encuesta que se aplicó **(*Ver Anexo 2-3*)**, se basó en la ISO/IEC 27002:2013 y a su vez en la metodología MAGERIT, para el diagnóstico de la gestión de riesgo, con el fin de poder identificar y minimizar los riesgos y amenazas a los que está expuesta la información, y también para poder

establecer controles a tomar en cuenta de aquí en adelante, lo cual nos ayuda a probar la variable dependiente:

Vd: Activos de información en la Sub gerencia de Informática y Telecomunicaciones

ii. **Entrevistas al personal de la Subgerencia de Informática y Telecomunicaciones:** entrevista al personal de la Subgerencia de Informática y Telecomunicaciones ***(Ver Anexo 4)***, teniendo mayor ahínco en el Sub Gerente, operador y técnicos informáticos. Estas entrevistas juntamente con las observaciones ayudarán a tener un mayor conocimiento de la situación actual de la Subgerencia de Informática y Telecomunicaciones en cuanto a su nivel de seguridad de la información y ver qué medidas han optado hasta el momento y que controles se deberán de seguir a partir de ello.

iii. **Inventario de activos y controles en la Subgerencia de Informática y Telecomunicaciones (MAGERIT):** Los activos son importantes en toda entidad, y en la Sub Gerencia no es la excepción. Al tener un reporte de activos nos permitirá obtener el riesgo al que están expuestos ellos. Una vez entendido esto nos permitirá proponer los controles y las medidas necesarias a tomar en cuenta para disminuir el riesgo. Todo ello nos ayuda a probar la variable independiente:

Vi: Desarrollo de un Sistema de Gestión de Seguridad de la Información

TABLA N° 4.3: ACTIVOS DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES

Tipo	Código	Activo
Bienes de información	BI-01	Archivo físico de las computadoras
	BI-02	Formularios de mantenimiento
	BI-03	Oficios
Bienes físicos	BF-01	SERVIDOR Proliant ML370 G6-SQL Server (BD y Aplicación)
	BF-02	SERVIDOR Proliant ML370 G6- services
	BF-03	SERVIDOR Proliant ML370 G6- Firewall – ClearOs
	BF-04	Computadora Personal Advance Core i7
	BF-05	Computadora Personal Lenovo Core i7
	BF-06	Computadora Personal Asus AMD
	BF-07	Computadora Personal HP - Compaq - Core i5
	BF-08	Computadora Personal Qualcom - Quad Core
	BF-09	Computadora Personal - Pentium IV
	BF-10	Router Cisco 837
	BF-11	Router D-Link - DGS 1008D
	BF-12	Switch 3Com BASELINE SWITCH 2816 - 24 ptos 10/100/1000
	BF-13	Switch HP - 16 ptos 10/100
	BF-14	Switch D-Link DGS 1008D - 8 ptos - 10/100/1000
	BF-15	Impresora Hp Laserjet P2055DN
	BF-16	Scanner Cannon Scanjet 3400C
	BF-17	HP Scanjet Enterprise 7500
	BF-18	Disco duro externo Toshiba 1 TB
Bienes de Software	BS-01	OREC
	BS-02	SQL Server 2008 R2
	BS-03	Windows Server 2008
	BS-04	Windows Seven 7
	BS-05	Microsoft Office 2013
	BS-06	Antivirus SMART SECURITY

Tipo	Código	Activo
Personas	P-01	Sub gerente
	P-02	OPERADOR
	P-03	TECNICO INFORMÁTICO I y II
	P-04	ASISTENTE TÉCNICO
Servicios	S-01	INTERNET
	S-02	SISTEMA INTEGRADO DE REGISTROS CIVILES
	S-03	SIGA
	S-04	SIAF
	S-05	TRAMITE VIRTUAL
	S-06	SISTEMA DE CAJA DE RENTAS
	S-07	COMPROBANTE DE PAGO

Fuente: *Elaboración propia*

4.3. DIAGNÓSTICO DE LA SITUACIÓN ACTUAL

4.3.1. INFORME DE DIAGNÓSTICO:

De los análisis de la situación actual que enfrenta la Subgerencia de Informática y Telecomunicaciones con su implicancia en el Área de Registro Civil, observamos deficiencias en la seguridad de la información por lo que es necesario y urgente dar los controles necesarios que ayuden a mitigar los incidentes y dar frente las amenazas y vulnerabilidades que se presenten. Con lo cual cabe mencionar que la información que maneja la Subgerencia de Informática y Telecomunicaciones es de importancia para toda la comunidad por lo que cualquier amenaza podría tener un enorme impacto en cuanto a la realización de las actividades con total normalidad de la Municipalidad distrital de Independencia. Por lo demás se deberá de tener en cuenta también mejoras en equipamiento y software, como también en las instalaciones donde se encuentra.

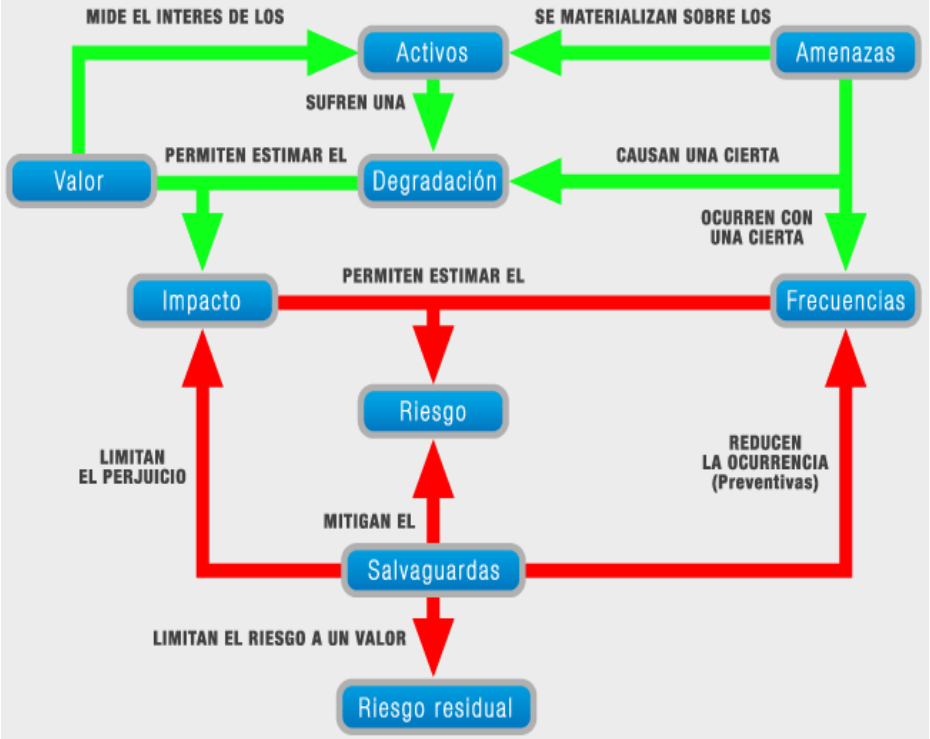
También es importante mencionar el papel que cumplen los usuarios en todo esto, como vemos en los resultados anteriores el nivel de conocimiento de los usuarios sobre seguridad de la información es vago o escaso y no le toman la importancia del caso. En base a esto también se debe considerar capacitar al usuario en estos temas y así podamos reducir los riesgos no solo para la Subgerencia de Informática y Telecomunicaciones y el Área de Registro Civil sino también dentro de toda la Municipalidad Distrital de Independencia.

4.3.2. MEDIDAS DE MEJORAMIENTO:

Lo que se propone ante la situación actual de la Subgerencia de Informática y Telecomunicaciones es el desarrollo de un Sistema de gestión de Seguridad de la información para minimizar los riesgos tomando en cuenta estándares que nos permitan seguir ciertos criterios para enfrentar las amenazas, tal es el caso de la ISO/IEC 27002:2013 y MAGERIT. En cuanto a la ISO, aun no es certificado, pero propone alternativas ante las amenazas a la seguridad de la información de cualquier entidad, alternativa y medida que permitirán dar mayor seguridad a los usuarios y a la comunidad en general.

En cuanto al equipamiento informático de la sub Gerencia, se recomienda actualizar sus equipos de cómputo, especialmente para aquellos que serán los administradores del sistema, así como también tomarle la atención necesaria a los activos que posee la Subgerencia de Informática y Telecomunicaciones ya que como vemos en el siguiente gráfico el nivel de riesgo es alto, especialmente en lo que concierne a los bienes físicos que posea. Las medidas a tomar se verán en el siguiente capítulo.

GRÁFICO N° 4.3: MAGERIT V3 Y 17 NUEVAS GUÍAS STIC.



Fuente: *http://www.securitybydefault.com/2012/10/ccn-cert-magerit-v3-y-17-nuevas-guias.html*

CAPÍTULO V

DISEÑO DE LA SOLUCIÓN

El presente capítulo se realiza teniendo en cuenta el ciclo PDCA que permite realizar una serie de pasos y procesos para la construcción de un SGSI, a continuación, se procede a realizar cada una de estas etapas:

5.1. PLANIFICAR EL SGSI

5.1.1. ALCANCE

Con el fin de mejorar la calidad en la prestación de servicios prestados por la Municipalidad Distrital de independencia se pretende aplicar el presente SGSI a los procesos, recursos informáticos y tecnológicas que hacen parte de la Sub Gerencia de Informática y Telecomunicaciones con el fin de establecer políticas para gestionar adecuadamente la seguridad de la información y debe ser aplicada y cumplida por todos los trabajadores de la Municipalidad, además se realiza el estudio piloto en el Área de Registro civil que tiene influencia de la Subgerencia de Informática y Telecomunicaciones para realizar algunos de sus procesos.

5.1.2. POLÍTICA DEL SISTEMA DE GESTIÓN

La Municipalidad distrital de Independencia pretende que la información manejada por la entidad en sus diferentes áreas; se encuentre debidamente protegida con el fin de preservar y salvaguardar la confidencialidad, disponibilidad e integridad de la información, ya que es una entidad pública.

5.1.3. METODOLOGÍA DE EVALUACIÓN DEL RIESGO

Para el proyecto se eligió la metodología MAGERIT; para el análisis y gestión de los riesgos, esto debido a que:

a. La metodología nos permite una identificación clara y definida del entorno de aplicación.

b. La metodología identifica en su análisis, riesgos críticos para la entidad, con lo cual se puede identificar inmediatamente posibles soluciones.

c. La metodología nos permite identificar valores cualitativos y cuantitativos, lo que hace fácil identificar las decisiones a tomar.

De acuerdo a MAGERIT:

El análisis de riesgo es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados los cuales son:

- **PASO 1:** Inventario de activos
- **PASO 2:** Valoración de los activos
- **PASO 3:** Amenazas (Identificación y Valoración)
- **PASO 4:** Salvaguardias

5.1.4. ANÁLISIS DE RIESGOS DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES

5.1.4.1. INVENTARIO DE ACTIVOS

Toda organización debe proteger los tres pilares de la seguridad de la información, los cuales son: primero la confidencialidad, segundo la integridad y por último la disponibilidad de la información; esto para velar por la

continuidad del negocio independientemente de su actividad social.

Para proteger la información de riesgos y amenazas se realizó el inventario de activos teniendo en cuenta la metodología MAGERIT que los clasifica en: Activos esenciales, Datos o información (Fundamentales), Servicios, Aplicaciones de software, Equipos informáticos, Personal, Redes de Comunicación, Soportes de información, Equipamiento auxiliar e Instalaciones.

A continuación, detallaremos cada uno de ellos:

a. ACTIVOS ESENCIALES

Los activos esenciales son aquellos que son importantes para la organización nos enfocaremos principalmente a los activos que tienen relación la Subgerencia de Informática y Telecomunicaciones con el Área de Registro Civil.

TABLA N° 5.1: INVENTARIO DE ACTIVOS - ACTIVOS ESENCIALES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[vr]	Datos vitales	[i_partidas]	Información de partidas civiles (base de datos y registro de partidas)
		[i_certificados]	Información de certificados civiles
		[i_normativa]	Información de normativa (Normas locales, nacionales, acuerdos, etc)
[per]	Datos de carácter personal	[i_financiera]	Información del área financiera de la municipalidad
[classified]	Datos clasificados	[e_s_registrador]	Ejecutable software registrador
		[d_históricos]	Datos históricos de partidas
		[d_partidas]	Documentación de partidas tramitadas

Fuente: *Elaboración propia*

b. DATOS O INFORMACIÓN (FUNDAMENTALES)

Debido a que los datos y/o la información son importantes para la organización esta parte, es fundamental; nos enfocaremos principalmente a los activos que tienen relación la Sub gerencia de Informática y Telecomunicaciones con el Área de Registro Civil.

TABLA N° 5.2: INVENTARIO DE ACTIVOS - DATOS DE INFORMACIÓN

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[files]	Ficheros	[a_partidas]	Archivos de partidas
		[a_usuarios]	Archivos de usuarios
		[a_financiera]	Archivos financieros
		[a_informes y partidas]	Archivos de informes y partidas
[backup]	Copias de respaldo	[a_copias de seguridad]	Archivo de Copias de seguridad de la información
[conf]	Datos de configuración	[d_configuracion_ser]	Datos de configuración de servidores y equipos
[int]	Datos de gestión interna	[d_gestionpartidas]	Datos de Gestión de partidas civiles
[password]	Credenciales	[pass_usuarios]	Contraseñas de acceso de usuarios

Fuente: *Elaboración propia*

c. CLAVES CRIPTOGRÁFICAS

Esta parte es importante para garantizar el cifrado de datos y comunicaciones, por el hecho de manejar información confidencial de todos los usuarios que se tienen.

TABLA N° 5.3: INVENTARIO DE ACTIVOS - CLAVES CRIPTOGRÁFICAS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[encrypt]	Claves de cifra	[cc_aplicaciones_caja]	Claves de cifra de aplicaciones de caja

Fuente: *Elaboración propia*

d. INVENTARIO DE SERVICIOS

Los servicios a continuación detallados son para usuarios y trabajadores.

TABLA N° 5.4: INVENTARIO DE ACTIVOS - INVENTARIO DE SERVICIOS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[ext]	A usuarios externos (bajo una relación contractual)	[s_u_externo]	Servicios prestados a usuarios externos (Usuarios partidas)
[int]	Interno (a usuarios de la propia organización)	[s_u_interno]	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.
[www]	World wide web	[s_internet]	Servicio de internet al que pueden acceder los empleados.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[email]	Correo electrónico	[s_correo]	Manejo de correos electrónicos
[file]	Almacenamiento de ficheros	[s_a_bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.
[ipm]	Gestión de privilegios	[g_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la Municipalidad.

Fuente: Elaboración propia

e. APLICACIONES DE SOFTWARE

Debido a que en el Área de Registro Civil se dedica al otorgamiento de partidas civiles, esta cuenta con un servidor y software registrador que se encuentra enlazado a la RENIEC, donde además se registra, actualiza y almacena el estado de cada partida, para generar reportes e imprimir certificados.

TABLA N° 5.5: INVENTARIO DE ACTIVOS - APLICACIONES DE SOFTWARE

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[app]	Servidor de aplicaciones	[server_app]	Servidor de aplicaciones
[dbms]	Sistema de gestión de bases de datos	[s_basededatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la Municipalidad.
[oficce]	Ofimática	[oficce]	Office 2010
[av]	Antivirus	[antivirus]	ESSET original con actualizaciones automáticas.
[os]	Sistema operativo	[os_win10]	Sistema operativo Windows 10, en su versión professional con actualizaciones automáticas activadas.

Fuente: Elaboración propia

f. EQUIPOS INFORMÁTICOS

Para los equipos informáticos de la entidad, se consideran aquellos que se encuentran en la Subgerencia de Informática y telecomunicaciones y los que se encuentran relacionados con el Área de Registro Civil.

TABLA N° 5.6: INVENTARIO DE ACTIVOS - EQUIPOS INFORMÁTICOS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[host]	Grandes equipos (Servidor de bases de datos, servidores de aplicación)	[s_aplicaciones]	Servidor Aplicaciones
		[s_database]	Servidor de Base de Datos
[mid]	Equipos medios (Equipos de trabajo conectados a través de red inalámbrica por red 802.1x)	[pc_trabajadores]	Equipos de mesa
[pc]	Equipos que son fácilmente transportados	[pc_portatiles]	Equipos Portatiles
[print]	Equipos de impresión	[e_impresoras]	Impresoras
[router]	Enrutadores	[r_enrutadores]	Enrutadores

Fuente: Elaboración propia

g. REDES DE COMUNICACIÓN

Para las redes de comunicación de la entidad, se consideran aquellos que se encuentran en la Subgerencia de Informática y telecomunicaciones y los que se encuentran relacionados con el Área de Registro Civil.

TABLA N° 5.7: INVENTARIO DE ACTIVOS - REDES DE COMUNICACIÓN

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[wifi]	Red inalámbrica	[r_wifi]	Red Inalámbrica
[lan]	Red local	[r_local]	Red local
[internet]	Internet	[internet]	Internet

Fuente: Elaboración propia

h. SOPORTES DE INFORMACIÓN (ALMACENAMIENTO ELECTRÓNICO)

Para los soportes de información de almacenamiento electrónico de la entidad, se consideran aquellos que se encuentran en la Subgerencia de Informática y telecomunicaciones y los que se encuentran relacionados con el Área de Registro Civil.

TABLA N° 5.8: INVENTARIO DE ACTIVOS - ALMACENAMIENTO ELECTRÓNICO

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[cd]	Discos	[a_cd]	Almacenamientos en Disco Duro
[cd]	Cederrom (CD_ROM)	[a_cd]	Almacenamiento en CD
[usb]	Memorias	[a_memorias]	Almacenamiento en Memorias
[dvd]	DVR	[a_dvd]	Almacenamiento en DVD

Fuente: Elaboración propia

i. SOPORTES DE INFORMACIÓN (ALMACENAMIENTO NO ELECTRÓNICO)

Para los soportes de información de almacenamiento no electrónico, se consideran aquellos que se encuentran en la Subgerencia de Informática y telecomunicaciones y los que se encuentran relacionados con el Área de Registro Civil.

TABLA N° 5.9: INVENTARIO DE ACTIVOS - ALMACENAMIENTO NO ELECTRÓNICO

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[printed]	Material impreso	c_documentaciónpartidas	Carpetas con la documentación de cada partida(documentación)
		c_reporteseinformes	Carpetas de reportes e informes impresos
		c_soprtesfinancieros	Carpetas recibos caja
		c_varios	Carpetas varias

Fuente: Elaboración propia

j. EQUIPAMIENTO AUXILIAR

Para el equipamiento auxiliar de almacenamiento no electrónico, se consideran aquellos que se encuentran en la Subgerencia de Informática y telecomunicaciones y los que se encuentran relacionados con el Área de Registro Civil.

TABLA N° 5.10: INVENTARIO DE ACTIVOS - EQUIPAMIENTO AUXILIAR

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[printed]	Sistemas de Alimentación ininterrumpida	u_computadores	Ups computadores
[suplly]	Suministros Esenciales	esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.
[Furniture]	Mobiliario	M_Mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.

Fuente: *Elaboración propia*

k. INSTALACIONES

Para las instalaciones, se consideran al de la Municipalidad Distrital de Independencia en la que se encuentra ubicada el área de estudio.

TABLA N° 5.11: INVENTARIO DE ACTIVOS – INSTALACIONES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización
[building]	Edificio	[e_municipalidad]	Local de la Municipalidad.

Fuente: *Elaboración propia*

I. PERSONAL

Para el personal, se consideran a los de las áreas de estudio los cuales detallamos a continuación en el siguiente Tabla N° 5.1-13.

TABLA N° 5.12: INVENTARIO DE ACTIVOS – PERSONAL

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo con la organización	Nombre de activo de acuerdo a la organización
[ui]	Usuarios internos	[e_personal]	Personal de la recepción, área civil.
[adm]	Administradores de sistemas	[a_sistemas]	Administrador de sistemas, personal de la Subgerencia de Informática y Telecomunicaciones.

Fuente: *Elaboración propia*

5.1.4.2. VALORIZACIÓN CUALITATIVA Y CUANTITATIVA DE LOS ACTIVOS

En esta parte se realiza la valoración cualitativa para cada uno de los activos teniendo en cuenta las dimensiones de seguridad como confiabilidad, integridad, autenticidad, disponibilidad y trazabilidad de acuerdo a la siguiente Tabla N° 5.1.4-14:

TABLA N° 5.13: CRITERIOS DE VALORACIÓN

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Fuente*: MAGERIT V3 Libro 2 Catálogo de elementos*

m. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE ACTIVOS ESENCIALES

TABLA N° 5.14: VALORACIÓN DE ACTIVOS ESENCIALES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[vr]	Datos vitales	[i_partidas]	Información de partidas civiles (base de datos y registro de partidas)	Confiabilidad	9
				Integridad	9
				Autenticidad	8
				Disponibilidad	7
				Trazabilidad	7
		[i_certificados]	Información de certificados civiles	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7
		[i_normativa]	Información de normativa (Normas locales, nacionales, acuerdos, etc)	Confiabilidad	4
				Integridad	3
				Autenticidad	3
				Disponibilidad	3
				Trazabilidad	3
[per]	Datos de carácter personal	[i_financiera]	Informacion del área financiera de la municipalidad	Confiabilidad	6
				Integridad	6
				Autenticidad	6
				Disponibilidad	5
				Trazabilidad	5
[classified]	Datos clasificados	[e_s_registrador]	Ejecutable software registrador	Confiabilidad	6
				Integridad	6
				Autenticidad	4
				Disponibilidad	3
				Trazabilidad	5
		[d_históricos]	Datos históricos de partidas	Confiabilidad	3
				Integridad	3
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	6
		[d_partidas]	Documentación de partidas tramitadas	Confiabilidad	6
				Integridad	6
				Autenticidad	5
				Disponibilidad	5
				Trazabilidad	5

Fuente: *Elaboración propia*

n. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE DATOS/INFORMACIÓN

TABLA N° 5.15: VALORACIÓN DE DATOS DE INFORMACIÓN

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[files]	Ficheros	[a_partidas]	Archivos de partidas	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7
		[a_usuarios]	Archivos de usuarios	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7
		[a_financiera]	Archivos financieros	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7
		[a_informes y partidas]	Archivos de informes y partidas	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7
[backup]	Copias de respaldo	[a_copias de seguridad]	Archivo de Copias de seguridad de la información	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7
[conf]	Datos de configuración	[d_configuracion_ser]	Datos de configuración de servidores y equipos	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7
[int]	Datos de gestión interna	[d_gestionpartidas]	Datos de Gestión de partidas civiles	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[password]	Credenciales	[pass_usuarios]	Contraseñas de acceso de usuarios	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	7

Fuente: *Elaboración propia*

o. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE CLAVES CRIPTOGRÁFICAS

TABLA N° 5.16: VALORACIÓN DE CLAVES CRIPTOGRÁFICAS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[encrypt]	Claves de cifra	[cc_aplicaciones_caja]	Claves de cifra de aplicaciones de caja	Confiabilidad	8
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	

Fuente: *Elaboración propia*

p. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE SERVICIOS

TABLA N° 5.17: VALORACIÓN DE SERVICIOS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[ext]	A usuarios externos (bajo una relación contractual)	[s_u_externo]	Servicios prestados a usuarios externos (Usuarios partidas)	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[int]	Interno (a usuarios de la propia organización)	[s_u_interno]	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[www]	World wide web	[s_internet]	Servicio de internet al que pueden acceder los empleados.	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[email]	Correo electrónico	[s_correo]	Manejo de correos electrónicos	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[file]	Almacenamiento de ficheros	[s_a_bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[ipm]	Gestión de privilegios	[g_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la Municipalidad.	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	

Fuente: *Elaboración propia*

q. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE SOFTWARE-APLICACIONES INFORMÁTICAS

TABLA N° 5.18: VALORACIÓN DE SOFTWARE-APLICACIONES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[app]	Servidor de aplicaciones	[server_app]	Servidor de aplicaciones	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[dbms]	Sistema de gestión de bases de datos	[s_basededatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la Municipalidad.	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[Oficce]	Ofimática	[oficce]	Office 2010	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	3
				Trazabilidad	
[av]	Antivirus	[antivirus]	ESSET original con actualizaciones automáticas.	Confiabilidad	7
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[os]	Sistema operativo	[os_win10]	Sistema operativo Windows 10, en su versión professional con actualizaciones automáticas activadas.	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	

Fuente: *Elaboración propia*

r. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE EQUIPOS INFORMÁTICOS

TABLA N° 5.19: VALORACIÓN DE EQUIPOS INFORMÁTICOS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[host]	Grandes equipos (Servidor de bases de datos, servidores de aplicación)	[s_aplicaciones]	Servidor Aplicaciones	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	
		[s_database]	Servidor de Base de Datos	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	6
				Trazabilidad	
[mid]	Equipos medios (Equipos de trabajo conectados a través de red inalámbrica por red 802.1x)	[pc_trabajadores]	Equipos de mesa	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[pc]	Equipos que son fácilmente transportados	[pc_portatiles]	Equipos Portatiles	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[print]	Equipos de impresión	[e_impresoras]	Impresoras	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	
[router]	Enrutadores	[r_enrutadores]	Enrutadores	Confiabilidad	7
				Integridad	7
				Autenticidad	6
				Disponibilidad	
				Trazabilidad	

Fuente: *Elaboración propia*

s. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE REDES DE COMUNICACIONES

TABLA N° 5.20: VALORACIÓN DE REDES DE COMUNICACIONES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[wifi]	Red inalámbrica	[r_wifi]	Red Inalámbrica	Confiabilidad	7
				Integridad	7
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[LAN]	Red local	[r_local]	Red local	Confiabilidad	7
				Integridad	7
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[Internet]	Internet	[internet]	Internet	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	

Fuente: *Elaboración propia*

t. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE SOPORTES DE INFORMACIÓN_ALMACENAMIENTO ELECTRÓNICO

TABLA N° 5.21: VALORACIÓN DE SOPORTES DE INFORMACIÓN -ALMACENAMIENTO ELECTRÓNICO

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[cd]	Discos	[a_cd]	Almacenamientos en Disco Duro	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[cd]	Cederrom (CD_ROM)	[a_cd]	Almacenamiento en CD	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
[USB]	Memorias	[a_memorias]	Almacenamiento en Memorias	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[dvd]	DVR	[a_dvd]	Almacenamiento en DVD	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	

Fuente: *Elaboración propia*

u. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE SOPORTES DE INFORMACIÓN_ALMACENAMIENTO NO ELECTRÓNICO

TABLA N° 5.22: VALORACIÓN DE SOPORTES DE INFORMACIÓN -ALMACENAMIENTO NO ELECTRÓNICO

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[printed]	Material impreso	c_documentaciónpartidas	Carpetas con la documentación de cada partida(documentación)	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		c_reporteseinformes	Carpetas de reportes e informes impresos	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		c_soprtesfinancieros	Carpetas recibos caja	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	
				Trazabilidad	
		c_varios	Carpetas varias	Confiabilidad	
				Integridad	7
				Autenticidad	
				Disponibilidad	
				Trazabilidad	

Fuente: *Elaboración propia*

v. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE EQUIPAMIENTO AUXILIAR

TABLA N° 5.23: VALORACIÓN DE EQUIPAMIENTO AUXILIAR

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[printed]	Sistemas de Alimentación ininterrumpida	u_computadores	Ups computadores	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[suplly]	Suministros Esenciales	esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[Furniture]	Mobiliario	m_mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	

Fuente: *Elaboración propia*

w. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE INSTALACIONES

TABLA N° 5.24: VALORACIÓN DE INSTALACIONES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[building]	Edificio	[e_municipalidad]	Local de la Municipalidad.	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	

Fuente: *Elaboración propia*

x. VALORACIÓN CUALITATIVA Y CUANTITATIVA DE PERSONAL

TABLA N° 5.25: VALORACIÓN DE PERSONAL

Código grupo de activo MAGERIT	Nombre Grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Dimensión de Seguridad	Criterio
[ui]	Usuarios internos	[e_personal]	Personal de la recepción, área civil.	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	
[adm]	Administradores de sistemas	[a_sistemas]	Administrador de sistemas, personal de la Subgerencia de Informática y Telecomunicaciones.	Confiabilidad	
				Integridad	
				Autenticidad	
				Disponibilidad	6
				Trazabilidad	

Fuente: *Elaboración propia*

5.1.4.3. IDENTIFICACIÓN DE AMENAZAS

La valoración de amenazas se realiza teniendo en cuenta la frecuencia con la que ocurre, las dimensiones de seguridad según MAGERIT y la escala de tango porcentual de impactos en los activos.

TABLA N° 5.26: ESCALA DE RANGO DE FRECUENCIA DE AMENAZAS

Vulnerabilidad	Rango	Valor
Frecuencia muy alta	1 vez al día	100
Frecuencia alta	1 vez cada 1 semanas	70
Frecuencia media	1 vez cada 2 meses	50
Frecuencia baja	1 vez cada 6 meses	10
Frecuencia muy baja	1 vez al año	5

Fuente: *Módulo sistemas de gestión de seguridad de información*

Las dimensiones de seguridad a trabajar son las siguientes:

TABLA N° 5.27: DIMENSIONES DE SEGURIDAD SEGÚN MAGERIT

Dimensiones de Seguridad a	Identificación
Confiabilidad	C
Integridad	I
Autenticidad	A
Disponibilidad	D
Trazabilidad	T

Fuente: *Módulo sistemas de gestión de seguridad de información*

El rango porcentual es el siguiente:

TABLA N° 5.28: VALOR CUANTITATIVO SEGÚN MAGERIT

Impacto	Valor cuantitativo
Muy alto	100%
Alto	75%
Medio	50%
Bajo	20%
Muy bajo	5%

Fuente: *Módulo sistemas de gestión de seguridad de información*

En el siguiente Tabla se procede a identificar las amenazas para el inventario de activos realizado.

TABLA N° 5.29: RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO

Relación de amenazas por activo identificando su frecuencia e impacto							
Amenaza	**Activo**	**Frecuencia de la amenaza**	**Impacto para cada Dimensión de seguridad (%)**				
			[A]	**[C]**	**[I]**	**[D]**	**[T]**
[N.1] Fuego [N.2] Daños por agua	**Equipos informáticos Instalaciones**	5				100%	
[I.1] Fuego [I.2] Daños por agua	**Equipos informáticos Instalaciones**	10				100%	
[N.1] Fuego [N.2] Daños por agua	**Soporte de almacenamiento electrónico y no electrónico**	5				100%	
[I.1] Fuego [I.2] Daños por agua	**Soporte de almacenamiento electrónico y no electrónico**	5				100%	
[N.1] Fuego	**Equipamiento**	5				50%	
[N.2] Daños por agua	**Auxiliar**						
[I.1] Fuego	**Equipamiento**	5				50%	
[I.2] Daños por agua	**Auxiliar**						
[N.*] Desastres industriales	**Equipos informáticos,**	10				100%	
	Soporte de Información	5				75%	
	Equipamiento Auxiliar	5				20%	
	Instalaciones	5				100	
[I.*] Desastres industriales	**Equipos Informáticos**	10				100%	
	Soporte de Información	5				75%	
	Equipamiento Auxiliar	5				20%	
	Instalaciones	5				100%	

Amenaza	Activo	Frecuencia de la amenaza	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[I.3] Contaminación mecánica	**Equipos Informáticos**	50				75%	
	Soporte de información	5				50%	
	Equipamiento Auxiliar	5				20%	
[I.4] Contaminación electromagnética	**Router de acceso inalámbrico.**	50				100%	
[I.5] Avería de origen físico o lógico	**Software - Aplicaciones Informáticas**	50				100%	
	Equipos informáticos	10				100%	
	Soportes de Información	5				20%	
	Equipamiento Auxiliar	5				20%	
[I.6] Corte del suministro eléctrico	**Equipos Informáticos**	50				100%	
	Soporte de Información (electrónicos)	5				50%	
	Ups computadores	5				5%	
[I.7] Condiciones inadecuadas de temperatura o humedad	**Equipos Informáticos**	50				100%	
[I.8] Fallo de servicios de comunicaciones	**Redes de comunicaciones (Red inalámbrica, red local e internet)**	50				100%	
[I.9] Interrupción de otros servicios y suministros esenciales.	**Equipamiento Auxiliar**	5				5%	

Amenaza	Activo	Frecuencia de la amenaza	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[I.10] Degradación de los soportes de almacenamiento de la información.	**Soportes de Información**	5				5%	
[E.1] Errores de los usuarios Datos/Información	**Archivos de partidas**	50		100%	100%	75%	
	Archivos de usuarios	5		50%	100%	50%	
	Archivos financieros	5		100%	100%	50%	
	Archivos de Informes y certificados expedidos	10		100%	100%	50%	
	Archivo de Copias de seguridad de la información	5		100%	100%	50%	
	Datos de configuración de servidores y equipos	5		100%	100%	50%	
	Datos de Gestión de partidas	5		100%	100%	100%	
	Contraseñas de acceso de trabajadores	5		50%	50%	50%	
[E.1] Errores de los usuarios	**Claves Criptográficas**	5		100%	100%	100%	
[E.1] Errores de los usuarios Servicios	**Servicios prestados a usuarios externos bajo relación contractual (Usuarios de partidas)**	5		50%	50%	50%	
	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.	5		100%	100%	75%	
	Servicio de internet al que pueden acceder los trabajadores	10		75%	50%	50%	
	Manejo de correos electrónicos	5		50%	50%	75%	
	Servicio de almacenamiento de información en el servidor de bases de datos.	10		75%	75%	75%	
	Manejo de privilegios de acuerdo al rol dentro de la municipalidad y el lugar de donde esté ingresando.	5		100%	75%	75%	

Amenaza	Activo	Frecuencia de la amenaza	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[E.1] Errores de los usuarios **Aplicaciones**	**Servidor de aplicaciones**	5		75%	75%	100%	
	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la Municipalidad.	5		100%	100%	100%	
	Office 2010	5		75%	50%	75%	
	McAfee original con actualizaciones automáticas.	5		75%	20%	75%	
	Sistema operativo Windows 10, en su versión professional con actualizaciones automáticas activadas.	10		75%	20%	75%	
[E.1] Errores de los usuarios. **Soporte de información**	**Soportes de Información almacenamiento electrónico.**	10		50%	50%	50%	
	Soportes de Información almacenamiento no electrónico.	10		50%	50%	50%	
[E.2] Errores del administrador	**Datos/Información**	50		100%	75%	50%	
	Claves criptográficas	5		100%	75%	50%	
	Servicios	5		75%	50%	75%	
	Aplicaciones	5		100%	75%	75	
	Redes de Comunicación	10		100	75%	75%	
[E.4] Errores de configuración	**Datos de configuración de servidores y equipos**	5			100%		
[E.7] Deficiencias en la organización	**Personal de recepción, área registro civil, Subgerencia de Informática y Telecomunicaciones.**	50				75%	
	Administrador de sistemas	5				75%	
[E.8] Difusión de software dañino	**Software – Aplicaciones Informáticas**	5		50%	50%	75%	

Amenaza	Activo	Frecuencia de la amenaza	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[E.9] Errores de [re-encaminamiento]	**Servicios**	5		20%			
	Software – Aplicaciones Informáticas	5		20%			
	Redes de comunicaciones	5		20%			
[E.14] Escapes de información	**Activos esenciales**	5		100%			
	Datos / información	5		100%			
[E.15] Escapes de información	**Datos / información**	10			100%		
[E.18] Escapes de información	**Datos / información**	10					
	Aplicaciones	5				50 %	
	Soporte Información	5				20 %	
[E.19] Fugas de información	**Datos / información**	10		75%			
	Claves criptográficas	5		75%			
	Servicios	10		75%			
	Aplicaciones	10		50%			
	Personal	10		75%			
[E.20] Vulnerabilidades de los programas (software)	**Servidor de aplicaciones**	5		75%	50%	20 %	
	Gestor base de datos, aplicación el proceso de gestión de las bases de datos manejadas al interior de la Municipalidad.	10		50%	20%	75 %	
	Office 2010	5		5%	5%	5%	
	McAfee original con actualizaciones automáticas.	5		75%	20%	100 %	
	Sistema operativo Windows 7, en su versión professional con actualizaciones automáticas activadas.	10		50%	20%	75 %	

Amenaza	Activo	Frecuencia de la amenaza	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[E.21] Errores de mantenimiento / actualización de programas (software)	**Servidor de aplicaciones**	5			20%	75%	
	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la Municipalidad.	10			20%	75%	
	Office 2010	5			20%	20%	
	McAfee original con actualizaciones automáticas.	10			5%	20%	
	Sistema operativo Windows 7, en su versión profesional con actualizaciones automáticas activadas	10			50%	50%	
[E.24] Caída del sistema por agotamiento de recursos	**Servicios**	5				100%	
	Equipos Informáticos	10				100%	
	Redes de comunicaciones	5				100%	
	Equipos Informáticos	5		75%		100%	
[E.25] Pérdida de equipos - Robo	**Soporte Información**	5		20%		100%	
	Equipamiento Auxiliar	5		5%		20%	
[E.28] Indisponibilidad del personal	**Personal de la recepción, área registro civil y Subgerencia de Informática y Telecomunicaciones .**	10				75%	
	Administrador de sistemas	5				100%	
[A.5] Suplantación de la identidad del usuario	**Datos / información**	5	75%	75%	75%		
	Claves criptográficas	5	75%	75%	50%		
	Servicios	5	50%	75%	50%		
	Aplicaciones	5	20%	75%	50%		
	Redes de comunicaciones	5	20%	75%	75%		

Amenaza	Activo	Frecuencia de la amenaza	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[A.6] Abuso de privilegios de acceso	**Datos / información**	5		75%	100%	5%	
	Claves criptográficas	5		75%	50%	5%	
	Servicios	5		50%	50%	75%	
	Equipos Informáticos	50		75%	75%	75%	
	Redes de comunicaciones	10		75%	50%	75%	
[A.7] Uso no previsto	**Servicios**	5		75%	75%	75%	
	Aplicaciones	10		75%	75%	75%	
	Equipos Informáticos	50		75%	75%	75%	
	Redes de comunicaciones	10		75%	75%	75%	
	Soporte de Información	5		20%	20%	20%	
	Equipamiento Auxiliar	5		20%	20%	20%	
	Instalaciones	10		75%	50%	20%	
[A.8] Difusión de software dañino	**Aplicaciones**	5		50%	75%	75%	
[A.11] Acceso no autorizado	**Datos / información**	10		100%	75%	50%	
	Claves criptográficas	5		50%	75%	20%	
	Servicios	5		75%	50%	50%	
	Aplicaciones	10		75%	50%	50%	
	Equipos Informáticos	10		75%	20%	75%	
	Redes de comunicaciones (Red inalámbrica, red local e internet)	10		75%	20%	75%	
	Soporte de información	5		20%	20%	20%	
	Equipamiento Auxiliar	5		5%	5%	5%	
	Instalaciones	5		75%	20%	20%	
[A.13] Repudio	**Servicios**	5			50%		75%

Amenaza	Activo	Frecuencia de la amenaza	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[A.14] Interceptación de información (escucha pasiva)	**Redes de comunicaciones**	5		75%			
[A.15] Modificación deliberada de la información	**Datos / información**	5			75%		
	Claves criptográficas	5			75%		
	Servicios	5			75%		
	Aplicaciones	5			75%		
[A.18] Destrucción de información	**Datos / información**	5				100%	
	Claves criptográficas	5				100%	
	Servicios	5				100%	
	Aplicaciones	5				100%	
	Soporte de la información	5				75%	
[A.19] Divulgación de información	**Datos / información**	10		100%			
	Claves criptográficas	5		100%			
	Soporte de Información	5					
[A.22] Manipulación de programas	**Aplicaciones**	10		100%	100%	100%	
[A.23] Manipulación de los equipos	**Equipos Informáticos**	50		75%		100%	
	Soportes de Información	5		20%		20%	
	Equipamiento Auxiliar	5		5%		5%	
[A.24] Denegación de servicio	**Equipos Informáticos**	5				75%	
	Servicios	5				75%	
	Redes de Comunicación	5				75%	
[A.25] Robo	**Equipos Informáticos**	5		75%		100%	
	Soporte de Información	5		75%		20%	
[A.26] Ataque destructivo	**Equipos Informáticos**	5				100%	
	Soporte de la Información	5				50%	
	Equipamiento Auxiliar	5				50%	
	instalaciones	5				75%	

Amenaza	Activo	Frecuencia de la amenaza	Impacto para cada Dimensión de seguridad (%)				
			[A]	[C]	[I]	[D]	[T]
[A.28] Indisponibilidad del Personal	**Personal**	5				75%	
[A.29] Extorsión	**Personal**	5		75%	75%	75%	
[A.30] Ingeniería Social	**Personal**	5		75%	75%	75%	

Fuente: *Elaboración propia*

En la siguiente Tabla se muestra la síntesis de la tabla anterior identificando el impacto por cada amenaza de acuerdo a la Tabla N° 5.28: “Valor cuantitativo según Magerit”.

TABLA N° 5.30: RESUMEN DE AMENAZAS POR IMPACTO

Resumen de amenazas por impacto					
Amenaza	Impacto para cada Dimensión de seguridad (%)				
	[A]	[C]	[I]	[D]	[T]
[N.1] Fuego				83%	
[N.2] Daños por agua				83%	
[I.*] Desastres industriales				74%	
[I.3] Contaminación mecánica				48%	
[I.4] Contaminación electromagnética				100%	
[I.5] Avería de origen físico o lógico				60%	
[I.6] Corte del suministro eléctrico				52%	
[I.7] Condiciones inadecuadas de temperatura o humedad				100%	
[I.8] Fallo de servicios de comunicaciones				100%	
[I.9] Interrupción de otros servicios y suministros esenciales.				5%	
[I.10] Degradación de los soportes de almacenamiento de la información.				5%	
[E.1] Errores de los usuarios		80%	73%	67%	
[E.2] Errores del administrador		95%	70%	65%	
[E.4] Errores de configuración			100%		
[E.7] Deficiencias en la organización				75%	
[E.8] Difusión de software dañino		50%	50%	75%	
[E.9] Errores de [re-encaminamiento]		20%			
[E.14] Escapes de información		100%	100%	35%	

Resumen de amenazas por impacto					
Amenaza	Impacto para cada Dimensión de seguridad (%)				
	[A]	[C]	[I]	[D]	[T]
[E.19] Fugas de información		70%			
[E.20] Vulnerabilidades de los programas (software)		51%	23%	55%	
[E.21] Errores de mantenimiento / actualización de programas (software)			23%	48%	
[E.24] Caída del sistema por agotamiento de recursos		75%		100%	
[E.25] Pérdida de equipos -Robo		13%		60%	
[E.28] Indisponibilidad del personal				88%	
[A.5] Suplantación de la identidad del usuario	48%	75%	60%		
[A.6] Abuso de privilegios de acceso		70%	65%	47%	
[A.7] Uso no previsto		59%	56%	51%	
[A.8] Difusión de software dañino		50%	75%	75%	
[A.11] Acceso no autorizado		61%	37%	41%	
[A.13] Repudio			50%		75%
[A.14] Interceptación de información (escucha pasiva)		75%			
[A.15] Modificación deliberada de la información			75%		
[A.18] Destrucción de información				95%	
[A.19] Divulgación de información		100%			
[A.22] Manipulación de programas		100%	100%	100%	
[A.23] Manipulación de los equipos		33%		42%	
[A.24] Denegación de servicio				75%	
[A.25] Robo		75%		60%	
[A.26] Ataque destructivo				69%	
[A.28] Indisponibilidad del Personal				75%	
[A.29] Extorsión		75%	75%	75%	
[A.30] Ingeniería Social		75%	75%	75%	

Fuente: *Elaboración propia*

Además el resumen del impacto por cada dimensión de acuerdo al cuadro de calor siguiente.

TABLA N° 5.31: RESUMEN IMPACTO POR DIMENSIÓN

Impacto para cada Dimensión de seguridad (%)				
[A]	**[C]**	**[I]**	**[D]**	**[T]**
48%	67%	65%	66%	75%

Fuente: *Elaboración propia*

El cual nos muestra que de acuerdo al cuadro de calor de la tabla 5.28 en la dimensión de Autenticidad “A” se tiene un impacto **“Medio”** de amenazas, en la dimensión de Confiabilidad “C” se tiene un impacto **“Alto”** de amenazas, en la dimensión de Integridad “I” se tiene un impacto **“Alto”** de amenazas, en la dimensión de Disponibilidad “D” se tiene un impacto **“Alto”** de amenazas y por último en la dimensión de Trazabilidad “T” se tiene un impacto **“Alto”** de amenazas.

5.1.4.4. SALVAGUARDAS

En esta parte ya habiendo realizado el inventario de activos, y habiendo identificado las amenazas, se definen las salvaguardas los cuales reducen el riesgo, en este caso se tiene en cuenta las salvaguardas definidas en MAGERIT.

TABLA N° 5.32: TIPOS DE SALVAGUARDAS SEGÚN MAGERIT

Efecto	Tipo
Preventivas: reducen la probabilidad	[PR] Preventiva
	[DR] Disuasoria
	[EL] Eliminatoria
Acotan la degradación	[IM] Minimizadora
	[CR] Correctiva
	[RC] Recuperativa
Consolidan el efecto de las demás	[MN] De monitorización
	[DC] De detección
	[AW] De concienciación
	[AD] Administrativa

Fuente: *MAGERIT V3 Libro 1*

A. SALVAGUARDAS DE ACTIVOS ESENCIALES

TABLA N° 5.33: SALVAGUARDAS DE ACTIVOS ESENCIALES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[vr]	Datos vitales	[i_partidas]	Información de partidas civiles (base de datos y registro de partidas)	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.
		[i_certificados]	Información de certificados civiles	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.
		[i_normativa]	Información de normativa (Normas locales, nacionales, acuerdos, etc)	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[per]	Datos de carácter personal	[i_financiera]	Informacion del área financiera de la municipalidad	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de oncienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
[classified]	Datos clasificados	[e_s_registrador]	Ejecutable software registrador	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw]de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.
		[d_históricos]	Datos históricos de partidas	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw]de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
		[d_partidas]	Documentación de partidas tramitadas	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.

Fuente: *Elaboración propia*

B. SALVAGUARDAS DE DATOS/INFORMACIÓN

TABLA N° 5.34: SALVAGUARDAS DE DATOS/INFORMACIÓN

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[files]	Ficheros	[a_partidas]	Archivos de partidas	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.
		[a_usuarios]	Archivos de usuarios	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.
		[a_financiera]	Archivos financieros	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[files]	Ficheros	[a_informes y partidas]	Archivos de informes y partidas	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.
				[el] eliminatoria	Gestión de contraseñas.
[backup]	Copias de respaldo	[a_copias de seguridad]	Archivo de Copias de seguridad de la información	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.
[conf]	Datos de configuración	[d_configuracion_ser]	Datos de configuración de servidores y equipos	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[int]	Datos de gestión interna	[d_gestionpartidas]	Datos de Gestión de partidas civiles	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.
				[el] eliminatoria	Gestión de contraseñas.
[password]	Credenciales	[pass_usuarios]	Contraseñas de acceso de usuarios	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[rc] recuperativa	Copias de seguridad (por lo menos dos respaldos guardados en sitios seguros).
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[ad] administrativa	Puesta en marcha el plan.

Fuente: *Elaboración propia*

C. SALVAGUARDAS DE CLAVES CRIPTOGRÁFICAS

TABLA N° 5.35: CRITERIOS DE VALORACIÓN

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[encrypt]	Claves de cifra	[cc_aplicaciones_caja]	Claves de cifra de aplicaciones de caja	[pr] preventiva	Clasificación y Encriptación de la información Gestión de privilegios.
				[im] minimizadora	Detección del servicio en caso de ataque.
				[cr] correctiva	Gestión de incidentes.
				[mn] de monitorización	Registro de descargas.
				[dc] de detección	Activación de IDS y Firewall software de monitorización y escaneo, manejo de antivirus.

Fuente: *Elaboración propia*

D. SALVAGUARDAS DE SERVICIOS

TABLA N° 5.36: SALVAGUARDAS DE SERVICIOS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[ext]	A usuarios externos (bajo una relación contractual)	[s_u_externo]	Servicios prestados a usuarios externos (Usuarios partidas)	[pr] preventiva	Clasificación de la información en este caso catalogada como confidencial.
				[rc] recuperativa	Copias de seguridad.
				[aw] de concienciación	Capacitación al personal de manejo de la información.
				[ad] administrativa	Puesta en marcha del plan.
[int]	Interno (a usuarios de la propia organización)	[s_u_interno]	Servicios prestados a trabajadores tanto al interior como haciendo uso de internet.	[pr] preventiva	Clasificación de la información en este caso catalogada como confidencial.
				[rc] recuperativa	Copias de seguridad.
				[aw] de concienciación	Capacitación al personal de manejo de la información.
				[ad] administrativa	Puesta en marcha del plan.
[www]	World wide web	[s_internet]	Servicio de internet al que pueden acceder los empleados.	[mn] de monitorización	Registro de descarga.
				[pr] preventiva	Clasificación de la información en este caso catalogada como confidencial.
				[rc] recuperativa	Copias de seguridad.
				[aw] de concienciación	Capacitación al personal de manejo de la información.
				[ad] administrativa	Puesta en marcha del plan.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[email]	Correo electrónico	[s_correo]	Manejo de correos electrónicos	[mn] de monitorización	Registro de descarga.
				[pr] preventiva	Clasificación de la información en este caso catalogada como confidencial.
				[rc] recuperativa	Copias de seguridad.
				[aw] de concienciación	Capacitación al personal de manejo de la información.
				[ad] administrativa	Puesta en marcha del plan.
[file]	Almacenamiento de ficheros	[s_a_bases de datos]	Servicio de almacenamiento de información en el servidor de bases de datos.	[mn] de monitorización	Registro de descarga.
				[pr] preventiva	Clasificación de la información en este caso catalogada como confidencial.
				[rc] recuperativa	Copias de seguridad.
				[aw] de concienciación	Capacitación al personal de manejo de la información.
				[ad] administrativa	Puesta en marcha del plan.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[ipm]	Gestión de privilegios	[g_privilegios]	Manejo de privilegios de acuerdo al rol dentro de la Municipalidad.	[pr] preventiva	Clasificación de la información en este caso catalogada como confidencial.
				[rc] recuperativa	Copias de seguridad.
				[aw] de concienciación	Capacitación al personal de manejo de la información.
				[ad] administrativa	Puesta en marcha del plan.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.

Fuente: *Elaboración propia*

E. SALVAGUARDAS DE SOFTWARE-APLICACIONES INFORMÁTICAS

TABLA N° 5.37 SALVAGUARDAS DE SOFTWARE-APLICACIONES INFORMÁTICAS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[app]	Servidor de aplicaciones	[server_app]	Servidor de aplicaciones	[pr] preventiva	Clasificación de la información en este caso catalogada como confidencial.
				[rc] recuperativa	Copias de seguridad.
				[aw] de concienciación	Capacitación al personal de manejo de la información.
[dbms]	Sistema de gestión de bases de datos	[s_basededatos]	Gestor base de datos, aplicación destinada a realizar el proceso de gestión de las bases de datos manejadas al interior de la Municipalidad.	[dc] de detección	Activación de IDS y Firewall software de monitorización y escaneo, manejo de antivirus.
				[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[mn] de monitorización	Registro de descarga.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.
				[cr] correctiva	Gestión de incidentes.
[Oficce]	Ofimática	[oficce]	Office 2010	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[mn] de monitorización	Registro de descarga.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[av]	Antivirus	[antivirus]	ESSET original con actualizaciones automáticas.	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[mn] de monitorización	Registro de descarga.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.
[os]	Sistema operativo	[os_win10]	Sistema operativo Windows 10, en su versión professional con actualizaciones automáticas activadas.	[pr] preventiva	Políticas de seguridad para el personal que tiene acceso a la información - Acceso restringido
				[aw] de concienciación	Capacitación al personal de manejo de información.
				[mn] de monitorización	Registro de descarga.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.

Fuente: *Elaboración propia*

F. SALVAGUARDAS DE EQUIPOS INFORMÁTICOS

TABLA N° 5.38: SALVAGUARDAS DE EQUIPOS INFORMÁTICOS

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[host]	Grandes equipos (Servidor de bases de datos, servidores de aplicación)	[s_aplicaciones]	Servidor Aplicaciones	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.
				[im] minimizadora	Detención del servicio en caso de ataque.
				[cr] correctiva	Gestión de incidentes.
				[mn] de monitorización	Registro de descarga, registro de acceso.
				[dc] de detección	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus.
				[aw] de concienciación	Capacitación de personal en el manejo.
		[s_database]	Servidor de Base de Datos	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.
				[im] minimizadora	Detención del servicio en caso de ataque.
				[cr] correctiva	Gestión de incidentes.
				[mn] de monitorización	Registro de descarga, registro de acceso.
				[dc] de detección	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus.
				[aw] de concienciación	Capacitación de personal en el manejo.

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[mid]	Equipos medios (Equipos de trabajo conectados a través de red inalámbrica por red 802.1x)	[pc_trabajadores]	Equipos de mesa	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[dc] de detección	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[rc] recuperativa	Copias de seguridad.
				[cr] correctiva	Gestión de incidentes.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.
[pc]	Equipos que son fácilmente transportados	[pc_portatiles]	Equipos Portatiles	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[dc] de detección	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[rc] recuperativa	Copias de seguridad.
				[cr] correctiva	Gestión de incidentes.
				[el] eliminatoria	Eliminación de cuentas sin contraseña.
[print]	Equipos de impresión	[e_impresoras]	Impresoras	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[cr] correctiva	Gestión de incidentes.
[router]	Enrutadores	[r_enrutadores]	Enrutadores	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[dc] de detección	Activación de Firewall, software de monitorización y escaneo, manejo de antivirus.
				[mn] de monitorización	Registro de descarga, registro de acceso.
				[cr] correctiva	Gestión de incidentes.
				[im] minimizadora	Detención del servicio en caso de ataque.

Fuente: *Elaboración propia*

G. SALVAGUARDAS DE REDES DE COMUNICACIONES

TABLA N° 5.39: SALVAGUARDAS DE REDES DE COMUNICACIONES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[wifi]	Red inalámbrica	[r_wifi]	Red Inalámbrica	[pr] preventiva	Politicas de gestión de la seguridad, gestión de privilegios.
				[im] minimizadora	Detención del servicio en caso de ataque.
				[cr] correctiva	Gestión de incidentes.
				[dr] disuasoria	Guardias de seguridad.
[LAN]	Red local	[r_local]	Red local	[pr] preventiva	Politicas de gestión de la seguridad, gestión de privilegios.
				[im] minimizadora	Detención del servicio en caso de ataque.
				[cr] correctiva	Gestión de incidentes.
				[dr] disuasoria	Guardias de seguridad.
[Internet]	Internet	[internet]	Internet	[pr] preventiva	Politicas de gestión de la seguridad, gestión de privilegios.
				[im] minimizadora	Detención del servicio en caso de ataque.
				[cr] correctiva	Gestión de incidentes.
				[dr] disuasoria	Guardias de seguridad.

Fuente: *Elaboración propia*

H. SALVAGUARDAS DE SOPORTES DE INFORMACIÓN ALMACENAMIENTO ELECTRÓNICO

TABLA N° 5.40: SALVAGUARDAS DE SOPORTES DE INFORMACIÓN ALMACENAMIENTO ELECTRÓNICO

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[cd]	Discos	[a_cd]	Almacenamientos en Disco Duro	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.
[cd]	Cederrom (CD_ROM)	[a_cd]	Almacenamiento en CD	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.
[USB]	Memorias	[a_memorias]	Almacenamiento en Memorias	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.
[dvd]	DVR	[a_dvd]	Almacenamiento en DVD	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.

Fuente: *Elaboración propia*

I. SALVAGUARDAS DE SOPORTES DE INFORMACIÓN ALMACENAMIENTO NO ELECTRÓNICO

TABLA N° 5.41: SALVAGUARDAS DE SOPORTES DE INFORMACIÓN ALMACENAMIENTO NO ELECTRÓNICO

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[printed]	Material impreso	c_documentaciónpartidas	Carpetas con la documentación de cada partida(documentación)	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.
		c_reporteseinformes	Carpetas de reportes e informes impresos	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.
		c_soprtesfinancieros	Carpetas recibos caja	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.
		c_varios	Carpetas varios	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.

Fuente: *Elaboración propia*

J. SALVAGUARDAS DE EQUIPAMIENTO AUXILIAR

TABLA N° 5.42: SALVAGUARDAS DE EQUIPAMIENTO AUXILIAR

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[printed]	Sistemas de Alimentación ininterrumpida	u_computadores	Ups computadores	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.
[suplly]	Suministros Esenciales	esenciales	Suministros esenciales tales como: Papel, sobres, carpetas, tinta, etc.	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.
[Furniture]	Mobiliario	m_mobiliario	Mobiliario: Estantes, armarios, escritorios, archivadores, etc.	[pr] preventiva	Políticas de gestión de la seguridad, gestión de privilegios.
				[aw] de concienciación	Capacitación de personal en el manejo.
				[ad] administrativa	Puesta en marcha del plan.
				[dr] disuasoria	Guardias de seguridad.

Fuente: *Elaboración propia*

K. SALVAGUARDAS DE INSTALACIONES

TABLA N° 5.43: SALVAGUARDAS DE INSTALACIONES

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[building]	Edificio	[E_Municipalidad]	Edificio de la Municipalidad.	[DR] Disuasoria	Guardias de seguridad.
				[DC] De detección	Detección de incendios.

Fuente: *Elaboración propia*

L. SALVAGUARDAS DE PERSONAL

TABLA N° 5.44: SALVAGUARDAS DE PERSONAL

Código grupo de activo MAGERIT	Nombre grupo de activo MAGERIT	Código activo de acuerdo a la organización	Nombre de activo de acuerdo a la organización	Tipo de protección	Descripción Salvaguarda
[ui]	Usuarios internos	[E_personal]	Personal de recepción, área civil y la Subgerencia de Informática y Telecomunicaciones.	[AW] De concienciación	Capacitación de personal en el manejo, cursos de capacitación y entrenamiento.
				[AD] Administrativa	Puesta en marcha del plan.
[adm]	Administradores de sistemas	[A_sistemas]	Administrador de sistemas	[AW] De concienciación	Capacitación de personal en el manejo, cursos de capacitación y entrenamiento.
				[AD] Administrativa	Puesta en marcha del plan.

Fuente: *Elaboración propia*

5.1.5. INFORME DE CALIFICACIÓN DE RIESGOS

Después de realizar todos los pasos de análisis de riesgo de MAGERIT se puede observar que existen activos de la Subgerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia que presentan riesgos catalogados como críticos y su probabilidad de frecuencia es alta tal es el caso de los equipos informáticos, datos e información, este riesgo puede generar perdida de la información, divulgación de la información confidencial, daño en equipos y servidor, manipulación y daños en la base de datos, propagación de virus y el cese de actividades.

Referente a los activos de redes de comunicaciones (routers e acceso inalámbrico), software y aplicaciones informáticas también se puede decir que el riesgo es catalogado como crítico, el cual puede ser causado por errores de usuarios y de administrador; de allí la importancia de establecer políticas de seguridad encaminadas a proteger los activos de la organización y minimizar los riesgos para que en caso de presentarse el impacto sea mínimo.

Condiciones inadecuadas de temperatura y humedad, corte del suministro eléctrico, avería de orden físico, lógico y amenazas como manipulación no autorizada de equipos puede ocasionar daños en las aplicaciones, en el servidor y los equipos que pueden originar perdida de información vital, y retraso.

Deficiencias en la organización por parte del personal, abuso de privilegios de acceso y uso no previsto son amenazas que se deben de tener en cuenta ya que de acuerdo al análisis de riesgos están catalogadas como importantes y pueden ocasionar grandes daños.

Por otra parte, los impactos generados por los desastres naturales como fuego e inundaciones son críticos en el caso de que se llegasen a presentar afortunadamente la posibilidad de que ocurra es muy baja, esto no quiere decir que no se deba de tener en cuenta al contrario también se debe considerar como una posibilidad y se debe establecer políticas y medidas de seguridad encaminadas a minimizar cada riesgo.

En este orden de ideas los activos con mayor necesidad de ser protegidos son: Equipos informáticos, datos e información, software y aplicaciones, redes de comunicación puesto que son vulnerables y blanco fácil de los atacantes.

De que se los debe proteger: Del uso no previsto, del abuso de privilegios, fallos en los servicios de comunicaciones, errores de usuarios y administradores del sistema, condiciones inadecuadas de seguridad, contaminación electromagnética y mecánica etc.

Como se los debe proteger: Definiendo e implementando políticas de seguridad que permitan capacitar al usuario y al administrador en el manejo y clasificación de la información, gestión de contraseñas, control de acceso, implementación de equipos y software que permitan mejorar la seguridad, seguridad física y lógica, actualizaciones permanentes del software, elaboración permanente de backups.

CAPÍTULO VI
CONSTRUCCIÓN DE LA SOLUCIÓN

6.1. CONSTRUCCIÓN

6.1.1. DECLARACIÓN DE APLICABILIDAD

En el presente capítulo habiendo ya realizado el proceso de análisis de riesgos por la metodología MAGERIT, en el cual se identificaron los activos de información críticos y los riesgos a los que se encuentran expuestos actualmente con la finalidad de determinar las estrategias a seguir para su mitigación.

Sin embargo, estas estrategias no definen explícitamente las acciones a realizar puesto que son generales. Es por este motivo que la norma ISO/IEC 27002:2013 exige que se desarrolle el documento denominado “Declaración de aplicabilidad” en el que se detalla la selección de los controles a implementarse para mitigar los riesgos identificados. Este documento debe presentar la selección de los controles incluidos en el Anexo 9, detallando qué controles ya se encuentran implementados, cuáles se debe implementar (detallando de manera general las pautas que se debe tener en cuenta en su implementación) y cuáles de ellos no se implementarán (detallando el motivo de su exclusión).

En la presente Declaración de aplicabilidad se presenta una explicación contextualizada de los controles presentados en la norma en relación a su aplicación en la Municipalidad Distrital de Independencia. Para ello se ha hecho uso del detalle de los controles que se encuentra en la ISO/IEC 27002:2013.

La declaración de aplicabilidad desarrollada como entregable final del proyecto se encuentra en la sección “Anexo 9:

Declaración de Aplicabilidad” en el documento de anexos que acompaña al presente proyecto.

6.1.2. POLIÍTICAS Y OBJETIVOS DE SEGURIDAD DE LA SUBGERENICA DE INFORMÁTICA Y TELECOMUNICACIONES

En el Anexo 9 se observa la descripción de controles a implementar de acuerdo a la ISO/IEC 27002:2013. La cual contiene 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES, además como producto final de la tesis en el Anexo 10 se tiene la Declaración de aplicabilidad junto con sus guías de implementación en el Anexo 11.

CAPÍTULO VII
IMPLEMENTACIÓN

7.1. MONITOREO Y EVALUACIÓN DE LA SOLUCIÓN

7.1.1. ELEMENTOS DEL MONITOREO Y EVALUACIÓN

Las acciones de monitoreo se realizarán más eficientemente cuando las actividades, recursos y activos relacionados se gestionen como un proceso, para ello se debe tener identificado la interacción entre los mismos. Además, se deberá tener en cuenta las medidas preventivas a tomar y llevar un registro de los mismos. Para llevar un control de todo esto, se propone realizarlo a través del ciclo de Deming (de Edwards Deming), también conocido como círculo PDCA (del inglés plan-do-check-act, = planificar-hacer-verificar-actuar). Es una estrategia de mejora continua de la calidad en cuatro pasos, que tienen por función:

a. Toma de datos y registro en las Tablas y anexos respectivos.
b. Contrastación de los datos contra el nivel esperado de cumplimiento
c. Decisión respecto de las acciones correctivas o de retroalimentación necesarias de acuerdo a la información obtenida
d. Implementación de las acciones correctivas o de retroalimentación.

GRÁFICO 7.1: CICLO DE DEMING

Fuente: *http://jessilogistic.blogspot.pe/2010/12/ciclo-deming.html*

7.1.2. PLAN DE MONITOREO Y EVALUACIÓN

El Plan de monitoreo y evaluación debe necesariamente dar respuesta al menos a las siguientes interrogantes: ¿Cómo se va a recoger la información?, ¿Quién va a recogerla?, ¿Cuándo se va a obtener?, ¿Cómo se va a analizar la información recogida?, ¿Quién la va a analizar?, ¿Cuándo se va a hacer el análisis?, ¿Quién va a recibir los resultados?, ¿En qué formato se van a distribuir?

7.2. BITÁCORA Y PUESTA A PUNTO

Para el registro de las observaciones, ideas, datos, avances y obstáculos en el desarrollo de las actividades que se llevan a cabo durante el proyecto, se empleó la siguiente Tabla para consolidar las condiciones bajo las cuales se desarrolló el proyecto.

TABLA N° 7.1: BITÁCORA PARA EL DESARROLLO DEL PROYECTO

Fecha	Etapa	Actividad	Observación
Del 01/01/2017 Al 30/04/2017	Análisis	Identificar fuentes de información	Se realizó de acuerdo a lo planificado
		Recopilar información	Se realizó de acuerdo a lo planificado
		Organizar información	Se realizó de acuerdo a lo planificado
		Analizar la información	Se realizó de acuerdo a lo planificado
Del 01/05/2017 Al 31/10/2017	Diseño	Plantear controles de seguridad	Se realizó de acuerdo a lo planificado
		Identificar Salvaguardas	Se realizó de acuerdo a lo planificado
	Construcción	Gestión de Riesgos	Se realizó de acuerdo a lo planificado
		Establecer la Declaración de aplicabilidad	Se realizó de acuerdo a lo planificado

Fuente: *Elaboración propia*

Una vez realizada la propuesta de mejora para el Sistema de seguridad de la Información, la puesta en operatividad dependerá de la adaptación al cambio de los actores principales.

CAPÍTULO VIII
RESULTADOS

Al finalizar la aplicación de nuestros instrumentos para la recolección de información y nuestras herramientas en el procesamiento de la misma, se pudo evidenciar por medio de los resultados la realidad que vive la Sub gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia en cuanto refiere al tema de seguridad de la información.

La muestra que se trabajo está dividida en la Sub Gerencia de Informática y Telecomunicaciones y el Área de Registro Civil, la cual nos servirá de estudio piloto para evidenciar la influencia de la Subgerencia de Informática y Telecomunicaciones con toda la Municipalidad. Además, se realizaron entrevistas al jefe de la Subgerencia de Informática y Telecomunicaciones y a la jefa del área de Registro Civil.

Además, los resultados van de acorde al planteamiento de nuestros objetivos los cuales se plasman a continuación:

- Resultado 1: de acuerdo con lo planteado en nuestro objetivo 1 se realizó el diagnóstico de la situación actual y en base a ello se desarrolló el ANEXO 9: que es la “DESCRIPCIÓN DE CONTROLES ISO/IEC 27002:2013 APLICADOS A LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA”.
- Resultado 2: para el resultado 2 se elaboró los “DIAGRAMAS DE PROCESOS DE NEGOCIO BPMN” el cual está en el Anexo 1, con el fin de poder obtener el mapa de riesgos en base a la Relación de amenazas por activo, e identificando su frecuencia e impacto
- Resultado 3: para este resultado se procedió a la identificar y la valorización de los activos de información de los procesos de negocio que se identificaron en el resultado anterior el cual se detalla en el

punto 5.1.4.2 VALORIZACIÓN CUALITATIVA Y CUANTITATIVA DE LOS ACTIVOS

- Resultado 4: para el resultado 4 en base a la identificación y valoración de los activos se pasó a evaluar los riesgos a los cuales están expuestos los activos identificados esto se plasmó en la TABLA N° 5.29: RELACIÓN DE AMENAZAS POR ACTIVO IDENTIFICANDO SU FRECUENCIA E IMPACTO
- Resultado 5: para este resultado tuvimos como objetivo la selección de controles y salvaguardas que nos permitan el tratamiento de los riesgos identificados por activo especificado en la TABLA N° 5.30: TIPOS DE SALVAGUARDAS SEGÚN MAGERIT, partiendo de esta tabla nacen las políticas de seguridad.
- Resultado 6 y 7: para los objetivos 6 y 7 planteados se obtuvo como resultados la “DECLARACIÓN DE APLICABILIDAD” y las “GUÍAS DE IMPLEMENTACIÓN” las cuales están especificadas en el Anexo 10 y 11.

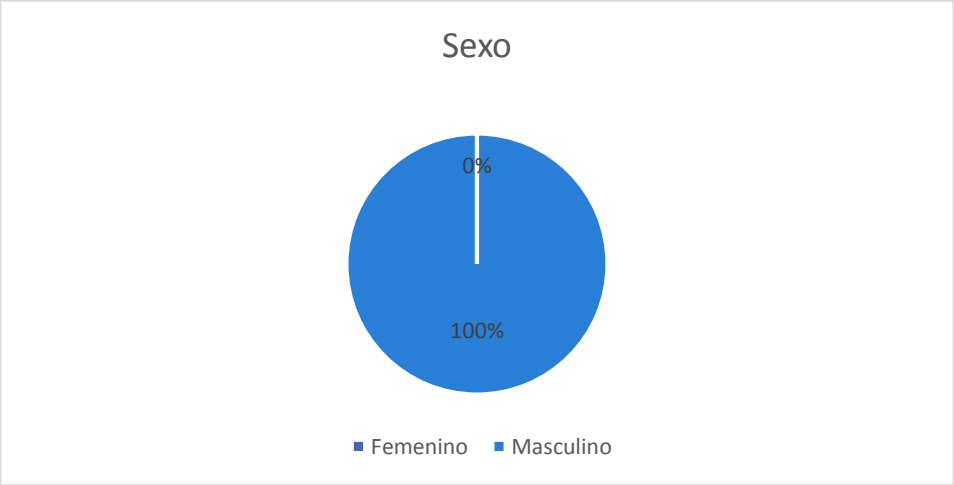
Del mismo modo mostramos de manera detallada los resultados obtenidos al procesar la información:

8.1. SUB GERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES, DESCRIPCIÓN DE RESULTADOS

Datos obtenidos de las encuestas realizadas a los trabajadores de la Sub Gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia. Modelo de encuesta, **(Ver Anexo 3)**.

1. En la pregunta 1, notamos que del 100% de nuestra muestra encuestada el 100% fueron varones y el 0% restante fueron mujeres. Lo cual nos demuestra que en la Subgerencia de informática y telecomunicaciones trabajan todos del sexo masculino.

GRÁFICO N° 8.1: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES.

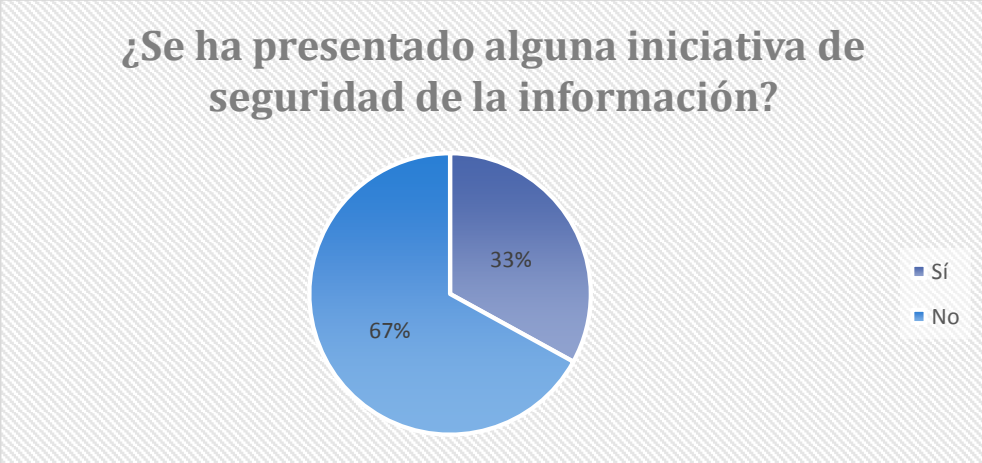


Fuente: Elaboración propia.

2. En la pregunta 2, notamos que el 100% de los encuestados nos indican que la Subgerencia de Informática y Telecomunicaciones se encuentra involucrada con 11 a 15 áreas de la Municipalidad. Lo cual nos indican que la Subgerencia se encuentra muy involucrada con la mayoría de las áreas de la Municipalidad.

3. En la pregunta 3, notamos que del 100% de nuestra muestra encuestada el 67% manifiesta que no se ha presentado alguna iniciativa de seguridad de información. Lo cual nos indica que no se ha tomado en consideración este tema tan importante para toda organización que implica la seguridad de su activo más importante como lo es la información.

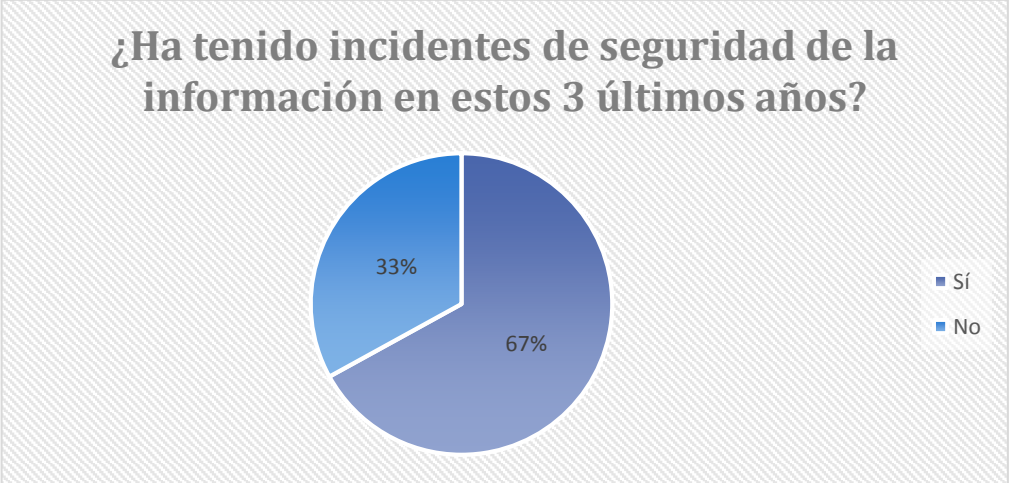
GRÁFICO N° 8.2: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



Fuente: Elaboración propia.

4. En la pregunta 4, notamos que del 100% de nuestra muestra encuestada el 67% manifiesta que no se ha presentado alguna iniciativa de tratamiento de riesgo. Lo cual nos indica que no se ha tomado en consideración este tema tan importante para toda organización que implica la seguridad de su activo más importante como lo es la información
5. En la pregunta 5, el 67% de los encuestados manifiesta que en los 3 últimos años si se han reportado incidentes sobre seguridad de la información, mientras que el 33% niega que se hayan reportado dichos casos. Lo cual nos refuerza los resultados de la pregunta 3 es decir al no tomar importancia sobre el tema de seguridad de la información tampoco se presentaron iniciativas para la protección de la misma.

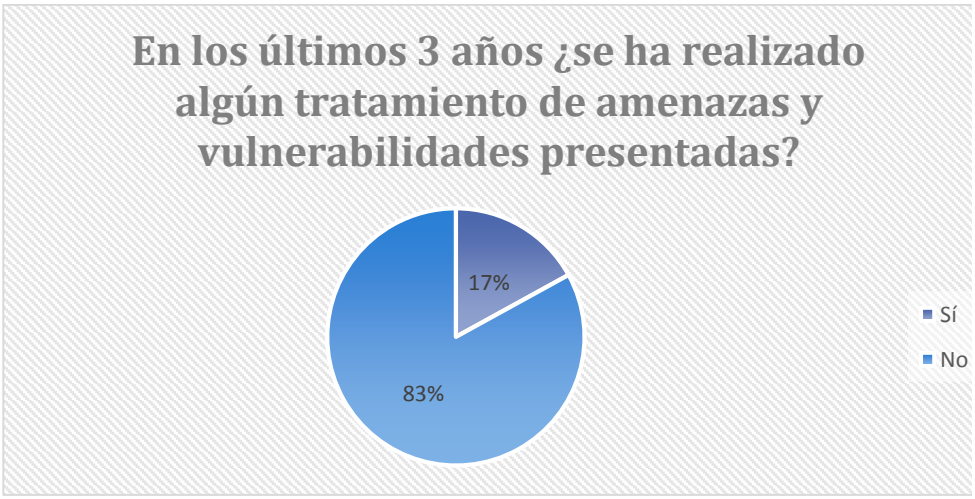
GRÁFICO N° 8.3: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



Fuente: Elaboración propia.

6. En la pregunta 6, el 83% de los encuestados manifiesta que en los últimos 3 años no se ha realizado ningún tratamiento de amenazas y vulnerabilidades, mientras que el 17% restante afirma que si se ha realizado. En esta parte de los resultados observamos que los encuestados manifiestan no haber realizado ningún tratamiento sobre los riesgos del área que maneja la mayor cantidad de datos importantes como lo es la Subgerencia de Informática y Telecomunicaciones, lo que cual resulta de gran preocupación puesto que estos que encontraría expuestos a amenazas y vulnerabilidades.

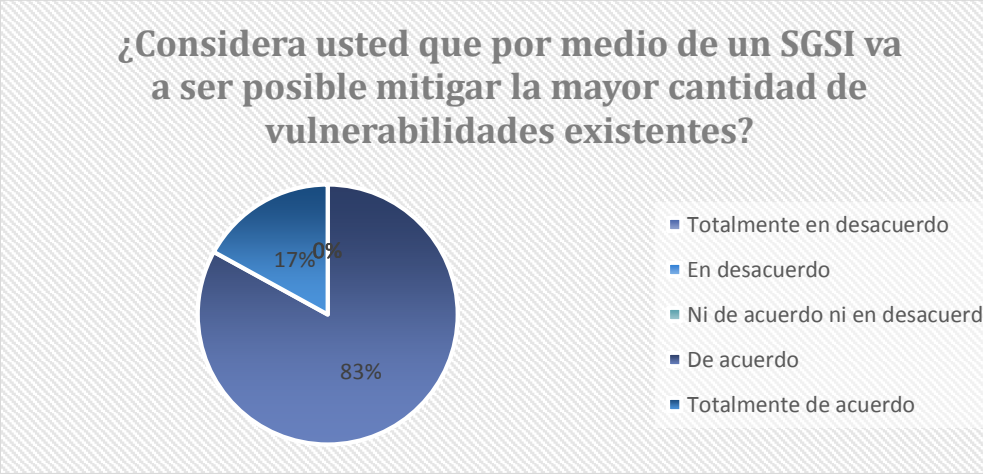
GRÁFICO N° 8.4: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



Fuente: Elaboración propia.

7. En la pregunta 7, el 83% de los encuestados afirma que se encuentra de acuerdo y el 17% restante está totalmente de acuerdo en que por medio de un SGSI va a ser posible mitigar la mayor cantidad de vulnerabilidades existentes. De los resultados obtenidos en la presente pregunta observamos que los encuestados apoyan la idea de la implementación de un Sistema de Gestión de Seguridad de la Información el cual favorecerá los procesos de la Subgerencia de Informática y Telecomunicaciones; implementados políticas de seguridad y todos los controles adecuados sobre la confidencialidad, integridad y disponibilidad de la información, para proteger la información de las partes interesadas que incluye usuarios, trabajadores y la sociedad en general.

GRÁFICO N° 8.5: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



Fuente: Elaboración propia.

8. En la pregunta 8, el 83% de los encuestados afirma que no se tiene definida una política para la realización de copias de seguridad de datos, mientras que el 17% afirma que si se han reportado dichos casos.

9. En la pregunta 9, el 83% de los encuestados manifiesta que no se tiene definida una política de restauración de los sistemas en caso de ataques informáticos, mientras que el 17% restante manifiesta que si se tiene definida dichas políticas. En esta parte de la encuesta observamos que se encuentra expuesto diariamente a riesgos como es el caso de la restauración de sistemas en caso de ataques informáticos que puedan ocurrir.

10. En la pregunta 10, el 100% de los encuestados afirma que recomendaría adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información. Esta pregunta nos permite ver que las encuestas manifiestan que se deberían adoptar políticas en cuanto al tema de protección de la información.

GRÁFICO N° 8.6: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES

Fuente: Elaboración propia.

11. En la pregunta 11, el 100% de los encuestados afirma que no se ha establecido algún tipo de organización interna dentro de la Sub Gerencia orientada a la seguridad de la información. La organización interna que debe existir dentro de la Sub Gerencia para la protección de la información.

12. En la pregunta 12, el 83% de los encuestados afirma que, si se ha permitido el acceso a la información sólo a personas debidamente autorizadas, mientras que el 17% afirma que si se han tenido casos en los que personas ajenas han tenido acceso a la información.

13. En la pregunta 13, el 67% de los encuestados afirma que, si se ha realizado la gestión de altas y bajas en el registro de usuarios, mientras que el 33% afirma que no se ha realizado dichos procedimientos.

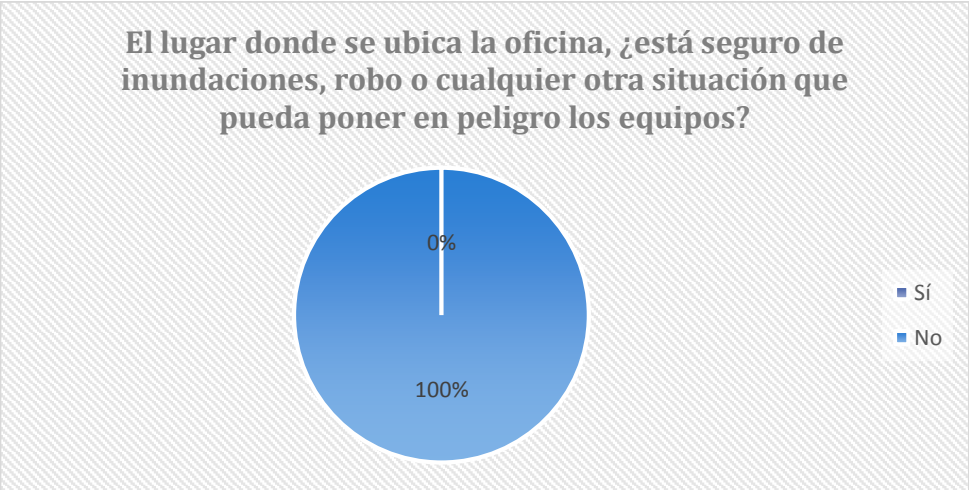
14. En la pregunta 14, el 100% de los encuestados afirma que no se ha realizado la gestión de acceso con privilegios por usuario. En esta parte de la encuesta realizada observamos de que no se tiene en consideración el tema de la gestión de privilegios de usuarios los

cuales deben ser distintos de acuerdo al tipo de cargo y acceso que requieran los mismos.

15. En la pregunta 15, el 67% de los encuestados afirma que el cambio de contraseñas a su cargo se ha realizado en un periodo de más de 1 año, mientras que el 33% de los encuestados afirma que lo ha realizado entre 6 meses y 1 año. El caso del cambio de contraseñas que deben ser actualizadas en un tiempo determinado para su mayor protección.

16. En la pregunta 16, el 100% de los encuestados afirma que no se siente seguro ante los riesgos que pueda sufrir en los ambientes de trabajo, ya sea robo o cualquier otra situación que pueda poner en peligro los equipos de información. El caso de infraestructura si bien es cierto la, municipalidad no cuenta con una infraestructura para la protección de datos se deben hacer planes para poder contrarrestare de alguna manera este problema.

GRÁFICO N° 8.7: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



Fuente: Elaboración propia.

17. En la pregunta 17, el 83% de los encuestados afirma que el medio físico donde se labora no son confiables, mientras que el 17% afirma que si lo son.

18. En la pregunta 18, el 100% de los encuestados manifiesta que no existe lugar suficiente para la documentación y los equipos. El caso del espacio en el que se encuentran los equipos y demás materiales que contienen la información.

19. En la pregunta 19, el 100% de los encuestados manifiesta que dentro del Área existen materiales que puedan ser inflamables o causar algún daño sobre la documentación o los equipos. Lo cual nos permite observar que son aplicables controles de seguridad de la información en cuanto a infraestructura.

20. En la pregunta 20, el 100% de los encuestados afirma que no se cuenta con una salida de emergencia. En esta parte de la encuesta realizada reforzamos la idea de que no se tiene en consideración el tema de seguridad de la información con la aplicación de controles necesarios para su implementación que permiten reducir riesgos constantes a los que se encuentra expuesto diariamente.

21. En la pregunta 21, el 67% de los encuestados afirma que los equipos si cuentan con un regulador, mientras que el 33% afirma que no se cuentan con dichos reguladores.

22. En la pregunta 22, el 100% de los encuestados afirma que los cables no están dentro de paneles y canaletas eléctricas. Esta parte de la encuesta nos permite reforzar la aplicación de controles de seguridad de la información que son necesarios.

23. En la pregunta 23, el 83% de los encuestados afirma que la institución no ha realizado auditorias en los sistemas de información, mientras que el 17% afirma que si se ha realizado.

24. En la pregunta 24, el 100% de los encuestados afirma que el cableado no se encuentra correctamente instalado.

25. En la pregunta 25, el 100% de los encuestados afirma que no se cuenta con pozo a tierra.

26. En la pregunta 26, el 50% de los encuestados afirma que se cuenta con mecanismos de seguridad asociados a servicios en red, mientras

que el 50% de los encuestados niega que si se cuenten con dichos mecanismos.

27. En la pregunta 27, el 83% de los encuestados afirma que se ha realizado revisiones técnicas tras efectuar cambios en los sistemas, mientras que el 17% niega que se hayan realizado dichas revisiones.

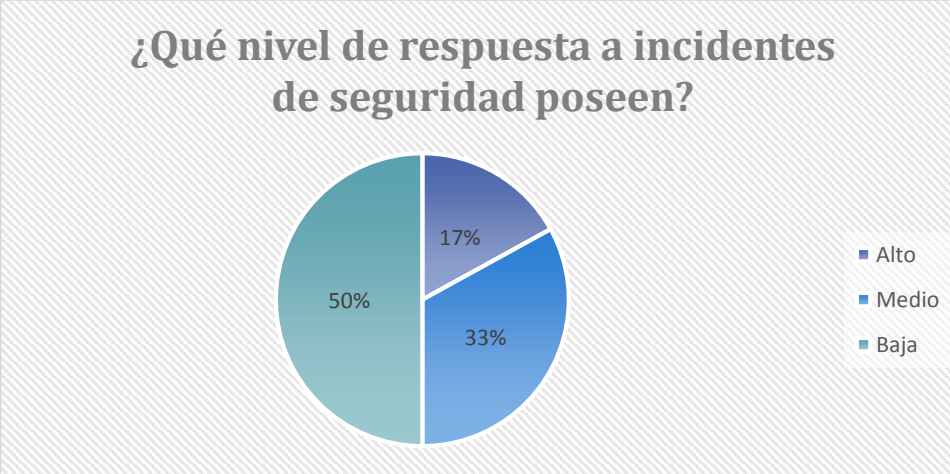
28. En la pregunta 28, el 100% de los encuestados afirma que no se tiene alguna especificación en cuanto a seguridad, de la línea otorgada por empresas privadas.

29. En la pregunta 29, el 100% de los encuestados manifiesta que la instalación eléctrica de la Sub Gerencia no es independiente de otras instalaciones. Esto es un peligro si nos referimos a seguridad de la información, implica que en cualquier momento se tengan problemas continuos de energía y junto con estos los equipos puedan ser dañados.

30. En la pregunta 30, el 50% de los encuestados manifiesta que en más de 1 año se ha dado mantenimiento a las instalaciones y suministros de energía, el 33% de las encuestas afirma que entre 6 meses y 1 año si se ha realizado dichos mantenimientos y el 17 % afirma que dicho mantenimiento se ha realizado entre 2 y 6 meses.

31. En la pregunta 31, el 50% de los encuestados manifiesta que poseen un nivel bajo de respuesta a incidentes de seguridad, el 33% manifiesta que su nivel de respuesta es medio y solo el 17% afirma que tienen un nivel alto de respuesta.

GRÁFICO N° 8.8: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



Fuente: Elaboración propia.

32. En la pregunta 32, el 100% de los encuestados afirma que si se han identificado puntos débiles de seguridad dentro de la Sub Gerencia.

33. En la pregunta 33, el 100% de los encuestados afirma que los sistemas operativos utilizados no son de uso gratuito. Entonces nosotros consideramos que deben tener en cuenta que sistemas operativos son de uso gratuito ya que este puede traer consigo una vulnerabilidad del mismo, es el caso de licencias de sistemas operativos los cuales deben estar vigentes.

34. En la pregunta 34, el 83% de los encuestados afirma que los activos de información no fueron manipulados o modificados por una entidad externa, mientras que el 17% afirma que si lo fueron. La manipulación de la información los encuestados afirmaron en su mayoría que no se han reportado incidentes de este caso, pero existe un porcentaje bajo que afirma que si se reportó dichos casos los cual genera la duda de la veracidad de la información brindada.

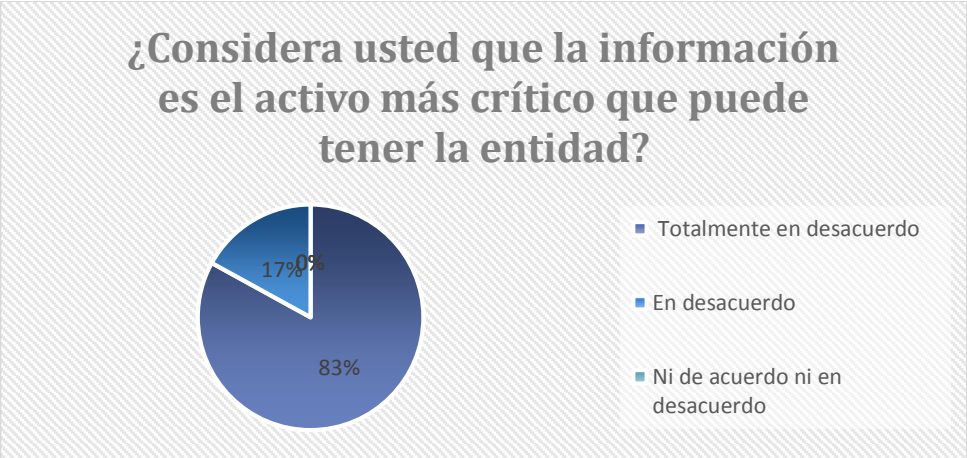
35. En la pregunta 35, el 50% de los encuestados afirma que no se ha podido tener acceso a la información en tiempo real y el 33% afirma que fueron por problemas de red, otro 33% afirma que fue por

problemas de energía eléctrica y por último el otro 33% restante afirmo que fueron por problemas con los equipos informáticos, mientras que el 50% restante afirma que si ha podido tener acceso. El acceso a la información que debe ser todo el tiempo, pero los encuestados manifiestan lo contrario.

36. En la pregunta 36, si su respuesta es negativa en la pregunta 35, el 33% de los encuestados manifestaron que presentaron problemas de red, el 33% presentaron problemas de energía eléctrica, el 33% presentaron problemas con los sistemas y el 33% presentaron problemas con los equipos informáticos. Esta pregunta nos permite observar que han existido problemas para el acceso a la información por diversos motivos informáticos y para el tema de seguridad de la información.

37. En la pregunta 37, el 83% de los encuestados afirma estar de acuerdo en que la información es el activo más crítico que puede tener la entidad, mientras que el 17% afirma que está totalmente de acuerdo.

GRÁFICO N° 8.-9: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



Fuente: Elaboración propia.

38. En la pregunta 38, el 100% de los encuestados afirma que al diseñar un Sistema de Gestión de Seguridad de la información va a ayudar a

gestionar la información y los recursos informáticos de manera óptima y segura.

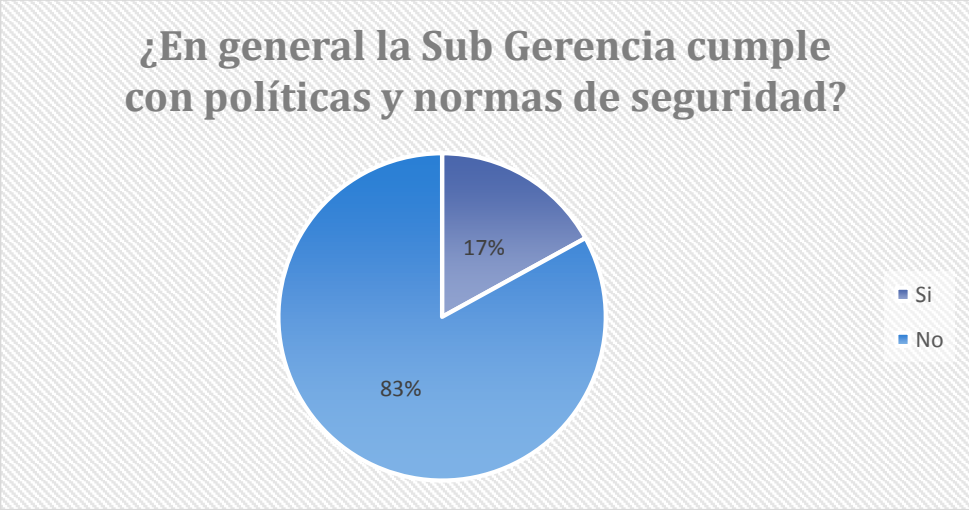
39. En la pregunta 39, el 67% de los encuestados manifiesta que no han recibido alguna capacitación en cuanto a seguridad de la información, mientras que el 33% afirma que si lo fueron. La capacitación permanente que deben tener los colaboradores que trabajan en la Subgerencia de Informática y Telecomunicaciones.

40. En la pregunta 40, el 67% de los encuestados manifiesta que cada 6 meses y 1 año se realizan un mantenimiento preventivo al hardware, el 16.5% manifiesta que cada 2 a 6 meses y el 16.5% restante afirma que lo realizan entre 1 y 2 meses. El mantenimiento de hardware que debe ser realizado permanentemente al contrario los encuestados manifiestan que esta se realiza cada año.

41. En la pregunta 41, el 50% de los encuestados afirma que se realiza mantenimiento preventivo al software, mientras que el 50% afirma realizan mantenimiento correctivo. En esta parte de la encuesta observamos que si se viene realizando mantenimientos preventivos y correctivos a los equipos de la Subgerencia.

42. En la pregunta 42, el 83% de los encuestados afirma que en general la Sub Gerencia no cumple con políticas y normas de seguridad, mientras que el 17% afirma que si los cumplen. En esta parte de la encuesta observamos que el cumplimiento de políticas y normas de seguridad, los encuestados manifiestan en su mayoría que actualmente no se cumplen. Tabla de resultados (Ver Anexo 8).

GRÁFICO N° 8.10: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



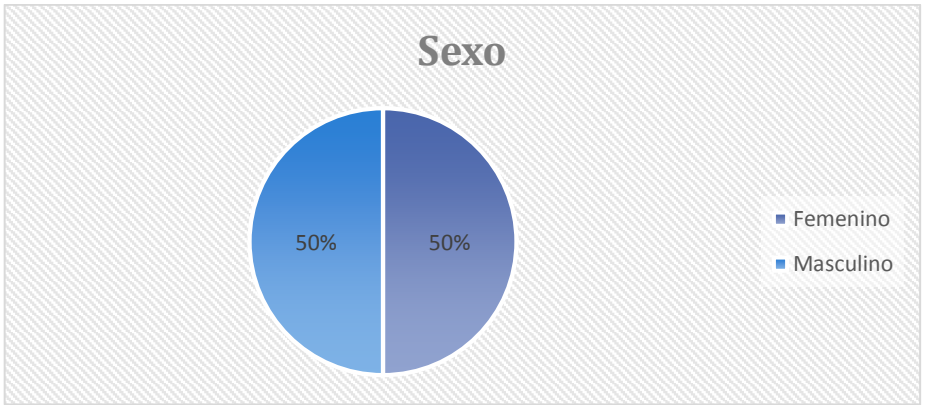
Fuente: Elaboración propia.

8.2. ÁREA DE REGISTRO CIVIL, DESCRIPCIÓN DE RESULTADOS

Datos obtenidos de las encuestas realizadas a los trabajadores del Área de Registro Civil de la Municipalidad Distrital de Independencia. Modelo de encuesta, **(Ver Anexo 3)**.

1. En la pregunta 1, el 50% de los encuestados son mujeres, mientras que el 50% son varones. Lo cual nos indica que la pluralidad de sexo es equitativa en esta área.

GRÁFICO N° 8.11: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES



Fuente: Elaboración propia.

2. En la pregunta 2, el 100% de los encuestados afirma que apaga los equipos informáticos debidamente después de utilizarlos. Lo cual nos indica que existe una orientación de protección de datos en esta área.
3. En la pregunta 3, el 75% de los encuestados afirma apaga los equipos haciendo clic en el botón de apagado del menú del sistema operativo, mientras que el 25% afirma lo apaga manteniendo presionando el botón de apagado del CPU. Lo cual nos indica que existe una orientación de protección de datos en esta área, pero aun así existe un pequeño porcentaje que manifiesta lo contario
4. En la pregunta 4, el 75% de los encuestados manifiesta que no se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro del área frente a cualquier desastre natural o humano, mientras que el 25% afirma que si se encuentra seguro. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que no se encuentran seguros en los ambientes en los cuales se encuentran laborando.

5. En la pregunta 5, el 75% de los encuestados manifiesta que no ha observado algún extinguidor cerca de los equipos informático, mientras que el 25% afirma que si han observado. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que no observan algún extintor en caso de ocurrencia de algún incidente.
6. En la pregunta 6, el 100% de los encuestados afirma que, si han manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU para hacerlos funcionar. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que han manipulado la entrada de corriente del CPU.
7. En la pregunta 7, el 50% de los encuestados afirma estar de acuerdo en que se siente responsable con el equipo informático que usa o utilizará en algún momento dentro del área, mientras que el 50% está ni de acuerdo ni en desacuerdo. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que la mitad de ellos sientes responsabilidad en cuanto al uso de su equipo informático lo cual implica en cuidado que tienen con los mismos.
8. En la pregunta 8, el 75% de los encuestados afirma que hace usted uso de los antivirus en los equipos informáticos, cuando ingresa o saca información en algún dispositivo de almacenamiento, mientras que el 25% restante afirma hacer uso solo a veces. En esta parte de la encuesta comprobamos la inexistencia de

información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que hacen uso del antivirus.

9. En la pregunta 9, el 75% de los encuestados afirma hacer uso de los antivirus cuando detecta un virus en la computadora que se le proporciona, mientras que el 25% restante activa el antivirus, detecta los virus y los elimina. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan la manera en la que hacen uso del antivirus.

10. En la pregunta 10, el 75% de los encuestados afirma que anualmente la Sub Gerencia de Informática y Telecomunicaciones cambia o actualizan la versión del antivirus, mientras que el 25% afirma que nunca lo hacen. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que anualmente cambian el antivirus.

11. En la pregunta 11, el 75% de los encuestados afirma que los problemas más frecuentes que solicita la atención del área de informática son por problemas con los equipos informáticos, mientras que el 25% afirma que son por problemas de red. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que presentan problemas con la atención de la Subgerencia de Informática y Telecomunicaciones.

12. En la pregunta 12, el 50% de los encuestados afirma hacer uso del SISTEMA OREC, mientras que el 50% no lo hacen. En esta parte de la encuesta comprobamos la inexistencia de información de

seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que la mitad de ellos hacen uso del sistema OREC que concierne a la oficina de RENIEC la cual la data se maneja directamente a dicho sistema mediante un servidor que se encuentra en la Subgerencia de Informática y Telecomunicaciones.

13. En la pregunta 13, el 100% de los encuestados afirma que siempre tiene un acceso a la información que proporciona la OREC. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que todos requieren de alguna u otra forma de la información brindada por el sistema.

14. En la pregunta 14, el 100% de los encuestados afirma que su clave de acceso a la OREC es diferente de su nombre, apellido, fecha de nacimiento o nombre de algún familiar. Los encuestados manifiestan la manera en que se encuentra su clave de acceso el cual es de suma importancia para la protección de la información.

15. En la pregunta 15, el 100% de los encuestados afirma que ningún familiar o amigo conoce su clave de acceso. Los encuestados manifiestan que la clave de acceso la cual poseen solo ellos la manejan.

16. En la pregunta 16, el 100% de los encuestados afirma que cambia su clave de acceso cada 30 días. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que cambian su clave de acceso cada mes por pedido de la oficina de RENIEC al contratarlo en la municipalidad no existe ninguna política con respecto a ese tema.

17. En la pregunta 17, el 50% de los encuestados afirma que el acceso al Sistema OREC dentro de la Municipalidad es más lenta dentro de la municipalidad que fuera de ella y el 50% de los encuestados afirma que es igual en ambos lugares. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que el acceso de información es lenta en comparación a otros sitios.

18. En la pregunta 18, el 100% de los encuestados afirma que no recibieron capacitación acerca de Seguridad de la Información en la Municipalidad. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que no han recibido ninguna capacitación con respecto al tema de seguridad de la información en la municipalidad.

GRÁFICO N° 8.12: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES

Fuente: Elaboración propia.

19. En la pregunta 19, el 100% de los encuestados afirma que Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que desearían tener mayor conocimiento con respecto al tema de seguridad de la información.

20. En la pregunta 20, el 75% de los encuestados afirma que le interesaría conocer más acerca del tema de Seguridad de la Información, a través de charlas y conferencias, mientras que el 25% afirma que le gustaría recibir folletos y boletines. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que se le informara más con respecto al tema de seguridad e la información por diferentes medios.

21. En la pregunta 21, el 100% de los encuestados afirma que el área de Registro civil no cumple con políticas y normas de seguridad. En esta parte de la encuesta comprobamos la inexistencia de información de seguridad de la información y de la aplicación de controles necesarios para su aplicación por ejemplo en esta parte los encuestados manifiestan que el general el Área de Registro Civil no cumple con políticas y normas de seguridad.

GRÁFICO N° 8.13: RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DEL ÁREA DE REGISTRO CIVIL

Fuente: Elaboración propia.

8.3. ENTREVISTA REALIZADA AL SUBGERENTE:

Respuestas obtenidas en la entrevista realizada a la subgerente de la Subgerencia de Informática y telecomunicaciones de la Municipalidad Distrital de Independencia, manifestó que:

A. Respuestas en el inciso de "Toma de decisiones con respecto a la seguridad de la información" (Anexo 8):

1. *"La Sub Gerencia de Informática y Telecomunicaciones no cuenta con un comité de seguridad de la información y las políticas van siendo establecidas de acuerdo con la necesidad."* Los cual nos indica que no existe una organización adecuada con respecto a este tema.

B. Respuestas en el inciso de "Mecanismos de control con respecto a la seguridad de la información" (Anexo 8):

1. *"No Existe algún tipo de manual o documento donde se especifique los controles para la seguridad de la información."* Nos permite realizar el diagnostico que indica que no se ha tomado en consideración el tema de seguridad de la información.

2. *“No se realiza un control de seguridad de la información en los trabajadores en la Municipalidad distrital de independencia.”*

   Nos permite realizar el diagnostico que indica que no se ha tomado en consideración el tema de seguridad de la información.

3. *“No se realiza un control a los accesos a la red y los permisos son asignados de acuerdo a la necesidad.”*

   Nos permite realizar el diagnostico que indica que no se ha tomado en consideración el tema de seguridad de la información.

4. *“No existen bitácoras donde se registran los sucesos de todos los usuarios que ingresan a la red.”*

   Nos permite realizar el diagnostico que indica que no se ha tomado en consideración el tema de seguridad de la información.

5. *“Se ha tenido casos de ingreso indebido.”*

   Se observa que debido a la inexistencia de políticas y normas de seguridad han tenido problemas con respecto a este tema.

6. *“Si se registran los accesos de personas a las áreas donde se encuentran los equipos servidores, pero dicho control no es tan eficiente.”*

   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.

C. Respuestas en el inciso de “Políticas de seguridad” (Anexo 8):

1. *“No existe un documento donde se especifique las políticas de seguridad de la información, se presentaron propuestas, pero no han sido aplicadas hasta la actualidad. Manifiesta que es de suma urgencia la elaboración de políticas de seguridad de la información.”*

Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas, el cual es un indicativo de que se necesita la implementación de un Sistema de Gestión de Seguridad de la Información.

D. Respuestas en el inciso "Nivel conocimiento de seguridad de la información por parte de su personal" (Anexo 8):

1. *"Frente a cualquier desastre natural, provocado o humano el personal no conoce cuales son los activos más importantes que debe proteger en relación a la información."*

   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.

E. Respuestas en el inciso "Backups y claves" (Anexo 8):

1. *"La administración de todos los servicios de tecnología de información que están a mi cargo se manejan a través de claves de autenticación que se otorgan al personal de acuerdo al área donde labora."*

   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.

2. *"Manifiesta que la alta dirección no necesariamente deba poseer las claves de autenticación, se pueden realizar controles más eficientes."*

   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.

3. *"Los procedimientos de Backups se realizan de acuerdo al área que maneja la información."*

   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.

F. Respuestas en el inciso "Backups y claves" (Anexo 8):

1. *"La administración de todos los servicios de tecnología de información que están a mi cargo se manejan a través de claves de autenticación que se otorgan al personal de acuerdo al área donde labora."*

   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.

G. Respuestas en el inciso “Problemas frecuentes” (Anexo 8):

1. *“Los problemas más frecuentes con los que se enfrenta el área que Usted tiene a cargo son de soporte a usuarios.”*
   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.
2. *“Frente a las actividades de su área se trata de realizar lo mejor posible de acuerdo a las necesidades requeridas.”*
   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.
3. *“Frente a los servicios que le brinda a los usuarios se tratan de atender todas.”*
   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.
4. *“Se encuentran archivados esos problemas la mayoría si pero no en su totalidad.”*
   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.
5. *“Se aplican medidas de acuerdo a las necesidades que se presenten.”*
   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.
6. *“No se ha realizado encuestas para estos problemas.”*
   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.
7. *“Si se emplean fichas de seguimiento de los equipos que se les brinda a los usuarios.”*
   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.

H. Respuestas en el inciso "Mantenimiento de los equipos" (Anexo 8):

1. *"Si existe un plan de mantenimiento para todos los equipos se realizan anualmente, en este procedimiento se actualiza antivirus y mantenimiento necesario para los equipos."*

   Lo cual implica que por la inexistencia de normas y políticas que permitan regular este tema ya se ha tenido problemas.

I. Respuestas en el inciso "Adquisición de software y hardware" (Anexo 8):

1. *"La adquisición de software se realiza mediante una evaluación del requerimiento por parte del área pertinente."*

   Lo cual nos indica que se ha establecido ciertas normas y políticas en determinados temas.

2. *"Si se realiza este procedimiento documentalmente."*

   Lo cual nos indica que se ha establecido ciertas normas y políticas en determinados temas.

3. *"Se presenta el informe correspondiente de adquisición."*

   Lo cual nos indica que se ha establecido ciertas normas y políticas en determinados temas.

4. *"Es evaluado por el área correspondiente y verificado de acuerdo al presupuesto asignado."*

   Lo cual nos indica que se ha establecido ciertas normas y políticas en determinados temas.

5. *"Se realiza la evaluación con el área de abastecimiento correspondiente."*

   Lo cual nos indica que se ha establecido ciertas normas y políticas en determinados temas.

8.4. GUÍA DE OBSERVACIÓN REALIZADA A LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES

Resultados obtenidos de la Guía de información **(Ver Anexo 8)** a la Subgerencia de Informática y telecomunicaciones de la Municipalidad Distrital de Independencia, se observó que:

A. Verificar el funcionamiento y cumplimiento adecuado de la red de cómputo, así como la inclusión de sus componentes, su aplicación y su uso.

1. La instalación de la red es flexible y adaptable a las necesidades de la Subgerencia de Informática y Telecomunicaciones: **"NO CUMPLE"**. Lo cual implica que se debe realizar la regulación mediante la aplicación de controles.
2. La lista de componentes de la red contiene todo el hardware requerido para su funcionamiento adecuado: **"NO CUMPLE"**. Lo cual implica que se debe realizar la regulación mediante la aplicación de controles.
3. La lista de componentes de la red contiene todo el software requerido para su funcionamiento adecuado: **"NO CUMPLE"**. Lo cual implica que se debe realizar la regulación mediante la aplicación de controles.
4. La red de cómputo es aprovechada al máximo en la Subgerencia de Informática y Telecomunicaciones: **"CUMPLE"**. Nos indica que no se requiere la aplicación de controles en esta área.
5. Los recursos de la red se comparten de acuerdo con las necesidades de la Subgerencia de Informática y Telecomunicaciones: **"CUMPLE"**. Nos indica que no se requiere la aplicación de controles en esta área.
6. La configuración de recursos de la red es la mejor para el uso correcto de los sistemas computacionales de la Subgerencia de Informática y Telecomunicaciones: **"NO CUMPLE"**. Lo cual

implica que se debe realizar la regulación mediante la aplicación de controles.

7. Se acepta la transferencia frecuente de grandes volúmenes de información: **"NO CUMPLE"**. Lo cual implica que se debe realizar la regulación mediante la aplicación de controles.
8. Existen niveles de acceso y seguridad en la red: **"CUMPLE"**. Nos indica que no se requiere la aplicación de controles en esta área.

B. Verificar la seguridad en el centro de cómputo, y calificar sólo una de las columnas de cada concepto según su grado de cumplimiento:

1. Evaluación de la seguridad en el acceso al sistema:

a. Evaluar los atributos de acceso al sistema: **40%**. Nos indica que no se requiere la aplicación de controles en esta área.
b. Evaluar los niveles de acceso al sistema: 6**0%**. Nos indica que no se requiere la aplicación de controles en esta área.
c. Evaluar la administración de contraseñas del sistema: **60%**.

   Nos indica que no se requiere la aplicación de controles en esta área.
d. Evaluar la administración de la bitácora de acceso al sistema: **40%**.

   Nos indica que no se requiere la aplicación de controles en esta área.
e. Evaluar el monitoreo en el acceso al sistema: **40%**. Nos indica que no se requiere la aplicación de controles en esta área.
f. Evaluar las funciones del administrador del acceso al sistema: **60%**. Nos indica que no se requiere la aplicación de controles en esta área.

g. Evaluar las medidas preventivas o correctivas en caso de siniestros en el sistema: **40%**. Nos indica que no se requiere la aplicación de controles en esta área.

2. Evaluación de la seguridad en el acceso al área física:

a. Evaluar el acceso del personal a la Subgerencia de Informática y Telecomunicaciones: **40%**.
   Nos indica que no se requiere la aplicación de controles en esta área.
b. Evaluar el acceso de los usuarios y terceros a la Subgerencia de Informática y Telecomunicaciones: **40%**.
   Nos indica que no se requiere la aplicación de controles en esta área.
c. Evaluar la administración de la bitácora de acceso físico al área de sistemas: **40%**.
   Nos indica que no se requiere la aplicación de controles en esta área.
d. Evaluar el control de entradas y salidas de bienes informáticos de la Subgerencia de Informática y Telecomunicaciones: **60%**.
   Nos indica que no se requiere la aplicación de controles en esta área.
e. Evaluar la vigilancia de la Subgerencia de Informática y Telecomunicaciones: **40%**.
   Nos indica que no se requiere la aplicación de controles en esta área.
f. Evaluar las medidas preventivas o correctivas en caso de siniestros en la Subgerencia de Informática y Telecomunicaciones: **60%** Nos indica que no se requiere la aplicación de controles en esta área.

CAPÍTULO IX
DISCUSIÓN DE RESULTADOS

Este proyecto abarcó lo que es el Sistema de Gestión de la Seguridad de la Información en la Subgerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia, por ser una de las dependencias con activos de información importantes para la institución, es por ello que al presentar alguna falla en cualquier momento puede ocasionar problemas e inconvenientes en el desarrollo normal de los procesos. A pesar de ello se ha observado que hasta el momento no se ha puesto mayor esfuerzo en lo que respecta a la seguridad de la información.

En el desarrollo del presente proyecto se han observado estudios e información sobre el tema en cuestión, incluso dentro de nuestra Facultad de Ciencias contamos con la tesis de Mory Garay el cual realiza el diagnóstico y diseño de un Sistema de Gestión de Seguridad de Información aplicado a una Empresa Constructora según el estándar internacional ISO/IEC 27001:2005 la cual no es certificada debido a que ahora se cuenta con la actualización al estándar internacional ISO/IEC 27001:2013, estas investigaciones se realizaron antes del cambio contractual por lo que fueron a grandes rasgos puesto que su aplicación de todo o en parte se está imponiendo de manera necesaria y obligatoria para las instituciones públicas ya que generalmente no cuentan con este tipo de políticas de seguridad ni mucho menos cuentan con un documento de aplicabilidad por lo cual están a la deriva.

En base a nuestros antecedentes vemos que a pesar de que nos encontramos en una etapa donde la información es importante, poco o nada se hace para salvaguardarlo y protegerla de los riesgos y amenazas a los que se ven expuestos diariamente ya que varios estudios confirman lo dicho.

La función de la Sub Gerencia de Informática y Telecomunicaciones no se limita solo a reparar computadoras o actualizar antivirus, sino va mucho más allá de ello, es un actor clave para proponer el cambio dentro de la institución y concientizar a proteger uno de los bienes más preciados el cual es la información.

Esperamos que a partir de este proyecto se tome conciencia sobre los riesgos a los que están expuestos los activos y se empiece por implantar políticas de seguridad, salvaguardas y controles, empezando por cosas que pueden parecer pequeñas al inicio pero que pueden formar parte de un cambio dentro de la institución permitiendo mantener el CID de la información aplicando las Políticas de seguridad y la Declaración de aplicabilidad el cual contiene la cláusula, la sección, el objetivo del control y la visión general de la implementación.

CONCLUSIONES

Habiendo finalizado con el desarrollo de SGSI (Sistema de Gestión de Seguridad de la Información), se ha podido llegar a las siguientes conclusiones.

- La Sub Gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia no cuenta con medidas de seguridad guiados y documentados, por lo cual el proyecto será de gran aporte como punto de partida a la minimización de los riesgos existentes y los que afectaran en el futuro a la institución.
- Se pudo identificar los riesgos en base al estudio realizado a los activos que surgieron en base a la identificación de procesos, con el cual se realizó la matriz de amenazas de cada activo según el estudio viendo la probabilidad de ocurrencia de cada uno de ellos.
- La valoración de los activos se realizó en base a cada proceso identificado dentro de nuestro alcance, en nuestro caso tomamos los procesos relacionados al Área de Registro Civil partiendo como base la guía de gestión de Riesgos que otorga MAGERIT el cual tiene nombre, código y la dimensión de la seguridad del activo, en la cual se aprecia el CID de la Información para su valoración como criterio.
- En base a la identificación delos procesos involucrados y los activos que contienen dentro del mismo se pudo realizar la evaluación de los riesgos y amenazas de cada uno de ellos y a los que están expuestos, se aprecia que en su mayoría de ellos están entre un estado de intolerable y extremo riesgo, por lo cual es oportuno implementar las medidas correctivas a ello, según el capítulo V.
- Se estableció la declaración de aplicabilidad mediante el ISO/IEC 27002:2013 la cual cuenta con 14 dominios, 35 objetivos de control y 114 controles, los cuales fueron adaptados al alcance de la solución del proyecto.

- Los resultados serán evidenciados una vez que se aplicado la declaración de aplicabilidad junto con sus políticas de medidas de control presentados en la tesis la cual abarca el plan de seguridad y las guías de implementación que contienen las salvaguardas correspondientes a cada activo.
- La metodología MAGERIT nos permitió identificar una serie de puntos importantes para el análisis y gestión de riesgos, fase fundamental en este estudio ya que se obtuvo resultados realistas del estado de riesgo actual en la Sub Gerencia de Informática y Telecomunicaciones, y como estudio piloto el Área de Registro Civil donde se supo escoger que medidas serán necesarias para mitigar el riesgo.
- Después de haber realizado el proyecto, la institución obtendrá un documento enfocado a la seguridad que será punto de partida para la creación de normativas de seguridad para los recursos informáticos y para el personal que laboran en la Sub Gerencia de Informática y Telecomunicaciones de la Municipalidad de Independencia, el cual es la Declaración de aplicabilidad documento que contiene la cláusula, la sección, el objetivo del control y la visión general de la implementación.

RECOMENDACIONES

- ✓ La implementación del SGSI estará sujeta a la aceptación y aplicación que la alta Gerencia apruebe, la cual es de suma importancia para mitigar los riesgos observados.
- ✓ Se sugiere que se establezca un comité de seguridad de la información el cual este encabezado por el Sub Gerente de Informática y Telecomunicaciones, el cual se encargara de la implementación del Sistema de Gestión de Seguridad de la Información.
- ✓ Se recomienda que haya una revisión periódica anual de las amenazas y riesgos a los que están expuestos los activos, de acuerdo con las normas y estándares ya que la tecnología está cambiando constantemente y deben ser controlados para evitar problemas futuros, todo esto apoyándose en la Declaración de aplicabilidad.
- ✓ Para mitigar los riesgos en la Municipalidad de Independencia se debería realizar la implementación SGSI que abarque a todas las áreas de la institución, asimismo el comité de Seguridad se debe encargar de programar y realizar la capacitación al personal 2 veces al año para que se cumplan las normas de seguridad establecidas en la Declaración de Aplicabilidad.

REFERENCIAS BIBLIOGRÁFICAS

TESIS DIGITAL

ALEXANDER, A. G. (2007). Diseño de un sistema de gestión de seguridad de información: Óptica ISO 27001:2005. Bogotá: Alfaomega Colombiana.

ALVAREZ, LUIS. "*Seguridad en informática (Auditoría de Sistemas).",* Tesis de Maestría., Universidad Iberoamericana, México D.F., México, 2010.

AMPUERO CHANG, CARLOS ENRIQUE. "*Diseño De Un Sistema De Gestión De Seguridad De Información Para Una Compañía De Seguros.",* Tesis de Grado, Pontificia Universidad Católica del Perú, Lima, Perú, 2011.

CAMACHO GOMEZ, PEDRO DANIEL Y RAMOS ARRIETA, WILMER. "*Metodología táctica para la Implantación de sistemas de información basado en métrica y COBIT.",* Tesis de Grado., Universidad Nacional Mayor de San Marcos, Lima, Perú, 2010.

DUQUE OCHOA, BLANCA RUBIELA. "*Metodologías de Gestión de Riesgos (O**ct**ave, MAGERIT, DAFP).”*, Tesis de Grado, Universidad de Caldas, Caldas, Colombia, 2010.

ESPINOZA AGUINAGA, HANS RYAN. “*Análisis Y Diseño De Un Sistema De Gestión De Seguridad De Información Basado En La Norma ISO/IEC 27001:2005 Para Una Empresa De Producción Y Comercialización De Productos De Consumo Masivo.",* Tesis de Grado, Pontificia Universidad Católica del Perú, Lima, Perú, 2013.

FERRERO RECASÉNS, EDUARDO. "*Análisis y Gestión de Riesgos del Servicio Imat del Sistema de Información de I.C.A.I."* Proyecto Fin de Carrera., Universidad Pontificia Comillas, Madrid, España, 2009.

MARTÍNEZ SARAVIA, VÍCTOR ENRIQUE. "*Concienciación en Seguridad de la Información, la estrategia para fortalecer el eslabón más*

débil de la cadena.", Tesis de Maestría., Fundación Universitaria Iberoamericana, Bogotá D.C., Colombia, 2010.

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. (2012).

MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. Madrid.

MORY GARAY, ALEJANDRO CESAR*. "Diagnóstico y Diseño de un Sistema de Gestión de Seguridad de Información aplicado a la empresa HM Contratistas S.A."*, Proyecto de tesis de grado, Universidad Nacional Santiago Antúnez de Mayolo de Huaraz, Ancash, Peru, 2014.

PALLAS MEGA, GUSTAVO. "*Metodología de Implantación de un SGSI en un grupo empresarial jerárquico."*, Tesis de Maestría, Universidad de la República, Montevideo, Uruguay, 2009.

RAMÍREZ CASTRO, ALEXANDRA. *"Actualización del Sistema de Gestión de Seguridad de la Información de una empresa a la norma ISO/IEC 27001:2013"***,** Trabajo Final de Master, UNIVERSITAT OBERTA DE CATALUNYA, Barcelona España 2014.

RIPOLL RIPOLL, JOSÉ ISMAEL. "*Seguridad en los Sistemas de Información (SSI)",* Apuntes. Universidad Politécnica de Valencia, Valencia, España, 2012.

TALABIS, M., & Martin, J. (2012). Information Security Risk Assessment Toolkit: Practical Assessments through Data Collection and Data (Primera ed.). Massachusetts: Elsevier Science.

TALAVERA ÁLVAREZ, JOSE. *"**Diseño de un Sistema de Gestión de Seguridad de la Información para una entidad pública del sector Salud"*, Trabajo de Fin de Carrera Instituto Nacional Materno Perinatal de Lima, Peru, 2015.

VILLENA AGUILAR, MOISES ANTONIO. "*Sistema de Gestión de Seguridad de Información para una institución financiera.",* Tesis de Grado, Pontificia Universidad Católica del Perú, Lima, Perú, 2011.

PÁGINA WEB

ISACA. (2012). CISM – *Certified Information Security Manager* – Review Manual 2013. ISACA.

ISO 27001. (2013). ISO 27001:2013. *Information technology* – Security techniques – Information Security management systems - Requirements.

ISO 27002. (2013). ISO 27002:2013. *Information technology* – Security techniques – Code of practice for information security control.

ISO 27799. (2008). ISO 27799:2008. *Health Informatics* – Information security management in health using ISO/IEC 27002.

ISO 31000. (2013). ISO 31000:2009*. Risk management* – Principles and guidelines.

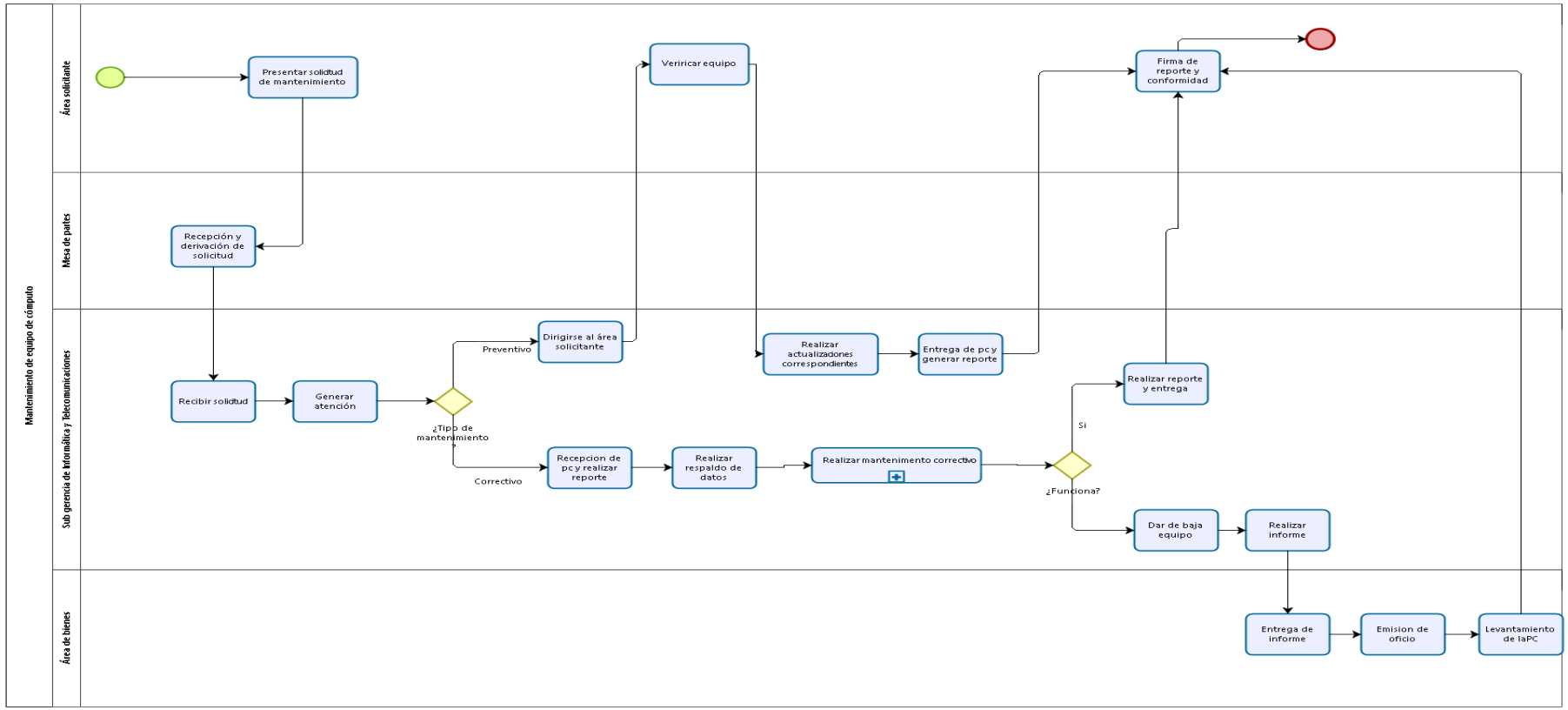
ISO 27000 en español, (S/A) [Acceso: 2016/05/12] Disponible desde: http://www.iso27000.es/

ANEXOS

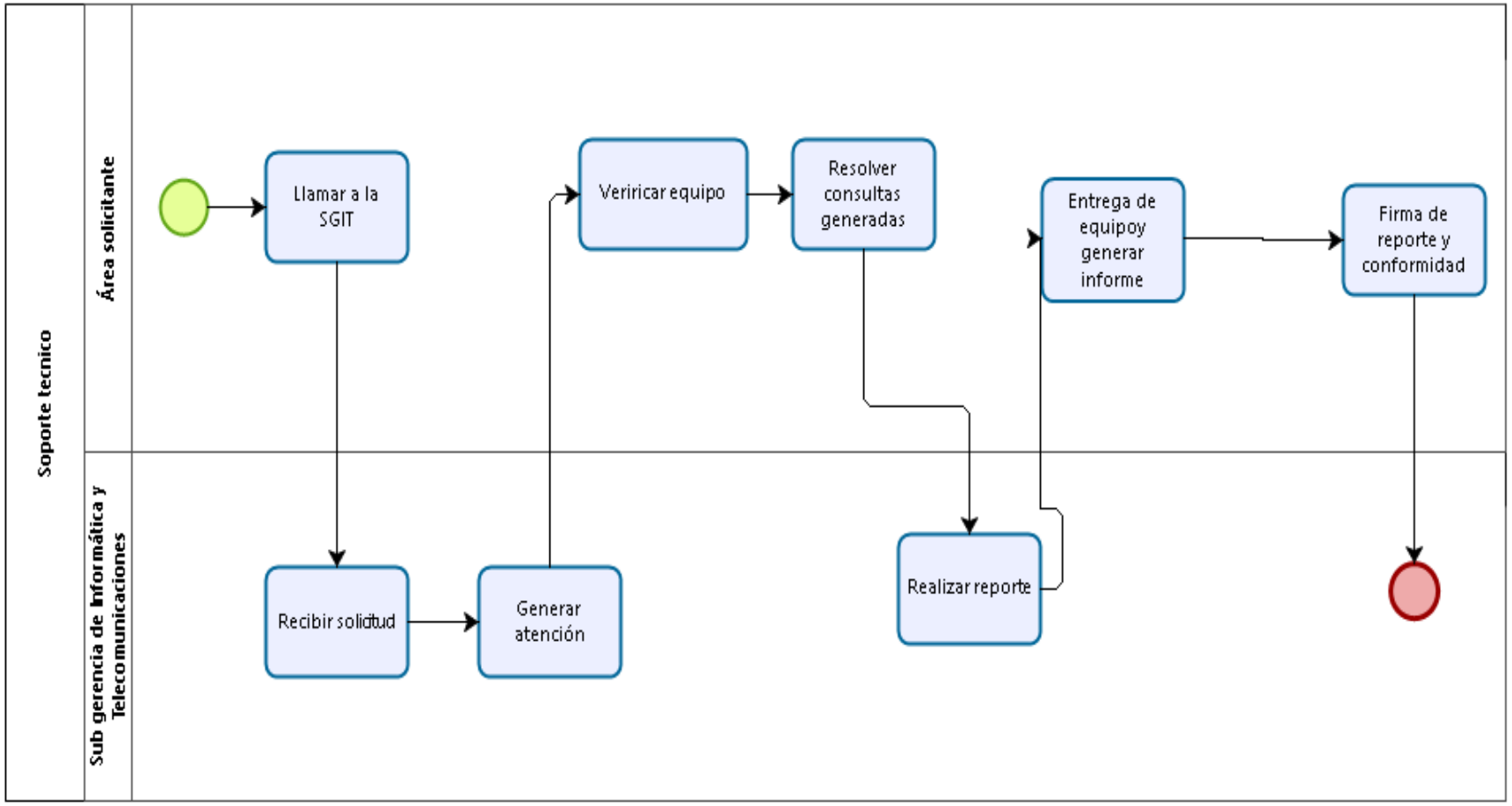
ANEXO 1: “DIAGRAMAS DE PROCESOS DE NEGOCIO BPMN”

GESTIÓN DE INFRAESTRUCTURA TECNOLÓGICA

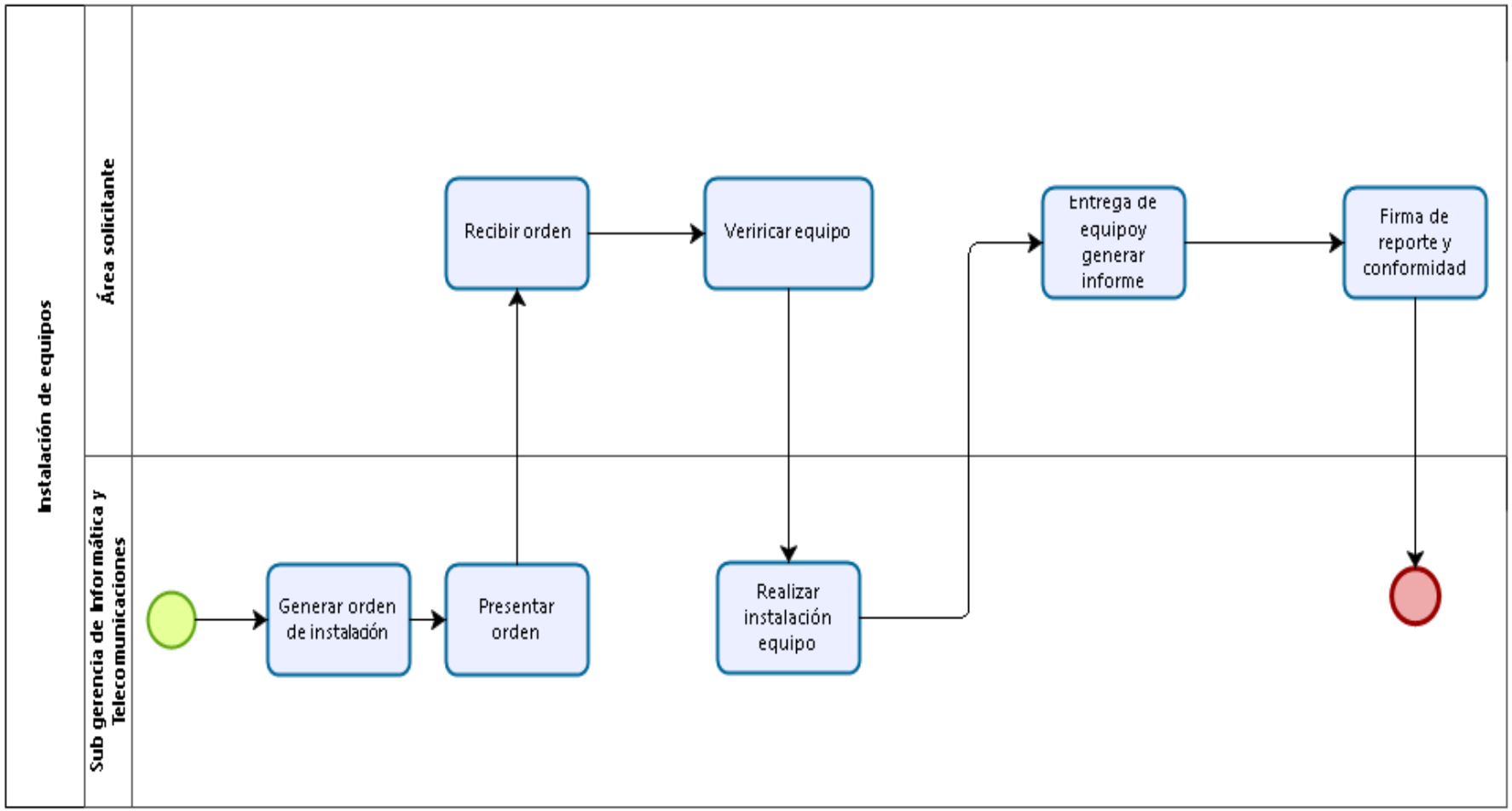
Mantenimiento de Equipo de Cómputo.



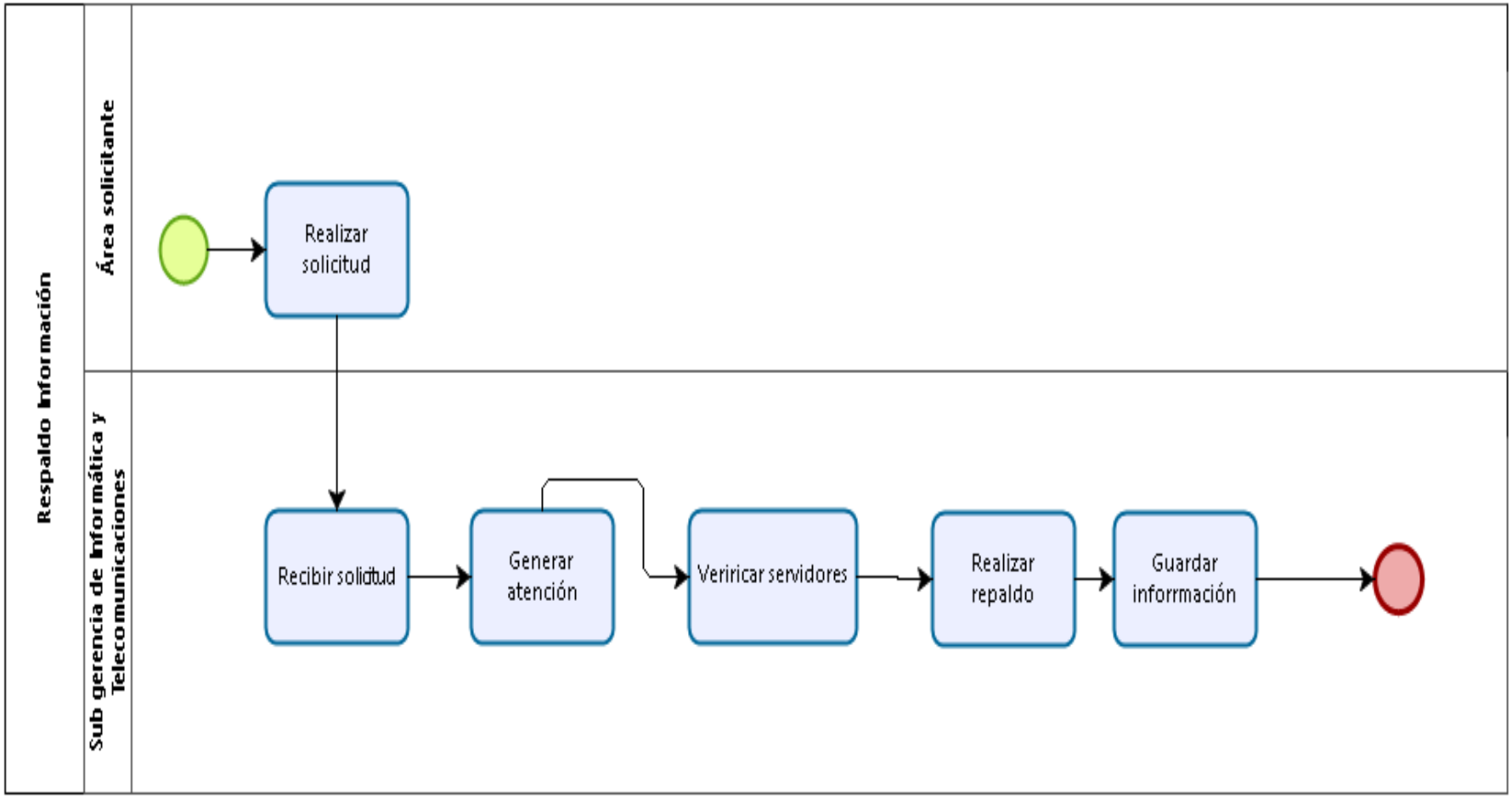
Soporte Técnico.



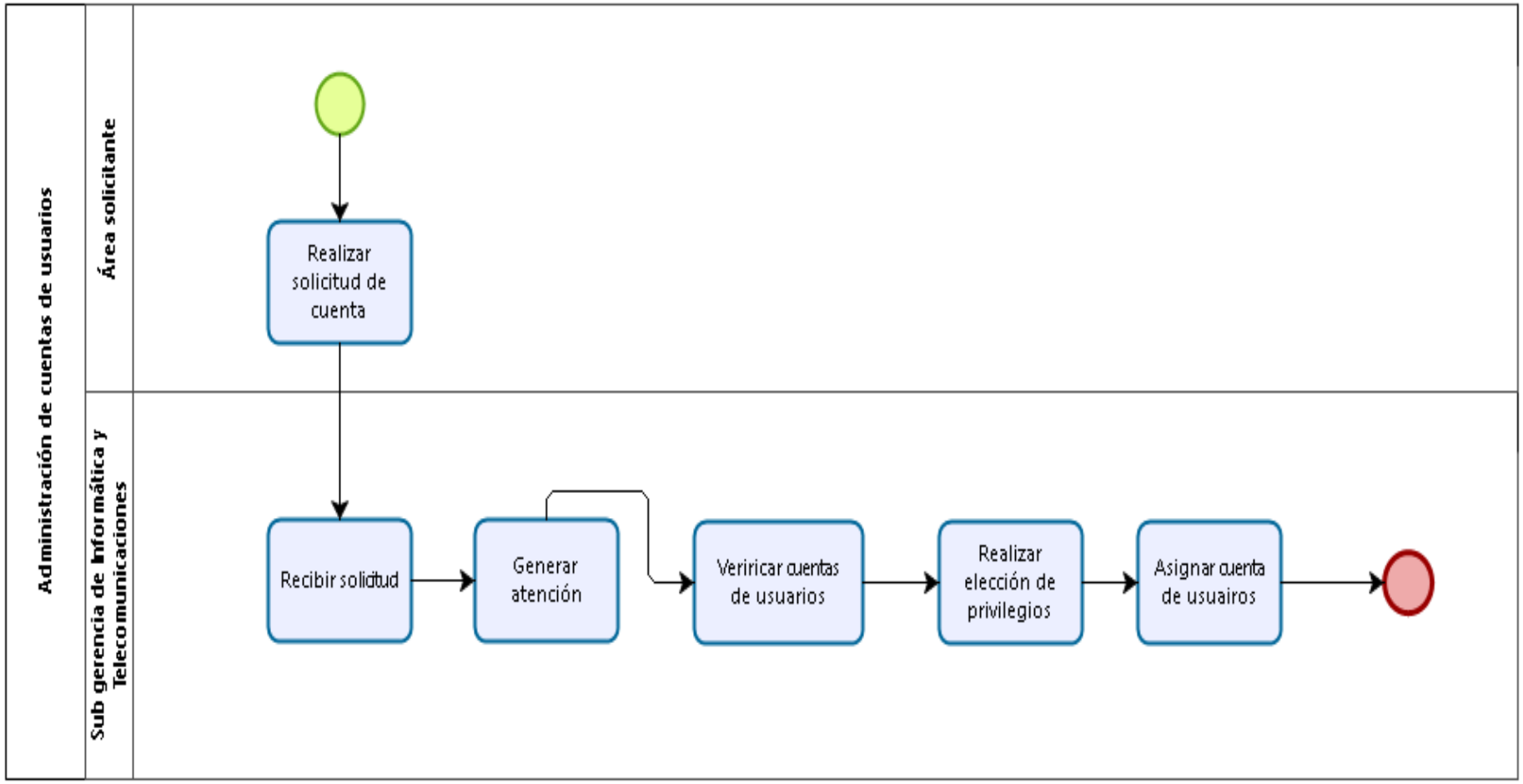
Instalación de equipos.



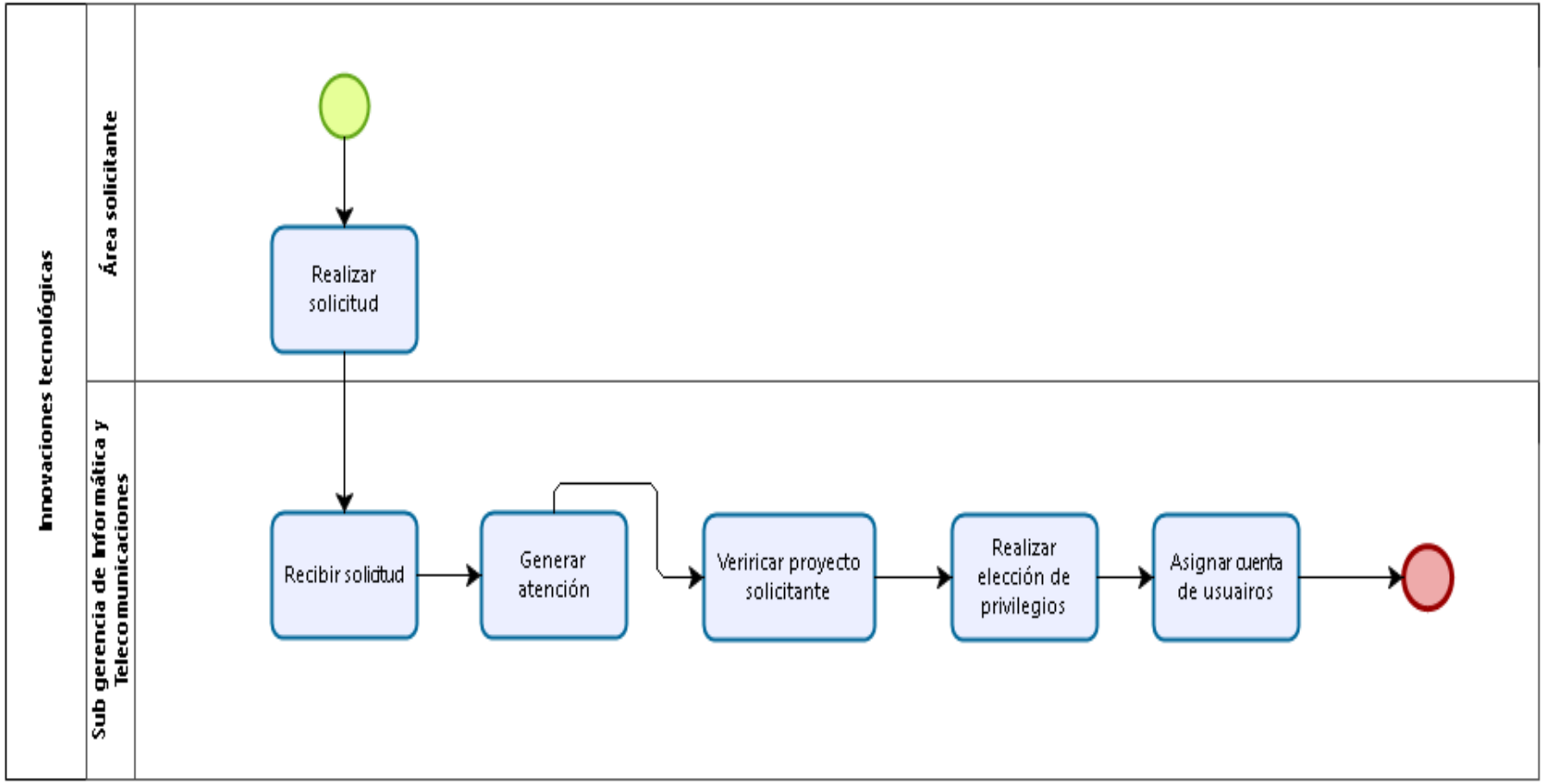
Respaldos de información.



Administración de cuentas de usuarios.

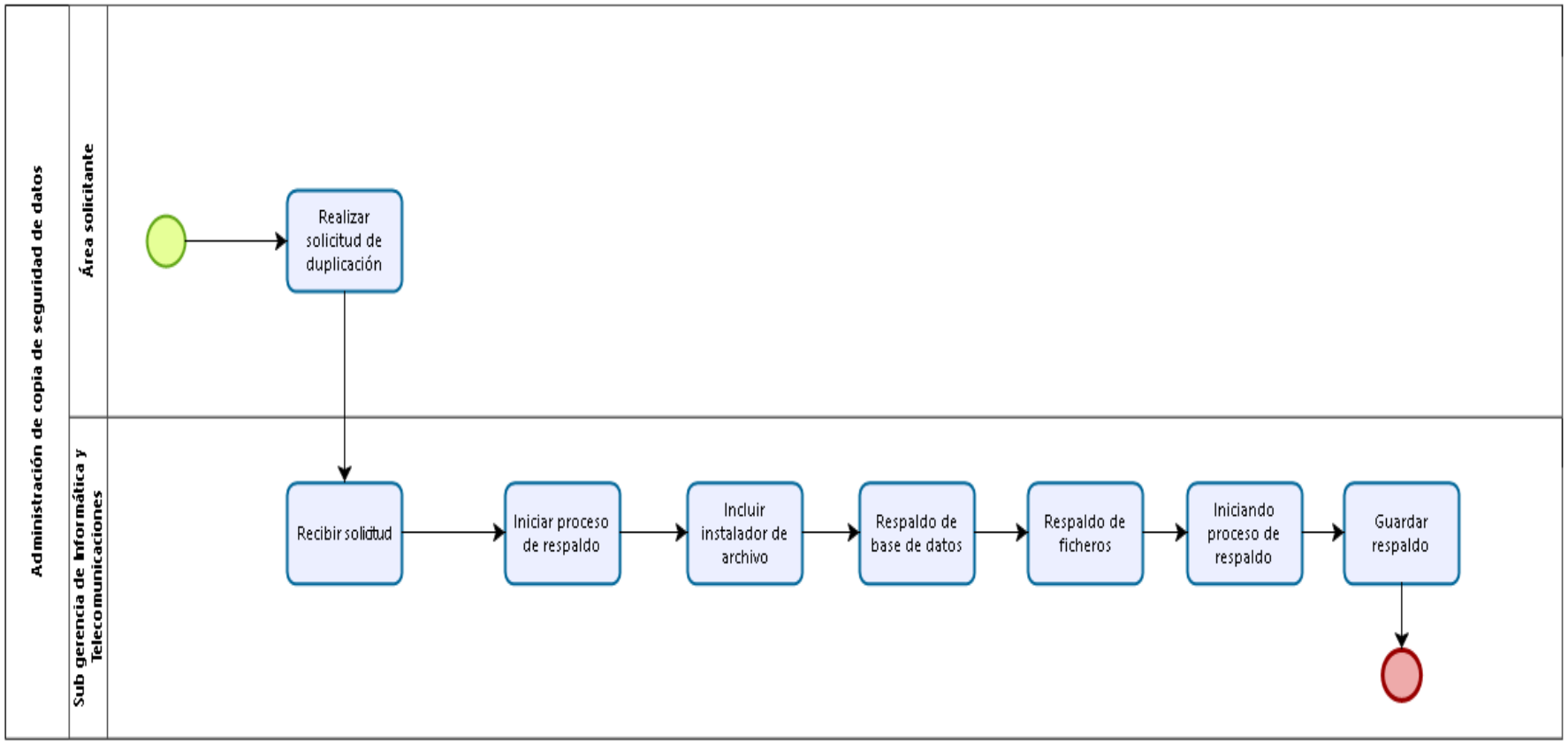


Innovaciones Tecnológicas.

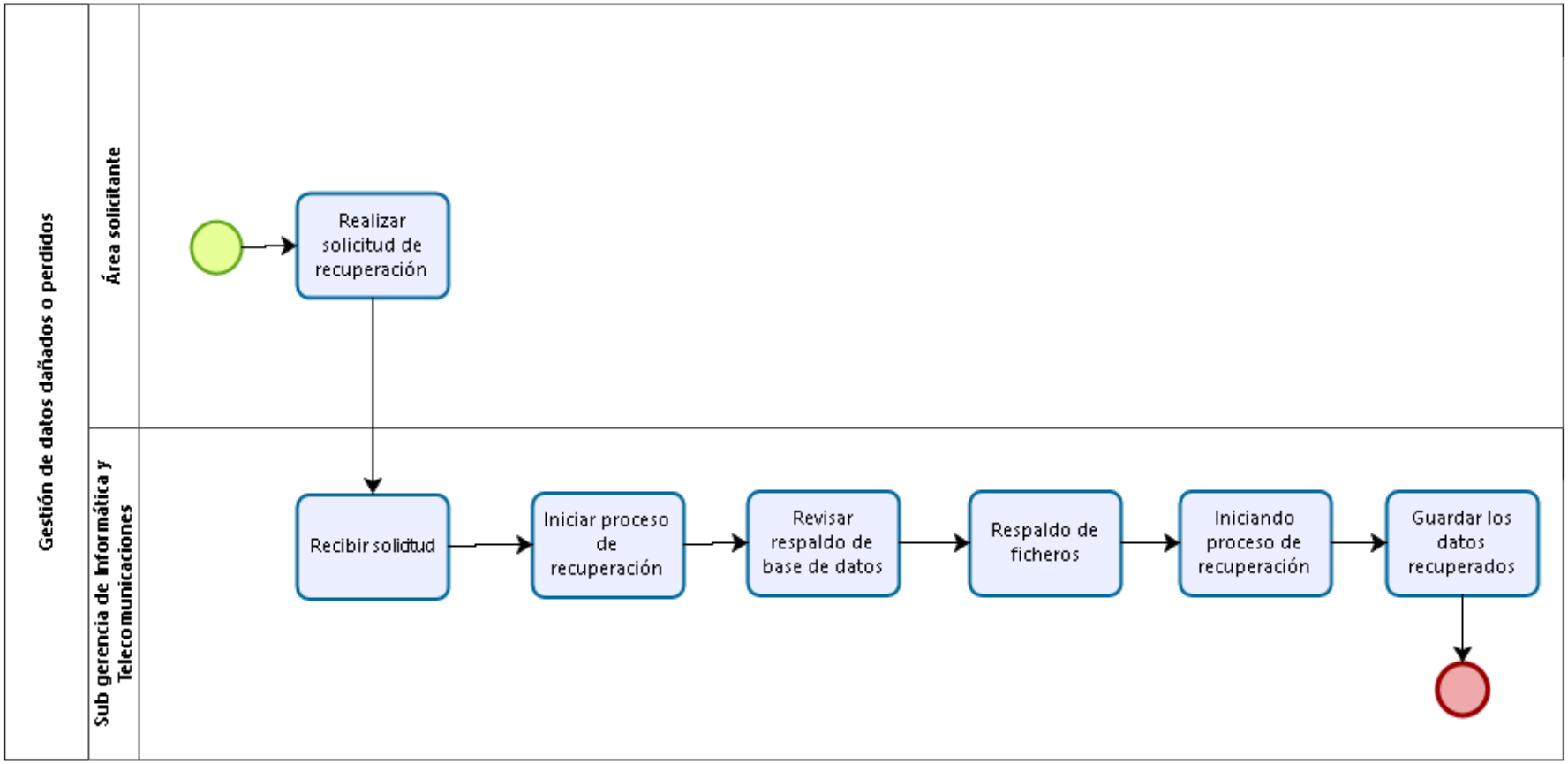


ADMINISTRACIÓN DE ALMACENAMIENTO

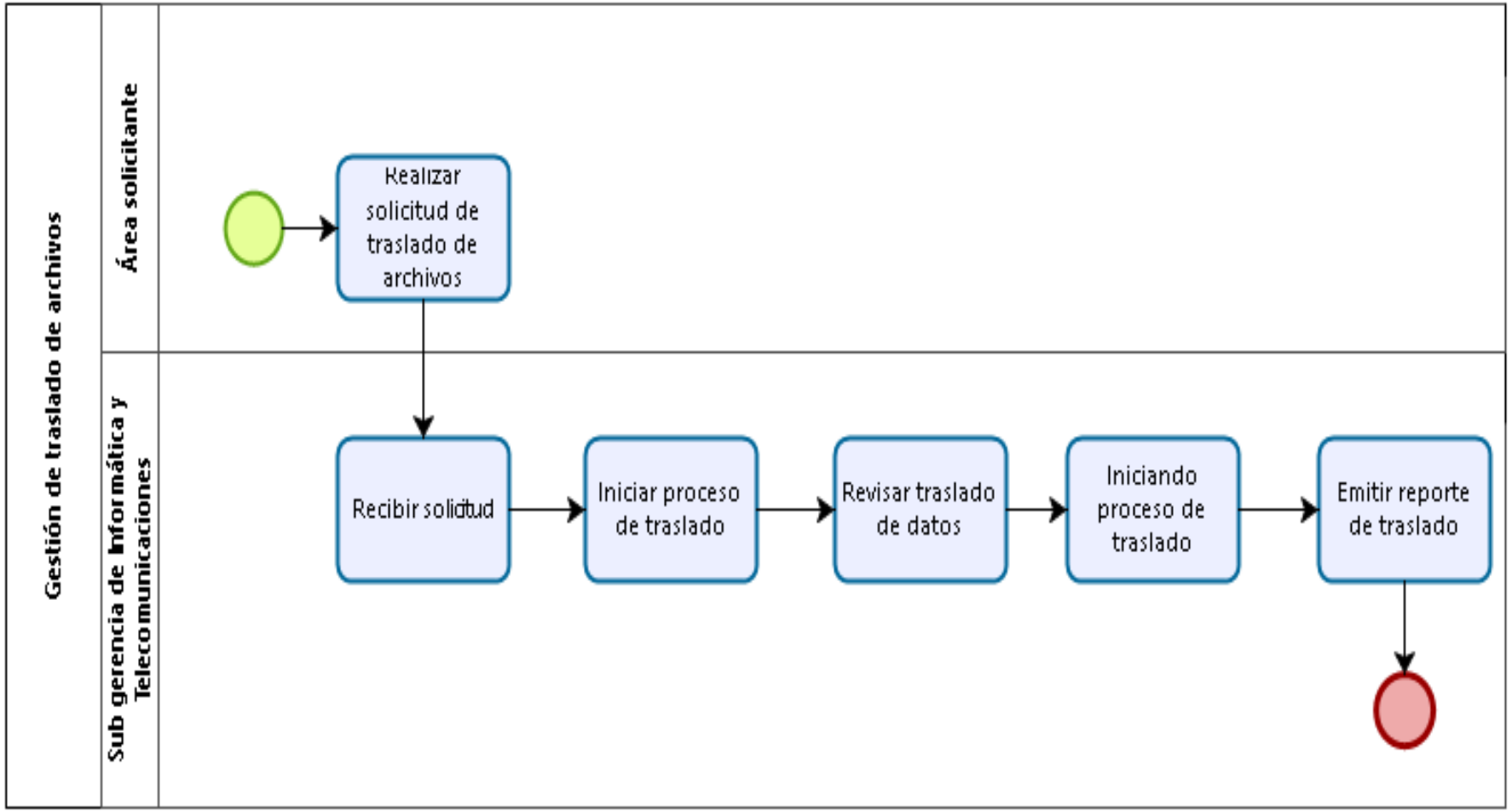
Administración de copia de seguridad



Gestión datos dañados o perdidos

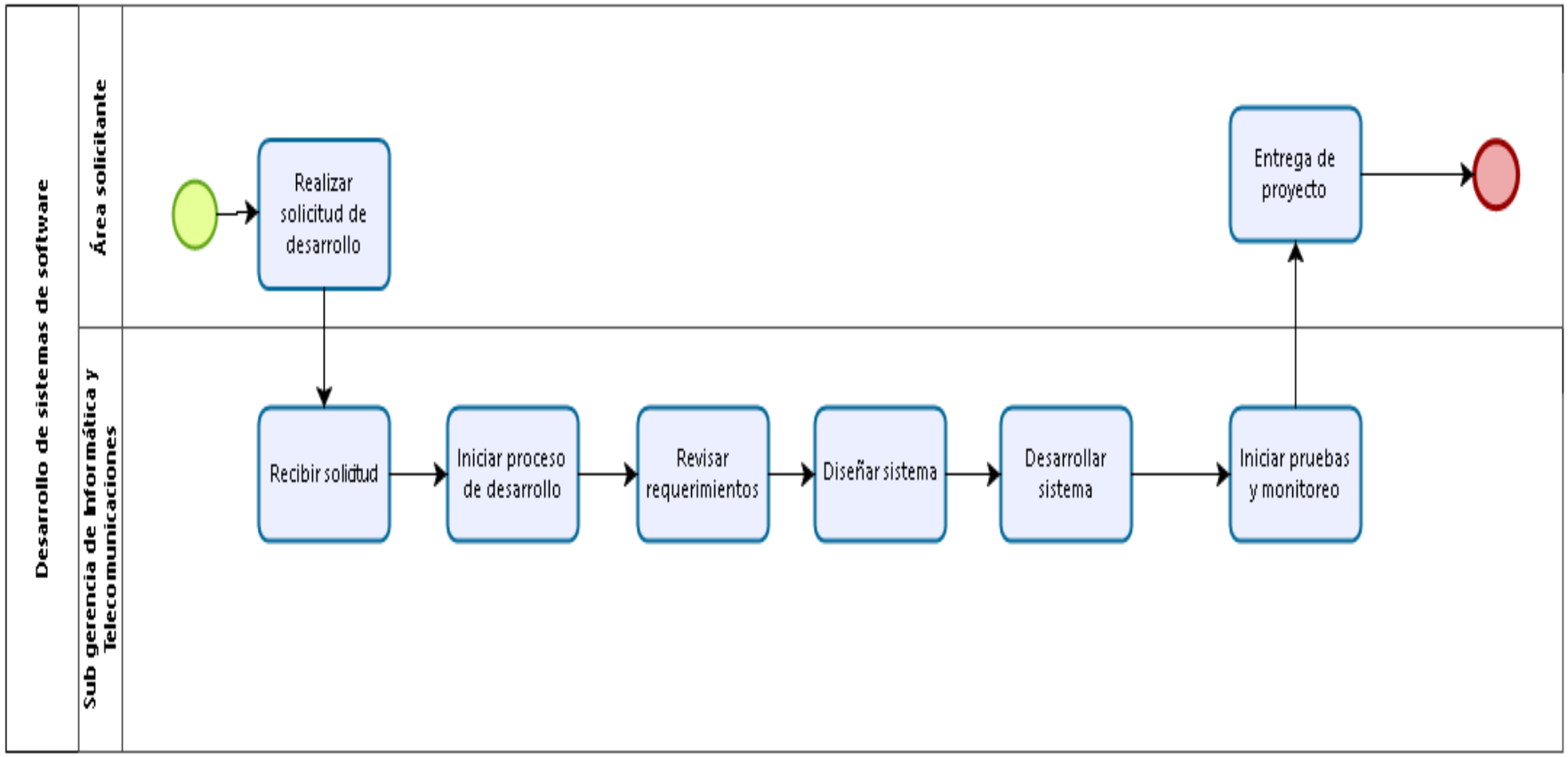


Traslado de archivos

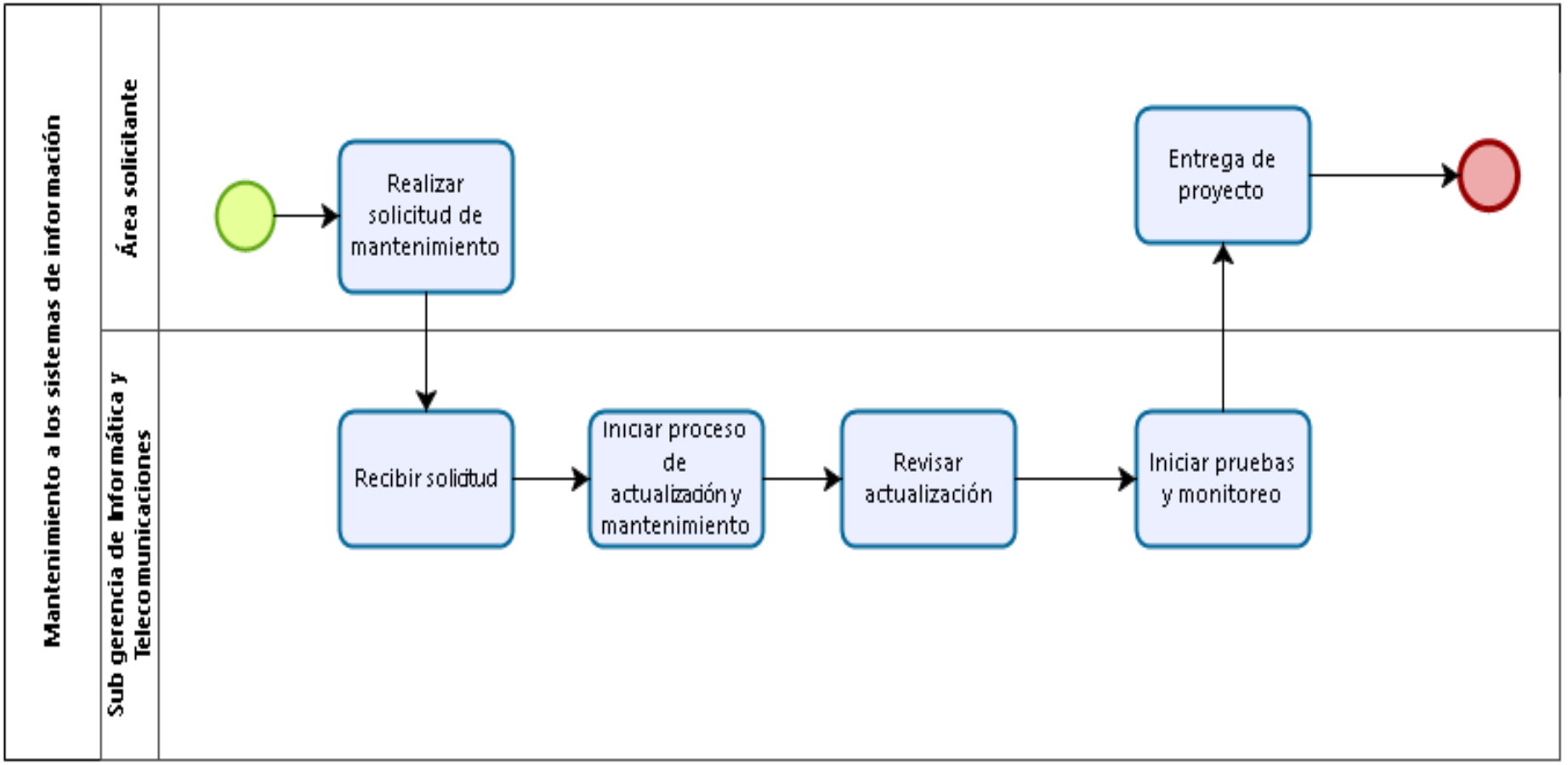


DESARROLLO DE SISTEMAS DE INFORMACIÓN

Desarrollo de Sistemas de Software.

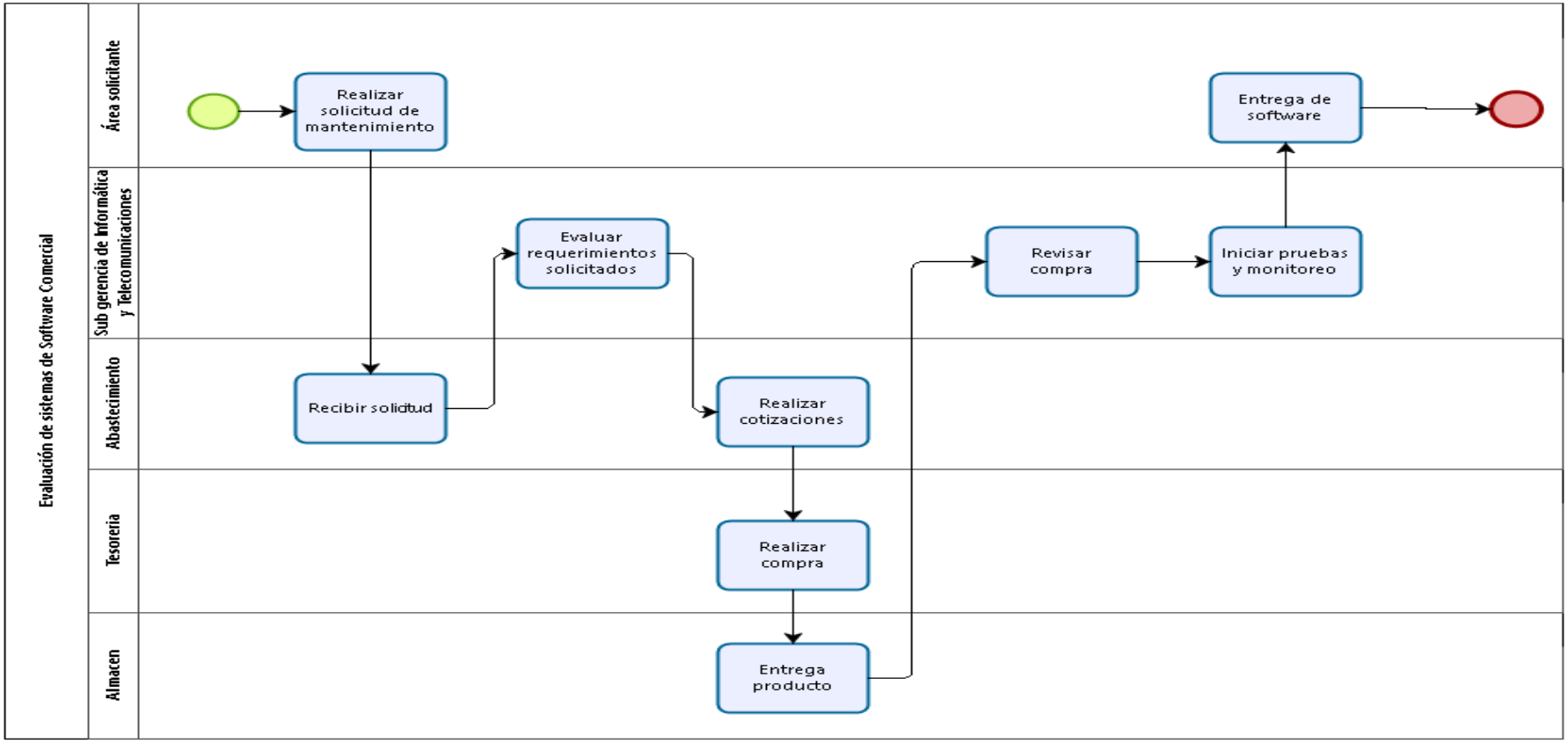


Mantenimiento a los Sistemas de Software.

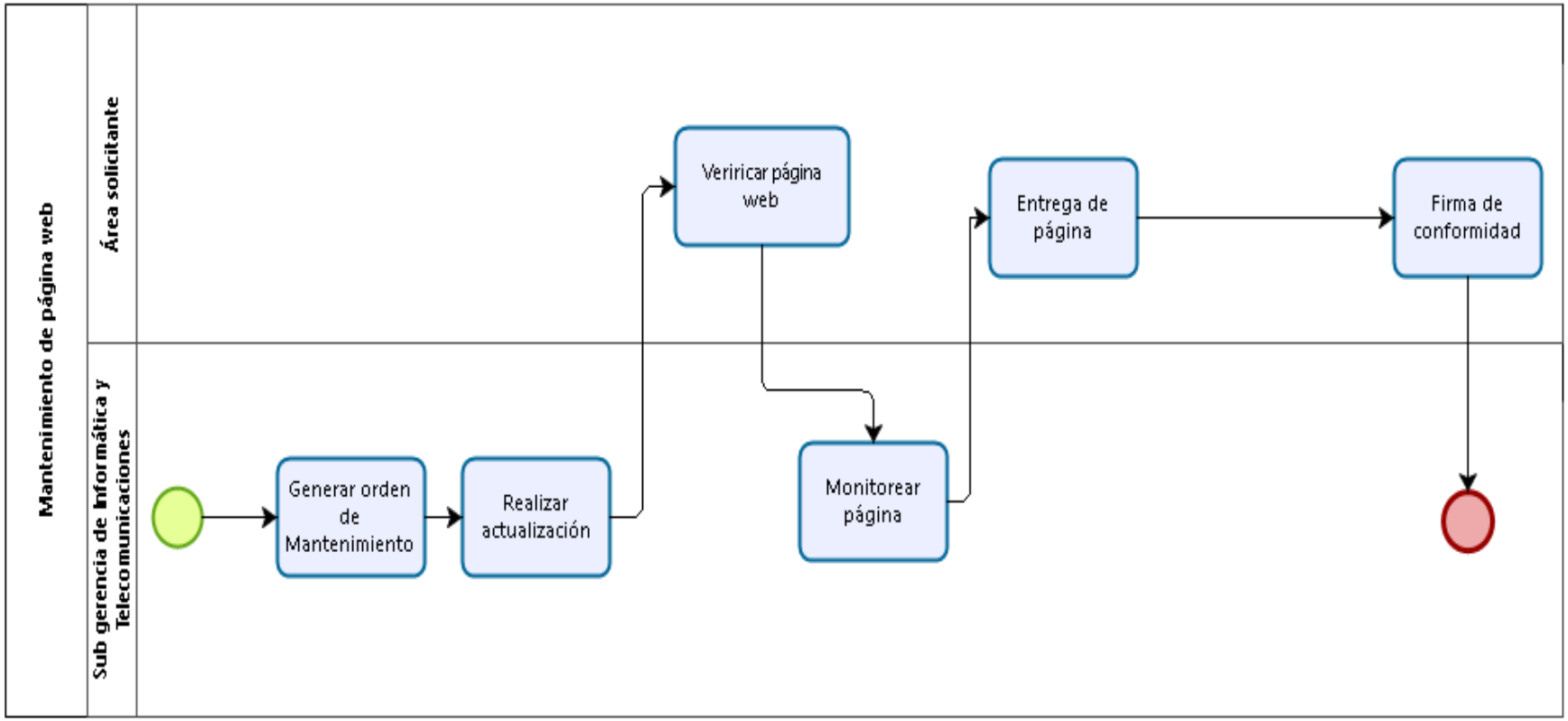


GESTIÓN DE SISTEMAS DE INFORMACIÓN

Evaluación de Sistemas de Software Comercial.



Mantenimiento de Página Web e Intranet.



ANEXO 2: "ENCUESTA REALIZADA A LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES"

UNIVERSIDAD NACIONAL SANTIAGO ANTUNEZ DE MAYOLO

Escuela profesional de Ingeniería de Sistemas e Informática

ENCUESTA SGIT

Como trabajador de la Municipalidad Distrital de Independencia le solicitamos completar esta pequeña encuesta para contribuir con su opinión a mejorar nuestros procesos y proteger la información.

Complete con un check el siguiente ítem:

1. Sexo: Hombre ( ) Mujer ( )

Ahora marque con una "X" su respuesta, basándose en su propia experiencia:

2. **¿Cuantas áreas se encuentran involucradas en algún proceso con la Sub Gerencia?**
   - **a.** 1 - 5
   - **b.** 6 – 10
   - **c.** 11 – 15
   - **d.** 15 a mas
3. **¿Se ha presentado alguna iniciativa de seguridad de la información?**
   - **a.** Si
   - **b.** No
4. **¿Se ha presentado alguna iniciativa de tratamiento de riesgo?**
   - **a.** Si
   - **b.** No
5. **¿Ha tenido incidentes de seguridad de la información en estos 3 últimos años?**
   - **a.** Si
   - **b.** No
6. **En los últimos 3 años se ha realizado algún tratamiento de amenazas y vulnerabilidades presentadas**
   - **a.** Si
   - **b.** No
7. **¿Considera usted que por medio de la evaluación de riesgos va a ser posible mitigar la mayor cantidad de vulnerabilidades existentes?**
   - **a.** Totalmente en desacuerdo ( )
   - **b.** En desacuerdo ( )
   - **c.** Ni de acuerdo ni en desacuerdo ( )
   - **d.** De acuerdo ( )
   - **e.** Totalmente de acuerdo ( )
8. **¿Se tiene definida una política para la realización de copias de seguridad de los datos?**
   - **a.** Si
   - **b.** No
9. **¿Se tiene definida una política de restauración de los sistemas en caso de ataques informáticos?**
   - **a.** Si
   - **b.** No
10. **¿Recomendaría usted adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información?**
    - **a.** Si
    - **b.** No
11. **¿Se ha establecido algún tipo de organización interna dentro de la Sub Gerencia orientada a la seguridad de la información?**
    - **a. Si**
    - **b. No**
12. **¿Se ha permitido el acceso a la información sólo a personas debidamente autorizadas?**
    - **a.** Si
    - **b.** No
13. **¿Se ha realizado la gestión de altas y bajas en el registro de usuarios?**
    - **a.** Si
    - **b.** No

14. **¿Se ha realizado la gestión de acceso con privilegios por usuario?**
    a. Si
    b. No
15. **¿Con qué frecuencia se cambian las contraseñas del pc a su cargo?**
    a. Entre 1 y dos meses
    b. Entre 2 y 6 meses
    c. Entre 6 meses y 1 año
    d. Más de 1 año
16. **¿El lugar donde se ubica la oficina está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?**
    a. Si
    b. No
17. **¿El material con que está construido las oficinas donde labora son confiables?**
    a. Si
    b. No
18. **¿Existe lugar suficiente para la documentación y los equipos?**
    a. Si
    b. No
19. **¿Dentro del Área existen materiales que puedan ser inflamables o causar algún daño sobre la documentación o los equipos?**
    a. Si
    b. No
20. **¿Se cuenta con una salida de emergencia?**
    a. Si
    b. No
21. **¿Los equipos cuentan con un regulador?**
    a. Si
    b. No
22. **¿Los cables están dentro de paneles y canaletas eléctricas?**
    a. Si
    b. No
23. **¿Se ha realizado auditorias en los sistemas de información?**
    a. Si
    b. No
24. **¿El cableado se encuentra correctamente instalado?**
    a. Si
    b. No
25. **¿Se cuenta con pozo a tierra?**
    a. Si
    b. No
26. **¿Se cuenta con mecanismos de seguridad asociados a servicios en red?**
    a. Si
    b. No
27. **¿se ha realizado revisiones técnicas tras efectuar cambios en los sistemas?**
    a. Si
    b. No
28. **¿Se tiene alguna especificación en cuanto a seguridad, de la línea otorgada por empresas privadas?**
    a. Si
    b. No
29. **¿La instalación eléctrica del equipo de cómputo es independiente de otras instalaciones?**
    a. Si
    b. No
30. **¿Con que periodo se les da mantenimiento a las instalaciones y suministros de energía?**
    a. Si
    b. No
31. **¿Qué nivel de respuesta a incidentes de seguridad poseen?**
    a. Alto
    b. Medio
    c. Baja
32. **¿Se ha identificado puntos débiles de seguridad dentro de la Sub Gerencia?**
    a. Si
    b. No
33. **¿Los sistemas operativos utilizados son privados o de uso gratuito?**
    a. Si
    b. No
34. **¿Los activos de información fue manipulado o modificado por una entidad externa?**
    a. Si
    b. No
35. **¿usted ha podido tener acceso a la información en tiempo real?**
    a. Si

b. No

Si su respuesta es sí pase a la pregunta 35 de caso contrario continúe

36. Marque con una "x" las siguientes afirmaciones :

AFIRMACIONES	1
a. Problemas de red	
b. Problemas de energía eléctrica	
c. Problemas con los sistemas.	
d. Problemas con los equipos informáticos	

37. ¿Considera usted que la información es el activo más crítico que puede tener la entidad?

a. Totalmente en desacuerdo ( )
b. En desacuerdo ( )
c. Ni de acuerdo ni en desacuerdo ( )
d. De acuerdo ( )
e. Totalmente de acuerdo ( )

38. ¿Considera usted que al diseñar un Sistema de Gestión de Seguridad de la información va a ayudar a gestionar la información y los recursos informáticos de manera óptima y segura?

a. Totalmente en desacuerdo ( )
b. En desacuerdo ( )
c. Ni de acuerdo ni en desacuerdo ( )
d. De acuerdo ( )
e. Totalmente de acuerdo ( )

39. ¿Han recibido alguna capacitación en cuanto a seguridad de la información?

a. Si
b. No

40. ¿Cada cuánto tiempo realizan un mantenimiento preventivo al hardware?

a. Entre 1 y dos meses
b. Entre 2 y 6 meses
c. Entre 6 meses y 1 año
d. Nunca

41. ¿Qué tipo de mantenimiento realizan al software?

e. Preventivo
f. Correctivo

42. ¿En general la Sub Gerencia cumple con políticas y normas de seguridad?

a. Si
b. No

ANEXO 3: "ENCUESTA APLICADA A LOS TRABAJADORES DEL ÁREA DE REGISTRO CIVIL"

UNIVERSIDAD NACIONAL SANTIAGO ANTUNEZ DE MAYOLO

Escuela profesional de Ingeniería de Sistemas e Informática

ENCUESTA ÁREA REGISTRO CIVIL

Instrucciones:

Para desarrollar este cuestionario, usted debe leer cada pregunta y escoger una de las alternativas propuestas con una "X" dentro de los paréntesis o llenar dentro de las líneas punteadas según sea su criterio.

1. **Sexo:**
   Masculino ( ) Femenino ( )
2. **Usted apaga los equipos informáticos debidamente después de utilizarlos**
   SI ( ) NO ( )
3. **Si tu respuesta es SÍ, Cómo apagas tu equipo después de trabajar**
   a. Apagando directamente el estabilizador. ( )
   b. Desenchufando el cable de energía de la computadora. ( )
   c. Manteniendo presionando el botón de apagado del CPU. ( )
   d. Haciendo clic en el botón de apagado del menú del sistema operativo. ( )
   e. Bajando la llave de energía.
   ( )
   f. Ninguno. ( )
4. **Se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro del área frente a cualquier desastre natural o humano**
   SI ( ) NO ( )
5. **Ha observado algún extinguidor cerca de los equipos informáticos**
   SI ( ) NO ( )
6. **Ha manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU para hacerlos funcionar**
   SI ( ) NO ( )
7. **Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro del área**
   SI ( ) NO ( )
8. **Hace usted uso de los antivirus en los equipos informáticos, cuando ingresa o saca información en algún dispositivo de almacenamiento**
   Si ( ) A veces ( ) Nunca ( )
9. **Que hace cuando detecta un virus en la computadora que se le proporciona**
   a. Activa el antivirus ( )
   b. Activa el antivirus, detecta los virus y los elimina ( )
   c. Borra el archivo ( )
   d. Formatea el dispositivo de almacenamiento ( )
   e. Llamar al área de informática ( )
10. **Cada que tiempo cambian o actualizan la versión del antivirus**
    a. Mensual ( )
    b. Trimestral ( )
    c. Semestral ( )

d. Anual ( )
e. Nunca ( ),

11. ¿Cuáles son los problemas más frecuentes que solicita la atención del área de informática?

a. Problemas de red
b. Problemas de energía eléctrica
c. Problemas con los sistemas.
d. Problemas con los equipos informáticos

12. Usted hace uso del SISTEMA OREC

SI ( ) NO ( )

Si su respuesta es NO pasar a la pregunta 15.

13. Que tan frecuente es su acceso a la información que proporciona la OREC

Siempre ( ) Casi siempre ( ) Nunca ( )

14. Normalmente su clave de acceso al OREC hace referencia a:

a. Su nombre y apellido ( )
b. Su fecha de nacimiento ( )
c. Teléfono (de casa o móvil) ( )
d. Nombre de su esposo(a) o hijo(a) ( )

15. La Clave con la cual ingresa al OREC es conocida también por:

a. Un compañero de trabajo ( )
b. Mi esposo(a) o hijo(a) ( )
c. No comparte con nadie su clave ( )

16. Cada que tiempo cambia su clave de acceso al OREC

Cada 7 días ( ) Cada 15 días ( ) Cada 30 días ( ) Cada año ( ) Nunca ( )

Y si nunca cambio su clave, cuál es y porque motivo no lo hizo

…….

17. Qué tan veloz es el acceso al Sistema OREC dentro de la Municipalidad

a. Es más rápido dentro de la municipalidad que fuera de ella ( )
b. Es más lenta dentro de la municipalidad que fuera de ella ( )
c. Es igual en ambos lugares ( )

18. Usted recibió alguna capacitación acerca de Seguridad de la Información en la Municipalidad

SI ( ) NO ( )

19. Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información

SI ( ) NO ( )

20. Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:

a. Folletos y boletines ( )

b. Charlas o conferencias ( )
c. Como parte de algún curso en tu carrera ( )

21. ¿En general el área cumple con políticas y normas de seguridad?

c. Si
d. No

Gracias por su colaboración

ANEXO 4: "ENTREVISTA APLICADA AL SUBGERENTE DE INFORMÁTICA Y TELECOMUNICACIONES"

UNIVERSIDAD NACIONAL SANTIAGO ANTUNEZ DE MAYOLO

Escuela profesional de Ingeniería de Sistemas e Informática

ENTREVISTA

Las entidades públicas de hoy en día manejan su información por medio de sistemas integrados u otros, los cuales muchos de ellos ven reflejado la vulnerabilidad de su información frente a cualquier peligro que se les presente. Es por ello que este proyecto de investigación busca encontrar los puntos débiles con respecto a todo lo que es la tecnología de información y comunicación va dirigido al **SUBGERENTE DE INFORMÁTICA Y TELECOMUNICACIONES** como agente beneficiario de la Seguridad de la Información.

A. Toma de decisiones con respecto a la seguridad de la información

1. **¿La Sub Gerencia de Informática y Telecomunicaciones cuenta con un comité de seguridad de la información?**

   SI ( )

   a. Las funciones del comité se encuentran detalladas en el manual de funciones y organización u otro documento_____
   b. Quién conforma ese comité_____
   c. Ese comité es plenamente identificable por la SGIT_____

   NO ( )

   a. Si no cuentan con ese comité, quienes son los encargados de establecer las políticas de seguridad de la información _____
   b. O, sólo las políticas son establecidas por sí mismo _____
   c. Estas políticas son conocidas por todos los usuarios_____
   d. A través de que medio se les dio a conocer_____

B. Mecanismos de control con respecto a la seguridad de la información:

1. ¿Existe algún tipo de manual o documento donde se especifique los controles para la seguridad de la información?_____
2. ¿De qué manera controla a sus trabajadores, con respecto al tema de seguridad de la información?_____
3. ¿De qué forma controla los accesos a la red y quién ordena que se genere esos permisos?_____
4. ¿Existen bitácoras donde se registran los sucesos de todos los usuarios que ingresan a la red?_____
5. Detecto en alguna ocasión algo indebido_____
6. ¿Se registran los accesos de personas a las áreas donde se encuentran los equipos servidores?_____

C. Políticas de seguridad

1. ¿Existe un documento donde se especifique las políticas de seguridad de la información?

SI ( )

a. ¿Quién elaboró ese documento y por quién fue aprobado?_____
b. ¿Sus trabajadores y usuarios conocen este documento?_____
c. ¿Se aplican estas políticas?_____
d. ¿Cada que tiempo se revisan esas políticas?_____

NO ( )

a. ¿Según Usted, a que cree que se deba, que hasta ahora no se implementa las políticas de seguridad de la información?_____
b. ¿Cree Usted, que es de suma urgencia la elaboración de políticas de seguridad de la información?_____
   Porqué_____
c. Y para su área_____

D. <u>Nivel conocimiento de seguridad de la información por parte de su personal</u>

1. Frente a cualquier desastre natural, provocado o humano ¿Su personal conoce cuales son los activos más importantes que debe proteger en relación a la información?
   SI ( )
   a. ¿Para ello existen procedimientos documentados para actuar antes, durante y después del desastre?_____
   b. ¿Ha realizado algún simulacro con defensa civil o tiene previsto hacerlo en el futuro?_____
   c. Lo cree necesario hacerlo con esta organización_____
   d. ¿Su área posee algún plan de contingencia, si no lo tiene ha motivado a sus trabajadores para elaborarlo?_____

   NO ( )
   a. ¿A qué se debe?_____

E. <u>Backups y claves</u>

1. La administración de todos los servicios de tecnología de información que están a su cargo se manejan a través de claves de autenticación_____
2. Cree usted necesario que la alta dirección deba poseer las claves (y su actualización de las mismas)_____
   Porqué_____

3. ¿Existe algún procedimiento para realizar backups, de la información que usted maneja?
   SI ( )
   a. ¿Están descritos en algún documento?_____
   b. ¿Se cumplen conforme están descritos?_____
   c. ¿Son depositados en algún lugar especial? _____
      Porqué_____
   d. Cada que tiempo se hace y quién los realiza_____

   NO ( )
   a. Porqué_____

F. Problemas frecuentes

1. ¿Cuáles son los problemas más frecuentes con los que se enfrenta el área que Usted tiene a cargo?_____
2. Frente a las actividades de su área_____
3. Frente a los servicios que le brinda a los usuarios_____
4. ¿Se encuentran archivados esos problemas? _____
5. ¿Qué estrategia usa para disminuir esos problemas frecuentes? _____
6. Existe alguna estadística de la evolución de esos problemas_____
7. Emplean tarjetas o fichas de seguimiento de los equipos que se les brinda a los usuarios_____

G. Mantenimiento de los equipos

1. ¿Existe un plan de mantenimiento para todos los equipos?
   SI ( )
   a. Cada qué tiempo lo realizan_____
   b. ¿Qué aspectos son los que toman en cuenta para ese mantenimiento?_____
   c. Cómo se trata el tema de los antivirus _____

H. Adquisición de software y hardware

1. ¿Cuál es el procedimiento para la adquisición de un SW o HW?_____
2. Este procedimiento se encuentra debidamente identificado en un documento_____Porqué_____ _____
3. ¿Quién justifica la adquisición?_____
4. ¿Quién evalúa la adquisición?_____
5. ¿Quién evalúa los proveedores?_____

ANEXO 5: "GUÍA DE OBSERVACIÓN APLICADA A LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES"

UNIVERSIDAD NACIONAL SANTIAGO ANTUNEZ DE MAYOLO

Escuela profesional de Ingeniería de Sistemas e Informática

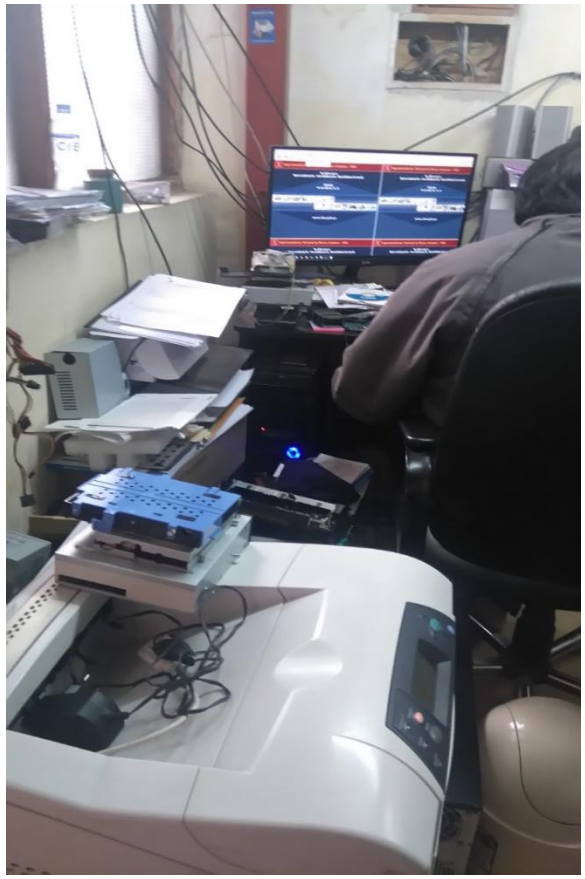
GUÍA DE OBSERVACIÓN

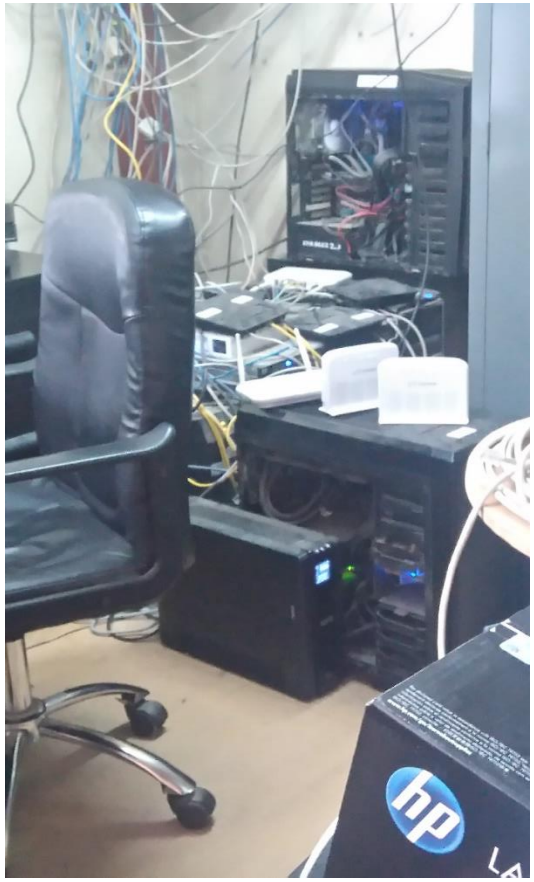
A. Verificar el funcionamiento y cumplimiento adecuado de la red de cómputo, así como la inclusión de sus componentes, su aplicación y su uso.	
Descripción del concepto	**Cumple**
1.- La instalación de la red es flexible y adaptable a las necesidades de la	
2.- La lista de componentes de la red contiene todo el hardware requerido para su funcionamiento adecuado.	
3.-La lista de componentes de la red contiene todo el software requerido para su funcionamiento adecuado.	
4.-La red de cómputo es aprovechada al máximo en la SGIT.	
5.-Los recursos de la red se comparten de acuerdo con las necesidades de	
6.-La configuración de recursos de la red es la mejor para el uso correcto de los sistemas computacionales de la SGIT.	
7.-Se acepta la transferencia frecuente de grandes volúmenes de	
8.-Existen niveles de acceso y seguridad en la red	

B. Verificar la seguridad en el centro de cómputo, y calificar sólo una de las columnas de cada concepto según su grado de cumplimiento					
Descripción del concepto		**100% Excelente**	**80% Cumple**	**60% Mínimo**	**40% Deficiente**
1.	**Evaluación de la seguridad en el acceso al sistema**				
	a. Evaluar los atributos de acceso al				
	b. Evaluar los niveles de acceso al				
	c. Evaluar la administración de contraseñas del sistema.				
	d. Evaluar la administración de la bitácora de acceso al sistema.				
	e. Evaluar el monitoreo en el acceso al sistema.				
	f. Evaluar las funciones del administrador del acceso al sistema.				
	g. Evaluar las medidas preventivas o correctivas en caso de siniestros en el				

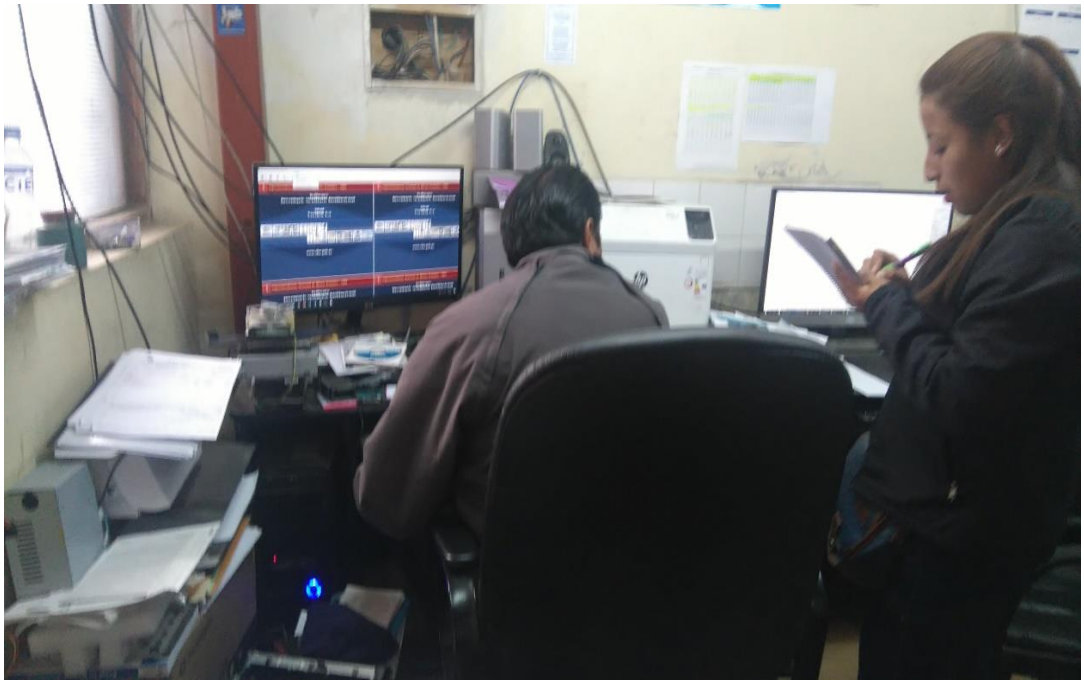
2.	**Evaluación de la seguridad en el acceso al área física**				
	a. Evaluar el acceso del personal a la SGIT.				
	b. Evaluar el acceso de los usuarios y terceros al SGIT.				
	c. Evaluar la administración de la bitácora de acceso físico al área de sistemas.				
	d. Evaluar el control de entradas y salidas de bienes informáticos de la SGIT.				
	e. Evaluar la vigilancia de la SGIT.				
	f. Evaluar las medidas preventivas o correctivas en caso de siniestros en la SGIT.				

ANEXO 6: “FOTOS REALIZADAS AL INTERIOR Y EXTERIOR DE LA OFICINA DE LA SGIT”





“Interior de la SGIT”



“Interior de la SGIT”

“Exterior de la SGIT”

“Exterior de la SGIT”

ANEXO 7: "RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SGIT"

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SGIT				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
1	**Sexo**	Femenino	0	0%
		Masculino	6	100%
		Total		**100%**
2	**¿Cuantas áreas se encuentran involucradas en algún proceso con la Sub Gerencia?**	1 a 5	0	0%
		6 a 10	0	0%
		11 a 15	4	67%
		15 a más	2	33%
		Total		**100%**
3	**¿Se ha presentado alguna iniciativa de seguridad de la información?**	Sí	2	33%
		No	4	67%
		Total		**100%**
4	**¿Se ha presentado alguna iniciativa de tratamiento de riesgo?**	Sí	3	50%
		No	3	50%
		Total		**100%**
5	**¿Ha tenido incidentes de seguridad de la información en estos 3 últimos años?**	Sí	2	33%
		No	4	67%
		Total		**100%**
6	**En los últimos 3 años se ha realizado algún tratamiento de amenazas y vulnerabilidades presentadas**	Sí	1	17%
		No	5	83%
		Total		**100%**
7	**¿Considera usted que por medio de la evaluación de riesgos va a ser posible mitigar la mayor cantidad de vulnerabilidades existentes?**	Totalmente en desacuerdo	0	0%
		En desacuerdo	0	0%
		Ni de acuerdo ni en desacuerdo	0	0%
		De acuerdo	5	83%
		Totalmente de acuerdo	1	17%
		Total		**100%**
8	**¿Se tiene definida una política para la realización de copias de seguridad de los datos?**	Sí	1	17%
		No	5	83%
		Total		**100%**
9	**¿Se tiene definida una política de restauración de los sistemas en caso de ataques informáticos?**	Sí	1	17%
		No	5	83%
		Total		**100%**

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SGIT				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
10	**¿Recomendaría usted adoptar políticas de seguridad encaminadas a proteger la información y evitar posibles daños de la información?**	Sí	6	100%
		No	0	0%
		Total		**100%**
11	**¿Se ha establecido algún tipo de organización interna dentro de la Sub Gerencia orientada a la seguridad de la información?**	Sí	0	0%
		No	6	100%
		Total		**100%**
12	**¿Se ha permitido el acceso a la información sólo a personas debidamente autorizadas?**	Sí	5	83%
		No	1	17%
		Total		**100%**
13	**¿Se ha realizado la gestión de altas y bajas en el registro de usuarios?**	Sí	4	67%
		No	2	33%
		Total		**100%**
14	**¿Se ha realizado la gestión de acceso con privilegios por usuario?**	Sí	0	0%
		No	6	100%
		Total		**100%**
15	**¿Con qué frecuencia se cambian las contraseñas del pc a su cargo?**	Entre 1 y dos meses	0	0%
		Entre 2 y 6 meses	0	0%
		Entre 6 meses y 1 año	2	33%
		Más de 1 año	4	67%
		Total		**100%**
16	**El lugar donde se ubica la oficina, ¿está seguro de inundaciones, robo o cualquier otra situación que pueda poner en peligro los equipos?**	Sí	0	0%
		No	6	100%
		Total		**100%**
17	**¿El material con que el que está construido las oficinas donde labora son confiables?**	Sí	1	17%
		No	5	83%
		Total		**100%**
18	**¿Existe lugar suficiente para la documentación y los equipos?**	Sí	0	0%
		No	6	100%
		Total		**100%**

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SGIT				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
19	**¿Dentro del Área existen materiales que puedan ser inflamables o causar algún daño sobre la documentación o los equipos?**	Sí	6	100%
		No	0	0%
		Total		**100%**
20	**¿Se cuenta con una salida de emergencia?**	Sí	0	0%
		No	6	100%
		Total		**100%**
21	**¿Los equipos cuentan con un regulador?**	Sí	4	67%
		No	2	33%
		Total		**100%**
22	**¿Los cables están dentro de paneles y canaletas eléctricas?**	Sí	0	0%
		No	6	100%
		Total		**100%**
23	**¿Se ha realizado auditorias en los sistemas de información?**	Sí	1	17%
		No	5	83%
		Total		**100%**
24	**¿El cableado se encuentra correctamente instalado?**	Sí	3	50%
		No	3	50%
		Total		**100%**
25	**¿Se cuenta con pozo a tierra?**	Sí	5	83%
		No	1	17%
		Total		**100%**
26	**¿Se cuenta con mecanismos de seguridad asociados a servicios en red?**	Sí	3	50%
		No	3	50%
		Total		**100%**
27	**¿se ha realizado revisiones técnicas tras efectuar cambios en los sistemas?**	Sí	5	83%
		No	1	17%
		Total		**100%**
28	**¿Se tiene alguna especificación en cuanto a seguridad, de la línea otorgada por empresas privadas?**	Sí	0	0%
		No	6	100%
		Total		**100%**
29	**¿La instalación eléctrica de la Sub Gerencia es independiente de otras instalaciones?**	Sí	0	0%
		No	6	100%
		Total		**100%**

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SGIT				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
30	**¿Con que frecuencia se les da mantenimiento a las instalaciones y suministros de energía?**	Entre 1 y dos meses	0	0%
		Entre 2 y 6 meses	1	17%
		Entre 6 meses y 1 año	2	33%
		Más de 1 año	3	50%
		Total		**100%**
31	**¿Qué nivel de respuesta a incidentes de seguridad poseen?**	Alto	1	17%
		Medio	2	33%
		Baja	3	50%
		Total		**100%**
32	**¿Se ha identificado puntos débiles de seguridad dentro de la Sub Gerencia?**	Sí	6	100%
		No	0	0%
		Total		**100%**
33	**¿Los sistemas operativos utilizados son de uso gratuito?**	Sí	0	0%
		No	6	100%
		Total		**100%**
34	**¿Los activos de información fueron manipulados o modificado por una entidad externa?**	Sí	1	17%
		No	5	83%
		Total		**100%**
35	**¿Usted ha podido tener acceso a la información en tiempo real?**	Sí	3	50%
		No	3	50%
		Total		**100%**
36	**Si su respuesta es negativa en la preg. 35, Marque con una "x" las siguientes afirmaciones :**	Problemas de red	1	33%
		Problemas de energía eléctrica	1	33%
		Problemas con los sistemas.	0	0%
		Problemas con los equipos informáticos	1	33%
		Total		**100%**
37	**¿Considera usted que la información es el activo más crítico que puede tener la entidad?**	Totalmente en desacuerdo	0	0%
		En desacuerdo	0	0%
		Ni de acuerdo ni en desacuerdo	0	0%
		De acuerdo	5	83%
		Totalmente de acuerdo	1	17%
		Total		**100%**

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DE LA SGIT				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
38	**¿Considera usted que al diseñar un Sistema de Gestión de Seguridad de la información va a ayudar a gestionar la información y los recursos informáticos de manera óptima y segura?**	Totalmente en desacuerdo	0	0%
		En desacuerdo	0	0%
		Ni de acuerdo ni en desacuerdo	0	0%
		De acuerdo	0	0%
		Totalmente de acuerdo	6	100%
		Total		**100%**
39	**¿Han recibido alguna capacitación en cuanto a seguridad de la información?**	Sí	2	33%
		No	4	67%
		Total		**100%**
40	**¿Cada cuánto tiempo realizan un mantenimiento preventivo al hardware?**	Entre 1 y dos meses	1	17%
		Entre 2 y 6 meses	1	17%
		Entre 6 meses y 1 año	4	67%
		Nunca	0	0%
		Total		**100%**
41	**¿Qué tipo de mantenimiento realizan al software?**	Preventivo	3	50%
		Correctivo	3	50%
		Total		**100%**
42	**¿En general la Sub Gerencia cumple con políticas y normas de seguridad?**	Si	1	17%
		No	5	83%
		Total		**100%**

ANEXO 8: "RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DEL ÁREA DE REGISTRO CIVIL"

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DEL ÁREA DE REGISTRO CIVIL				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
1	**Sexo**	Femenino	2	50%
		Masculino	2	50%
		Total		**100%**
2	**¿Usted apaga los equipos informáticos debidamente después de utilizarlos?**	Sí	4	100%
		No	0	0%
		Total		**100%**
3	**Si tu respuesta es SÍ, ¿Cómo apagas tu equipo después de trabajar?**	Apagando directamente el estabilizador.	0	0%
		Desenchufando el cable de energía de la computadora.	0	0%
		Manteniendo presionando el botón de apagado del CPU.	1	25%
		Haciendo clic en el botón de apagado del menú del sistema operativo.	3	75%
		Bajando la llave de energía.	0	0%
		Ninguno.	0	0%
		Total		**100%**
4	**¿Se siente seguro en los ambientes donde se encuentran los equipos informáticos dentro del área frente a cualquier desastre natural o humano?**	Sí	3	75%
		No	1	25%
		Total		**100%**
5	**¿Ha observado algún extinguidor cerca de los equipos informáticos?**	Sí	1	25%
		No	3	75%
		Total		**100%**
6	**¿Ha manipulado alguna vez las entradas de corriente al CPU, los cables del teclado, mouse y conexiones de red que conectan al CPU para hacerlos funcionar?**	Sí	4	100%
		No	0	0%
		Total		**100%**

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DEL ÁREA DE REGISTRO CIVIL				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
7	**¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro del área?**	Totalmente en desacuerdo	0	0%
		En desacuerdo	0	0%
		Ni de acuerdo ni en desacuerdo	2	50%
		De acuerdo	2	50%
		Totalmente de acuerdo	0	0%
		Total		**100%**
8	**¿Hace usted uso de los antivirus en los equipos informáticos, cuando ingresa o saca información en algún dispositivo de almacenamiento?**	Sí	3	75%
		A veces	1	25%
		Nunca	0	0%
		Total		**100%**
9	**¿Que hace cuando detecta un virus en la computadora que se le proporciona?**	Activa el antivirus	3	75%
		Activa el antivirus, detecta los virus y los elimina	1	25%
		Borra el archivo	0	0%
		Formatea el dispositivo de almacenamiento	0	0%
		Llamar al área de informática	0	0%
		Total		**100%**
10	**¿Cada que tiempo cambian o actualizan la versión del antivirus?**	Mensual	0	0%
		Trimestral	0	0%
		Semestral	0	0%
		Anual	3	75%
		Nunca	1	25%
		Total		**100%**
11	**¿Cuáles son los problemas más frecuentes que solicita la atención del área de informática?**	Problemas de red	1	25%
		Problemas de energía eléctrica	0	0%
		Problemas con los sistemas.	0	0%
		Problemas con los equipos informáticos	3	75%
		Total		**100%**
12	**¿Usted hace uso del SISTEMA OREC?**	Sí	2	50%
		No	2	50%
		Total		**100%**

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DEL ÁREA DE REGISTRO CIVIL				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
13	**Si su respuesta es NO pasar a la pregunta 18. ¿Que tan frecuente es su acceso a la información que proporciona la OREC?**	Siempre	2	100%
		Casi siempre	0	0%
		Nunca	0	0%
		Total		**100%**
14	**Normalmente su clave de acceso al OREC hace referencia a:**	Su nombre y apellido	0	0%
		Su fecha de nacimiento	0	0%
		Teléfono	0	0%
		Nombre de un familiar	0	0%
		Otro	2	100%
		Total		**100%**
15	**La Clave con la cual ingresa al OREC es conocida también por:**	Un compañero de trabajo	0	0%
		Un familiar	0	0%
		No comparte con nadie su clave	2	100%
		Total		**100%**
16	**¿Cada que tiempo cambia su clave de acceso al OREC?**	Cada 7 días	0	0%
		Cada 15 días	0	0%
		Cada 30 días	2	100%
		Cada año	0	0%
		Nunca	0	0%
		Total		**100%**
17	**¿Qué tan veloz es el acceso al Sistema OREC dentro de la Municipalidad?**	Es más rápido dentro de la municipalidad que fuera de ella	0	0%
		Es más lenta dentro de la municipalidad que fuera de ella	1	50%
		Es igual en ambos lugares	1	50%
		Total		**100%**
18	**¿Usted recibió alguna capacitación acerca de Seguridad de la Información en la Municipalidad?**	Sí	0	0%
		No	4	100%
		Total		**100%**
19	**¿Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información?**	Si	4	100%
		No	0	0%
		Total		**100%**

RESULTADOS DE LA ENCUESTA APLICADA A LOS TRABAJADORES DEL ÁREA DE REGISTRO CIVIL				
ID	**PREGUNTA**	**RESPUESTA**	**CANTIDAD**	**PORCENTAJE**
20	**Si le interesaría conocer más acerca del tema de Seguridad de la Información, a través de que medio te gustaría ser informado:**	Folletos y boletines	1	25%
		Charlas o conferencias	3	75%
		Como parte de algún curso en tu carrera	0	0%
		Total		**100%**
21	**¿En general cree usted que el área de Registro civil cumple con políticas y normas de seguridad?**	Si	0	0%
		No	4	100%
		Total		**100%**

ANEXO 9: “DESCRIPCIÓN DE CONTROLES ISO/IEC 27002:2013 APLICADOS A LA SUBGERENCIA DE INFORMÁTICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA”

5. Políticas de Seguridad

5.1. Generalidades: La Municipalidad Distrital de Independencia debe contar con una política de seguridad, la cual expresa una intención global de la dirección de la institución.

5.2. Objetivo: Describir las reglas que conciernen a acciones o decisiones para alcanzar los objetivos. En algunos casos puede ser de utilidad identificar previamente los procesos clave asociados con el asunto principal de la política para pasar posteriormente a identificar las reglas de operación de los procesos.

5.3. Alcance: Esta política se debe aplicar a todo el sistema de redes y telecomunicaciones, ya que cada institución debe adecuarse a la necesidad de sus usuarios y valorar los controles aplicables.

5.4. Responsables:

5.4.1. El responsable del Área informática: Se encargará de elaborar la política de seguridad con la participación del área de la Subgerencia de Informática y Telecomunicaciones, la cual cuente con objetivos alcanzables y aplicables a la realidad, así como su cumplimiento.

5.5. Políticas

5. Políticas de Seguridad	5.1	Dirección de la Alta Gerencia para la Seguridad de la Información	
	5.1.1	Política de Seguridad de la Información	Se requiere establecer las políticas necesarias que definan los lineamientos internos para asegurar los activos de información críticos que contienen información confidencial o son vitales para la continuidad de las operaciones de la municipalidad.
	5.1.2	Revisión de las Políticas de Seguridad de la Información	En el documento: “Política de Seguridad de la Información” se establece un procedimiento de revisión de la política de seguridad

6. Organización de la Seguridad de la Información

6.1. Generalidades: La Municipalidad Distrital de Independencia debe establecer la administración de la seguridad de la información, como parte fundamental de los objetivos y actividades de la misma.

6.2. Objetivo: Definir formalmente un ámbito de gestión para efectuar tareas tales como la aprobación de las políticas de seguridad, la coordinación de la implementación de la seguridad y la asignación de funciones y responsabilidades.

6.3. Alcance: Esta política se debe aplicar a todo el sistema de redes y telecomunicaciones, involucrando a las demás áreas.

6.4. Responsables:

6.4.1. El responsable del Área informática: Se encargará de habilitar y facultar de conocimiento al personal involucrado, con asesoramientos en materia de seguridad de la información.

6.4.2. El responsable de redes y telecomunicaciones: Sera el encargado de administrar adecuadamente la seguridad, por lo que se establecerán las medidas adecuadas para la protección de la información.

6.5. Políticas

6. Organización de la Seguridad de la Información	6.1	Organización Interna	
	6.1.1	Roles y Responsabilidades para la seguridad de la información	Se debe establecer las responsabilidades y roles requeridos tanto en el equipo de seguridad, así como para los trabajadores, en la cual se debe establecer como mínimo un comité de seguridad de la información que pueda implementar y dar el mantenimiento al SGSI.
	6.1.2	Segregación de funciones	Las actividades de cada área son conocidas, sin embargo, la documentación que es generada casi son nulas, además de no existir gráficos unificados que nos muestren el flujo de la información a través de los diferentes procesos.
	6.1	Organización Interna	
	6.1.3	Contacto con autoridades	Establecer el flujo a seguir para la notificación de un incidente de seguridad de la información, del mismo modo la identificación de las autoridades pertinentes, lo cual ayudara a que no sucedan estos desapercibidos, estableciendo los controles adecuados por parte de las autoridades.
	6.1.4	Contacto con grupos de interés especial	La Municipalidad de Independencia debe establecer los flujos correctos de comunicación con los grupos de interés (RENIEC, MEF, otros), con la finalidad de mantener un canal de comunicación (información), tomando como buenas prácticas usadas por la institución alertando las posibles vulnerabilidades que puedan afectar al respaldo de la información.
	6.1.5	Seguridad de la Información en gerencia de proyectos	Este proyecto debe ser gestionado dentro de los alcances y deberá ser gestionado mediante una metodología que cuente con la gestión de riesgos y debe seguir los lineamientos de la seguridad de la información, con la finalidad de garantizar el cumplimiento de los requisitos de seguridad de la Municipalidad.

	6.2	Dispositivos móviles y teletrabajo	
	6.2.1	Política de dispositivos móviles	No es considerado ya que no aplica para nuestro estudio dado a que no se utilizan dispositivos móviles en los procesos del alcance del proyecto
	6.2.2	Teletrabajo	No es considerado ya que no aplica para nuestro estudio dado a que no se utilizan dispositivos móviles en los procesos del alcance del proyecto

7. Seguridad en los Recursos Humanos

7.1. Generalidades: Debe educarse e informar al personal desde su ingreso y en forma continua, cualquiera sea su situación de actividad, acerca de las medidas de seguridad que afectan al desarrollo de sus funciones y de las expectativas depositadas en ellos en materia de seguridad y asuntos de confidencialidad.

7.2. Objetivo: Reducir los riesgos de error humano, comisión de actos ilícitos, uso inadecuado de instalaciones y recursos y manejo no autorizado de la información, junto a la definición de posibles sanciones que se aplicarán en caso de incumplimiento.

7.3. Alcance: La política de seguridad de la institución debe ser aplicada por todos los trabajadores, en el transcurso de sus actividades y tareas involucradas.

7.4. Responsables:

7.4.1. El responsable del Área informática: Se encargará de entregar y hacer de conocimiento de la política de seguridad al área de recursos humanos para su adaptación a las funciones de puesto.

7.4.2. Área de Recursos Humanos: Es su responsabilidad incluir las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informar a todo el personal que ingresa

de sus obligaciones respecto del cumplimiento de la Política de Seguridad de la Información, gestionar los Compromisos de Confidencialidad con el personal y coordinar las tareas de capacitación de usuarios respecto a las necesidades actuales en seguridad.

7.4.3. Área Jurídica: Se encargará de la confección del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en el organismo, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento de las Políticas en seguridad y en el tratamiento de incidentes de seguridad que requieran de su intervención.

7.5. Políticas

7. Seguridad en los Recursos Humanos	7.1	Previo al Empleo	
	7.1.1	Verificación de antecedentes	Debe realizarse la verificación de los antecedentes del personal, lo cual nos permitirá filtrar a aquellas personas que puedan constituir un riesgo para la Municipalidad o la información que se maneja ya sea por conflicto o intereses personales.
	7.1.2	Términos y condiciones de empleo	Se debe establecer las condiciones de empleo, las cuales se deben comunicar a las personas seleccionadas previo a la firma del contrato, en la cual se detalle las responsabilidades que tiene en cuanto a la seguridad de la información; la cual acepta antes de iniciar sus labores en la institución.
	7.2	Durante el Empleo	
	7.2.1	Responsabilidades de la Alta Gerencia	Se debe especificar la responsabilidad de la alta gerencia en cuanto a la implementación y el mantenimiento del SGSI puesto a que esto corresponde al plan estratégico de la Municipalidad y a los intereses de los usuarios como parte activa en los requerimientos.
	7.2.2	Conciencia, educación y capacitación de Seguridad de la Información	Se debe establecer un plan de capacitación para los colaboradores, acerca de la política de seguridad de la información, del mismo modo la evaluación que nos permitirá medir el nivel de conocimiento del tema.

	7.2.3	Proceso disciplinario	Establecer penalizaciones disciplinarias aplicadas a los colaboradores que infrinjan las condiciones del empleo en cuanto a la seguridad de la información.
	7.3	Término y Cambio de Empleo	
	7.3.1	Termino de responsabilidades o cambio de empleo	El periodo de tiempo al cual se encuentra sujeta el colaborador debe cumplir con los términos y condiciones establecidos en el momento de incorporarse, lo que permitirá a la Municipalidad protegerse de posibles filtraciones realizadas por trabajadores cesados.

8. Gestión de Activos

8.1. Generalidades: La institución debe clasificar los activos de información de acuerdo a la sensibilidad y criticidad de la información que contienen o bien de acuerdo a la funcionalidad que cumplen y rotulados en función a ello, con el objeto de señalar cómo ha de ser tratada y protegida dicha información

8.2. Objetivo: La institución debe tener el conocimiento preciso sobre los activos que posee como parte importante de la administración de riesgos.

8.3. Alcance: La clasificación de activos abarca a toda la institución porque cuenta con al menos cada área con un activo físico o lógico en riesgo.

8.4. Responsables:

8.4.1. El responsable del Área informática: Se encargará de elaborar y mantener un inventario de activos de información, mostrando los propietarios de los activos del área (directivos o gestores responsables de proteger sus activos) y los detalles relevantes (por. ej., ubicación, nº de serie, nº de versión, estado de desarrollo / pruebas / producción, etc.).

8.5. Políticas

8. Gestión de Activos	8.1	Responsabilidad de los Activos	
	8.1.1	Inventario de activos	Dado que la información sensible es utilizada para fines de Registros civiles, la institución debe manejar un inventario de activos, en el cual se detalle la ubicación y el tipo del mismo, la cual nos permitirá realizar la relación con las políticas de uso según su categoría.
	8.1.2	Propiedad de los activos	Los activos de información deben ser asignados a un almacenero (custodio) encargado del inventario, clasificación y protección de los activos, así como de la destrucción en caso sea necesaria y la revisión de las restricciones en cuanto a accesos.
	8.1.3	Uso aceptable de los activos	Debe especificarse y documentar a que se define como uso aceptable en cuanto a manejo información personal y sensible mediante una política o procedimiento que debe ser de conocimiento obligatorio para el personal del área
	8.2	Clasificación de la información	
	8.2.1	Clasificación de la información	Se debe realizar una clasificación de los activos identificados según su criticidad para el negocio o el nivel de confidencialidad que se les debe otorgar.
	8.2.2	Etiquetado de la información	La clasificación de la información debe ser dependiendo del contexto, por este motivo se debe revisar la clasificación periódicamente.
	8.2.3	Manejo de activos	Se debe mantener un correcto uso de la información, se debe realizar el etiquetado que identifique la información según la clasificación previamente definida.
	8.3	Manejo de medios	
	8.3.1	Gestión de medios removibles (Extraíbles)	Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la Municipalidad.

	8.3.2	Eliminación de medios	Para eliminar los medios que contienen información confidencial se debe seguir un protocolo que asegure su correcto desecho, de manera que no puedan ser reutilizados por otras personas ajenas.
	8.3.3	Transporte de medios físicos	Se deben establecer protocolos que aseguren la información en su transferencia física de manera que en la entrada y salida de datos u archivos se garantice la no manipulación de la misma.

9. Control de Acceso

9.1. Generalidades: cada institución debe aplicar el impedimento el acceso no autorizado a los sistemas de información, así también se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

9.2. Objetivo: Controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

9.3. Alcance: Los procedimientos comprenden todas las etapas del ciclo de DEMING de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

9.4. Responsables:

9.4.1. El responsable de redes y telecomunicaciones: Sera el encargado de controlar el flujo de la información en los diferentes niveles de acceso, comprendiendo todas las etapas del ciclo de DEMING de los accesos de los usuarios.

9.4.2. El responsable del Área informática: Se encargará de concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

9.5. Políticas

9. Control de Acceso	9.1	Requerimientos de Negocio para el Control de Accesos	
	9.1.1	Política de Control de Acceso	El control de acceso a la información de Registros Civiles debe estar documentada y debe ser de conocimiento del personal, también debe definir los niveles de escalamiento para la autorización del uso de información en caso sea requerida
	9.1.2	Política en el uso de servicios de red	Establecer una política de accesos a nivel de red que nos permita establecer los lineamientos en cuanto a segmentación de redes, accesos de externos a la red interna, monitoreo, etc.
	9.2	Gestión de Accesos de Usuario	
	9.2.1	Registro y baja del usuario	Para poder mitigar el riesgo de acceso no autorizado, se debe mantener un procedimiento de altas y sobre todo bajas de usuarios de los sistemas que maneja la Municipalidad.
	9.2.2	Gestión de privilegios	Contar con una correcta gestión de privilegios que permitirá limitar el acceso según las funciones o áreas a las cuales cada colaborador pertenece.
	9.2.3	Gestión de información de autenticación secreta de usuarios	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado que permitirá tener una trazabilidad de las acciones realizadas por los usuarios.
	9.2.4	Revisión de derechos de acceso de usuarios	La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.

	9.2.5	Eliminación o ajuste de derechos de acceso	Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.
	9.3	Responsabilidades del Usuario	
	9.3.1	Uso de información de autenticación secreta	Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la institución en el uso de información confidencial para la autenticación.
	9.4	Control de Acceso de Sistemas y Aplicaciones	
	9.4.1	Restricción de acceso a la información	Si bien se cuenta con el control básico, se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos.
	9.4.2	Procedimientos de inicio de sesión segura	Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro enfocado a proteger la información de inicio de sesión del usuario en los sistemas.
	9.4.3	Sistema de gestión de contraseñas	Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad. Establecer requisitos mínimos en cuanto a la complejidad de contraseñas.
	9.4.4	Uso de programas y utilidades privilegiadas	El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.
	9.4.5	Control de acceso al código fuente del programa	Se debería restringir el acceso al código fuente de las aplicaciones software.

10. Cifrado

10.1. Generalidades: La Sub Gerencia de Informática y Telecomunicaciones debe aplicar medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

10.2. Objetivo: Adoptar el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

10.3. Alcance: Estas medidas y técnicas criptográficas debe abordar a todos los activos relacionados con el riesgo de pérdida de información o manipulación inadecuada del mismo.

10.4. Responsables:

10.4.1. El responsable de redes y telecomunicaciones: Sera el encargado de definir las medidas y técnicas aplicables y que se adapten a la realidad de la institución para llevar un control adecuado del flujo de la información.

10.5. Políticas

10. Cifrado	10.1	Controles Criptográficos	
	10.1.1	Restricción de acceso a la información	Debe manejarse y activar controles criptográficos que garanticen que la información debe mantenerse bajo custodia para tener la integridad de la información y evitar que se pueda transferir la información
	10.1.2	Procedimientos de inicio de sesión segura	En el proceso del proyecto se debe considerar la gestión de claves puesto que permitirá que la persona que cuente con clave será responsable de la información que maneja, ya que también debe realizarse la renovación de claves.

11. Seguridad Física y del Entorno

11.1. **Generalidades:** establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la institución, contra accesos físicos no autorizados. El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

11.2. Objetivo: minimizar los riesgos de daños e interferencias a la información y a las operaciones de la Municipalidad Distrital de Independencia.

11.3. Alcance: los controles de protección de la información se enfocarán en las áreas que cuenten con información sensible con riesgo de pérdida.

11.4. Responsables:

11.4.1. El responsable de redes y telecomunicaciones: Sera el encargado de definir los controles de protección de la información y telecomunicaciones.

11.4.2. El responsable del Área informática: Se encargará del transporte y la disposición final presentan riesgos que deben ser evaluados, especialmente en casos en los que el equipamiento perteneciente a la institución esté físicamente fuera del mismo.

11.5. Políticas

11. Seguridad Física y del Entorno	11.1	Áreas Seguras	
	11.1.1	Perímetro de seguridad física	Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica. El objetivo es establecer un límite de accesos entre los usuarios y colaboradores.
	11.1.2	Controles físicos de entrada	Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso. El personal debe estar debidamente identificado en todo momento.
	11.1.3	Seguridad de oficinas, despachos y recursos	Se debería diseñar y aplicar un sistema de seguridad física a las oficinas e instalaciones de la Municipalidad.
	11.1.4	Protección contra amenazas externas y del ambiente	Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes, que puedan afectar tanto natural como provocados (incendios).
	11.1.5	Trabajo en áreas seguras	Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.
	11.1.6	Áreas de acceso público, entrega y carga.	No se considera dado que el envió de los activos de información se realizan directamente al área correspondiente
	11.2	Áreas Seguras	
	11.2.1	Instalación y protección de equipo	Los equipos se deberían instalarse y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.
	11.2.2	Servicios de soporte (instalaciones de suministro)	Los equipos críticos relacionados al mantenimiento de información sensible deben contar con medidas que aseguren su funcionamiento en caso de caída de algún servicio sobre el que se soporten (fluido eléctrico, por ejemplo)
	11.2.3	Seguridad en el cableado	Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.

	11.2.4	Mantenimiento de equipos	Los equipos que cuenten con acceso a información critica deberán seguir un procedimiento de mantenimiento adecuado de manera que la información que contienen no sea comprometida.
	11.2.5	Retiro de activos	La Municipalidad debe establecer políticas que limiten el retiro de la información sensible de las instalaciones a excepción de ser para cumplir con alguno de los servicios que brinda
	11.2.6	Seguridad del equipo y activos fuera de la instalación	La Municipalidad debe asegurar que cualquier uso externo de la información que maneja la oficina de registros, haya sido previamente autorizado por las personas correspondientes.
	11.2.7	Eliminación segura o reúso del dispositivo de almacenamiento	Los equipos informáticos que se den de baja o se cambien de ambiente deben haber pasado por un proceso de limpieza que elimine de manera adecuada la información que puedan contener
	11.2.8	Equipo informático de usuario desatendido	Los usuarios deberán mantener la seguridad de sus equipos incluso cuando no estén trabajando con los mismos
	11.2.9	Política del puesto de trabajo despejado y bloqueo de pantalla	Los usuarios deberán mantener sus escritorios libres de cualquier información sensible que pueda usar un agente externo como consecuencia de sus exposiciones como parte de un olvido o mala gestión

12. Seguridad en la operativa

12.1. Generalidades: La Municipalidad Distrital de Independencia debe crear condiciones que garanticen la confidencialidad, integridad y disponibilidad de la información que se produce y se recibe a través de diferentes canales de operación.

12.2. Objetivo: Adoptar medidas de seguridad encaminadas a prevenir la proliferación y expansión de software malicioso que son catalogadas como amenazas en potencia, garantizar el adecuado funcionamiento de los

sistemas de información y designar responsables encargados de adoptar todas las medidas de seguridad necesarias para prevenir posibles ataques.

12.3. Alcance: Esta política se debe aplicar a todo el sistema informático (red, servidores, comunicaciones y equipos) etc.

12.4. Responsables:

12.4.1. El responsable de la seguridad informática: Sera el encargado de definir procedimientos para el control actualización y modificación de los sistemas operativos tanto de servidores como Pc's.

- Para la actualización, modificación y mantenimiento debe estar debidamente documentada.
- Se debe tener mecanismos para el reporte y manejo de incidentes
- Se debe tener políticas de control para el uso de correo electrónico, consulta de páginas, navegación en internet y uso de redes sociales.
- Adquirir antivirus licenciado y verificar que las actualizaciones se estén realizando periódicamente.
- Establecer y verificar políticas de control de usuarios mediante contraseñas y gestión de privilegios.
- Controlar la realización de copias de seguridad.
- Todo procedimiento debe ser debidamente documentado.

12.4.2. El responsable del Área informática: Se encargara de adoptar todas las políticas establecidas por el responsable de la seguridad y verificara el cumplimiento de las mismas.

12.5. Políticas

12. Seguridad en la operativa	**12.1**	**Responsabilidades y procedimientos de operación**	
	12.1.1	Documentación de procedimientos de operación	Los sistemas operativos se actualizarán permanentemente y toda actualización y modificación será autorizada por el responsable de seguridad y debidamente documentada y realizada por el área de informática.
	12.1.2	Gestión de cambios	Los cambios deben ser evaluados y aprobados previamente y se tendrán en cuenta los siguientes aspectos: Evaluación del cambio y posible impacto, planificación, prueba, e identificación de responsabilidades en caso de que el cambio sea fallido.
	12.1.3	Gestión de capacidades	Se necesitará monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.
	12.1.4	Separación de entornos de desarrollo, prueba y producción	Cada entorno de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.
	12.2	Protección contra código malicioso	
	12.2.1.	Controles contra el código malicioso	Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.
	12.3	Copias de seguridad	
	12.3.1	Copias de seguridad de la información	Es necesario realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación a una política de respaldo (Backup) convenida.
	12.4	Registro de actividad y supervisión	
	12.4.1	Registro y gestión de eventos de actividad	Se tiene que producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.

	12.4.2	Protección de los registros de información	Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.
	12.4.3	Registros de actividad del administrador y operador del sistema	Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.
	12.4.4	Sincronización de relojes	Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación a una fuente de sincronización única de referencia.
	12.5	Control del software en explotación	
	12.5.1	Instalación del software en sistemas en producción	Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.
	12.6	Gestión de la vulnerabilidad técnica	
	12.6.1	Gestión de las vulnerabilidades técnicas	Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.
	12.6.2	Restricciones en la instalación de software	Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
	12.7	Consideraciones de las auditorías de los sistemas de información	
	12.7.1	Controles de auditoría de los sistemas de información	Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.

13. Seguridad en las telecomunicaciones

13.1. Generalidades: La Municipalidad Distrital de Independencia debe crear condiciones que garanticen la seguridad en cuanto a las telecomunicaciones.

13.2. Objetivo: Adoptar medidas de seguridad encaminadas a prevenir la mala implementación de redes de telecomunicaciones dentro de la entidad para poder garantizar su debida seguridad.

13.3. Alcance: Esta política se debe aplicar a todo el sistema de redes y telecomunicaciones.

13.4. Responsables:

13.4.1. El responsable de redes y telecomunicaciones: Sera el encargado de definir procedimientos para el control implementación y modificación de las telecomunicaciones.

13.4.2. El Responsable del Área informática: Se encargara de adoptar todas las políticas establecidas por el responsable de la redes y verificara el cumplimiento de las mismas.

13.5. Políticas

13. Seguridad en las telecomunicaciones	13.1	Gestión de la seguridad en las redes	
	13.1.1	Controles de red	Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.
	13.1.2	Mecanismos de seguridad asociados a servicios en red	Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.
	13.1.3	Segregación de redes	Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.
	13.2	Intercambio de información con partes externas	
	13.2.1	Políticas y procedimientos de intercambio de información	Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.
	13.2.2	Acuerdos de intercambio	Los acuerdos deberían abordar la transferencia segura de información entre la municipalidad y las partes externas.

	13.2.4	Acuerdos de confidencialidad y secreto	Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.

14. Adquisición, desarrollo y mantenimiento de sistemas de información

14.1. Generalidades: Se debe documentar y aprobar los requerimientos de seguridad a aplicar en la implementación de los sistemas de información; se debe llevar a cabo adecuadas políticas de seguridad para las bases de datos, los sistemas operativos, todo esto con el fin de evitar que personas conocedoras de los procesos puedan cometer fraudes o ilícitos y si es el caso identificarlos de manera inmediata.

14.2. Objetivo: Adoptar medidas de seguridad en la implementación de los sistemas de información.

14.3. Alcance: Esta política se debe aplicar a todos los sistemas informáticos tanto sistemas operativos como software requerido para la Municipalidad.

14.4. Responsables:

14.4.1. Responsable de la seguridad informática, el propietario de la información y el área de auditoria interna se encargaran de definir e implementar controles en el desarrollo y mantenimiento de sistemas de información.

14.4.2. El responsable del Área informática, se encargará de definir el procedimiento para asignar claves, de garantizar el cumplimiento de los requisitos de seguridad del software, de controlar los cambios en los sistemas etc.

14.4.3. El responsable del área legal y administrativa, se encargara del licenciamiento del software adquirido y en el caso del software desarrollado por la organización de establecer las políticas de derechos de autor y fijar las condiciones de los contratos y de entrega.

14.5. Políticas

14. Adquisición, desarrollo y mantenimiento de los sistemas de información	14.1	Requisitos de seguridad de los sistemas de información.	
	14.1.1	Análisis y especificación de los requisitos de seguridad.	Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.
	14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.
	14.1.3	Protección de las transacciones por redes telemáticas.	La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.
	14.2	Seguridad en los procesos de desarrollo y soporte.	
	14.2.1	Política de desarrollo seguro de software.	Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la Municipalidad.
	14.2.2	Procedimientos de control de cambios en los sistemas.	En el ciclo de DEMING de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la Municipalidad.
	14.2.4	Restricciones a los cambios en los paquetes de software.	Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.

	14.2.5	Uso de principios de ingeniería en protección de sistemas.	Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.
	14.2.6	Seguridad en entornos de desarrollo.	Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de DEMING de desarrollo del sistema.
	14.2.7	Externalización del desarrollo de software.	La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.
	14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.
	14.2.9	Pruebas de aceptación.	Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.
	14.3	Datos de prueba	
	14.3.1	Protección	Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.

15. Relaciones con suministradores

15.1. Generalidades: Las relaciones con suministradores se debe verificar correctamente dentro de la Municipalidad Distrital de Independencia.

15.2. Objetivo: Garantizar que todos los servicios proporcionados por terceros sean correctamente verificados.

15.3. Alcance: Esta política la debe verificar los trabajadores del área de la Subgerencia de Informática y Telecomunicaciones.

15.4. Responsables:

15.4.1. El responsable del Área informática debe concientizar y capacitar a los empleados para que estén atentos a eventos sospechosos y en caso de presentarse los reporten de inmediato.

15.5. Políticas

15. Relaciones con suministradores	15.1	Seguridad de la información en las relaciones con suministradores.	
	15.1.1	Política de seguridad de la información para suministradores.	Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de terceras personas.
	15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la Municipalidad.
	15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.
	15.2	Gestión de la prestación del servicio por suministradores.	
	15.2.1	Supervisión y revisión de los servicios prestados por terceros.	Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.
	15.2.2	Gestión de cambios en los servicios prestados por terceros.	Se deberían administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.

16. Gestión de los incidentes de seguridad de la información

16.1. Generalidades: Los trabajadores de la Municipalidad Distrital de Independencia deben tener muy clara la obligación de reportar formalmente fallas, eventos y debilidades de manera inmediata al responsable de la seguridad.

16.2. Objetivo: Garantizar que todos los eventos maliciosos, como fallas y debilidades de la seguridad de la información sean comunicados de manera inmediata.

16.3. Alcance: Esta política la deben cumplir todos los trabajadores de la Municipalidad.

16.4. Responsables:

16.4.1. **Responsable de la seguridad informática:** El responsable de la seguridad debe establecer un protocolo el cual deben conocer todos empleados para conozcan cual es el procesos a seguir en caso de presentarse una falla. Es decir cómo y a quien reportarlo para que se tomen los correctivos necesarios.

16.4.2. **El Responsable del Área informática** debe concientizar y capacitar a los empleados para que estén atentos a eventos sospechosos y en caso de presentarse los reporten de inmediato.

16.5. Políticas

16. Gestión de incidentes en la Seguridad de la Información	16.1	Gestión de incidentes de seguridad de la información y mejoras.	
	16.1.1	Responsabilidades y procedimientos.	Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
	16.1.2	Notificación de los eventos de seguridad de la información.	Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.
	16.1.3	Notificación de puntos débiles de la seguridad.	Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la Municipalidad.
	16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.
	16.1.5	Respuesta a los incidentes de seguridad.	Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.
	16.1.6	Aprendizaje de los incidentes de seguridad de la información.	Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.
	16.1.7	Recopilación de evidencias.	La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.

17. Gestión de la continuidad del negocio

17.1. Generalidades: Es indispensable que toda empresa disponga de un procesos de gestión de continuidad del negocio en caso de llegarse a presentar una eventualidad como un desastre natural, robo, daños en los servidores etc.

17.2. Objetivo: Asegurar el funcionamiento continuo de la organización.

17.3. Alcance: Esta política se debe aplicar a todos los procesos críticos y prioritarios de la municipalidad.

17.4. Responsables:

17.4.1. El comité de seguridad junto con el responsable de la seguridad informática debe identificar las amenazas, evaluar los riesgos identificar controles preventivos, desarrollar un plan estratégico y un plan de contingencia.

17.4.2. El Responsable del Área informática participara en la elaboración y documentación del plan de contingencia.

17.5. Políticas

17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	17.1	Continuidad de la seguridad de la información.	
	17.1.1	Planificación de la continuidad de la seguridad de la información.	La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.
	17.1.2	Implantación de la continuidad de la seguridad de la información.	La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.
	17.2	Redundancias.	
	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.

18. Cumplimiento

18.1. Generalidades: Todas las empresas deben cumplir con las obligaciones estipuladas por la ley.

18.2. Objetivo: Cumplir con todas las obligaciones estipuladas por la ley Alcance: Esta política se debe aplicar a todo el personal de la empresa.

18.3. Alcance: Esta política se debe aplicar a todos los procesos críticos y prioritarios de la municipalidad.

18.4. Responsables:

18.4.1. Responsable de la seguridad informática: Este se encargara de definir procedimientos encaminados a cumplir con todas las normas y restricciones legales, se encargara de realizar revisiones periódicas a la empresa para verificar el cumplimiento de las políticas de seguridad, solicitar auditorias periódicas, documentar y dar a conocer los requisitos normativos.

18.4.2. Todos los empleados y directivos están obligados a conocer y dar a conocer a cumplir y hacer cumplir la presente política y la normativa vigente.

18.5. Políticas

18. Cumplimiento	18.1	Cumplimiento de los requisitos legales y contractuales.	
	18.1.1	Identificación de la legislación aplicable.	Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.

	18.1.2	Derechos de propiedad intelectual (DPI).	Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.
	18.1.3	Protección de los registros de la organización.	Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.
	18.1.4	Protección de datos y privacidad de la información personal.	Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.
	18.1.5	Regulación de los controles criptográficos.	Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.
	18.2	Revisiones de la seguridad de la información.	
	18.2.1	Revisión independiente de la seguridad de la información.	Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la Municipalidad.
	18.2.2	Cumplimiento de las políticas y normas de seguridad.	Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.
	18.2.3	Comprobación del cumplimiento.	Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.

ANEXO 10: "DECLARACIÓN DE APLICABILIDAD"

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
5. Políticas de Seguridad	5.1	Dirección de la Alta Gerencia para la Seguridad de la Información							
	5.1.1	Política de Seguridad de la Información	Si		Se requiere establecer las políticas necesarias que definan los lineamientos internos para asegurar los activos de información críticos que contienen información confidencial o son vitales para la continuidad de las operaciones de la municipalidad.	Redacción del documento: "Política de Seguridad de la Información", en el caso sea pertinente, establecer políticas para cada uno de los casos que así lo requiera. El cual debe ser comunicado a todos los colaboradores de la municipalidad.	x	x	
	5.1.2	Revisión de las Políticas de Seguridad de la Información	Si		En el documento: "Política de Seguridad de la Información" se establece un procedimiento de revisión de la política de seguridad.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
6. Organización de la Seguridad de la Información	6.1	Organización Interna							
	6.1.1	Roles y Responsabilidades para la seguridad de la información	Si		Se debe establecer las responsabilidades y roles requeridos tanto en el equipo de seguridad, así como para los trabajadores, en la cual se debe establecer como mínimo un comité de seguridad de la información que pueda implementar y dar el mantenimiento al SGSI.		x	x	
	6.1.2	Segregación de funciones	Si	Existe organigramas (flujogramas) no unificados ni ligado a las funciones del área de SGIT	Las actividades de cada área son conocidas, sin embargo, la documentación que es generada casi son nulas, además de no existir gráficos unificados que nos muestren el flujo de la información a través de los diferentes procesos.	Es de suma importancia establecer los límites de acceso a la información crítica que tiene cada área durante el flujo de la misma como parte de la atención al público en general		x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
6. Organización de la Seguridad de la Información	6.1.3	Contacto con autoridades	Si		Establecer el flujo a seguir para la notificación de un incidente de seguridad de la información, del mismo modo la identificación de las autoridades pertinentes, lo cual ayudara a que no sucedan estos desapercibidos, estableciendo los controles adecuados por parte de las autoridades.			x	
	6.1.4	Contacto con grupos de interés especial	Si		La Municipalidad de Independencia debe establecer los flujos correctos de comunicación con los grupos de interés (Reniec, MEF, otros), con la finalidad de mantener un canal de comunicación (información) , tomando como buenas prácticas usadas por la institución alertando las posibles vulnerabilidades que puedan afectar al respaldo de la información.			x	x

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
6. Organización de la Seguridad de la Información	6.1.5	Seguridad de la Información en gerencia de proyectos	Si		Este proyecto debe ser gestionado dentro de los alcances y deberá ser gestionado mediante una metodología que cuente con la gestión de riesgos y debe seguir los lineamientos de la seguridad de la información, con la finalidad de garantizar el cumplimiento de los requisitos de seguridad de la Municipalidad.			x	
	6.2	Dispositivos móviles y teletrabajo							
	6.2.1	Política de dispositivos móviles	Si		No es considerado ya que no aplica para nuestro estudio dado a que no se utilizan dispositivos móviles en los procesos del alcance del proyecto		X		

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
6. Organización de la Seguridad de la Información	6.2.2	Teletrabajo	Si		No es considerado ya que no aplica para nuestro estudio dado a que no se utilizan dispositivos móviles en los procesos del alcance del proyecto.			X	
7. Seguridad en los Recursos	7.1	Previo al Empleo							
	7.1.1	Verificación de antecedentes	Si		Debe realizarse la verificación de los antecedentes del personal, lo cual nos permitirá filtrar a aquellas personas que puedan constituir un riesgo para la Municipalidad o la información que se maneja ya sea por conflicto etc o intereses personales.		x	x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
7. Seguridad en los Recursos	7.1.2	Términos y condiciones de empleo	Si		Se debe establecer las condiciones de empleo, las cuales se deben comunicar a las personas seleccionadas previo a la firma del contrato, en la cual se detalle las responsabilidades que tiene en cuanto a la seguridad de la información; la cual acepta antes de iniciar sus labores en la institución.		x		X
	7.2	Durante el Empleo							
	7.2.1	Responsabilidades de la Alta Gerencia	Si		Se debe especificar la responsabilidad de la alta gerencia en cuanto a la implementación y el mantenimiento del SGSI puesto a que esto corresponde al plan estratégico de la Municipalidad y a los intereses de los usuarios como parte activa en los requerimientos.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
7. Seguridad en los Recursos	7.2.2	Conciencia, educación y capacitación	Si		Se debe establecer un plan de capacitación para los colaboradores, acerca de la política de seguridad de la información, del mismo modo la evaluación que nos permitirá medir el nivel de conocimiento del tema.		x	x	
	7.2.3	de Seguridad de la Información	Si		Establecer penalizaciones disciplinarias aplicadas a los colaboradores que infrinjan las condiciones del empleo en cuanto a la seguridad de la información.			x	
	7.3	Término y Cambio de Empleo							
	7.3.1	Termino de responsabilidades o	Si		El periodo de tiempo al cual se encuentra sujeta el colaborador debe cumplir con los términos y condiciones establecidos en el momento de incorporarse, lo que permitirá a la Municipalidad protegerse de posibles filtraciones realizadas por trabajadores cesados.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
8. Gestión de Activos	8.1	Responsabilidad de los Activos							
	8.1.1	Inventario de activos	Si		Dado que la información sensible es utilizada para fines de Registros civiles, la institución debe manejar un inventario de activos, en el cual se detalle la ubicación y el tipo del mismo, la cual nos permitirá realizar la relación con las políticas de uso según su categoría.		x	x	
	8.1.2	Propiedad de los activos	Si		Los activos de información deben ser asignados a un almacenero (custodio) encargado del inventario, clasificación y protección de los activos, así como de la destrucción en caso sea necesaria y la revisión de las restricciones en cuanto a accesos.	Debe identificarse a la persona responsable que realice el seguimiento, control de los activos y la revisión de las restricciones en cuanto a accesos.	x	x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
8. Gestión de Activos	8.1.3	Uso aceptable de los activos	Si		Debe especificarse y documentar a que se define como uso aceptable en cuanto a manejo información personal y sensible mediante una política o procedimiento que debe ser de conocimiento obligatorio para el personal del área.		x	x	
	8.2	Clasificación de la información							
	8.2.1	Clasificación de la información	Si		Se debe realizar una clasificación de los activos identificados según su criticidad para el negocio o el nivel de confidencialidad que se les debe otorgar.		x	x	
	8.2.2	Etiquetado de la información	Si		La clasificación de la información debe ser dependiendo del contexto, por este motivo se debe revisar la clasificación periódicamente.			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
8. Gestión de Activos	8.2.3	Manejo de activos	Si		Se debe mantener un correcto uso de la información, se debe realizar el etiquetado que identifique la información según la clasificación previamente definida.			x	X
	8.3	Manejo de medios							
	8.3.1	Gestión de medios removibles (Extraíbles)	Si		Se deberían establecer procedimientos para la gestión de los medios informáticos removibles acordes con el esquema de clasificación adoptado por la Municipalidad.			x	
	8.3.2	Eliminación de medios	Si		Para eliminar los medios que contienen información confidencial se debe seguir un protocolo que asegure su correcto desecho, de manera que no puedan ser reutilizados por otras personas ajenas.	En el caso de las inscripciones del registro civil, al momento de la recepción, la información que no va ser archivada debe ser triturada con la finalidad de que esta no sea reconstruida.	x	x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
8. Gestión de Activos	8.3.3	Transporte de medios físicos	Si		Se deben establecer protocolos que aseguren la información en su transferencia física de manera que en la entrada y salida de datos u archivos se garantice la no manipulación de la misma.			x	
9. Control de Accesos	9.1	Requerimientos de Negocio para el Control de Accesos							
	9.1.1	Política de Control de Acceso	Si		El control de acceso a la información de Registros Civiles debe estar documentada y debe ser de conocimiento del personal, también debe definir los niveles de escalamiento para la autorización del uso de información en caso sea requerida			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
9. Control de Accesos	9.1.2	Política en el uso de servicios de red	Si		Establecer una política de accesos a nivel de red que nos permita establecer los lineamientos en cuanto a segmentación de redes, accesos de externos a la red interna, monitoreo, etc.	Los niveles de control de acceso deben ser establecidos según los lineamientos de uso del personal y al acceso que van a tener tanto interna y externamente.		x	
	9.2	Gestión de Accesos de Usuario							
	9.2.1	Registro y baja del usuario	Si		Para poder mitigar el riesgo de acceso no autorizado, se debe mantener un procedimiento de altas y sobre todo bajas de usuarios de los sistemas que maneja la Municipalidad.			x	X
	9.2.2	Gestión de privilegios	Si		Contar con una correcta gestión de privilegios que permitirá limitar el acceso según las funciones o áreas a las cuales cada colaborador pertenece.	Se debe establecer la segregación de funciones en base al cargo del empleador, de este modo se puede diseñar un control de privilegio de accesos.		x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
9. Control de Accesos	9.2.3	Gestión de información de autenticación secreta de usuarios	Si	Todos los usuarios de los sistemas cuentan con autentificación mediante password, como una buena práctica de la Municipalidad.	La asignación y uso de derechos de acceso con privilegios especiales debería ser restringido y controlado que permitirá tener una trazabilidad de las acciones realizadas por los usuarios.			x	
	9.2.4	Revisión de derechos de acceso de usuarios	Si		La asignación de información confidencial para la autenticación debería ser controlada mediante un proceso de gestión controlado.			x	
	9.2.5	Eliminación o ajuste de derechos de acceso	Si		Los propietarios de los activos deberían revisar con regularidad los derechos de acceso de los usuarios.			x	
	9.3	Responsabilidades del Usuario							

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
9. Control de Accesos	9.3.1	Uso de información de autenticación secreta	Si		Se debería exigir a los usuarios el uso de las buenas prácticas de seguridad de la institución en el uso de información confidencial para la autenticación.			x	X
	9.4	Control de Acceso de Sistemas y Aplicaciones							
	9.4.1	Restricción de acceso a la información	Si	Todos los sistemas cuentan con acceso a través de usuario y contraseña	Si bien se cuenta con el control básico, se debería restringir el acceso de los usuarios y el personal de mantenimiento a la información y funciones de los sistemas de aplicaciones, en relación a la política de control de accesos.		x	x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
9. Control de Accesos	9.4.2	Procedimientos de inicio de sesión segura	Si		Cuando sea requerido por la política de control de accesos se debería controlar el acceso a los sistemas y aplicaciones mediante un procedimiento seguro enfocado a proteger la información de inicio de sesión del usuario en los sistemas.			x	X
	9.4.3	Sistema de gestión de contraseñas	Si		Los sistemas de gestión de contraseñas deberían ser interactivos y asegurar contraseñas de calidad. Establecer requisitos mínimos en cuanto a la complejidad de contraseñas.			x	X
	9.4.4	Uso de programas y utilidades privilegiadas	Si		El uso de utilidades software que podrían ser capaces de anular o evitar controles en aplicaciones y sistemas deberían estar restringidos y estrechamente controlados.			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
9. Control de Accesos	9.4.5	Control de acceso al código fuente del programa	Si		Se debería restringir el acceso al código fuente de las aplicaciones software.			x	
10. Cifrado	10.1	Controles Criptográficos							
	10.1.1	Restricción de acceso a la información	Si		Debe manejarse y activar controles criptográficos que garanticen que la información debe mantenerse bajo custodia para tener la integridad de la información y evitar que se pueda transferir la información			x	
	10.1.2	Procedimientos de inicio de sesión segura	Si		En el proceso del proyecto se debe considerar la gestión de claves puesto que permitirá que la persona que cuente con clave será responsable de la información que maneja, ya que también debe realizarse la renovación de claves.			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
11. Seguridad Física y del Entorno	11.1	Áreas Seguras							
	11.1.1	Perímetro de seguridad física	Si	Los documentos que ingresan a la oficina de registros están almacenados en la misma oficina bajo la custodia de la jefa del área.	Se deberían definir y utilizar perímetros de seguridad para la protección de las áreas que contienen información y las instalaciones de procesamiento de información sensible o crítica. El objetivo es establecer un límite de accesos entre los usuarios y colaboradores.			x	
	11.1.2	Controles físicos de entrada	Si		Las áreas seguras deberían estar protegidas mediante controles de entrada adecuados para garantizar que solo el personal autorizado dispone de permiso de acceso. El personal debe estar debidamente identificado en todo momento.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
11. Seguridad Física y del Entorno	11.1.3	Seguridad de oficinas, despachos y recursos	Si		Se debería diseñar y aplicar un sistema de seguridad física a las oficinas e instalaciones de la Municipalidad.			x	
	11.1.4	Protección contra amenazas externas y del ambiente	Si		Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes, que puedan afectar tanto natural como provocados (incendios).			x	
	11.1.5	Trabajo en áreas seguras	Si		Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras.			x	
	11.1.6	Áreas de acceso público, entrega y carga.	Si		No se considera dado que los envíos de los activos de información se realizan directamente al área correspondiente			x	
	11.2	Intercambio de información con partes externas							

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
11. Seguridad Física y del Entorno	11.2.1	Instalación y protección de equipo	Si		Los equipos se deberían instalarse y proteger para reducir los riesgos de las amenazas y peligros ambientales y de oportunidades de acceso no autorizado.			x	
	11.2.2	Servicios de soporte (instalaciones de suministro)	Si		Los equipos críticos relacionados al mantenimiento de información sensible deben contar con medidas que aseguren su funcionamiento en caso de caída de algún servicio sobre el que se soporten (fluido eléctrico, por ejemplo)			x	
	11.2.3	Seguridad en el cableado	Si		Los cables eléctricos y de telecomunicaciones que transportan datos o apoyan a los servicios de información se deberían proteger contra la intercepción, interferencia o posibles daños.			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
11. Seguridad Física y del Entorno	11.2.4	Mantenimiento de equipos	Si		Los equipos que cuenten con acceso a información crítica deberán seguir un procedimiento de mantenimiento adecuado de manera que loa información que contienen no sea comprometida.			x	
	11.2.5	Retiro de activos	Si		La Municipalidad debe establecer políticas que limiten el retiro de la información sensible de las instalaciones a excepción de ser para cumplir con alguno de los servicios que brinda			x	X
	11.2.6	Seguridad del equipo y activos fuera de la instalación	Si		La Municipalidad debe asegurar que cualquier uso externo de la información que maneja la oficina de registros, haya sido previamente autorizado por las personas correspondientes.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
11. Seguridad Física y del Entorno	11.2.7	Eliminación segura o reúso del dispositivo de almacenamiento	Si		Los equipos informáticos que se den de baja o se cambien de ambiente deben haber pasado por un proceso de limpieza que elimine de manera adecuada la información que puedan contener			x	
	11.2.8	Equipo informático de usuario desatendido	Si		Los usuarios deberán mantener la seguridad de sus equipos incluso cuando no estén trabajando con los mismos			x	
	11.2.9	Política del puesto de trabajo despejado y bloqueo de pantalla	Si		Los usuarios deberán mantener sus escritorios libres de cualquier información sensible que pueda usar un agente externo como consecuencia de sus exposición como parte de un olvido o mala gestión			x	
12. Seguridad en la operativa	**12.1**	**Responsabilidades y procedimientos de operación**							

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
12. Seguridad en la operativa	12.1.1	Documentación de procedimientos de operación	Si	Actualmente se cuenta con guías de procesos desactualizados.	Se necesitará documentación de los procesos que se tienen con la finalidad de que se entiendan los flujos de información crítica que existe, para que se pueda realizar una evaluación continua sobre le nivel de riesgo existente y establecer nuevos controles necesarios.			x	
	12.1.2	Gestión de cambios	Si		Se deberá realizar el control de los cambios que afectan a la seguridad de la información en la Municipalidad y procesos de negocio, las instalaciones y sistemas de procesamiento de información.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
12. Seguridad en la operativa	12.1.3	Gestión de capacidades	Si		Se necesitará monitorear y ajustar el uso de los recursos junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.			x	X
	12.1.4	Separación de entornos de desarrollo, prueba y producción	Si	Actualmente todo se desarrolla en un mismo entorno.	Cada entorno de desarrollo, pruebas y operacionales deberían permanecer separados para reducir los riesgos de acceso o de cambios no autorizados en el entorno operacional.			x	
	12.2	Protección contra código malicioso							
	12.2.1.	Controles contra el código malicioso	Si		Se deberían implementar controles para la detección, prevención y recuperación ante afectaciones de malware en combinación con la concientización adecuada de los usuarios.			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
12. Seguridad en la operativa	12.3	Copias de seguridad							
	12.3.1	Copias de seguridad de la información	Si		Es necesario realizar y pruebas regulares de las copias de la información, del software y de las imágenes del sistema en relación con una política de respaldo (Backup) convenida.			x	X
	12.4	Registro de actividad y supervisión							
	12.4.1	Registro y gestión de eventos de actividad	Si		Se tiene que producir, mantener y revisar periódicamente los registros relacionados con eventos de actividad del usuario, excepciones, fallas y eventos de seguridad de la información.			x	
	12.4.2	Protección de los registros de información	Si		Se debería proteger contra posibles alteraciones y accesos no autorizados la información de los registros.			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
12. Seguridad en la operativa	12.4.3	Registros de actividad del administrador y operador del sistema	Si		Se deberían registrar las actividades del administrador y del operador del sistema y los registros asociados se deberían proteger y revisar de manera regular.			x	
	12.4.4	Sincronización de relojes	Si		Se deberían sincronizar los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o de un dominio de seguridad y en relación con una fuente de sincronización única de referencia.			x	
	12.5	Control del software en explotación							
	12.5.1	Instalación del software en sistemas en producción	Si		Se deberían implementar procedimientos para controlar la instalación de software en sistemas operacionales.			x	
	12.6	Gestión de la vulnerabilidad técnica							

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
12. Seguridad en la operativa	12.6.1	Gestión de las vulnerabilidades técnicas	Si		Se debería obtener información sobre las vulnerabilidades técnicas de los sistemas de información de manera oportuna para evaluar el grado de exposición de la organización y tomar las medidas necesarias para abordar los riesgos asociados.			x	X
	12.6.2	Restricciones en la instalación de software	Si		Se deberían establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.	El modo de instalación de software en los equipos de la municipalidad debería estar disponible únicamente para aquellos usuarios que tiene autorización para su uso.		x	
	12.7	Consideraciones de las auditorías de los sistemas de información							

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
12. Seguridad en la operativa	12.7.1	Controles de auditoría de los sistemas de información	Si		Se deberían planificar y acordar los requisitos y las actividades de auditoría que involucran la verificación de los sistemas operacionales con el objetivo de minimizar las interrupciones en los procesos relacionados con el negocio.			x	
13. Seguridad en las telecomunicaciones	13.1	Gestión de la seguridad en las redes							
	13.1.1	Controles de red	Si		Se deberían administrar y controlar las redes para proteger la información en sistemas y aplicaciones.			x	X
	13.1.2	Mecanismos de seguridad asociados a servicios en red	Si		Se deberían identificar e incluir en los acuerdos de servicio (SLA) los mecanismos de seguridad, los niveles de servicio y los requisitos de administración de todos los servicios de red, independientemente de si estos servicios se entregan de manera interna o están externalizados.			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
13. Seguridad en las telecomunicaciones	13.1.3	Segregación de redes	Si		Se deberían segregar las redes en función de los grupos de servicios, usuarios y sistemas de información.			x	
	13.2	Intercambio de información con partes externas							
	13.2.1	Políticas y procedimientos de intercambio de información	Si		Los acuerdos deberían abordar la transferencia segura de información comercial entre la organización y las partes externas.			x	
	13.2.2	Acuerdos de intercambio	Si		Los acuerdos deberían abordar la transferencia segura de información entre la municipalidad y las partes externas.			x	
	13.2.3.	Mensajería electrónica	No		No se considera el control, por no poseer servicio de mensajería electrónica.				
	13.2.4	Acuerdos de confidencialidad y secreto	Si		Se deberían identificar, revisar y documentar de manera regular los requisitos para los acuerdos de confidencialidad y "no divulgación" que reflejan las necesidades de la organización para la protección de información.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	14.1	Requisitos de seguridad de los sistemas de información.							
	14.1.1	Análisis y especificación de los requisitos de seguridad.	Si		Los requisitos relacionados con la seguridad de la información se deberían incluir en los requisitos para los nuevos sistemas o en las mejoras a los sistemas de información ya existentes.			x	
	14.1.2	Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Si		La información de los servicios de aplicación que pasan a través de redes públicas se debería proteger contra actividades fraudulentas, de disputa de contratos y/o de modificación no autorizada.		x	x	
	14.1.3	Protección de las transacciones por redes telemáticas.	Si		La información en transacciones de servicios de aplicación se debería proteger para evitar la transmisión y enrutamiento incorrecto y la alteración, divulgación y/o duplicación no autorizada de mensajes o su reproducción.		x	x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	14.2	Seguridad en los procesos de desarrollo y soporte.							
	14.2.1	Política de desarrollo seguro de software.	Si		Se deberían establecer y aplicar reglas para el desarrollo de software y sistemas dentro de la Municipalidad.			x	
	14.2.2	Procedimientos de control de cambios en los sistemas.	Si		En el ciclo de DEMING de desarrollo se deberían hacer uso de procedimientos formales de control de cambios.			x	
	14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	Si		Las aplicaciones críticas para el negocio se deberían revisar y probar para garantizar que no se han generado impactos adversos en las operaciones o en la seguridad de la Municipalidad.			x	
	14.2.4	Restricciones a los cambios en los paquetes de software.	Si		Se deberían evitar modificaciones en los paquetes de software suministrados por terceros, limitándose a cambios realmente necesarios. Todos los cambios se deberían controlar estrictamente.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	14.2.5	Uso de principios de ingeniería en protección de sistemas.	Si		Se deberían establecer, documentar, mantener y aplicar los principios de seguridad en ingeniería de sistemas para cualquier labor de implementación en el sistema de información.			x	
	14.2.6	Seguridad en entornos de desarrollo.	Si		Las organizaciones deberían establecer y proteger adecuadamente los entornos para las labores de desarrollo e integración de sistemas que abarcan todo el ciclo de DEMING de desarrollo del sistema.			x	
	14.2.7	Externalización del desarrollo de software.	Si		La organización debería supervisar y monitorear las actividades de desarrollo del sistema que se hayan externalizado.			x	
	14.2.8	Pruebas de funcionalidad durante el desarrollo de los sistemas.	Si		Se deberían realizar pruebas de funcionalidad en aspectos de seguridad durante las etapas del desarrollo.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
14. Adquisición, desarrollo y mantenimiento de los sistemas de información	14.2.9	Pruebas de aceptación.	Si		Se deberían establecer programas de prueba y criterios relacionados para la aceptación de nuevos sistemas de información, actualizaciones y/o nuevas versiones.			x	
	14.3	Datos de prueba							
	14.3.1	Protección	Si		Los datos de pruebas se deberían seleccionar cuidadosamente y se deberían proteger y controlar.		x	x	X
15. Relaciones con suministradores	15.1	Seguridad de la información en las relaciones con suministradores.							
	15.1.1	Política de seguridad de la información para suministradores.	Si		Se deberían acordar y documentar adecuadamente los requisitos de seguridad de la información requeridos por los activos de la organización con el objetivo de mitigar los riesgos asociados al acceso por parte de terceras personas.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
15. Relaciones con suministradores	15.1.2	Tratamiento del riesgo dentro de acuerdos de suministradores.	Si		Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes a cada proveedor que puede acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI que dan soporte a la información de la Municipalidad.			x	
	15.1.3	Cadena de suministro en tecnologías de la información y comunicaciones.	Si		Los acuerdos con los proveedores deberían incluir los requisitos para abordar los riesgos de seguridad de la información asociados con la cadena de suministro de los servicios y productos de tecnología de información y comunicaciones.			x	
	15.2	Gestión de la prestación del servicio por suministradores.							

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
15. Relaciones con suministradores	15.2.1	Supervisión y revisión de los servicios prestados por terceros.	Si		Las organizaciones deberían monitorear, revisar y auditar la presentación de servicios del proveedor regularmente.			x	
	15.2.2	Gestión de cambios en los servicios prestados por terceros.	Si		Se deberían administrar los cambios a la provisión de servicios que realizan los proveedores manteniendo y mejorando: las políticas de seguridad de la información, los procedimientos y controles específicos. Se debería considerar la criticidad de la información comercial, los sistemas y procesos involucrados en el proceso de reevaluación de riesgos.			x	
16. Gestión de incidentes en la Seguridad de la Información	16.1	Gestión de incidentes de seguridad de la información y mejoras.							
	16.1.1	Responsabilidades y procedimientos.	Si		Se deberían establecer las responsabilidades y procedimientos de gestión para garantizar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
16. Gestión de incidentes en la Seguridad de la Información	16.1.2	Notificación de los eventos de seguridad de la información.	Si		Los eventos de seguridad de la información se deberían informar lo antes posible utilizando los canales de administración adecuados.			x	
	16.1.3	Notificación de puntos débiles de la seguridad.	Si		Se debería requerir anotar e informar sobre cualquier debilidad sospechosa en la seguridad de la información en los sistemas o servicios tanto a los empleados como a contratistas que utilizan los sistemas y servicios de información de la Municipalidad.			x	
	16.1.4	Valoración de eventos de seguridad de la información y toma de decisiones.	Si		Se deberían evaluar los eventos de seguridad de la información y decidir su clasificación como incidentes.			x	
	16.1.5	Respuesta a los incidentes de seguridad.	Si		Se debería responder ante los incidentes de seguridad de la información en atención a los procedimientos documentados.			x	
	16.1.6	Aprendizaje de los incidentes de seguridad de la información.	Si		Se debería utilizar el conocimiento obtenido del análisis y la resolución de incidentes de seguridad de la información para reducir la probabilidad y/o impacto de incidentes en el futuro.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
16. Gestión de incidentes en la Seguridad de la Información	16.1.7	Recopilación de evidencias.	Si		La organización debería definir y aplicar los procedimientos necesarios para la identificación, recopilación, adquisición y preservación de la información que puede servir de evidencia.		x	x	
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	17.1	Continuidad de la seguridad de la información.							
	17.1.1	Planificación de la continuidad de la seguridad de la información.	Si		La organización debería determinar los requisitos para la seguridad de la información y su gestión durante situaciones adversas como situaciones de crisis o de desastre.			x	
	17.1.2	Implantación de la continuidad de la seguridad de la información.	Si		La organización debería establecer, documentar, implementar y mantener los procesos, procedimientos y controles para garantizar el mantenimiento del nivel necesario de seguridad de la información durante situaciones adversas.			x	
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información.	Si		La organización debería verificar regularmente los controles de continuidad de seguridad de la información establecidos e implementados para poder garantizar su validez y eficacia ante situaciones adversas.			x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
17. Aspectos de seguridad de la información en la gestión de la continuidad del negocio	17.2	Redundancias.							
	17.2.1	Disponibilidad de instalaciones para el procesamiento de la información.	Si		Se debería implementar la suficiente redundancia en las instalaciones de procesamiento de la información y en correspondencia con los requisitos de disponibilidad.			x	
18. Cumplimiento	18.1	Cumplimiento de los requisitos legales y contractuales.							
	18.1.1	Identificación de la legislación aplicable.	Si		Se deberían identificar, documentar y mantener al día de manera explícita para cada sistema de información y para la organización todos los requisitos estatutarios, normativos y contractuales legislativos junto al enfoque de la organización para cumplir con estos requisitos.		x	x	
	18.1.2	Derechos de propiedad intelectual (DPI).	Si		Se deberían implementar procedimientos adecuados para garantizar el cumplimiento con los requisitos legislativos, normativos y contractuales relacionados con los derechos de propiedad intelectual y utilizar productos software original.		x	x	

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
18. Cumplimiento	18.1.3	Protección de los registros de la organización.	Si		Los registros se deberían proteger contra pérdidas, destrucción, falsificación, accesos y publicación no autorizados de acuerdo con los requisitos legislativos, normativos, contractuales y comerciales.		x	x	
	18.1.4	Protección de datos y privacidad de la información personal.	Si		Se debería garantizar la privacidad y la protección de la información personal identificable según requiere la legislación y las normativas pertinentes aplicables que correspondan.		x	x	
	18.1.5	Regulación de los controles criptográficos.	Si		Se deberían utilizar controles de cifrado de la información en cumplimiento con todos los acuerdos, la legislación y las normativas pertinentes.		x	x	
	18.2	Revisiones de la seguridad de la información.							
	18.2.1	Revisión independiente de la seguridad de la información.	Si		Se debería revisar el enfoque de la organización para la implementación (los objetivos de control, los controles, las políticas, los procesos y procedimientos para la seguridad de la información) y gestión de la seguridad de la información en base a revisiones independientes e intervalos planificados o cuando tengan lugar cambios significativos en la Municipalidad.			x	X

ISO 27002:2013 Controles de Seguridad			Aplicabilidad (Si/No)	Controles Actuales	Comentarios (Justificación de Exclusión)	Visión general de la implementación	Controles seleccionados y razones de selección		
Cláusula	Sección	Objetivo de control					L	N	VR
18. Cumplimiento	18.2.2	Cumplimiento de las políticas y normas de seguridad.	Si		Los gerentes deberían revisar regularmente el cumplimiento del procesamiento y los procedimientos de información dentro de su área de responsabilidad respecto a las políticas, normas y cualquier otro tipo de requisito de seguridad correspondiente.			x	x
	18.2.3	Comprobación del cumplimiento.	Si		Los sistemas de información se deberían revisar regularmente para verificar su cumplimiento con las políticas y normas de seguridad dispuestas por la información de la organización.			x	x

ANEXO 11: "GUÍAS DE IMPLEMENTACIÓN"

Guía de implementación de la cláusula de Política de Seguridad (PS)

Debería establecer el compromiso de la gerencia y el enfoque de la organización para gestionar la seguridad de la información. El documento de la política de seguridad debería contener como mínimo:

- Una definición de seguridad de la información y sus objetivos globales, el alcance de la seguridad y su importancia como mecanismo que permite compartir la información.
- El establecimiento del objetivo de la gerencia como soporte de los objetivos y principios de la seguridad de la información.
- Un marco para colocar los objetivos de control y mandos, incluyendo la estructura de evaluación de riesgo y gestión de riesgo.
- Una breve explicación de las políticas, principios, normas, y requisitos de conformidad más importantes para la organización.
- Una definición de las responsabilidades generales y específicas en materia de gestión de la seguridad de información, incluida la comunicación de las incidencias de seguridad.
- Las referencias a documentación que pueda sustentar la política; por ejemplo, políticas y procedimientos mucho más detallados para sistemas de información específicos o las reglas de seguridad que los usuarios deberían cumplir.

Esta política debería distribuirse por toda la organización, llegando hasta todos los destinatarios en una forma que se apropiada, entendible y accesible. La política debería tener un propietario que sea responsable del desarrollo, revisión y evaluación de la política de seguridad. La revisión debe incluir oportunidades de evaluación para mejorar la política de seguridad de información de la organización y un acercamiento a la gestión de seguridad de información en respuesta a los cambios del ambiente organizacional, circunstancias del negocio, condiciones legales o cambios en el ambiente técnico.

La revisión de la política de seguridad de información debe tomar en cuenta los resultados de las revisiones de la gestión. Deben existir procedimientos definidos de la gestión de revisión, incluyendo un calendario o periodo de revisión.

El output para la revisión de la gestión debe incluir información acerca de:

- Mejoras en el alcance de la organización para gestionar seguridad de información y sus procesos.
- Mejoras en los objetivos de control controles.
- Mejoras en la asignación de recursos y/o responsabilidades.

Guía de implementación de la cláusula de Seguridad física y ambiental (SFA)

Las siguientes pautas deben ser consideradas e implementadas donde sea apropiado para los perímetros de seguridad físicos.

- El perímetro de seguridad debería estar claramente definido y el lugar y fuerza de cada perímetro debe depender de los requerimientos de seguridad del activo entre el perímetro y los resultados de la evaluación de riesgos.
- El perímetro de un edificio o un lugar que contenga recursos de tratamiento de información debería tener solidez física (por ejemplo, no tendrá zonas que puedan derribarse fácilmente). Los muros externos del lugar deberían ser sólidos y todas las puertas exteriores deberían estar convenientemente protegidas contra accesos no autorizados, por ejemplo, con mecanismos de control, alarmas, rejas, etc. Las ventanas y puertas deben estar cerradas con llave cuando estén desatendidas.
- Se debería instalar un área de recepción manual u otros medios de control del acceso físico al edificio o lugar. Dicho acceso se debería permitir solo al personal autorizado.
- Las barreras físicas se deberían extender, si es necesario, desde el suelo real al techo real para evitar entradas no autorizadas o contaminación del entorno.
- Se debería instalar sistemas adecuados de detección de intrusos de acuerdo a estándares regionales, nacionales o internacionales y deben ser regularmente probados.
- Los recursos de procesamiento de información manejadas por la organización deben ser físicamente separadas de las que son manejadas por externos.

Para los controles físicos de entrada deberían considerarse las siguientes pautas:

- Las visitas a las aéreas seguras se deberían supervisar, a menos que el acceso haya sido aprobado previamente, y se debe registrar la fecha

y momento de entrada y salida. Los visitantes solo tendrán acceso para propósitos específicos y autorizados, proporcionándoles instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia.

- Se debería controlar y restringir solo al personal autorizado el acceso a la información sensible y al tratamiento de los recursos. Se deberían usar controles de autenticación, por ejemplo, tarjetas con número de identificación personal (PIN), para autorizar y validar el acceso. Se debería mantener un rastro auditable de todos los accesos, con las debidas medidas de seguridad.
- Se debería exigir a todo el personal que lleve puesta alguna forma de identificación visible y se le pedirá que solicite a los extraños no acompañados y a cualquiera que no lleve dicha identificación visible, que se identifique.
- Se debe garantizar el acceso restringido al personal de apoyo tercerizado, hacia áreas de seguridad o a los recursos de procesamiento de información sensibles, solo cuando este sea requerido. Este acceso debe ser autorizado y monitoreado.
- Se deberían revisar y actualizar regularmente los derechos de acceso a las áreas de seguridad.

Para la seguridad física de las oficinas se deberían considerar las siguientes pautas:

- Se debería tomar en cuenta regulaciones y estándares de salud y seguridad.
- Se deben instalar equipos con clave para evitar el acceso del público.
- Donde sea aplicable, los edificios deben ser discretos y deben dar una mínima indicación de su propósito, sin signos obvios, fuera o dentro del edificio, que identifiquen la presencia de actividades de tratamiento de información.

- Los directorios y las guías telefónicas internas identificando locaciones de los recursos de información sensible no deben ser fácilmente accesibles por el público.

Guía de implementación de la cláusula de Gestión de comunicaciones y operaciones (GC)

Para proteger la documentación de sistemas de accesos no autorizados se debería considerar las siguientes pautas:

- La documentación de sistemas se debería almacenar con seguridad.
- La lista de acceso a la documentación se sistemas se debería limitar al máximo, y ser autorizada por el propietario de la aplicación.
- La documentación de sistemas mantenida en una red pública o suministrada vía una red pública se debería proteger adecuadamente.

Por otro lado, los registros de auditoría deberían incluir, cuando sea relevante:

- Identificaciones de usuarios.
- Fecha y hora de conexión y desconexión.
- Identidad del terminal o locación si es posible.
- Registros de éxito y fracaso de los intentos de acceso al sistema.
- Registros de éxito o fracaso de datos y de otros intentos de acceso a recursos.
- Cambios en la configuración del sistema.
- Uso de privilegios.
- Uso de las instalaciones y aplicaciones del sistema.
- Archivos accedidos y el tipo de acceso.
- Direcciones de red y protocolo.
- Las alarmas realizadas por el sistema de control de accesos.
- Activación y desactivación de los sistemas de protección, como los sistemas antivirus y los sistemas de detección de intrusos.

El nivel de monitoreo requerido para las instalaciones individuales debe ser determinado por una evaluación de riesgos. Una organización debe cumplir con todos los requerimientos legales aplicables a sus actividades de monitoreo. Las áreas que deben ser consideradas incluyen:

- Acceso autorizado, incluyendo detalles como:
- La identificación del usuario.
- La fecha y hora de los eventos clave.

- El tipo de evento.
- Los archivos ingresados.
- El programa o recursos utilizados.
- Todas las operaciones privilegiadas como:
- Uso de cuentas privilegiadas, como supervisores, administradores.
- Puesta en marcha y parada del sistema.
- Conexión o desconexión de un recurso de entrada o salida.
- Intentos de accesos no autorizados, como:
- Intentos fallidos.
- Acciones con fallas o rechazadas que involucran datos y otros recursos.
- Violaciones a la política de acceso y las notificaciones de los firewalls y entradas de red.
- Las alertas de los sistemas de detección de intrusos del propietario.
- Alertas o fallas del sistema, como:
- Alertas o mensajes de consola.
- Excepciones de registro en el sistema.
- Alarmas de la gerencia de red.
- Alarmas levantadas por los sistemas de control de accesos.
- Cambios o intentos de cambio a la configuración y controles de los sistemas de seguridad.

Guía de implementación de la cláusula de Control de accesos (CA)

Se deberían establecer claramente en una política de accesos las reglas y los derechos de cada usuario o grupo de usuarios. Los controles de acceso son lógicos y físicos y estos deben ser considerados juntos. Se debería dar a los usuarios y proveedores de servicios una especificación clara de los requisitos de negocio cubiertos por los controles de acceso.

Esta política debería contemplar lo siguiente:

- Requisitos de seguridad de cada aplicación de negocio individualmente.
- Identificación de toda la información relativa a las aplicaciones y los riesgos que la información está enfrentando.
- Políticas para la distribución de la información y las autorizaciones.
- Coherencia entre las políticas de control de accesos y las políticas de clasificación de la información en los distintos sistemas y redes.
- Legislación aplicable y las obligaciones contractuales respecto a la protección del acceso a los datos o servicios.
- Perfiles de acceso de usuarios estandarizados según las categorías comunes de trabajo.
- Administración de los derechos de acceso en un entorno distribuido en red que reconozca todos los tipos disponibles de conexión.
- Segregación de los roles de control de acceso, como el pedido de acceso, autorización de acceso, administración de accesos.

Se debería controlar el acceso a los servicios de información multiusuario mediante un proceso formal de registro, que debería incluir:

- La utilización de un identificados único para cada usuario, de esta forma puede vincularse a los usuarios y responsabilizarse de sus acciones.
- La comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o el servicio de información.

- Verificación de la adecuación del nivel de acceso asignado al propósito del negocio y su consistencia con la política de seguridad de la organización.
- La entrega a los usuarios de una relación escrita de sus derechos de acceso.
- La petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso.
- La garantía de que no se provea acceso al servicio hasta que se haya completado los procesos de autorización.
- El mantenimiento de un registro formalizado de todos los autorizados para usar el servicio.
- La eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la organización o cambien de trabajo en ella.
- La revisión periódica y eliminación de identificadores y cuentas de usuarios redundantes.

Se debería controlar la asignación de privilegios, por un proceso formal de autorización en los sistemas multiusuario. Se deberían considerar los pasos siguientes:

- Identificar los privilegios asociados a cada elemento del sistema, por ejemplo, el sistema operativo, el sistema gestor de base de datos y cada aplicación.
- Asignar privilegios a los individuos según los principios de “necesidad de sus usos” y “caso por caso” y en línea con la política de control de acceso.
- Mantener un proceso de autorización y un registro de todos los privilegios asignados.
- Promover el desarrollo y uso de rutinas del sistema para evitar la asignación de privilegios a los usuarios.

El proceso de controlar la asignación de contraseñas debe incluir los siguientes requisitos:

- Requerir que los usuarios firmen un compromiso para mantener secreto sus contraseñas personales y las compartidas por un grupo solo entre los miembros de dicho grupo.
- Proporcionar inicialmente una contraseña temporal segura que forzosamente deben cambiar inmediatamente después.
- Establecer procedimientos para verificar la identidad de un usuario antes de proveer una contraseña nueva, de reemplazo o temporal.
- Establecer un conducto seguro para hacer llegar las contraseñas temporales a los usuarios. Se debería evitar su envío por terceros o por mensajes no cifrados de correo electrónico.
- Las contraseñas temporales deben ser únicas para cada individuo y no deben ser obvias.
- Los usuarios deberían remitir acuse de recibo de sus contraseñas.

Guía de implementación de la cláusula de Adquisición, desarrollo y mantenimiento de sistemas de información (ADM)

Para minimizar la corrupción de los sistemas de información, se deberían mantener estrictos controles sobre la implantación de cambios. La introducción de nuevos sistemas y cambios mayores al sistema existente debe seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación.

Este proceso debe incluir una evaluación de riesgos, un análisis de los impactos de los cambios y una especificación de los controles de seguridad necesarios. Este proceso debe también asegurar que no se comprometa la seguridad y los procedimientos de control existentes, que a los programadores de soporte se les dé acceso solo a partes del sistema necesarias para su trabajo y que se debe tener una aprobación y acuerdo formal para cualquier cambio.

La aplicación y sus procedimientos de control de cambios deberían estar integrados siempre que sea posible. Este proceso debería incluir:

- El mantenimiento de un registro de los niveles de autorización acordados.
- La garantía de que los cambios se realizan por usuarios autorizados.
- La revisión de los controles y procedimientos de integridad para asegurarse que los cambios no los debilitan.
- La identificación de todo el software, información, entidades de bases de datos y hardware que requiera mejora.
- La obtención de la aprobación formal para propuestas detalladas antes de empezar el trabajo.
- La garantía de la aceptación por parte del usuario autorizado de los cambios antes de cualquier implantación.

Además, se deberían revisar y probar las aplicaciones cuando se efectúen cambios. Este proceso debería incluir:

- La revisión de los procedimientos de control de la aplicación y de la integridad para asegurar que los cambios en el sistema operativo no han sido comprometidos.
- La garantía de que el plan de soporte anual y el presupuesto cubren las revisiones y las pruebas del sistema que requieran los cambios del sistema operativo.
- La garantía de que la modificación de los cambios del sistema operativo se realiza a tiempo para que puedan hacerse las revisiones apropiadas antes de su implantación.

ANEXO 12: "MATRIZ DE CONSISTENCIA"

TITULO	FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	VARIABLES	INDICADORES
"DESARROLLO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MINIMIZAR RIESGOS EN LOS ACTIVOS DE INFORMACIÓN EN LA SUB GERENCIA DE INFORMATICA Y TELECOMUNICACIONES DE LA MUNICIPALIDAD DISTRITAL DE INDEPENDENCIA 2016"	**PROBLEMA GENERAL** ¿De qué manera el desarrollo de un Sistema de Gestión de Seguridad de la Información minimizara los riesgos en los activos de información2 de la Sub Gerencia de Informática y Telecomunicaciones?	**OBJETIVO GENERAL** Desarrollar un sistema de gestión de seguridad de la información, para minimizar riesgos en los activos de información de la Sub Gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia.	**HIPOTESIS GENERAL** El desarrollo de un sistema de seguridad de la información implementa controles de seguridad que minimizan los riesgos en los activos de información de la Municipalidad Distrital de Independencia Huaraz.	**VARIABLE DEPENDIENTE** - Activos de información en la Sub gerencia de Informática y Telecomunicaciones de la Municipalidad Distrital de Independencia	a) Nivel de confidencialidad de Hardware y Software b) Nivel de integridad de Hardware y Software c) Nivel de disponibilidad de Hardware y Software
PROBLEMAS ESPECÍFICOS:		**OBJETIVOS ESPECÍFICOS**		**VARIABLE INDEPENDIENTE**	
a) ¿De qué manera el Sistema de Gestión de Seguridad de la Información influirá en la mejora de problemas tecnológicos?		• Diagnosticar la situación actual y elaborar la documentación requerida por las normas adoptadas para el SGSI. • Elaborar la matriz de amenazas y vulnerabilidades de los procesos del alcance.		- Sistema de Gestión de Seguridad de la Información.	a) Cantidad de Incidentes reportados b) Cantidad de vulnerabilidades y amenazas

PROBLEMAS ESPECÍFICOS:	OBJETIVOS ESPECÍFICOS:		VARIABLE INDEPENDIENTE :	
b) ¿En qué medida se reducirán los problemas de normativa con el desarrollo del Sistema de Gestión de la Seguridad de la Información? c) ¿Cómo influirá el Sistema de Gestión de Seguridad de la Información en el nivel de conocimiento del personal involucrado en las áreas de estudio?	• Identificar y realizar la valorización de los activos de información de los procesos de negocio que conforman el alcance. • Identificar, analizar y evaluar los riesgos a los cuales están expuestos los activos identificados en el punto anterior. • Seleccionar sistemas de control para el tratamiento de los riesgos identificados y así establecer políticas de seguridad. • Diseñar la declaración de aplicabilidad que permita implementar estrategias de mitigación de los riesgos identificados. • Elaborar la documentación requerida por las normas adoptadas para el SGSI.		- Sistema de Gestión de Seguridad de la Información.	c) Nivel de Conocimiento de RRHH d) Cantidad de capacitaciones de RRHH e) Cantidad de controles implantados