UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO

Trabajo de Titulación Modalidad: Proyecto de investigación, presentado previo a la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos

ÁREA: Administrativas informáticas

LÍNEA DE INVESTIGACIÓN: Normas y Estándares

AUTOR: Mayra Elizabeth Aillón Carrasco

TUTOR: Ing. Dennis Vinicio Chicaiza Castillo Mg.

Ambato - Ecuador

septiembre – 2021

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Mayra Elizabeth Aillón Carrasco, estudiante de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, septiembre 2021.

Firmado electrónicamente por:
DENNIS VINICIO CHICAIZA CASTILLO

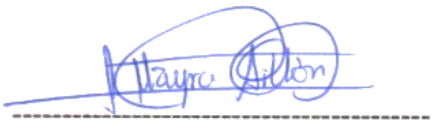
Ing. Dennis Vinicio Chicaiza Castillo Mg.

TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, septiembre 2021.



Mayra Elizabeth Aillón Carrasco
C.C180451021-0
AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por la señorita Mayra Elizabeth Aillón Carrasco, estudiante de la Carrera de Ingeniería en Sistemas Informáticos y Computacionales, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN APLICANDO LA NORMA ISO/IEC 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, septiembre 2021.

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Elsa Pilar Urrutia, Mg.

PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
VICTOR HUGO GUACHIMBOSA VILLALBA

PhD. Víctor Guachimbosa
PROFESOR CALIFICADOR

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

PhD. Julio Balarezo
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, septiembre 2021.

Mayra Elizabeth Aillón Carrasco

C.C180451021-0

AUTOR

Agradecimiento

Un agradecimiento a mi querida Facultad de Ingeniería en Sistemas, Electrónica e Industrial y de manera especial a la Carrera de Ingeniería en Sistemas Computacionales e Informáticos que me acogió en sus aulas para mi formación a nivel profesional.

De manera especial a mi tutor Ingeniero Dennis Chicaiza que me guió y me brindó su apoyo en el desarrollo del presente proyecto de titulación.

Un profundo agradecimiento al Ingeniero Luis Carrasco, que me abrió las puertas de la Unidad de Gestión Tecnológica del GADM. San Pedro de Pelileo para realizar el proyecto de investigación.

Mayra Elizabeth Aillón Carrasco

Dedicatoria

El presente trabajo de titulación lo dedico a Dios permitirme alcanzar una de mis metas propuestas, brindándome la capacidad para culminar mis estudios universitarios.

A mi amado esposo Rodrigo que día a día me incentivó con sus palabras de apoyo para que continúe mis estudios y siempre estuvo a mi lado en los buenos y malos momentos junto a mis hijas Brithanny y Amelita que son el pilar fundamental y el motor de mi vida.

A mis queridos padres Benjamín y Carmita por inculcarme buenos valores y a mis adorados hermanos Paulina, Oscar, Verónica, Alba y Tatiana que con su cariño incondicional guiaron mi camino y de una u otra manera contribuyeron para alcanzar mis objetivos.

Mayra Elizabeth Aillón Carrasco

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

Tabla de Gráficos

RESUMEN EJECUTIVO

El proyecto de investigación tiene como finalidad la mitigación de riesgos y protección de la información que es manejada diariamente en el Gobierno Autónomo Descentralizado Municipal San Pedro de Pelileo, por medio de la aplicación de políticas que se basan en la norma ISO 27001 en el ámbito de seguridad en cuanto al control de accesos gestión de activos, seguridad física, restricciones del personal, entre otros.

Se obtuvo un análisis del estado actual en que encuentra la institución mediantes la aplicación de técnicas como entrevista, encuesta mismas que se aplicó al jefe, técnicos de la Unidad de Gestión tecnológica y a funcionarios de la municipalidad además con las visitas constantes se determinó la existencia de falencias como el ambiente físico en que se encuentra el cuarto de servidores no cuenta con las adecuaciones correspondientes y están expuestas a gran cantidad de riesgos puesto que las instalaciones físicas no son adecuadas, la utilización incorrecta de contraseñas por parte de los funcionarios municipales etc.

De acuerdo a los datos que arrojo el análisis se procedió a la creación de políticas que se basan en la norma ISO 27001 para su aprobación aplicación en la unidad de Gestión Tecnológica del Gobierno Municipal San Pedro de Pelileo con ello se busca que los funcionarios den cumplimiento a las políticas establecidas para que exista un control estricto en las áreas que existen falencias en cuanto a seguridad siempre buscando la mejora continua con la aplicación de monitoreos constantes de todas las áreas existentes.

Palabras claves: Auditoría de seguridad, ISO 27001, seguridad física, seguridad ambiental, confidencialidad, integridad.

ABSTRACT

The purpose of the research project is to mitigate risks and protect the information that is handled daily in The Gobierno Autónomo Descentralizado Municipal San Pedro de Pelileo, through the application of policies that are based on the ISO 27001 standard in the field of security in terms of access control, asset management, physical security, personnel restrictions, among others.

An analysis of the current state of the institution was obtained through the application of techniques such as interviews, a survey that was applied to the chief, technicians of the Technological Management Unit and officials of the municipality, in addition to constant visits, the existence of Failures such as the physical environment in which the server room is located does not have the corresponding adaptations and they are exposed to a large number of risks since the physical facilities are not adequate, the incorrect use of passwords by municipal officials, etc.

According to the data provided by the analysis, policies were created that are based on the ISO 27001 standard for their application approval in the Technological Management unit of the San Pedro de Pelileo Municipal Government. to the policies established so that there is strict control in the areas where there are shortcomings in terms of security, always seeking continuous improvement with the application of constant monitoring of all existing areas.

Keywords: Security audit, ISO 27001, physical security, environmental security, confidentiality, integrity.

INTRODUCCIÓN

En vista de que la seguridad de la información es un punto muy importante que hay que tener en consideración en todas las instituciones, puesto que pueden ser víctimas de un ataque informático y afectar los recursos institucionales por no aplicar políticas que permitan la mitigación de riesgos que se generan dentro de las organizaciones.

Sería imposible decir que existe la protección total a nivel de seguridad en una institución, puesto que siempre va a existir un índice de inseguridad pero si se logra reducir esto. Toda entidad maneja información reservada para su organización es por ello que se debe garantizar la integridad y confiabilidad de la misma.

Este proyecto está fundamentado en la aplicación de estrategias que se basan en la norma ISO 27001, mediante las cuales se podrá instituir políticas que permitan salvaguardar los recursos institucionales además de la gestión de riesgos encontrados y con ello se logra el aseguramiento de cada uno de los activos institucionales.

Los estándares ISO 27001 se los puede implementar en cualquier empresa o institución no importa a que se dediquen ni el tamaño que posean su propósito el aseguramiento de la información mediante la creación de políticas que permitan la gestión

CAPÍTULO 1

MARCO TEÓRICO

1.1 Tema

AUDITORÍA DE SEGURIDAD DE LA INFORMACIÓN, APLICANDO LA NORMA ISO/IEC 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO.

1.2 Antecedentes Investigativos

Para el presente trabajo, se revisó bibliografías de autores de la carrera de Ingeniería en Sistemas Computacionales e Informáticos que han realizado investigaciones similares, en las cuales se encontraron los siguientes trabajos:

El trabajo elaborado por: Jorge Giovanni Ulloa Barrera (2018) previo a la obtención del título de Ingeniero en Sistemas con el tema: "AUDITORÍA INFORMÁTICA APLICANDO LA METODOLOGÍA COBIT EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE SAN CRISTÓBAL DE PATATE", concluye que : "El sistema organizacional del GAD Municipal de San Cristóbal de Patate, no garantiza con cumplir con los criterios de información los cuales son efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad de los datos y la información manejada en la institución de forma diaria que permite alcanzar las metas y objetivos institucionales"[1].

Trabajo ejecutado por Ramiro Alejandro Guevara Tucta (2017), previo a la obtención del título de Ingenieros en sistemas el con el tema: "SISTEMA DE GESTIÓN DE

SEGURIDAD DE LA INFORMACIÓN BASADO EN LA NORMA ISO/IEC 27001 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN DEL DISTRITO 18D01 DE EDUCACIÓN" concluye que : "Se evidenció que no se gestionan adecuadamente los activos informáticos por lo que la información que se procesa a través de los mismos está expuesta en gran medida ante amenazas y vulnerabilidades"[2].

Tesis desarrollada por: Sandra Maribel Criollo Tasinchana (2017) en la Universidad Técnica de Ambato previo a la obtención del título de Ingeniero en Sistemas con el tema: "ANÁLISIS E IMPLANTACIÓN DE LA NORMA ISO/IEC 27002:2013 PARA EL DEPARTAMENTO INFORMÁTICO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DEL CANTÓN SALCEDO" concluye que : "La información recolectada en los departamentos del GAD Municipal del Cantón Salcedo se puede concluir que se encuentra expuesta a ataques internos o externos. La falta de controles, políticas y conocimientos sobre la seguridad de la información en una institución la hace vulnerable a diversos ataques, por tal motivo se llegado a definir políticas de seguridad ya que estas serían la base para controlar y proteger los activos de la institución" [3].

1.2.1Contextualización del problema

En la actualidad, las empresas que manejan grandes y pequeñas cantidades de información a nivel mundial, son blancos fáciles de ataques informáticos debido a que no cuentan con las debidas normas de seguridad, es por eso que los organismos internacionales encargados de la seguridad de la información, mediante la utilización de estándares logran minimizar el riesgo de ataques informáticos, que provocan perdida de información ocasionando así grandes problemas a nivel empresarial; por este motivo es imprescindible que las empresas puedan evaluar los riesgos asociados, para que establezcan las estrategias y controles adecuados y así aseguren una permanente protección para salvaguardar la información. Un sin número de empresas han optado por la implantación de sistemas de gestión con el fin de garantizar la eficacia y fiabilidad de sus procesos de negocio [4].

En el Ecuador, la seguridad de la información no es un campo que se ha estudiado a fondo, aunque es un área importante ya que todas las empresas manejan sistemas de información, por este motivo están expuestos a ataques para vulnerar los sistemas y así violentar la información.

En la provincia del Tungurahua las diferentes instituciones públicas y privadas que manejan información, tienen una gran preocupación por las amenazas que representan los ataque informáticos, es por eso que han realizado grandes esfuerzos para minimizar estos riegos utilizando una serie de procesos informáticos; las auditorías permiten obtener resultados reales de las falencias con las que cuentan las instituciones.

El Gobierno Autónomo Descentralizado San Pedro de Pelileo, maneja grandes cantidades de información delicada como información financiera, información catastral entre otros; esto hace que sean vulnerables para amenazas y al no contar con las debidas políticas de seguridad en la institución podría ocasionar la filtración de información; la institución se beneficiará ya que se logrará confidencialidad a gran escala de la información. Además, se logrará mayor eficiencia y eficacia en la institución.

1.2.2 Fundamentación Teórica

1.2.2.1 Auditoria de Seguridad

La auditoría de seguridad sirve para comprobar que las medidas de seguridad y control de los sistemas informáticos se adecúan a la normativa que se ha desarrollado para la protección de los datos; además identifica las deficiencias, y propone medidas correctivas o complementarias.

Al obtener los resultados, se detallan, archivan y reportan a cada uno de los responsables mismos que deberán establecer medidas para prevenir, reforzar y proceder a la corrección pero siempre siguiendo un proceso secuencial que permita a los administradores la mejora de la seguridad de los sistemas y así se aprende de los errores cometidos.

Al realizar auditorías de seguridad de un Sistema de Información, se llega a conocer en ese momento cuál es la situación exacta de los activos de la información en cuanto a protección, control y medidas de seguridad.

1.2.2.2 Estándares de Seguridad de la Información

Son aquellos los mismos que proporcionan un marco de gestión de seguridad de la información disponible por cualquier tipo de organización, pública o privada, grande o pequeña. Estos estándares contienen excelentes prácticas las cuales son recomendadas en seguridad de la información estas sirven para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la Seguridad de la Información (SGSI) [5].

1.2.2.3 ISO/IEC 27001

Esta norma específica los requisitos para la creación, implementación, funcionamiento, supervisión, revisión, mantenimiento y mejora de un SGSI documentado, teniendo en cuenta los riesgos empresariales generales de la organización. Es decir, explica cómo diseñar un SGSI y establecer los controles de seguridad, de acuerdo con las necesidades de una organización o de partes de la misma, pero no aclara mediante qué procedimientos se ponen en práctica. Por ejemplo, uno de los principales requisitos es la realización de un análisis de riesgos con unas determinadas características de objetividad y precisión, pero no aporta indicaciones de cuál es la mejor manera de llevar a cabo dicho análisis. Puede ejecutarse con una herramienta comercial, con una aplicación diseñada expresamente para la empresa, mediante reuniones, entrevistas, tablas o cualquier otro método que se estime oportuno. Todos estos recursos servirán para cumplir la norma, siempre y cuando se observen los requisitos de objetividad del método, los resultados sean repetibles y la metodología se documente[5].

1.2.2.4 Sistemas de Información

Un sistema de información es el conjunto de elementos o componentes relacionados con la información que interaccionan entre sí para lograr un objetivo: facilitar y/o recuperar información.
Para entender a los sistemas de información hay que estar al tanto de que existen necesidades en las organizaciones y comunidades que deben ser satisfechas, además hay que dominar las complejidades de cómo se maneja la información y cuáles son las potencialidades de los medios que se emplean para organizar y recuperar información.

Regularmente el término "sistema de información" es usado de manera errónea, en la mayoría de los casos los recursos materiales de un sistema de información están constituidos casi en su totalidad por sistemas informáticos. Estrictamente, un sistema de información no tiene por qué disponer de dichos recursos. Entonces se podría decir que los sistemas de información informáticos son un subconjunto de los sistemas de información.

1.2.2.5 Amenaza

Es cualquier cosa que provoque un daño a nuestro activo. Por ejemplo, si un virus corrompe el ordenador en donde el alumno tiene su trabajo final, no podrá acceder al momento de presentarlo y tal vez lo pierda.

1.2.2.6 Riesgo

Es una situación del mundo real, en el cual hay una exposición a la adversidad conformada por un sin número de circunstancias del entorno donde hay posibilidad de pérdidas. Los riesgos informáticos son exposiciones los mismos que pueden ser atentados y amenazas a los sistemas de información.

1.2.2.7 Tipos de Riesgos

a) Spam

"Son aquellos que acarrean virus a la PC cuando abrimos las páginas que son restringidas por ejemplo porno, correos no deseados entre otras, este tipo de páginas provocan que nuestros equipos se infecten" [6].

b) Piratería

"El software ilegal incrementa los riesgos de exposición a virus que pueden destruir los sistemas, también información valiosa para los usuarios. De este modo, puede generar grandes conflictos en los sistemas y por ello causar cuantiosos perjuicios económicos. Altas posibilidades de pérdida total de los datos y no teniendo acceso al servicio de atención al cliente, actualizaciones del software, documentación técnica, formación y solución de errores" [6].

c) Fuga de Información

"Al perder información involucra grandes problemas por ejemplo, cuando se nos encarga una ingeniería social" [6].

d) Ataques Informáticos

"Los ataque informáticos aprovechan las debilidad o falla en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente informático; a fin de obtener un beneficio, por lo usualmente de índole económico, causando un efecto negativo en la seguridad del sistema, que luego se ve repercutido directamente en los activos de la organización.

Para menguar el impacto negativo causado por ataques, existen procedimientos y mejores prácticas que proporcionan la lucha contra las actividades delictivas y

reducen notablemente el campo de acción de los ataques. Uno de los pasos más importantes en seguridad, es la educación. Comprender cuáles son las debilidades más comunes que pueden ser aprovechadas y cuáles son sus riesgos asociados, permitirá conocer de qué manera se ataca un sistema informático ayudando a identificar las debilidades y riesgos para luego desplegar de manera inteligente estrategias de seguridad efectivas" [6].

1.2.2.8 Aspectos de seguridad que compromete un ataque

"La seguridad compuesta por tres elementos esenciales que forman parte de los objetivos que intentan implicar los atacantes. Estos elementos son la confidencialidad, la integridad y la disponibilidad de los recursos. Con lo expuesto, el atacante intentará explotar las vulnerabilidades de un sistema o de una red para hallar una o más debilidades en alguno de los tres elementos de seguridad" [6].

a) Confidencialidad.

"Un atacante podría substraer información sensible como contraseñas u otro tipo de datos que viajan en texto claro a través de redes confiables, quebrantando la confidencialidad al permitir que otra persona, que no es el destinatario, tenga acceso a los datos. Un ejemplo que compromete este elemento es el envenenamiento de la tabla ARP (ARP Poisoning)" [6].

b) Integridad.

"Mientras la información se trasfiere a través de los protocolos de la comunicación, los atacantes podrían interceptar el mensaje y realizar cambios en determinados bits del texto cifrado con la intención de alterar los datos del criptograma. Este tipo de ataques se denomina Bit-Flipping y son considerados ataques contra la integridad de la información. El ataque no se lleva a cabo de manera directa contra el sistema de cifrado

pero sí en contra de un mensaje o de una serie de mensajes cifrados. En el extremo, esto puede convertirse en un ataque de denegación de servicio contra todos los mensajes en un canal que utiliza cifrado" [6].

c) Disponibilidad.

"Los atacantes podrían utilizar los recursos de la organización, como sería el caso del ancho de banda de la conexión DSL para inundar de mensaje el sistema víctima y forzar la caída del mismo, negando así los recursos y servicios a los usuarios legítimos del sistema. Esto se conoce como Denial of Service (DoS) y atenta directamente contra la integridad de la información"[6].

1.2.2.9 Vulnerabilidades

" Son las inseguridades que posee el activo tanto por problemas tecnológicos, como problemas de procedimientos. Está demostrado que la gran mayoría de pérdidas de activos son por falta de procedimientos o desconocimiento.

Dichas vulnerabilidades no son más que el producto de los fallos causados por el inadecuado diseño de un software, así como también puede ser provocado por las limitaciones tecnológicas con que fue diseñado.

Hay algunos tipos des de vulnerabilidades. La primera es conocida como vulnerabilidad teórica, y el segundo, que es de interés para el usuario, la vulnerabilidad real, que comúnmente se lo conoce como Exploit " [7].

1.2.2.10 Tipos de vulnerabilidades en informática

Las vulnerabilidades no deben tomarse a la ligera, ya que puede ocasionarnos un sinnúmero de peligros, aunque no estemos utilizando datos o documentos importantes.

Esto es un tema muy serio, y es estudiado y clasificado por un sin fin de empresas y organizaciones.

Su clasificación es básicamente la siguiente:

Calificación	Definición
Crítica	Este tipo de vulnerabilidad permite la propagación de amenazas sin que sea necesaria la participación del usuario.
Importante	Este tipo de vulnerabilidad es capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios, como así también, la integridad o disponibilidad de los recursos de procesamiento que este disponga.
Moderada	Este es uno de los tipos de vulnerabilidades más sencillas de combatir, ya que el riesgo que presenta se puede disminuir con medidas tales como configuraciones predeterminadas, auditorías y demás. Aparte, las vulnerabilidades moderadas no son aprovechables en todo su potencial ya que no afecta a una gran masa de usuarios.
Baja	Este tipo de vulnerabilidad es realmente muy difícil de aprovechar por un atacante, y su impacto es mínimo, ya que no afecta a una gran masa de usuarios.

Tabla 1 Tipos de vulnerabilidades

1.2.2.10 Ciclo de deming

La norma ISO/IEC 27001 está basada en el ciclo de Deming que cuenta con cuatro etapas fundamentales que son: Planificar, hacer, chequear y actuar (PHVA) gracias a ello existe una mejora continua, la productividad de los empleados aumenta y puede ser aplicado en cualquier área de la institución

1.3 Objetivos

13.1 Objetivo General

Realizar una auditoría de seguridad de la información, aplicando la Norma ISO/IEC 27001 en el Gobierno Autónomo Descentralizado San Pedro de Pelileo.

1.3.2 Objetivos Específicos

- Analizar la situación actual del manejo de la información en el Gobierno Autónomo Descentralizado San Pedro de Pelileo.
- Analizar los riesgos existentes en el Gobierno Autónomo Descentralizado San Pedro de Pelileo.
- Realizar la auditoria con la norma ISO/IEC 27001 en el Gobierno Autónomo Descentralizado San Pedro de Pelileo.
- Generar un manual de políticas de seguridad para el manejo de la información en el Gobierno Autónomo Descentralizado San Pedro de Pelileo.

CAPÍTULO II

METODOLOGÍA

2.1 Materiales

2.1.1 Institucionales

- Universidad Técnica de Ambato
- Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Biblioteca virtual de la Universidad técnica de Ambato
- Gobierno Autónomo Descentralizado San Pedro de Pelileo
- Repositorio

2.1.2 Humanos

- Tutor de la tesis de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.
- Personal del Gobierno Autónomo Descentralizado San Pedro de Pelileo.
- Investigador
- Docentes FISEI

2.1.3 Materiales

- Pc de escritorio
- Internet
- Energía Eléctrica

- Materiales de Oficina
- Impresora
- Disco para almacenamiento de información

2.1.4 Recurso Económico

Económico (presupuesto y financiamiento).

Para el financiamiento del proyecto el investigador contará con los siguientes gastos:

N.-	Materiales	Cantidad	Valor Unitario	Valor total
1	Laptop	1	1200	1200.00
2	Internet	300 horas	0.60	180.00
3	Energía Eléctrica	500 horas	0,05	25.00
4	Impresora	1	120.00	120.00
5	Papel	3 resma	11.25	11.25
6	Tintas de Impresora	4	5.00	20.00
7	Transporte	100	2.00	200.00
8	Otros Gastos			100.00
			Total USD	1856.25

Tabla 2 Materiales y Costo

2.2 Métodos

2.2.1 Modalidad de la Investigación

Se utilizará los siguientes tipos de investigación:

2.2.1.1 Investigación de campo

La investigación de campo se da lugar en del Gobierno Autónomo Descentralizado San Pedro de Pelileo, para obtendrá la información necesaria para la realización de este trabajo.

2.2.1.2 Investigación bibliográfica y documental

Se utilizara la investigación documental porque la información que se necesita para el desarrollo de la investigación se encuentra documentado ya sea en revistas, artículos científicos, libros entre otros, de trabajos similares que nos puedan ayudar para realizar la auditoria de seguridad de la información.

2.2.1.3 Investigación Aplicada

Se utiliza la investigación aplicada que permita conocer la problemática que existe en el Gobierno autónomo Descentralizado San Pedro de Pelileo.

2.2 Población y Muestra

2.2.1 Población

Los funcionarios de la municipalidad de quienes se recogerá la información**:**

Departamento	Número de funcionarios municipales
ADMINISTRACIÓN DE ACTIVOS	2
ADMINISTRACIÓN DE JUSTICIA	2
ADMINISTRACIÓN DE SERVICIOS PÚBLICOS	2
AGUA POTABLE	2
ALCALDÍA	2
ASESORÍA JURÍDICA	2
MOYA	2
CAMAL MUNICIPAL	2
DEPARTAMENTO ADMINISTRATIVO	2
DEPARTAMENTO DE AGUA	2

POTABLE Y ALCANTARILLADO	
DEPARTAMENTO DE CATASTROS Y AVALÚOS	4
DEPARTAMENTO DE DESARROLLO DE LA COMUNIDAD	2
DEPARTAMENTO DE OBRAS PÚBLICAS	2
DEPARTAMENTO DE ORDEN Y CONTROL	2
DEPARTAMENTO DE PLANIFICACIÓN DESARROLLO Y ORDENAMIENTO	2
DEPARTAMENTO DE SERVICIOS PÚBLICOS	2
DEPARTAMENTO FINANCIERO	2
REGISTRO DE LA PROPIEDAD	2
TALENTO HUMANO	2
TESORERÍA	2
Total	**42**

Tabla 3 Personal de donde se obtendrá Información

2.2.2 Muestra

De acuerdo a la investigación no se requiere realizar el cálculo la muestra porque se recolectará la información en cada uno de los departamentos del Gobierno autónomo Descentralizado San Pedro de Pelileo.

2.4 Procesamiento y Análisis de Datos

Se procederá a realizar la recolección de información necesaria para realizar la auditoria en el Gobierno Autónomo Descentralizado San Pedro de Pelileo.

De los datos obtenidos se procederá a la selección de la información que permita cumplir con los objetivos.

Resultados generados al realizar la auditoria de seguridad de la información.

CAPITULO III

3 Análisis y discusión de resultados

3.1 Situación Actual

El Gobierno Autónomo Descentralizado San Pedro de Pelileo es la institución encargada de avance y desarrollo del Cantón San Pedro de Pelileo a través de la planificación, gestión, dotación de servicios y de la acción oportuna de sus departamentos que cumplen con una función específica para el progreso cantonal.

Entre los departamentos que componen la institución se enmarcan:
Gestión Tecnológica , Administración de Activos, Administración de Justicia, Administración de Servicios Públicos, Agua Potable y Alcantarillado, Alcaldía, Asesoría Jurídica, La Moya, Camal Municipal, Administrativo, Agua Potable y Alcantarillado, Catastros y Avalúos, Desarrollo de la Comunidad, Obras Públicas, Orden y Control, Planificación, Desarrollo y Ordenamiento Territorial Servicios Públicos, Financiero, Registro de la Propiedad, Talento Humano y Tesorería.

Previa la investigación a diferentes funcionarios de los departamentos de la institución, se pudo verificar que en diversos casos el personal desconocía las políticas de seguridad tanto del sistema informático que manejan como el de los equipos tecnológicos a su cargo.

En La Unidad de Gestión Tecnológica se constató que cada funcionario tiene un rol asignado con opciones de uso en el sistema informático, dependiendo del perfil que desempeñan dentro de la entidad.

Además se visualizó que dicho departamento cuenta con un espacio mínimo en el que se alojan los servidores y demás equipos que almacenan información de gran importancia a nivel institucional.

3.1.2 Alcance del Proyecto

El desarrollo del proyecto se enfoca directamente en el Departamento de Gestión Tecnológica del Gobierno Autónomo Descentralizado San Pedro de Pelileo al ser el promotor del aseguramiento, confidencialidad de la información y responsable de la correcta funcionalidad de las instalaciones y equipamientos.

Como primer paso se procedió a la recolección de información mediante la entrevista al jefe de la Unidad de Gestión Tecnológica y la aplicación de una encuesta a jefes y asistentes técnicos administrativos, con el propósito de establecer los problemas concernientes a seguridad y políticas aplicadas dentro del Gobierno Autónomo Descentralizado San Pedro de Pelileo.

Mediante visitas realizadas a la municipalidad se puedo determinar la existencia de un sinnúmero de falencias que afectan a la seguridad de la institución como instalaciones en mal estado problemas en el cableado, desorden en varias áreas.

Posteriormente se aplicará una guía con estándares de seguridad según las normas ISO/IEC 27001, mismas que permitirán mitigar los riesgos de confidencialidad e integridad de los datos y de la información.

3.1.2 Análisis de los niveles de seguridad de la institución.

Las técnicas de recolección de datos aplicadas al personal fueron primordiales para identificar las deficiencias presentes en las medidas de seguridad de la información con las que opera el GADM San Pedro de Pelileo.

Entrevista realizada al jefe del Departamento de Gestión Tecnología GADM San Pedro de Pelileo.

PREGUNTA	RESPUESTA
1. **¿La Unidad de Gestión Tecnológica cuenta con políticas de seguridad para la gestión de información?** **Si ( )** **No ( )** **Cuales**	Si los empleados tiene conocimiento de algunas políticas que se aplican dentro de la institución como por ejemplo Gestión de usuarios Restricciones en el internet
1. **¿El personal del GADM. San Pedro de Pelileo tiene conocimientos de las políticas de seguridad existentes?** **Si ( )** **No ( )**	Si tienen conocimiento en lo que se refiere a algunas restricciones que se aplican dentro GADM San Pedro de Pelileo.
2. **¿Cada empleado tiene responsabilidades asignadas del uso de los recursos de la institución?** **Si ( )** **No ( )**	Si los empleados tienen conocimiento de las responsabilidades sobre los recursos que manejan a su cargo.
3. **¿Se lleva un control adecuado del**	Si solo personal autorizado puede tener

acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema del GAD San Pedro de Pelileo? **Si ( )** **No( )**	acceso al sistema mas no personal ajeno a la institución.
5. ¿Se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno? **Si ( )** **No ( )**	Si cada usuario solo puede manejar lo referente a su cargo asignado.
6. ¿El sistema Cabildo al momento de ingresar una contraseña solicita que esta tenga letras números y caracteres especiales? **Si ( ) No ( )**	No el sistema Cabildo no tiene ese control establecido aunque los usuarios deberían utilizar combinaciones en las contraseñas.
7. ¿Se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la institución? **Si ( ) No ( )**	Se realiza un mantenimiento completo cada 6 meses a nivel de todos los equipos, también cuando un equipo presenta un fallo y los funcionarios lo solicita..

Indique cada cuanto tiempo **a) 2 meses** **b) 3 meses** **c) 6 meses** **d) cada año**	
8. ¿Qué hace La Unidad de Gestión Tecnológica cuando el sistema tiene algún fallo?	Acude al sitio para verificar el fallo presentado y así poderlo reparar.
9. Se realizan monitoreo constantemente al sistema para evitar cualquier eventualidad. **Si ( )** **No ( )**	Si se realizan monitoreo constantes para evitar fallos al sistema pero no se tiene un manual que nos ayude para realizarlo de de una manera correcta
10. Cuentan con un sistema de inventario de recursos informáticos de la institución **Si ( )** **No ( )**	Si se tiene un inventario en el cual constan todos los recursos informáticos del GADM San Pedro de Pelileo pero no se encuentra actualizado.
11. ¿El departamento cuenta con personal que tengan amplios conocimientos en seguridad de la información? **Si ( )** **No ( )**	Si el personal tiene conocimientos en seguridad de la información, pero no existe una persona que se encargue específicamente de ese trabajo.

12. ¿Cada Departamento del GAD San Pedro de Pelileo tiene asignada políticas de seguridad? **Si ( )** **No ( )**	No existen políticas asignadas en los diferentes departamentos de la institución.
13. ¿Cuenta el Departamento con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema? **Si ( ) No ( )**	Si al momento que un empleado deja de pertenecer a la institución procede al bloqueo del usuario con el cual fue asignado para desempeñar sus labores.
14. ¿Se revisa periódicamente el cableado en todos los departamentos de la institución? **Si ( ) No ( )**	Si se realiza un control del cableado constante mente dentro de la institución.
15. ¿Se realizan copias de seguridad de la información? **Si ( ) No ( )** **Cada cuanto tiempo**	Se realiza copias de seguridad cada mes pero cada empleado debería realizar una copia de sus equipos cada determinado tiempo.

Tabla 4. Desarrollo de preguntas-entrevista

Elaborado por el Investigador.

3.1.3 Evaluación de datos obtenidos

Encuesta aplicada a jefes y asistentes técnicos administrativos en cada departamento del GADM San Pedro de Pelileo.

DEPARTAMENTO	N.- de Encuestados
ADMINISTRACIÓN DE ACTIVOS	2
ADMINISTRACIÓN DE JUSTICIA	2
ADMINISTRACIÓN DE SERVICIOS PÚBLICOS	2
AGUA POTABLE	2
ALCALDÍA	2
ASESORÍA JURÍDICA	2
MOYA	2
CAMAL MUNICIPAL	2
DEPARTAMENTO ADMINISTRATIVO	2
DEPARTAMENTO DE AGUA POTABLE Y ALCANTARILLADO	2
DEPARTAMENTO DE CATASTROS Y AVALÚOS	4
DEPARTAMENTO DE DESARROLLO DE LA COMUNIDAD	2
DEPARTAMENTO DE OBRAS PÚBLICAS	2
DEPARTAMENTO DE ORDEN Y CONTROL	2
DEPARTAMENTO DE PLANIFICACIÓN DESARROLLO Y	2

ORDENAMIENTO	
DEPARTAMENTO DE SERVICIOS PÚBLICOS	2
DEPARTAMENTO FINANCIERO	2
REGISTRO DE LA PROPIEDAD	2
TALENTO HUMANO	2
TESORERÍA	2
Total	**42**

Tabla 5. Personal del G.A.D. San Pedro de Pelileo

Elaborado por el Investigador.

3.1.4 Tabulación de encuestas

1.- ¿La Unidad de Gestión Tecnológica cuenta con políticas de seguridad para la gestión de información?

Opciones	N.- Res puestas	Porcentaje
SI	18	43%
NO	24	57%
Total	42	100%

Tabla 6 Resultado Pregunta 1

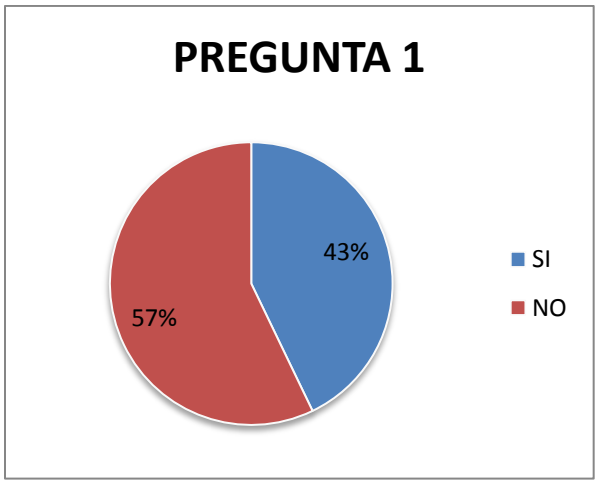


Figura 1 Resultado Pregunta 1

Análisis e Interpretación: De un total de 42 encuestados 18 que corresponde al 43% indican que La Unidad de Gestión Tecnológica del GADM San Pedro de Pelileo si cuenta con políticas de seguridad, mientras que 24 que corresponde al 57% manifiesta que el departamento no tiene políticas de seguridad.

En base a los resultados obtenidos de la aplicación de las encuestas revelan que La Unidad de Gestión Tecnológica no cuenta con políticas de seguridad.

¿Cuáles?

Opciones	N.- Res puestas	Porcentaje
BASE DE DATOS SEGURA	4	22%
PERFILES DE USUARIO	6	33%
DESCONOCEN EL TIPO DE CONTROL	8	45%
TOTAL	18	100%

Tabla 7. Resultado Pregunta 1 Cuales

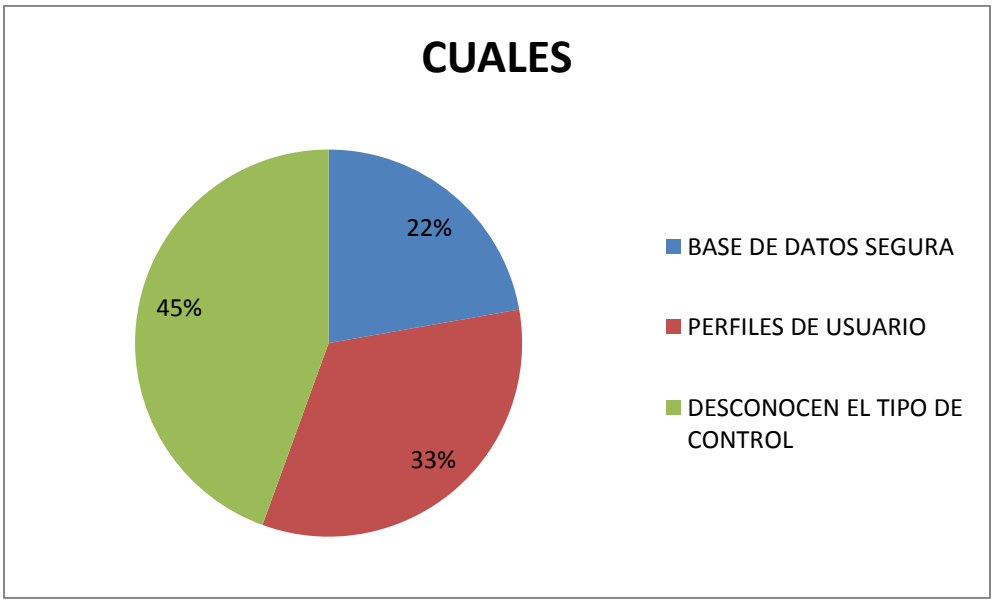


Figura 2. Resultado Pregunta 1 Cuales

Análisis e Interpretación: De un total de 18 encuestados que respondieron que si, 8 que corresponde al 45% respondieron que desconocen el tipo de políticas existentes, 6 que corresponde al 33% respondieron que se aplica perfiles de usuario, 4 que corresponde al 22 % señalan que las bases de datos son seguras.

De los empleados del GADM San Pedro de Pelileo que respondieron que se aplican políticas de seguridad según los datos obtenidos la mayoría manifiestan que desconocen el tipo de control que se aplica en la seguridad de la información.

2.- ¿El personal del GAD San Pedro de Pelileo tiene conocimientos de las políticas de seguridad existentes?

Opciones	N.- Res puestas	Porcentaje
SI	15	36%
NO	27	64%
TOTAL	42	100%

Tabla 8 Resultado Pregunta 2

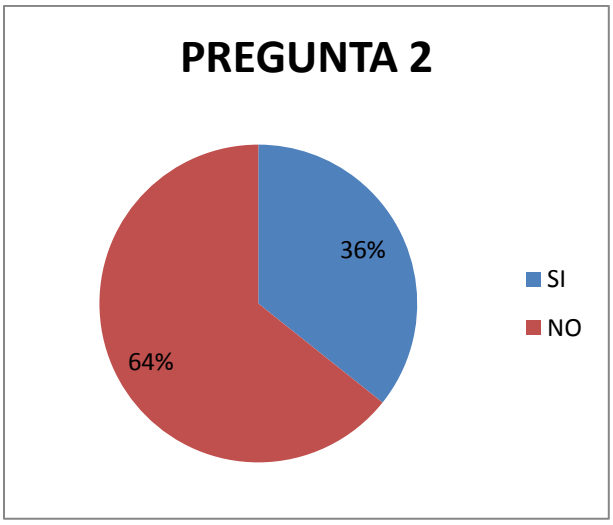


Figura 3. Resultado Pregunta 2

Análisis e Interpretación: Del total de 42 encuestados 15 que corresponde al 36% indican que el personal del GADM San Pedro de Pelileo si tienen conocimiento de las políticas existente, mientras que 27 que corresponde el 64% indican que el personal del GADM San Pedro de Pelileo no tienen conocimiento de las políticas existente.

Según los datos obtenidos en la aplicación de las encuestas revelan que los empleados de la institución desconocen de las políticas existentes en el GADM San Pedro de Pelileo.

3.- ¿Cada empleado tiene responsabilidades asignadas del uso de los recursos de la institución?

Opciones	N.- Res puestas	Porcentaje
SI	30	29%
NO	12	71%
TOTAL	42	100%

Tabla 9. Resultado Pregunta 3

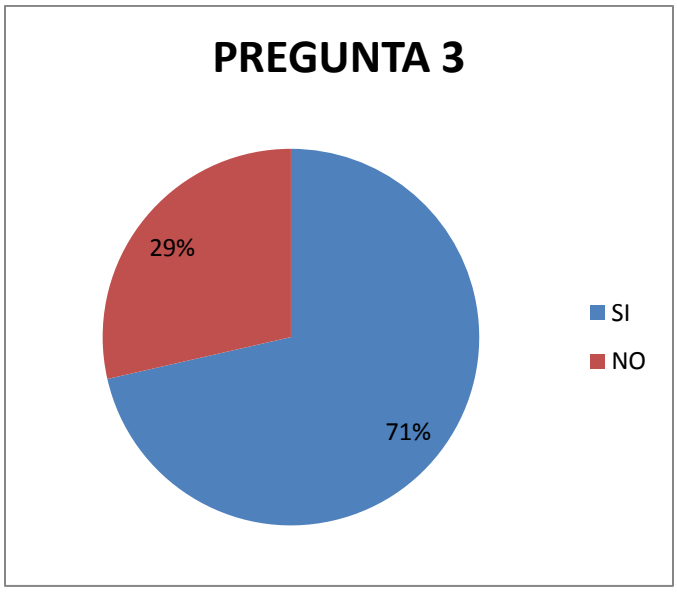


Figura 4. Resultado Pregunta 3

Análisis e Interpretación: Del 100% de los encuestados 30 que corresponde al 71% indican que el personal del GADM San Pedro de Pelileo si tienen responsabilidades del uso de los recursos de la institución, mientras 12 que corresponde el 29% indican que el personal del GADM San Pedro de Pelileo no tienen responsabilidades asignadas en el uso de los recursos.

Los datos obtenidos en la aplicación de las encuestas revelan que los empleados de la institución si tienen responsabilidades asignadas en el uso de los recursos del GADM San Pedro de Pelileo.

4.- ¿Se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema del GAD San Pedro de Pelileo?

Opciones	N.- Res puestas	Porcentaje
SI	36	86%
NO	6	14%
TOTAL	42	100%

Tabla 10. Resultado Pregunta 4

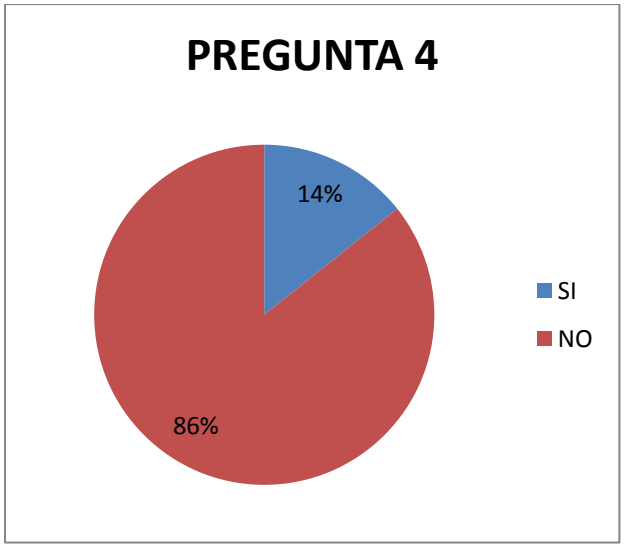


Figura 5. Resultado Pregunta 4

Análisis e Interpretación: Del 100% de los encuestados 36 que corresponde al 86% indican que se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema del GAD San Pedro de Pelileo, mientras 6 que corresponde el 14% indican que no lleva un control adecuado del acceso del personal para que personas no autorizadas si puedan acceder a los equipos y sistema del GAD San Pedro de Pelileo.

De los datos obtenidos en la aplicación de las encuestas revelan que si se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema del GAD San Pedro de Pelileo esto es muy importante dentro de la institución.

5.- ¿Se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno?

Opciones	N.- Res puestas	Porcentaje
SI	34	81%

NO	8	19%
TOTAL	42	100%

Tabla 11. Resultado Pregunta 5

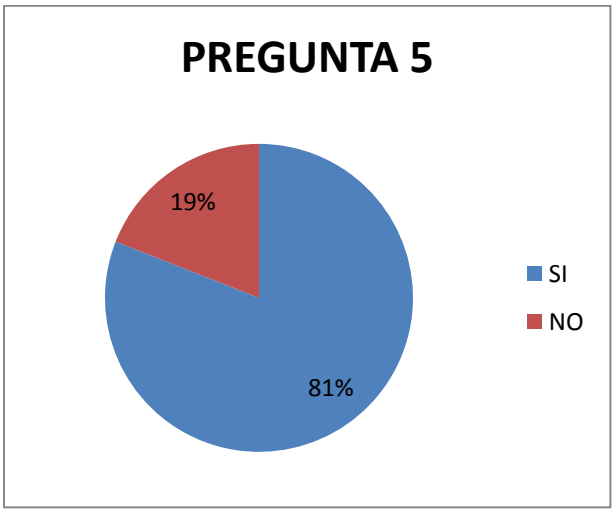


Figura 6. Resultado Pregunta 5

Análisis e Interpretación: Del 100% de los encuestados 34 que corresponde al 81% indican que tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno, mientras 8 que corresponde el 19% indican que no tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno.

De los datos obtenidos en la aplicación de las encuestas la gran mayoría de empleados afirman que se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno dentro de la institución.

6.- ¿El sistema al momento de ingresar una contraseña solicita que esta tenga letras números y caracteres especiales?

Opciones	N.- Res puestas	Porcentaje
SI	19	45%

NO	23	55%
TOTAL	42	100%

Tabla 12. Resultado Pregunta 6

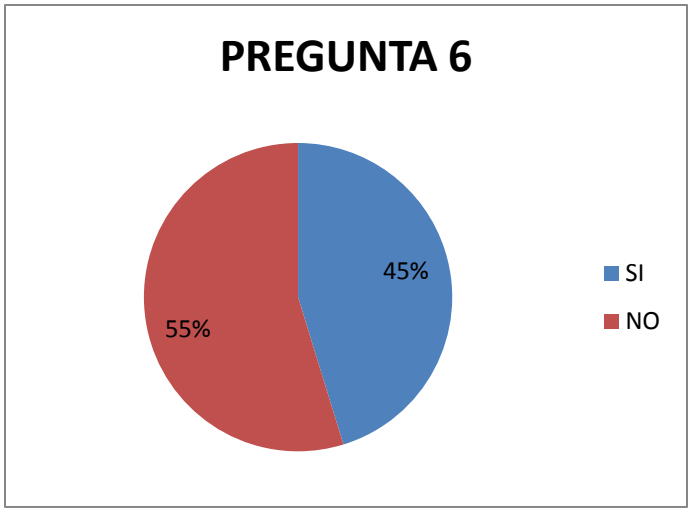


Figura 7. Resultado Pregunta 6

Análisis e Interpretación: Del total de 42 encuestados 19 que corresponde al 45% indican que el sistema al momento de ingresar una contraseña solicita que esta tenga letras números y caracteres especiales mientras que el 23 que corresponde al 55% manifiestan que no solicita ese tipo de seguridad.

De los datos obtenidos de la aplicación de la encuesta se puede determinar que el sistema en el momento de ingresar la contraseña no solicita que esta tenga letras números y caracteres especiales.

7.- ¿Se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la institución?

Opciones	N.- Res puestas	Porcentaje
SI	36	86%
NO	6	14%

TOTAL	42	100%

Tabla 13. Resultado Pregunta 7

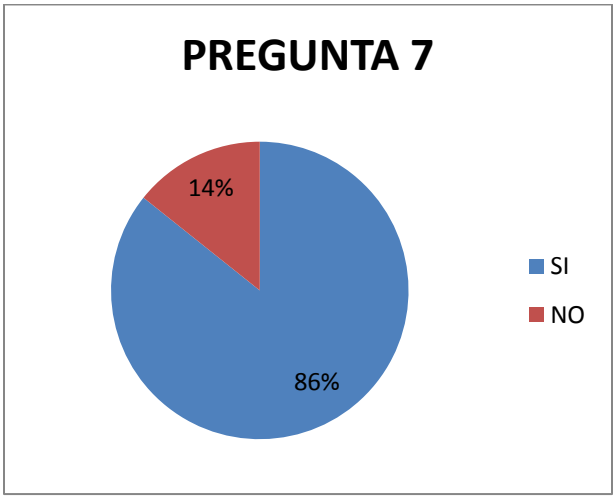


Figura 8. Resultado Pregunta 7

Análisis e Interpretación: Del total de 42 encuestados 36 que corresponde al 86% indican que se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la institución mientras que 6 que corresponde al 14% manifiestan que no lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la institución.

De los datos obtenidos de la aplicación de la encuesta se puede determinar que se lleva un manteniendo correctivo y preventivo en los equipos de la institución.

Indique cada cuanto tiempo

a) 2 meses

b) 3 meses

c) 6 meses

d) cada año

Opciones	N.- Res puestas	Porcentaje
2 MESES	9	25%

3 MESES	7	20%
6 MESES	17	47%
CADA AÑO	3	8%
TOTAL	36	100%

Tabla 14. Resultado Pregunta 8

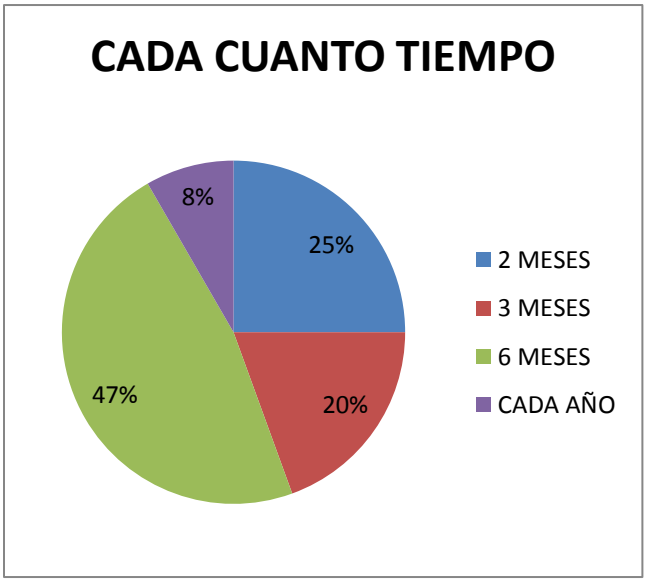


Figura 9. Resultado Pregunta 8

Análisis e Interpretación: de los 36 encuestados que respondieron que si 17 que corresponde al 47% dicen que el mantenimiento en los equipos se realiza cada 6 meses, 9 que corresponde al 25% manifiestan que se realiza el manteniendo en los equipos cada 2 meses, 7 que corresponde al 20% exponen que se realiza el mantenimiento en los equipos cada tres meses y 3 que corresponde al 8% manifiestan que se realiza cada año.

De los datos obtenidos de la aplicación de la encuesta se puede determinar que se realiza el mantenimiento a los equipos de la institución cada 6 meses.

8.- ¿Qué hace La Unidad de Gestión Tecnológica cuando el sistema tiene algún fallo?

Opciones	**N.- Res puestas**	**Porcentaje**

SOLUCIONAN EL PROBLEMA	30	72%
INFORMAR EL FALLO	10	24%
ACUDEN CUANDO SE LES LLAMA	1	2%
SUSPENDE EL SISTEMA	1	2%
TOTAL	42	100%

Tabla 15. Resultado Pregunta 8

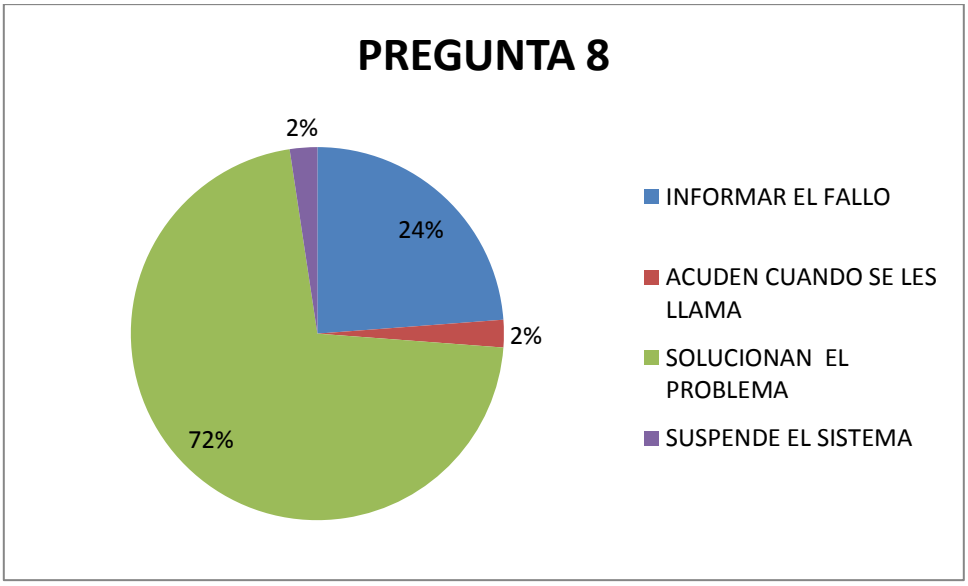


Figura 10. Resultado Pregunta 8

Análisis e Interpretación: Del total de 42 encuestados 30 que corresponde al 72% indican que cuando el sistema presenta un fallo el Unidad de Gestión Tecnológica solucionan el problema, 10 que corresponde al 24 % manifiestan que el departamento informa el fallo que tiene el sistema, 1 que corresponde al 2% manifiesta que acuden cuando se les llama, mientras que 1 que corresponde al 2% expone que suspende el sistema.

De los datos obtenidos de la aplicación de la encuesta se puede determinar que cuando el sistema presenta un fallo La Unidad de Gestión Tecnológica soluciona el problema.

9.- Se realizan monitoreos constantemente al sistema para evitar cualquier eventualidad?

Opciones	N.- Res puestas	Porcentaje
SI	31	26%
NO	11	74%
TOTAL	42	100%

Tabla 16. Resultado Pregunta 9

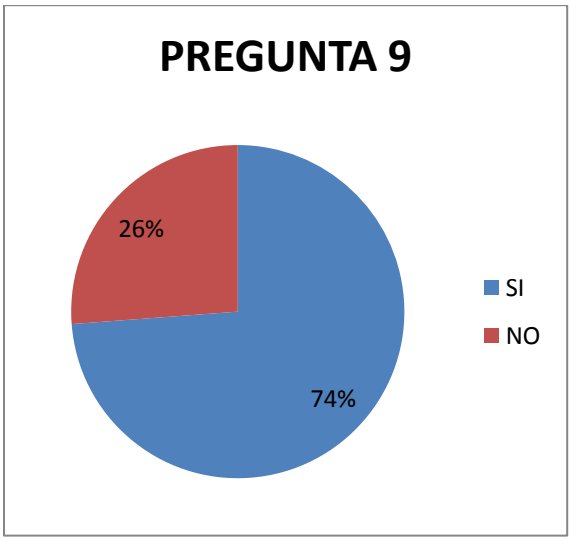


Figura 11.Resultado Pregunta 9

Análisis e Interpretación: Del total de 42 encuestados 31 que corresponde al 74% indican que se realizan monitoreos constantes para evitar cualquier eventualidad en el sistema, mientras que 11 que corresponde al 26% exponen que no se lleva monitoreos constantes en el sistema.

De los datos obtenidos de la aplicación de la encuesta se puede determinar que si se lleva monitoreos constantes en el sistema y de esta manera se evitan eventualidades.

10.- Cuentan con un sistema de inventario de recursos informáticos de la institución?

Opciones	N.- Res puestas	Porcentaje
SI	38	90%
NO	4	10%
TOTAL	42	100%

Tabla 17. Resultado Pregunta 10

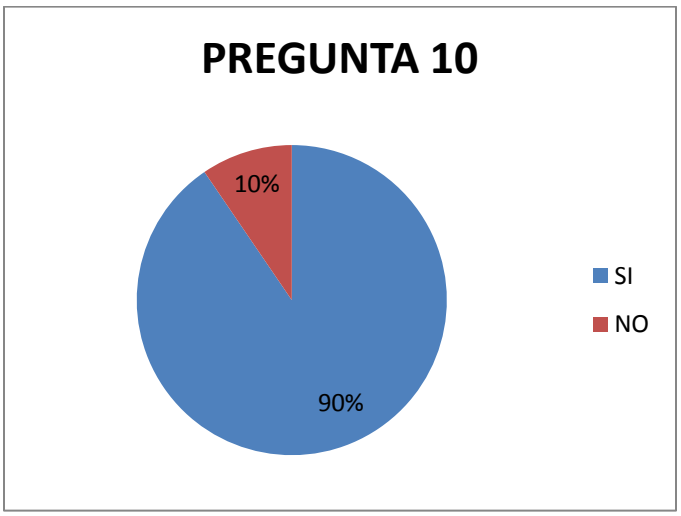


Figura 12. Resultado Pregunta 10

Análisis e Interpretación: Del total de 42 encuestados 38 que corresponde al 90% indican que si se cuenta con un inventario de los recursos informáticos de la institución, mientras que 4 que corresponde al 10% exponen que no se lleva in inventario de los recursos informáticos.

De los datos obtenidos de la aplicación de la encuesta se puede determinar que si se lleva un inventario de los recursos institucionales.

11.- ¿El departamento cuenta con personal que tengan amplios conocimientos en seguridad de la información?

Opciones	N.- Res puestas	Porcentaje
SI	36	86%
NO	6	14%
TOTAL	42	100%

Tabla 18. Resultado Pregunta 11

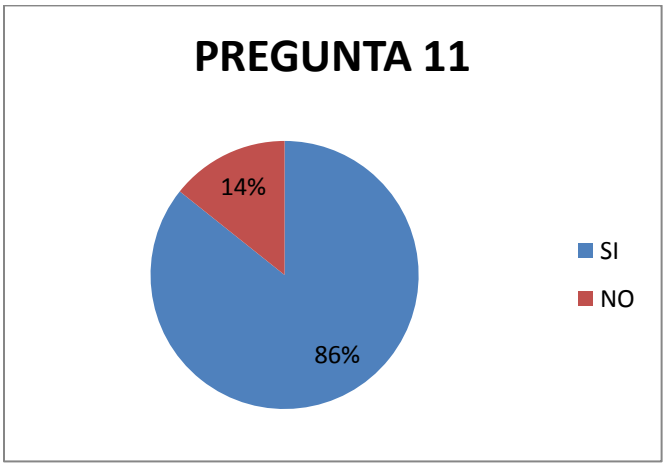


Figura 13. Resultado Pregunta 11

Análisis e Interpretación: Del total de 42 encuestados 36 que corresponde al 86% indican departamento cuenta con personal que tengan amplios conocimientos en seguridad de la información, mientras que 4 que corresponde al 14% manifiestan que no hay el personal con amplios conocimientos en seguridad de la información.

De los datos obtenidos de la aplicación de la encuesta se puede determinar que si existe en La Unidad de Gestión Tecnológica personal con amplios conocimientos en seguridad de la información.

12.- ¿Cada Departamento del GAD San Pedro de Pelileo tiene asignada políticas de seguridad?

Opciones	N.- Res puestas	Porcentaje

SI	10	76%
NO	32	24%
TOTAL	42	100%

Tabla 19. Resultado Pregunta 12

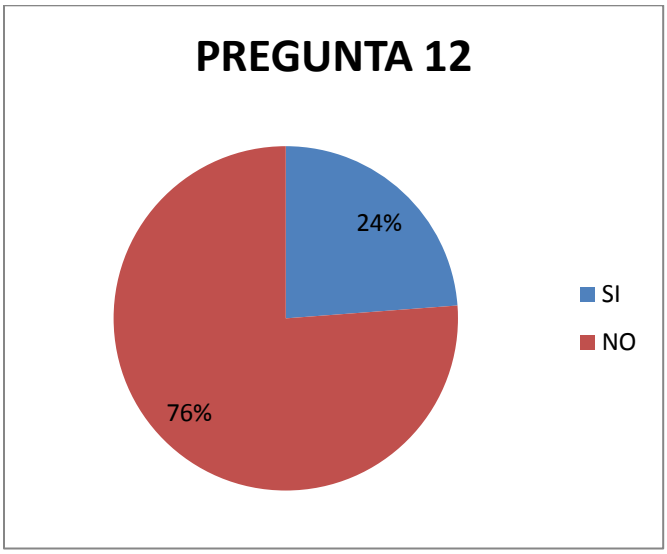


Figura 14. Resultado Pregunta 12

Análisis e Interpretación: Del 100% de los encuestados 10 que corresponde al 24% indican que cada Departamento del GADM San Pedro de Pelileo tiene asignada políticas de seguridad, mientas que 32 que corresponde al 76% manifiestan que en cada Departamento del GADM San Pedro de Pelileo no tiene asignada políticas de seguridad.
De los datos obtenidos en la aplicación de las encuestas revelan que en cada Departamento del GADM San Pedro de Pelileo no existen asignadas políticas de seguridad.

13.- ¿Cuenta el Departamento con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema?

Opciones	N.- Res puestas	Porcentaje
SI	25	40%

NO	17	60%
TOTAL	42	100%

Tabla 20. Resultado Pregunta 13

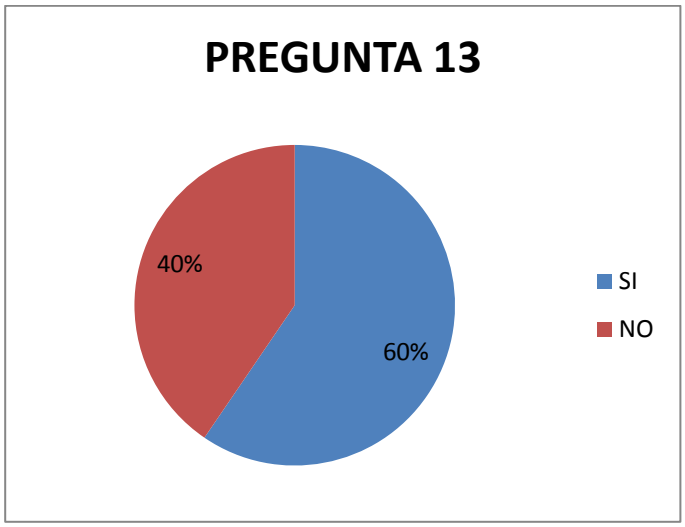


Figura 15. Resultado Pregunta 13

Análisis e Interpretación: Del 100% de los encuestados 25 que corresponde al 60% indican que el Departamento si tiene políticas de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema, mientas que 17 que corresponde al 40% manifiestan el Departamento no tiene políticas de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema.

De los datos obtenidos en la aplicación de las encuestas revelan que el Departamento si cuenta con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le suprima todos los accesos al sistema.

14.- ¿Se revisa periódicamente el cableado en todos los departamentos de la institución?

Opciones	N.- Res puestas	Porcentaje
SI	26	62%
NO	16	38%

TOTAL	42	100%

Tabla 21. Resultado Pregunta 14

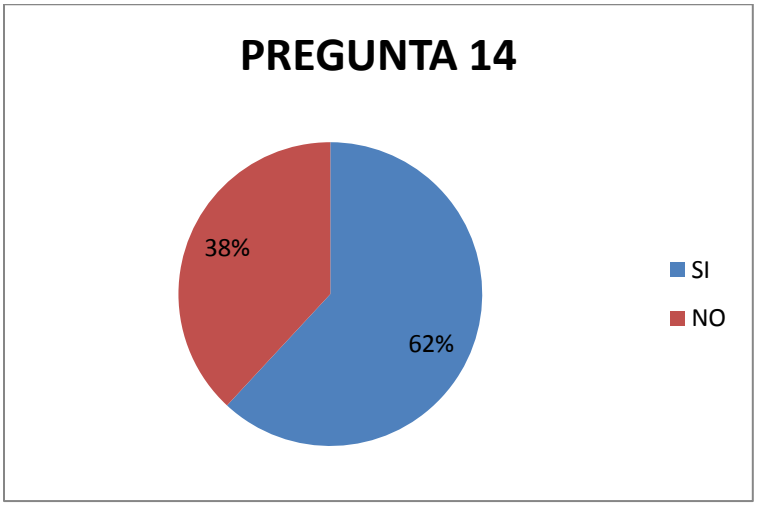


Figura 16. Resultado Pregunta 14

Análisis e Interpretación: Del 100% de los encuestados 26 que corresponde al 62% indican si se realizan periódicamente el cableado de los departamentos de la institución mientas que 16 que corresponde al 38% manifiestan que no se revisa el cableado de la institución periódicamente.

De los datos obtenidos en la aplicación de las encuestas revelan que se revisa periódicamente el cableado en los departamentos de la institución.

15.- ¿Se realizan copias de seguridad de la información?

Opciones	N.- Res puestas	Porcentaje
SI	29	69%
NO	13	31%
TOTAL	42	100%

Tabla 22. Resultado Pregunta 15

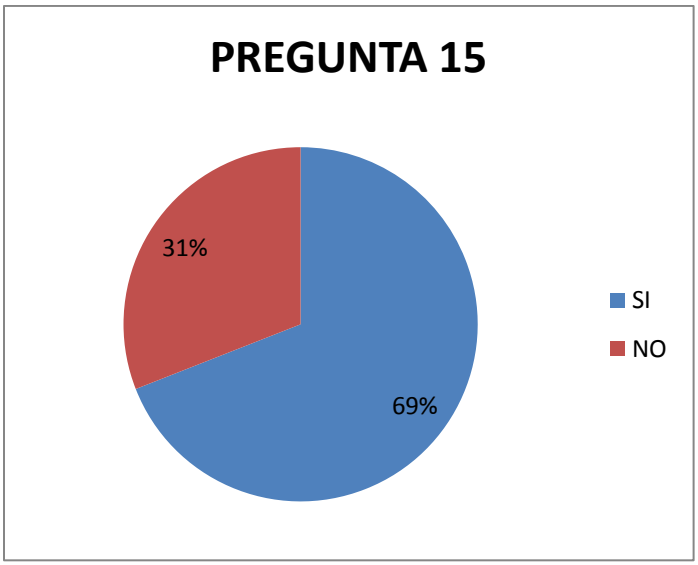


Figura 17. Resultado Pregunta 15

Análisis e Interpretación: Del 100% de los encuestados 29 que corresponde al 69% indican que si se realizan copias de seguridad de la información, mientas que 13 que corresponde al 31% manifiestan que no se realiza copias de seguridad de la información. Según los datos obtenidos la gran mayoría de empleados de la institución manifiestan que si se realizan copias de seguridad dentro del GADM San Pedro de Pelileo.

¿Cada cuánto tiempo?

Opciones	N.- Res puestas	Porcentaje
DIARIO	8	28%
CADA MES	2	7%
CADA 3 MESES	1	4%
CADA 6 MESE	2	7%
CADA AÑO	1	3%
CADA PERIODO DE TIEMPO	3	10%
NO SABEN CADA CUANTO TIEMPO	12	41%
TOTAL	29	100%

Tabla 23. Resultado Pregunta 15 Cada cuanto tiempo

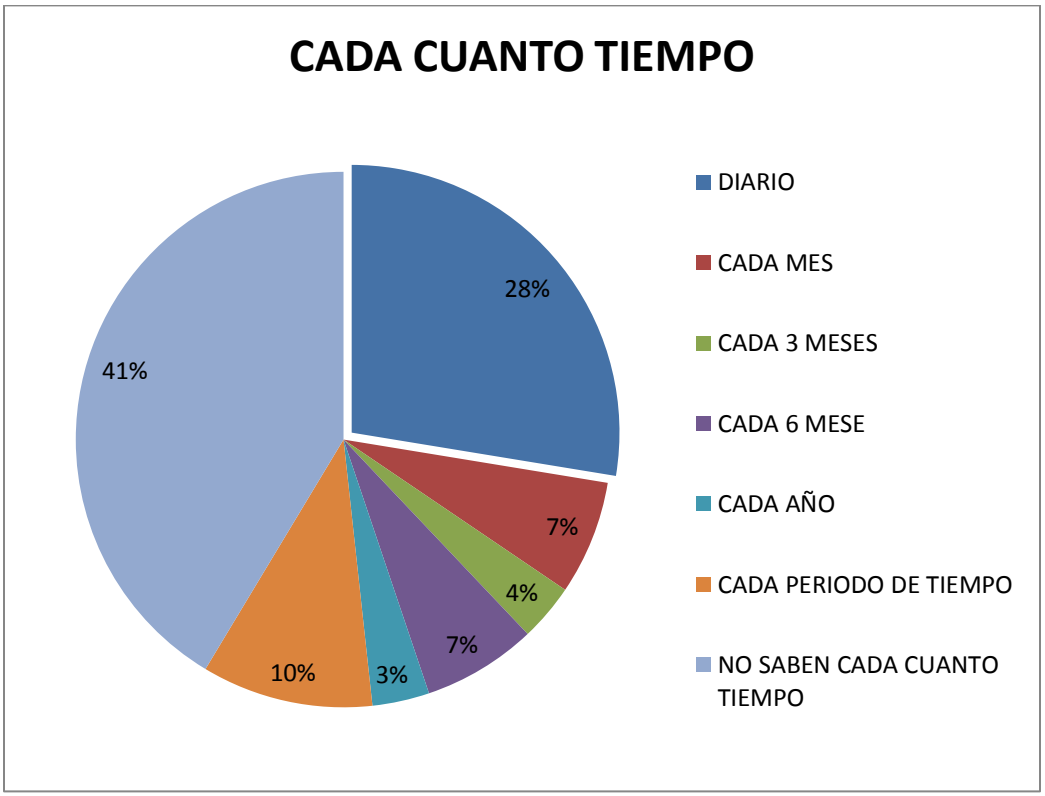


Figura 18. Resultado Pregunta 15 Cada cuanto tiempo

Análisis e Interpretación: De los 29 empleados que respondieron que si, 8 que representa el 28% respondieron que se realiza copias diario, 2 que representa el 7% respondieron que cada mes, 1 que representa el 4% respondió que cada tres meses, 2 que representa el 7% respondieron que cada 6 meses, 1 que representa al 3 % respondió que cada año, 3 que corresponden al 10% respondieron que cada periodo de tiempo, y 12 que representan al 41 % respondieron que no saben cada cuanto tiempo se realizan copias de seguridad de la información.

De los datos obtenidos en la aplicación de las encuestas revelan que los empleados no saben cada cuanto tiempo se realizan copias de seguridad de la información.

3.1.5 RIESGOS OBTENIDOS

Según los resultados obtenidos en las encuestas, y en las visitas se observa que el Unidad de Gestión Tecnológica del GAD San Pedro de Pelileo cuenta con políticas de seguridad básicas que no permiten el correcto aseguramiento de la información; razón por la cual es recomendable utilizar una normativa estricta y confiable que garantice la confidencialidad y seguridad de la información. Entre los riegos detectados se citan:

Los empleados de la institución desconocen las políticas de seguridad que tiene La Unidad de Gestión Tecnológica para la gestión de la información, por lo que son propensos a la manipulación inadecuada de la información personal e institucional, es por ello que se debería realizar periódicamente la socialización de las políticas vigentes.

Durante el registro de nuevos usuarios y cambios de contraseña, el sistema no requiere la utilización de caracteres especiales, letras y números; por este motivo el personal de la institución crea contraseñas simples, dando paso a que personal no autorizado y malintencionado pueda acceder a usuarios ajenos mediante ingeniería social y realizar cambios no deseados en el sistema.

Las instalaciones físicas no cuentan con las seguridades respectivas que brinden el aseguramiento de los recursos existentes en el Gobierno Autónomo Descentralizado San Pedro de Pelileo.

3.2 POLÍTICAS DE SEGURIDAD EXISTENTES DENTRO DE LA INSTITUCIÓN

3.2.1 Políticas de Seguridad

3.2.1.1 Unidad de Gestión Tecnológica

La Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado San Pedro de Pelileo cuenta con tres funcionarios encargados del correcto funcionamiento de servidores, manejo y gestión del sistema Cabildo y asistencia técnica a cada uno de los departamentos que componen a la institución.

La información que se recopila de las diferentes actividades que cumplen los funcionarios mediante el sistema cabildo es ingresada, modificada, almacenada para que pueda ser útil en los diferentes tramites que se realiza en esta institución.

3.2.1.2 Ubicación de la Unidad de Gestión Tecnológica

Se encuentra ubicado en la parte posterior de la municipalidad, el ingresos se lo puede realizar por la puerta que se encuentra ubicada en la Av. Eugenio espejo.

Figura 19. Ilustre Municipalidad San Pedro de Pelileo

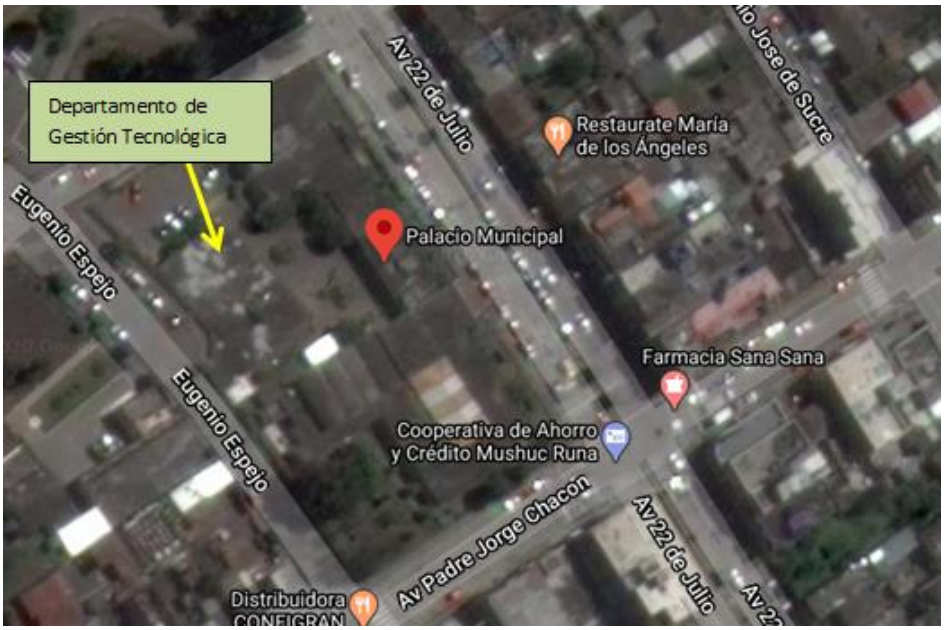


Figura 20. Imagen Satelital Google Earth de la Unidad de Gestión Tecnológica

Figura 21. Entrada Principal al Unidad de Gestión Tecnológica

Figura 22. Ingreso al Unidad de Gestión Tecnológica

La Unidad de Gestión Tecnológica está ubicada en el primer piso del Departamento Financiero, en área está expuesta a riesgos por terremotos, erupciones volcánicas, filtraciones de agua en épocas de invierno por lo que es necesario que la información que se almacena en los servidores en este departamento pueda ser respaldada en otro lugar fuera de la municipalidad o en servidores externos en caso de suceder cualquiera de estas eventualidades.

Figura 23. Unidad de Gestión Tecnológica

3.2.1.3 Cuarto de servidores

Los servidores de la institución se encuentran alojados en la parte trasera de la Unidad de Gestión Tecnológica, el área asignada para esta labor es muy reducida, cuenta con un ventilador, 3 rack en los cuales están alojados los routers, servidores y demás equipos tecnológicos de la institución.

El área donde están ubicados los servidores no cuenta con las medidas necesarias para su funcionamiento, las canaletas se encuentran deterioradas, el cableado y equipos está desorganizado varios de ellos sin sus respectivas identificaciones.

Las ventanas no cuentan con sus respectivas protecciones por consiguiente esto resulta un problema puesto que gente inescrupulosa podrían substraer los equipos por esta área.

Figura 24. Cuarto de servidores de la Unidad de Gestión Tecnológica

Figura 25. Ventilador en el cuarto de servidores de la Unidad de Gestión Tecnológica

3.2.1.4 Administradores del Sistema en la Unidad de Gestión Tecnológica

Los 3 funcionarios de la unidad atienden y solucionan cada uno de los problemas informáticos que se presentan dentro de la institución, ya sean en el sistema o en los recursos informáticos que no funcionan correctamente.

3.2.1.5 Restricciones de usuarios

Los funcionarios de los diferentes departamentos tienen restringido el acceso para instalación de programas innecesarios para el desempeño de sus actividades, y en caso de requerirlos el técnico de sistemas es quien ejecuta la instalación en el usuario de soporte mediante el ingreso de usuario y contraseña y una vez validado el acceso continúa con la instalación correspondiente.

A continuación se detalla el personal que no posee privilegios de administrador de equipos:

- Funcionarios de Administración de Activos
- Funcionarios de Administración de Justicia
- Funcionarios de Administración de Servicios Públicos
- Funcionarios de Agua Potable
- Funcionarios de Alcaldía
- Funcionarios de Asesoría Jurídica
- Funcionarios de La Moya
- Funcionarios del Camal Municipal
- Funcionarios del Departamento Administrativo
- Funcionarios del Departamento de Agua Potable y Alcantarillado
- Funcionarios del Departamento de Catastros y Avalúos
- Funcionarios del Departamento de Desarrollo de la Comunidad
- Funcionarios del Departamento de Obras Públicas

- Funcionarios del Departamento de Orden y Control
- Funcionarios del Departamento de Planificación y Desarrollo
- Funcionarios del Departamento Financiero
- Funcionarios del Registro de la Propiedad
- Funcionarios de Talento Humano
- Funcionarios de Tesorería

Únicamente los funcionarios de la Unidad de Gestión Tecnológica tienen acceso al usuario administrador para la instalación del software que permita el desarrollo de las actividades requeridas, encargados enunciados a continuación:

- Técnico de Servidores
- Técnico encargado del Sistema
- Jefe de Gestión Tecnológica

3.2.1.6 Gestión de Contraseñas.

No se cuenta con un manual para el manejo adecuado de contraseñas en el sistema y equipos que permitan a los funcionarios salvaguardar la información que operan.

Las contraseñas de los servidores públicos no son modificadas periódicamente ya que no poseen una guía que indique el tiempo de vida útil de las mismas, y lo hacen en el momento que cada servidor público lo crea conveniente y con contraseñas de su elección sin tomar en cuenta las restricciones necesarias.

3.2.1.7 Políticas, Normas y Estándares

Para determinar las normas, estándares y políticas de seguridad existentes en la municipalidad, se realizaron entrevistas, encuestas, visitas al personal responsable de la

Unidad de Gestión Tecnológica y en los demás departamentos de la institución, obteniendo la información siguiente:

3.2.1.8 Políticas de Seguridad

La Unidad de Gestión Tecnológica carece de un manual con políticas de seguridad en caso de inconvenientes con los recursos informáticos, es por ello que el técnico a cargo decide la solución óptima sobre el activo, por ejemplo cuando un equipo presenta un fallo el funcionario a cargo informa sobre el particular al técnico de la Unidad de Gestión Tecnológica, quien acude al lugar donde fue solicitado y verifica que tipo de problema posee el equipo y lo repara, de no existir solución el equipo es reemplazado, dado de baja en el inventario y almacenado en una bodega.

3.2.1.9 Problemas en el Sistema

Cuando existe un problema en el sistema y no puede ser solucionado, los técnicos encargados son notificados mediante una llamada telefónica, es decir que cuando en un departamento tienen algún inconveniente llaman a la Unidad de Gestión Tecnológica para que éste dé solución en el momento que se detecta el fallo, procediendo con la suspensión del sistema para que no exista pérdida de información, en caso de que no se haya guardado o modificado algún dato, este se almacena en una tabla de respaldo y mediante la búsqueda conjuntamente con el funcionario que realizo esta actividad es restablecido al sistema.

3.2.1.10 Problemas en los equipos

Los equipos con problemas correctivos son llevados a la Unidad de Gestión Tecnológica para su reparación mediante procesos conocidos por el técnico responsable.

Para la adquisición de nuevos equipos se verifican las características del mismo, las proformas de los proveedores y se comunica al Departamento Administrativo para que a través de Compras Públicas realice la adquisición de los equipos.

3.2.2 Gestión de Activos

3.2.2.1 Activos Institucionales

La Unidad de Gestión Tecnológica cuenta con un inventario de los equipos institucionales existentes cada uno con código asignado, descripción del activo, nombre del responsable y el departamento al cual pertenece.

En el inventario constan los equipos como laptops, impresoras, pc de escritorio, switch entre otros, mismos que se encuentran detallados a continuación:

EQUIPO	CARACTERÍSTICAS
Pc de Escritorio	Marca: Hp Cantidad: 171 Disco: 1 Gb disco Processor I7, i3, dual core, Pentium 4
Laptops	Marca: Hp, Sony, Toshiba Cantidad: 40 Disco: 1 Gb disco Processor: I7, i3, Core duo, Pentium 4
Switch	Marca: CISCO, HP Cantidad: 10 Numero de puertos: 24
Servidores	Cantidad: 9 Marca: HP, PROLIAN
Impresoras	Cantidad: 147

	Marca: Lexmark, Samsung, HP, Epson.
Copiadoras	Cantidad: 10 Marca: Brother, Hp, Lexmark, Ricoh, Xerox.
Plotter	Marca: HP Cantidad: 3
Proyector	Marca: Epson Cantidad: 10
UPS	Marca: APS Cantidad: 26
Router	Cantidad:8
Radios Comunicación	Marca: Kenwood Cantidad:1
Pizarra Digital	Marca: Sin marca y modelo Cantidad: 2
Escáner	Marca: Epson Cantidad: 18
Discos Duros Externos	Cantidad: 19 Capacidad 500GB Fabricante: Western, Toshiba
Monitor	Marca: LG, Samsung Cantidad: 24
Tarjetas Inalámbricas PCI	Cantidad: 15
Lector de Código de Barras	Cantidad : 1

Tabla 24. Equipos de la institución

Elaborada por el investigador

Además existe un inventario de los sistemas o software que son manejados en las diferentes áreas del GADM San Pedro de Pelileo registrados con su nombre y el departamento al que corresponden:

SISTEMA / SOFTWARE
SISTEMAS PAQUETES INFORMÁTICOS
SISTEMA DE CONTROL Y COBRO PARA EL PARQUEADERO DEL MERCADO REPÚBLICA DE ARGENTINA
SISTEMA CABILDO PRISHARD MÓDULO DE CONTABILIDAD, PRESUPUESTO, RRHH, ACTIVOS
SISTEMA CABILDO PRISHARD SISTEMA DE CÁLCULO, FACTURACIÓN, RECAUDACIÓN
SISTEMA DE TURNOS (TES)
SOFTWARE NAVEGACIÓN Y MONITOREO (GR)
SOFTWARE DE GIS DESKTOP SINGLE USE (FIALL)

Tabla 25. Sistema y software utilizado en el G.A.D.M San Pedro de Pelileo

Elaborada por el investigador

3.2.2. 3 Problemas en servidores

Uno de los recursos importantes con el que cuenta la unidad de Gestión Tecnología son los servidores, es por ello que cuando se detectan problemas en algún de ellos se sigue el siguiente procedimiento:

Paso 1. Rescatar la información necesaria (respaldos).

Paso 2. Realizar un análisis e identificar qué problemas puede tener.

Paso 3. Realizar un informe técnico del equipo y comunicar al Jefe inmediato para su conocimiento.

Cabe recalcar que el área donde se encuentran los servidores es reducida y no existen las adecuaciones necesarias correspondientes para su funcionamiento y mantenimiento.

3.2.2.4 Copias de seguridad

En cuanto a las copias de seguridad dentro de la municipalidad son llevadas a cabo de manera mensual, para ello el gestor de base de datos Oracle automáticamente saca respaldos a fin de que no se pierda la información.

Las copias de seguridad son almacenadas en los servidores que se encuentran en la unidad de Gestión Tecnológica instalados en el cuarto de servidores; sin embargo, es importante señalar que la institución no cuenta con servidores externos por lo que de suceder una eventualidad se perdería la información con la que se labora en la municipalidad.

3.2.2.5 Manejo de cuentas de usuarios

La Unidad de Gestión Tecnológica asigna dos usuarios en los equipos de la municipalidad, el administrador e invitado, en el usuario administrador se instalan los programas pertinentes, y en el usuario invitado es donde los funcionarios realizan las actividades diarias.

3.2.2.6 Registros de equipamiento de la institución

Activos fijos y bodega son los encargados del control de los bienes de la institución, recursos entregados mediante un Acta de Entrega/ Recepción, en la cual los funcionarios adquieren la responsabilidad de salvaguardar cada uno de los activos dotados.
La Unidad de Sistemas maneja el inventario de equipos como CPUs, pantallas, laptops, impresoras, servidores, entre otros. En el inventario se registra el código, nombre del responsable del equipo, departamento al que pertenece y una descripción del equipo.

Figura 26. Codificación de equipos del G.A.D. San Pedro Pelileo

3.2.2.7 Almacenamiento de contraseñas

Los funcionarios son quienes deciden la forma adecuada de la gestión de sus contraseñas y lo hacen en agendas o blocks de notas; en este caso Gestión Tecnológica únicamente sugiere que las contraseñas no sean guardadas en lugares que se encuentren a la vista de cualquier persona ya que podrían ser blancos fáciles para que alguien malintencionado haga mal uso de esta información reservada, por lo que no es recomendable el almacenamiento de contraseñas en archivos digitales que estén almacenados en el ordenador o en unidades USB y discos externos.

Las contraseñas de los servidores son responsabilidad del jefe de la Unidad de Gestión Tecnológica conjuntamente con el técnico de servidores y técnico de redes quienes son el personal encargado del correcto funcionamiento de estos equipos.

3.2.2.8 Uso y manejo de recursos informáticos

Los equipos informáticos como pc´s, laptops pantallas, teclados, mouses a consecuencia del manejo inadecuado, por el tiempo o por factores externos dejan de funcionar correctamente. El responsable del recurso da a conocer del fallo y según los resultados de la evaluación por

parte de un técnico de la Unidad de Gestión Tecnológica es reemplazado por otro o a su reparado.

.

Cuando un equipo va a ser desechado, se realiza un informe técnico donde se indica que el mismo no tiene reparo por lo que es enviado a bodega para su registro y almacenamiento.

Figura 27. Recursos informáticos que han sido dados de baja en el G.A.D. San Pedro de Pelileo

Cada empleado tiene asignada una estación de trabajo con recursos y usuarios personales que no pueden ser compartidos, ya que en caso de ocurrir problemas en el sistema o pérdida de equipos la responsabilidad o acción efectuada recae sobre la persona a cargo tanto de los insumos como del usuario del sistema.

3.2.3 Seguridad del Personal

3.2.3.1 Confidencialidad en el manejo de información

La información manejada en los diferentes departamentos de la municipalidad es reservada y confidencial no puede ser divulgada. Para manejo de información entre departamentos se utiliza el correo institucional generado para cada funcionario a fin de evitar el uso de unidades de almacenamiento externas.

3.2.3.2 Cumplimiento de reglamentos y actividades de funcionarios

Dentro de la institución los funcionarios cumplen con los reglamentos establecidos en la municipalidad, de acuerdo al perfil de cada empleado tienen asignadas actividades a las cuales debe dar cumplimiento para justificar su jornada laboral.

Los jefes departamentales crean una matriz de actividades al inicio de la semana en la cual fija actividades a todos quienes están a su cargo, al finalizar la semana verifica el porcentaje de avance de cada actividad y si esta ha sido concluida en su totalidad, indica que concluyó caso contrario, el estado es asignado como pendiente.

Los funcionarios tienen bloqueado el acceso a redes sociales y a páginas que puedan interferir en sus labores, el uso del internet es solo para cumplir con las actividades referentes a las labores que realizan.

3.2.3.3 Utilización de correo institucional

Los servidores tienen un correo institucional el cual es utilizado para asignación de actividades, consultas entre los diferentes departamentos, videoconferencias, envío y recepción de documentación en el ámbito laboral

3.2.3.4 Restricciones de acceso a personal

El acceso a la Unidad de Gestión Tecnológica no se encuentra restringido, cualquier persona o funcionario puede ingresar para solicitar información (reportes), asistencia técnica, capacitaciones para el manejo del sistema u otros requerimientos.

3.2.3.5 Recursos compartidos

Dentro de la municipalidad no se comparte recursos como computadoras, correos institucionales entre otros, a cada funcionario se le asigna su equipo y cuenta de correo desempeño de sus actividades, existen recursos que si son compartidos en las oficinas como: impresoras, líneas telefónicas, suministros de oficina etc.

3.2.3.6 Uso de firmas electrónicas

El uso de firma electrónicas facilita el trabajo al momento de realizar compras públicas, y demás trámites pertinentes, evitando en ocasiones que las dos partes estén presentes para realizar las gestiones pertinentes que beneficien a la institución, los contratos de firmas electrónicas tienen una validez de dos años.

En la municipalidad se implementó la utilización de la firma electrónica a raíz de la aparición de la pandemia, dejando de ser necesaria la manipulación de bolígrafos para la rúbrica de los jefes departamentales quienes en su gran mayoría utilizan la firma electrónica para varios trámites.

3.2.3.7 Seguridad para soporte de la información

En la municipalidad existen cámaras de seguridad en algunas áreas, y el respectivo personal de seguridad, pero en la Unidad de Gestión de la Tecnológica no existen cámaras dentro que brinden la seguridad oportuna a los recursos existentes como son equipos, servidores, en los cuales esta soportada toda la información.

3.2.3.8 Incidencias

En la municipalidad a diario existen pequeñas incidencias con los equipos, mismas son reportadas, a la unidad de sistemas para que sean solucionadas oportunamente, en ocasiones existe inconvenientes con los servidores por lo que el sistema que se utiliza por los demás

departamentos de la institución en esos momentos es dado de baja, para la oportuna solución pero no se maneja un documento en el cual exista la gestión de dichas incidencias.

3.2.4 Seguridad Física

3.2.4.1 Almacenamiento de información

La información manejada en la municipalidad se refleja en el sistema cabildo dependiendo del área de trabajo y se encuentra almacenada en los servidores ubicados en el data center, mientras que la información de los trámites es alojada en los equipos de cómputo que posee cada empleado a su cargo.

3.2.4.2 Acceso al data center

En la unidad de Gestión Tecnológica de la municipalidad tienen acceso al data center solamente el personal de esta unidad pero por encontrarse junto a las oficinas en ocasiones funcionarios de otros departamentos han ingresado a esta área sin la respectiva autorización, pero no se ha suscitado ningún inconveniente hasta el momento además no existen las seguridades correspondientes en esta área por el lugar donde se encuentra ubicado.

3.2.4.3 Instalaciones físicas en la Unidad de Gestión Tecnológica

Existen cuarteos en el techo del edificio en el que se encuentran las oficinas de Gestión Tecnológica, generando preocupación en los técnicos de esta área; es por ello que, constantemente se verifica que no existan filtraciones de agua en esta sección para evitar daños en los equipos informáticos ahí alojados.
El mantenimiento correctivo y preventivo de los equipos se lo realiza en el área de ingreso a la unidad.

3.2.4.4 Factores ambientales

En cada departamento de la municipalidad existe un extintor, en el cuarto de servidores existe un detector de humo el cual se activa en caso de incendios para que se tomen las medidas necesarias para la evacuación.

Las instalaciones de la Unidad de Gestión Tecnológica son de hormigón armado con la división de aluminio señalada, cuentan con un medidor de temperatura y un ventilador para evitar la concentración de calor.
Al momento de generarse una sobrecarga de energía, los UPS podrían proteger a los equipos de cómputo, por lo que es necesario que los equipos de la institución posean UPS que garanticen la seguridad de los equipos y eviten averías y pérdida de información.

3.2.4.5 Uso de UPS

Algunos equipos de cómputo existentes en la municipalidad tienen a su disposición un UPS para que en caso de suceder una eventualidad (apagón) la información pueda ser salvaguardada oportunamente en un lapso de 10 minutos.

En la data center existen UPS que permiten que los equipos permanezcan funcionando por el lapso de una hora, es así que cuando se registra un corte de energía eléctrica o variaciones de voltajes se evita la pérdida de la información que se maneja en el sistema.
Los equipos que no cuentan con los respectivos UPS cuando existe un corte de energía eléctrica pierden la información con la que se haya estado trabajando por lo que tienen retomar nuevamente el trabajo que no se guardó.

3.2.4.6 Desastres naturales

La municipalidad está expuesta a catástrofes naturales como erupciones volcánicas, terremotos, incendios, entre otros; sin embargo, no se han realizado capacitaciones a nivel municipal en caso de ocurrir alguna de estas eventualidades, es por ello que inclusive la Unidad de Gestión Tecnológica desconoce cómo salvaguardar la información existente, por

lo que es necesario impartir normativas para sobrellevar estos sucesos y reducir el riesgo latente de perder información de gran importancia para la institución.

3.2.4.7 Utilización de antivirus en la Municipalidad

La institución utiliza el antivirus Kaspersky como una de las medidas de seguridad de los equipos, el mismo que es instalado en un servidor en el cual se encuentra centralizado todos los procesos, para su distribución a cada pc cliente de las actualizaciones de las bases de virus.

El técnico de redes es el encargado de revisar cada seis meses todos los equipos de la municipalidad.

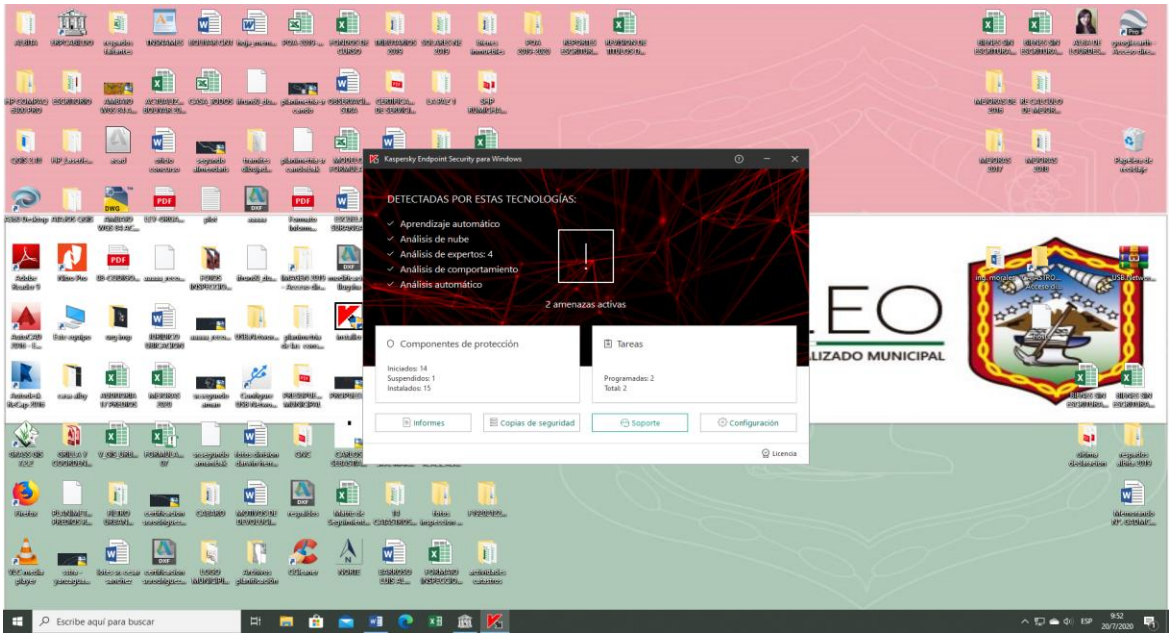


Figura 28. Antivirus utilizado en el G.A.D. San Pedro de Pelileo

3.2.4.8 Señalética

En la municipalidad existen señaléticas de peligro, prohibiciones, números de emergencias, señales para respetar el distanciamiento social y normas de bioseguridad, sin embargo, en la Unidad de Gestión Tecnológica se evidencia una sola puerta de ingreso que también es utilizada como salida de emergencia.

Figura 29. Señalética existente en G.A.D.M San Pedro de Pelileo

3.2.4.9 Equipos de seguridad dentro de la municipalidad

Las cámaras de seguridad son un recurso de gran importancia dentro de la institución para obtener información en caso de robos o manejo inadecuado de un recurso por parte de personal no autorizado. En la Unidad de Gestión Tecnológica no existen cámaras de seguridad interiores, por lo tanto de suceder algún hecho no se podría verificar lo ocurrido.

3.2.4.10 Instalaciones eléctricas

Las instalaciones eléctricas se revisan constantemente para que no existan daños en el cableado, en caso de ocurrir algún desperfecto por este motivo y al darse un corte de energía, son los UPS los que abastecen de energía a los equipos por un lapso de tiempo para que se salvaguarde la información, pero hay una gran cantidad de equipos que no cuentan con UPS por lo que podría existir pérdida de información cuando se dé un apagón.

3.2.4.11 Ingreso y salida del personal

El ingreso y salida a la municipalidad se lo hace por la puerta principal ubicada en la avenida 22 de Julio y la secundaria que da a la calle Calle Celiano Monge.
El personal municipal debe registrar los ingresos y salidas (total 4) a la institución usando un lector de huella del iris del ojo, o la huella digital instalado en el hall del establecimiento. Por la situación de emergencia sanitaria en la que nos encontramos se ha visto la necesidad de implementar un lector adicional al igual que se permite registrar la asistencia manual en hojas de seguimiento con la finalidad de evitar las aglomeraciones del personal.

Las medidas preventivas adoptadas por la municipalidad son el control del uso obligatorio de mascarillas, la toma de temperatura y la respectiva desinfección para evitar la propagación de la pandemia.

3.2.5 Accesos en la municipalidad

3.2.5.1 Número de conexiones Fallidas

En la municipalidad el número máximo de conexiones fallidas que se puede realizar en los servidores es tres, el personal de la Unidad de Gestión Tecnológica son los únicos que tiene acceso a estos recursos por este motivo hasta la fecha no se registra ingresos incorrectos de ninguna manera.

3.2.5.2 Sistema ERP Cabildo

La mayoría de los departamentos municipales (Agua Potable y Alcantarillado, Avalúos y Catastros, Planificación y Desarrollo, Financiero, entre otros) manejan el Sistema ERP Cabildo, para emisión de claves catastrales, ingresos y actualizaciones prediales, emisiones y cobros.

Para el ingreso al sistema se debe realizar la correcta autentificación de las credenciales pero el sistema no cuenta con un bloque cuando se autentican varias veces incorrectamente la contraseña del usuario.

La información con la que se trabaja es reservada y esta almacenada en la base de datos, de la cual se puede extraer reportes en función de las necesidades existentes; no obstante, es imprescindible solicitar a la Unidad de Gestión Tecnológica la obtención de reportes de mayor dificultad y que no se encuentran habilitados en el sistema.

Figura 30. Sistema utilizado dentro del G.A.D. San Pedro de Pelileo

3.2.5.3 Manejo de red

La institución utiliza red LAN para la conexión interna de los equipos informáticos, es por ello que la mayoría de departamentos cuentan con los respectivos switch o routers. Los departamentos y oficinas en los que se encuentran equipos de red son:

- Administración de Justicia
- Administración de Servicios Públicos
- La Moya
- Camal Municipal
- Departamento de Catastros y Avalúos
- Departamento de Desarrollo de la Comunidad
- Departamento de Planificación y Desarrollo
- Registro de la Propiedad
- Gestión Tecnológica
- Agua Potable y Alcantarillado
- Registro de la Propiedad
- Biblioteca

En el data center existe el diagrama de red de los puntos de conexiones de la municipalidad que se detalla a continuación:

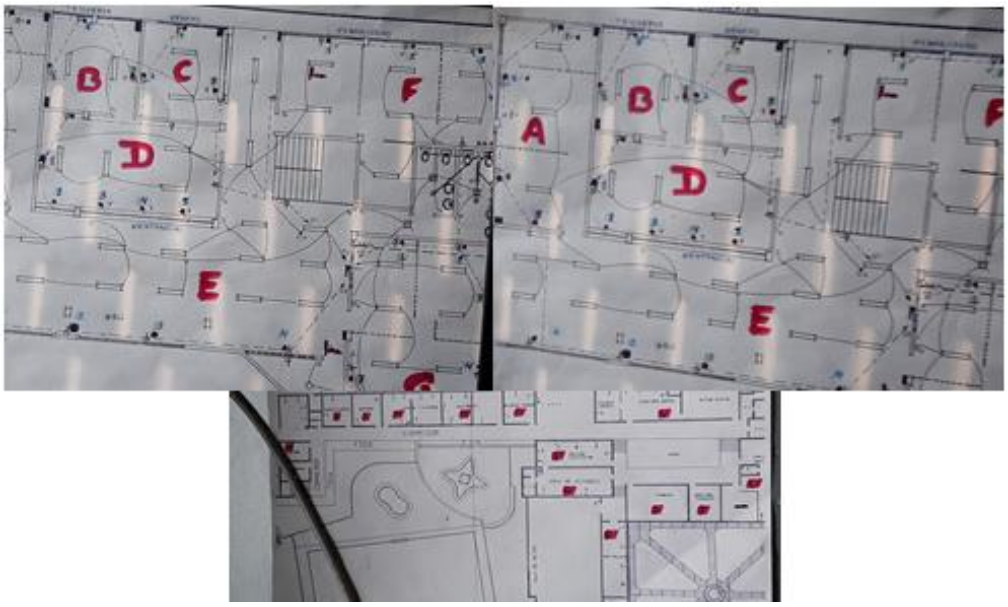


Figura 31. Diagrama de Red del G.A.D. San Pedro de Pelileo

3.2.5.4 Manejo de cableado

Desde los routers o switch se reparte la conexión a los equipos mediante el cable UTP y el sistema de cableado estructurado que se utiliza dentro de la institución es con el estándar ANSI EIA/TIA-568-B; las instalaciones están cubiertas por canaletas hasta llegar de forma segura a los puertos desde los cuales se distribuyen a cada ordenador.

Figura 32. Diagrama de Red del G.A.D. San Pedro de Pelileo

3.2.5.5 Información manejada en el sistema

La información que se maneja dentro del sistema del gobierno municipal está almacenada en la base de datos, y la habilitación de la misma depende del departamento y cargo de cada empleado, es decir que existen restricciones para que cada uno tenga acceso a las opciones necesarias conforme las actividades designadas en su perfil al momento de ser contratados, activación que será efectuada por la Unidad de Gestión Tecnológica mediante un requerimiento formal por parte de los directores departamentales.

3.2.5.6 Aplicaciones informáticas

Los equipos que son utilizados por los funcionarios de la municipalidad tienen instaladas todas las aplicaciones necesarias para el cumplimiento oportuno de sus actividades, en caso de requerir la instalación de alguna aplicación extra, los empleados comunicarán a la Unidad de Gestión Tecnológica su necesidad e inmediatamente los técnicos del área darán solución a la petición, además lo funcionarios municipales no tienen el acceso para realizar ninguna instalación en los equipos.

3.3 ESTRATEGIA DE SOLUCIÓN DE TOMANDO A CONSIDERACIÓN LA NORMATIVA ISO/IEC 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO

Después de haber realizado un análisis riguroso de las vulnerabilidades y riesgos existentes dentro del Gobierno Autónomo Descentralizado Municipal de San Pedro de Pelileo al aplicar el estándar ISO/EC 27001 se ha podido determinar que no se cumplen con las respectivas normativas de seguridad en determinadas áreas, por ende es necesaria la implementación de políticas de seguridad que ayuden en la gestión adecuada de la información que se maneja dentro de la municipalidad, es necesario que estos estándares sean aprobados y puestos en marcha por la Unidad de Gestión Tecnológica.

Existe un sinnúmero de vulnerabilidades al manejar información por lo que es necesaria la utilización de políticas que permitan mitigar los riesgos, esto se conseguirá siempre los funcionarios cumplan con lo establecido y se dé la revisión constante de la Unidad de Gestión Tecnológica.

Hoy en día la seguridad a nivel institucional y empresarial es un punto extremadamente importante que se debe tener en consideración, con el auge de las nuevas tecnologías cada vez es más indispensable el uso adecuado de los recursos institucionales, evitando así la filtración o pérdida de información, es por ello que se requiere una guía con sugerencias para el uso adecuado de los recursos en la municipalidad. En su gran mayoría las organizaciones cuentan con políticas que ayudan en el aseguramiento de los recursos, pero no todas tienen éxito en su aplicación, la mayor parte ellas fracasan por las malas prácticas por parte del personal o por desconocimiento de las normativas existentes, razón por la cual es importante la socialización de todas las medidas a seguir.

La Unidad de Gestión Tecnológica es la encargada de velar por la protección de los recursos informáticos, así como también de la adquisición de equipamientos necesarios para cada departamento a través de una estrategia definida que evite la pérdida de los recursos informáticos y económicos.
Varias instituciones han sido expuestas por no tener clara la temática a seguir, ocasionando grandes problemas a nivel de seguridad donde se compromete información relevante, por ello el personal debe tener pleno conocimiento de la importancia que conlleva el seguir las medidas de cuestiones de seguridad y lo que se debe hacer en caso de suscitar eventualidades.

3.3.1 Objetivos

- Elaborar políticas de seguridad que permitan la mitigación de riesgos existentes y resguardo de información en la Unidad de Gestión Tecnológica del Gobierno Autónomo Descentralizado Municipal de San Pedro de Pelileo.

- Mejorar el ambiente laboral de los funcionarios de la municipalidad.
- Aumentar la confiabilidad de los recursos institucionales.

3.3.2 DIAGRAMA ORGANIZACIONAL DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO SAN PEDRO DE PELILEO

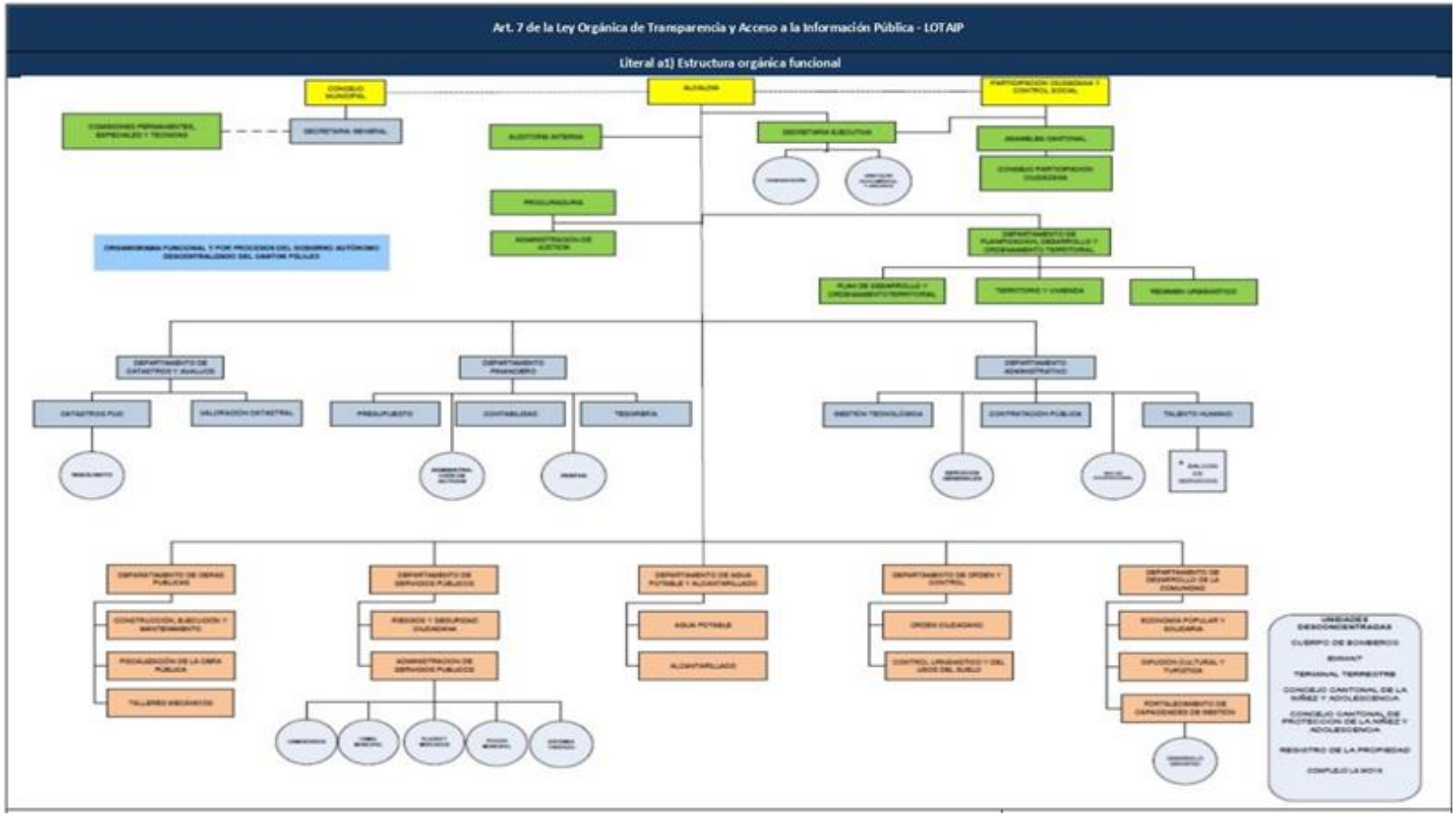


Figura 33. Organigrama institucional

Tomado desde https://pelileo.gob.ec

Misión

"Mejorar la calidad de vida de los habitantes del Cantón Pelileo, con una cuidadosa planificación, regulación y entrega de servicios e infraestructura pública".

Visión

"Ser un gobierno participativo, ejemplo de trabajo e integridad, generador de oportunidades, y garante de derechos de los ciudadanos, del medio ambiente y del patrimonio cantonal".

3.3.3 Establecimiento de Políticas en el Gobierno Autónomo Descentralizado Municipal de San Pedro de Pelileo.

Con la creación de este documento se busca contribuir en la estandarización de controles, medidas, procedimientos y normas de seguridad de la información en cada uno de los departamentos que conforman la municipalidad.

3.3.3.1 Control de Acceso a la Información

- **Objetivo:** Minimizar los riesgos por pérdida o mal uso de información por el personal no autorizado al uso o manipulación de este recurso.

3.3.3.2 Responsabilidad del jefe de la unidad

El jefe de la unidad es el responsable de informar, evaluar, establecer y promover mediante circulares, socializaciones, capacitaciones, correos institucionales, sitios web o por otros medios cada uno de los procedimientos de seguridad existentes. Además es quien asigna responsabilidades al técnico de seguridad informática para que oportunamente realice las

revisiones correspondientes, a fin de comprobar que se esté dando fiel cumplimiento de las políticas establecidas.

3.3.3.3 Privilegios asignados a usuarios

Es importante que los usuarios tanto del sistema informático, como de la red de la municipalidad tengan asignados identificadores y contraseñas de uso personal.

A los funcionarios municipales que tienen acceso al sistema Cabildo, se les otorgarán los permisos únicamente para la ejecución de funciones conforme el cargo desempeñado.

El personal de la municipalidad es responsable de las acciones que se hayan desarrollado dentro de cada usuario.

Los funcionarios debe respetar el uso adecuado de su usuario, por ningún motivo debe utilizar la cuenta de otro empleado, así fuere el caso que éste lo hubiera autorizado.

Los funcionarios municipales están en la obligación de informar al jefe departamental, cualquier suceso que se haya detectado e interfiera con la confiabilidad de los datos con los que se encuentre trabajando, éste a su vez debe comunicar a la Unidad de Gestión Tecnológica, para que realice las respectivas verificaciones y se dé solución al problema generado.

Los usuarios deben proteger la información manejada con el fin de evitar inconvenientes que pueden ocasionar pérdida de datos o modificaciones no deseadas.

3.3.3.4 Asignación de cuentas

En el momento que a los funcionarios municipales se les asigna una cuenta de usuario deben firmar un documento en el que indique que conocen las políticas de seguridad y se hacen responsables del manejo que se dé.

Para solicitar la asignación de una cuenta o modificación del cargo se debe hacer la petición por escrito a la Unidad de Gestión Tecnológica misma que aprobará el requerimiento.

No se debe crear usuarios para personal que no pertenezca a la municipalidad salvo el caso que cuenten con la autorización debidamente aprobada por la Unidad de Gestión Tecnológica.

Se debe llevar un estricto control de los privilegios de usuario de los funcionarios municipales para que no puedan acceder a modificaciones o eliminaciones personales si no están autorizados a realizar estas actividades.

Se restringe la creación de usuarios que no especifiquen claramente quien es el responsable para evitar el mal uso de estos recursos.

Las cuentas de usuarios que no se estén siendo utilizadas por un lapso de cinco minutos, deben ser suspendidas automáticamente en el sistema.

Cuando los funcionarios municipales cesen de sus funciones, se debe informar a la Unidad de Gestión Tecnológica para que el técnico encargado suspenda la cuenta de inmediato.

3.3.3.5 Manejo de contraseñas

Las contraseñas de servidores deben ser almacenadas en un gestor de contraseñas por contener información delicada.
Los funcionarios municipales por ningún deben almacenar contraseñas en ningún tipo de archivo que sea guardado en USB u ordenadores, además no deben ser escritas en papeles que se hallen a la vista de terceros.

Se debe restringir el uso de contraseñas antiguas y evitar la utilización de contraseñas similares a las que ya hayan sido manejadas.

Cuando se crea el usuario respectivo, la contraseña para el primer ingreso será asignada por el técnico creador y luego de ello deberá ser modificada por la que el usuario crea conveniente respetando las sugerencias para la generación de la misma.

Los equipos como routers y switches, traen una contraseña por defecto; por consiguiente, serán modificados cuando se activen para su uso respectivo.

El número de intentos máximos consecutivos para el ingreso al sistema introduciendo una contraseña incorrecta es tres, y el usuario queda bloqueado.

Es indispensable que un equipo o cuenta que no sea utilizada consecutivamente por un periodo de 5 minutos cierre la sesión automáticamente, para su restablecimiento debe autentificarse correctamente.

En caso de existir inconvenientes en el sistema, el mismo rechazará el ingreso de usuarios hasta que se realicen las correcciones correspondientes.

No se permitirá a los funcionarios la vulneración del sistema, y de ocurrir, esta se considerará como infracción leve o grave dependiendo de la contravención.
Es necesario que la longitud mínima de una contraseña sea de 8 caracteres, mismos que debe contener alternadamente la combinación entre números, letras mayúsculas, minúsculas y caracteres especiales.

En los servidores se recomienda la utilización de contraseñas largas y robustas, con una longitud mínima de 12 caracteres, siempre utilizando las combinaciones de caracteres numéricos y alfanuméricos.

Por ningún motivo se debe revelar el usuario y contraseña personal o permitir que se encuentre a la vista o alcance terceros.

Si por algún motivo los funcionarios municipales sospechan que sus credenciales de ingreso están siendo utilizadas por alguien, se debe realizar el cambio correspondiente y dar aviso al encargado de la Unidad de Gestión Tecnológica.

Las contraseñas no deben contener datos como nombre, fechas de nacimiento, números telefónicos, celulares o algún dato que pueda ser fácil de investigar.

En la implementación de contraseñas en lo posible se recomienda usar la menor cantidad de datos personales y guardarla en un lugar seguro.

Cuando un funcionario municipal pierda el acceso al equipo o sistema asignado deberá notificar a la Unidad de Gestión Tecnológica para restablecimiento correspondiente.

Los funcionarios municipales por ningún motivo deben utilizar misma contraseña de las cuentas personales para el manejo de equipos o sistemas dentro de la municipalidad.

3.3.3.5 Acceso a la información

Es necesario que la información sea protegida, para ello es recomendable que se utilicen algoritmos de cifrado para que personal no autorizado carezca de acceso a datos reservados.

La información que es compartida mediante la red, debe estar protegida para contrarrestar el uso inadecuado de dicho recurso.

El uso de dispositivos móviles no debe interferir en el desempeño laboral de cada uno de los funcionarios, tampoco se podrá acceder a la red sin la autorización de la Unidad correspondiente, salvo que se realicen las justificaciones pertinentes.

El manejo de información es delicado, es por ello que cuando se aplique la modalidad de teletrabajo, los entregables deberán ser remitidos a los jefes departamentales y ellos a su

vez son los responsables de presentar los reportes de trabajo al departamento de recursos humanos.

Se debe realizar monitoreos contantes en la red de la municipalidad para encontrar vulnerabilidades que puedan provocar la fuga de información.

3.3.3.6 Uso del sistema de gestión documental, correo institucional y sistemas municipales.

Los funcionarios municipales están en la obligación de brindar la seguridad en el manejo de cuentas institucionales que estén a su cargo.

Los empleados de la municipalidad deben ser cautelosos con la gestión de cuentas institucionales, sistema de gestión documental y sistemas municipales porque son los responsables de cualquier manejo inadecuado que se dé dentro de ellos.

Los funcionarios que no den el correcto uso a los sistemas existentes en la municipalidad deben ser sancionados siguiendo el procedimiento respectivo.

3.3.3.7 Gestión de privilegios en equipos

La Unidad de Gestión Tecnológica debe establecer usuarios en cada uno de los equipos asignados al personal municipal, permitiendo única y exclusivamente el uso de los recursos que son necesarios para el desempeño de sus funciones.

Por ningún motivo los empleados municipales que no pertenezcan al área de Gestión Tecnológica podrán tener acceso al usuario administrador.

Los empleados municipales que requieran la instalación de aplicaciones extras deberán solicitar a la Unidad de Gestión Tecnología la ejecución de dicha acción.

3.3.3.8 Restricciones a personal externo

Al personal que no trabaje en la municipalidad se restringe el uso de equipos informáticos y sistemas de carácter institucional.

3.3.3.9 Uso del internet

Los servidores municipales no están autorizados a utilizar internet para actividades que no estén acorde con sus funciones.
Los empleados de la municipalidad que justifiquen el uso de internet podrán tener acceso al mismo, pero se les restringe el acceso a redes sociales o plataformas de entretenimiento que puedan interferir en el desempeño laboral. El requerimiento será mediante un informe detallado de las tareas para las cuales es indispensable su uso, el mismo que ira dirigido al jefe de la Unidad de Gestión Tecnológica para su aprobación o negación luego de la evaluación correspondiente.

Realizar charlas para incentivar a los funcionarios municipales a la concientización del uso inadecuado del recurso de internet y los peligros que conlleva la navegación por páginas de dudosa procedencia.

Incentivar a los funcionarios municipales al no uso de la red para compartir información delicada con el propósito de mitigar las fugas de información.

Para la recepción o envío de información laboral los funcionaros municipales deben hacer uso de las cuentas institucionales.

3.3.4 GESTIÓN DE ACTIVOS

- **Objetivo**: Afianzar la seguridad dentro de la Municipalidad para mitigar los riesgos que pueden ser ocasionados de manera voluntaria o involuntaria en los equipos

informáticos y que atentan con el desenvolvimiento de las labores de los funcionarios municipales.

Los funcionarios municipales no están autorizados para almacenar información que no sea de carácter laboral, como archivos de videos, música ente otros.
Los funcionarios municipales no están autorizados para la instalación de programas de dudosa procedencia puesto que pueden contener virus informáticos que a la larga puedan causar daños a los equipos y a la red municipal.

La Unidad de Gestión Tecnológica es la única que realiza el escaneo y monitoreo de red para detectar puertos en los cuales existan vulnerabilidades, salvo el caso que se asigne los permisos correspondientes a terceros y puedan realizar esta actividad.
Los técnicos de la Unidad de Gestión Tecnológica deben realizar revisiones periódicas cada seis meses para verificar el correcto uso de los recursos de la institución.

Impedir que existan monitoreos a nivel de red por personal externo que pretenda captar cualquier tipo información de la municipalidad.

No enviar información reservada de la municipalidad desde cuentas de otros funcionarios.

Se restringe el uso de líneas telefónicas o recursos institucionales para acciones de carácter personal.

3.3.4.1 Responsabilidades en equipos y bienes

Hay que instituir convenios en los cuales el personal se comprometa a utilizar los recursos institucionales solo en favor de la municipalidad.

Los funcionarios municipales son los responsables de los equipos asignados, por lo que deben llevar un control de los mismos para que al momento de la devolución no tengan inconvenientes.

3.3.4.2 Etiquetado e inventario de activos

Todos los bienes físicos de la institución deben ser previamente etiquetados e ingresados a un inventario que será actualizado constantemente a fin de llevar un control ordenado de los activos institucionales, y de facilitar el seguimiento del estado de conservación de los mismos.

3.3.5 Responsabilidades del Personal

- **Objetivo:** Evitar la manipulación inadecuada de recursos institucionales con la aplicación de técnicas para los usos adecuado de los mismos.

Los funcionarios que ingresen a trabajar en la municipalidad tienen que recibir la capacitación respectiva para el manejo correcto de recursos y cumplimiento de tareas asignadas.

Es indispensable que en el contrato de trabajo se especifique el acuerdo para que no exista la divulgación de información confidencial de la institución.

Los funcionarios municipales están en la obligación de dar a conocer cualquier problema que se les manifieste en el ambiente laboral.

El técnico de seguridad deberá monitorear cada tres meses los usuarios de los funcionarios municipales.

Los empleados de la Unidad de Gestión Tecnológica están en la obligación de dar solución a los problemas de seguridad o funcionamiento de los equipos institucionales así como de salvaguardar la información con la que toda la municipalidad trabaja.

Instaurar normas que permitan salvaguardar la información en caso de existir desastres naturales como erupciones volcánicas, terremotos, incendios, entre otros.

Salvaguardar la información de equipos en casos de reemplazos o asignaciones temporales de cargos.

Cuando un funcionario municipal cese de sus funciones deberá hacer la entrega de los bienes a él confiados para el cumplimiento de sus actividades.
En caso de que un bien se haya extraviado es obligación del funcionario reportar la pérdida del mismo para que se tomen las medidas correspondientes.

3.3.5.1 Acceso del personal a la Unidad de Gestión Tecnológica y servidores

Se debe llevar un registro de ingreso del personal que no sea parte de la unidad.

Restringir el acceso de personal no autorizado al área de servidores para evitar daños o pérdidas en los equipos.

El personal de sistemas es el único autorizado al ingreso en el cuarto de servidores para validar el buen funcionamiento de los mismos; no obstante, en caso de requerir personal externo este deberá ser acreditado por el jefe de la unidad.

Es indispensable que el cuarto de servidores cuente con las seguridades de ingreso pertinentes.

3.3.4.2 Informes de debilidades a nivel de seguridad

Los funcionarios municipales deben informar oportunamente los problemas relacionados con la seguridad de los equipos y la periodicidad de la ocurrencia para que el departamento técnico siga las medidas necesarias.

Los funcionarios municipales deben conocer el procedimiento a seguir en caso de incidentes en los recursos, para que estos sean dados a conocer al departamento técnico.

Los técnicos de la Unidad de Gestión Tecnológica deberán notificar al jefe inmediato la existencia de vulnerabilidades en el sistema.

Los funcionarios municipales deben saber que en caso de encontrar una vulnerabilidad y tratar de utilizarla para su beneficio están cometiendo una infracción por manejo inadecuado de los recursos institucionales.
El ordenador que presente un desperfecto durante el trabajo dejará de ser utilizado y de ser necesario será trasladado a la unidad respectiva para su reparación.

La Unidad de Gestión Tecnología es la responsable de instalar y desinstalar programas necesarios para las labores del personal.

3.3.4.3 Normas de confidencialidad

Los funcionarios municipales por ningún motivo deberán divulgar información reservada de la institución ni revelar sus credenciales de usuario.

3.3.4.4 Administración de recursos informáticos dentro de la municipalidad.

La Unidad de Gestión Tecnológica es la encargada de velar por el correcto funcionamiento de los recursos informáticos y del mantenimiento oportuno del hardware y software.

Ejecutar controles periódicos que permitan evaluar el nivel del servicio brindado por parte del personal de la Unidad de Gestión Tecnológica dentro de la municipalidad.

Actualizar oportunamente el inventario de los recursos informáticos que forman parte de los activos institucionales.

3.3.4.5 Asignación de recursos y actividades

La Unidad de Gestión Tecnológica será la encargada de solicitar los recursos informáticos necesarios en las dependencias municipales para su posterior asignación.

Los técnicos de la unidad serán los encargados de brindar capacitaciones sobre cualquier tipo de modificaciones que se lleven a cabo en el sistema sin que sea requerido.

El Jefe de la Unidad de Gestión Tecnológica es el encargado de realizar la capacitación respectiva del manejo del sistema y de los recursos asignados al personal.

Los funcionarios municipales que fueran víctimas de manipulaciones inadecuadas en los equipos o en el sistema deben comunicar el incidente a la Unidad de Gestión Tecnológica para que tomen las medidas pertinentes.

3.3.6 Restricciones de Instalación

- **Objetivo:** Garantizar el adecuado funcionamiento de los recursos informáticos y la confidencialidad de la información en la municipalidad.

Las aplicaciones instaladas en los equipos informáticos que son entregadas a los funcionarios municipales para su uso, son puestas en funcionamiento por los técnicos de la Unidad de Gestión Tecnológica de acuerdo a los requerimientos del personal.

3.3.6.1 Instalación de protección antivirus

Todos los ordenadores y servidores de la municipalidad deberán contar con una protección antivirus con sus actualizaciones y configuraciones correspondientes.

Siempre que se instale software en los equipos se deberá verificar su procedencia para evitar riesgos a nivel de seguridad.

La Unidad de Gestión Tecnológica deberá dar solución inmediata a problemas relacionados con el antivirus a fin de proteger los equipos.

3.3.6.2 Copias de seguridad

Los técnicos de la Unidad de Gestión Tecnológica deben realizar copias de seguridad semanalmente, o cuando existan modificaciones en los ficheros para que en caso de ocurrir alguna eventualidad los datos puedan ser recuperados.

Cuando existe pérdida de información se debe indagar hasta dar con la causa y documentar lo suscitado.

El técnico encargado de los servidores debe clasificar la información más relevante para que sea respaldada oportunamente.

El encargado de la Unidad de Gestión Tecnológica es quien determina las medidas que se debe seguir con el almacenamiento de la información cuando un servidor no está funcionando correctamente.

Es recomendable que la información delicada que se almacena en los servidores sean guardados en servidores externos como medida de seguridad ante desastres naturales como terremotos o erupciones volcánicas.

3.3.6.3 Medidas a seguir para la reutilización o desecho de equipos

Cuando un recurso de la institución vaya a ser utilizado por otro funcionario de otro departamento, se debe eliminar toda la información existente del usuario anterior e instalar las aplicaciones para el uso del nuevo empleado de la municipalidad.

Los equipos que van a ser desechados deben ser revisados por un técnico el mismo que determinará mediante un informe técnico que este ha dejado de funcionar adecuadamente por lo que será trasladado a bodega para su almacenamiento respectivo.

Los equipos que hayan sido dados de baja no pueden ser reutilizados por ningún motivo puestos que estos bienes ya han cumplido su vida útil.

En un equipo que vaya a ser dado de baja se debe eliminar los archivos por completo para que no puedan ser recuperados por alguien inescrupuloso que podría hacer mal uso del mismo.

Los equipos que ya no funcionan adecuadamente y ya se hayan dado de baja pero no se ha procedido con el borrado de archivos deben ser custodiados para que no exista contacto con el personal no autorizado.

3.3.7 SEGURIDAD FÍSICA EN LA MUNICIPALIDAD

- **Objetivo: Resguardar** equipamientos e información de la municipalidad mediante la aplicación de normas a seguir para la mitigación de riesgos por catástrofes naturales, por manipulación inadecuada o robo.

3.3.7.1 Accesos a copias de seguridad

Los servidores donde se almacena toda la información de copias de seguridad deben estar ubicados en un lugar adecuado y seguro al cual no tengan acceso personal que no trabaje en el área de sistemas.

Todos los dispositivos en los que se almacena información de la municipalidad no pueden estar al alcance de personas no autorizadas.

Debe implementarse la protección contra rayos en las áreas donde están instalados los servidores puesto que almacenan información reservada de toda la municipalidad.

Se debe aplicar un control riguroso en el departamento puesto que se procesa información de toda la municipalidad para evitar fugas.

En caso de que un funcionario solicite información que se encuentre respaldada en servidores se solicitará mediante oficio por el director departamental indicando el motivo para el cual se requiere.

Cuando se entrega información de respaldo que es confidencial, a un funcionario municipal se debe llenar una hoja en la cual conste el responsable, una descripción del motivo, la fecha y la firma de respaldo.

3.3.7 .2 Seguridad en caso de Incendios en las instalaciones

Es necesario que exista una alarma que se active en caso de que ocurra un incendio dentro de la municipalidad de Pelileo.

En cada departamento debe ser obligatorio la existencia de extintores y la señalética respectiva y los protocolos a seguir si se presenta un incidente evitando inconvenientes tanto con el recurso humano como con los demás recursos.

Se prohíbe fumar dentro de las instalaciones de la municipalidad.

La sala donde se almacenan los equipos debe estar adecuada con materiales que no sean inflamables para que en caso de incendio esto se pueda consumir.

Esta área no puede por ningún motivo estar contigua a espacios en los cuales se encuentre material que sea de fácil combustión.

Toda el área debe estar construida de material que sea resistente al fuego y que no se pueda consumir.

Es necesaria la adecuación de un falso piso en el cuarto de servidores sobre el piso el cual debe ser de un material no inflamable que sea resistente al fuego.

Ser debe controlar que no existan filtraciones de agua en el cuarto de servidores, toda el área debe ser impermeable.

Se debe asignar la responsabilidad a un técnico para que verifique constantemente que las instalaciones cuentan con los factores físicos y ambientales para el correcto funcionamiento del área de servidores.

Es necesario la capación constante y la simulación de un incendio dentro de la municipalidad para que los empleados estén en la capacidad de reaccionar adecuadamente en el caso de que ocurra este tipo de desastre.

3.3.7.3 Suministro eléctrico y red

El cableado dentro de las instalaciones debe estar cubierto por sus respectivas canaletas, para evitar daños.

En cada uno de los departamentos de la municipalidad deben existir reguladores de energía que impidan variaciones de voltaje evitando así daños en los equipos.

Es necesario el uso de UPS en cada una de las áreas donde existen equipos dentro de la municipalidad para evitar que se apaguen los equipos y por ende la pérdida de información por cortes de energía inesperados.

El cableado de red debe estar aislado de cualquier otro tipo de cableado para evitar cualquier tipo de interferencia.

Las áreas en donde exista alto voltaje deben contar con sus respectivas restricciones y señalética adecuadas indicando que es un área de peligro.

3.3.7.4 Ingreso y salida del Personal

Los funcionarios municipales para el ingreso y salida deben realizar su respectivo registro en el sistema o mediante hojas que lleve la institución a la hora respectiva en las cuales empieza y termina su jornada laboral.
Los empleados deben portar su credencial entregada por la institución para que se pueda identificar quien es y el cargo que desempeña.

Los funcionarios municipales que no pertenecen al área de sistemas no están autorizados para realizar ingresos a áreas como cuarto de servidores o a equipos de los técnicos solamente podrán ingresar a la unidad de Gestión Tecnológica para solicitar algún tipo de información necesaria mas no para realizar manipulaciones en los equipos.

3.3.7.5 Seguridad

Es necesario la instalación de cámaras de seguridad en áreas estratégicas de la municipalidad para evitar robos, pérdida de equipos u otros percances.

El personal de seguridad debe realizar rondas contantemente por las instalaciones de la municipalidad para resguardad los recursos institucionales.

3.3.7.6 Conexiones a la red

Es necesaria la instalación de un sistema para detectar cuando personal ajeno a la municipalidad intenten acceder a la red.
Realizar un monitoreo constante para la detección de puertos que se encuentren abiertos por el técnico encargado del área de red de la municipalidad.

Configuración adecuada del alcance de las redes wifi existentes dentro de la municipalidad.

Los funcionarios municipales no deben conectarse a redes wifi abiertas desconocidas.

3.3.7.7 Seguridad de recursos fuera de la municipalidad.

Los empleados son responsables de los equipos, que se les haya asignado para su uso fuera de la municipalidad, el mismo que debe ser cuidado y comunicar su estado oportunamente mediante un informe detallado.
Es necesario que el funcionario dé aviso a la Unidad de gestión Tecnológica si los equipos necesitan algún tipo de mantenimiento que no puedan ser solucionados por parte de ellos.

3.3.8 Mejoras dentro de la Unidad de Gestión Tecnológica

- **Objetivo:** Vigilar constantemente que se esté acatando a las políticas establecidas para el correcto funcionamiento e integridad de los recursos institucionales.

Una vez implementado las políticas de seguridad dentro de la municipalidad es necesario que la Unidad de Gestión Tecnológica realice monitoreos constantes para verificar que se estén dando cumplimiento a lo establecido y se minimice los riesgos existentes, una vez que se ha encontrado las vulnerabilidades existentes en la municipalidad es necesario que se dé solución oportunamente por los técnicos de la Unidad con el fin de evitar que estos fallos continúen afectando a la seguridad de la institución.

Es necesario que los técnicos de la Unidad de Gestión Tecnológica realicen cada año la revisión y mejora continua de las políticas establecidas dentro de la Unidad de Gestión Tecnológica

CAPITULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

En la Unidad de Gestión Tecnológica de la Municipalidad de San Pedro de Pelileo no existe un manual de acciones que se deban tomar en caso de ocurrir alteraciones de información; motivo por el cual, el técnico encargado es quien decide qué acciones y medidas tomar en estos casos.

Las instalaciones del cuarto de servidores son reducidas por cuanto no existen las adecuaciones necesarias para su correcto funcionamiento, además se evidencian fisuras en el techo y filtraciones de agua en épocas de invierno estando en riesgo los equipos de esta unidad.

Existe un riesgo inminente en la municipalidad al no disponer de cámaras de video vigilancia que ayuden en el control de la seguridad de los activos institucionales.

Gran parte de los funcionarios municipales no cierran la sesión de usuario de los sistemas utilizados, quedando expuestos a que otro empleado realice modificaciones que afecten a la información reservada de la institución.

No se aplican los controles necesarios en cuanto al manejo y gestión de contraseñas por parte de los funcionarios municipales.

4.2 Recomendaciones

La Unidad de Gestión Tecnológica deberá instituir las políticas de seguridad en la municipalidad y difundir las mismas con el propósito de crear hábitos y buenas prácticas en el manejo y gestión de la información.

Es indispensable que en la Unidad de Gestión Tecnológica exista un técnico encargado del área de seguridad que realice el monitoreo constante y periódico de los procesos y normativas a seguir en caso de vulneraciones.

Es preciso que se apliquen controles que brinden seguridad al sistema para el uso adecuado de contraseñas puesto que los empleados municipales utilizan contraseñas débiles ocasionando un riesgo inminente en el sistema, además se debe notificar a los funcionarios que no almacenen su contraseña en lugares que estén a la vista del personal.

Se debe capacitar constantemente a los funcionarios municipales respecto a las medidas de seguridad a tomar en cuanto al manejo de información con la finalidad de avalando su seguridad y confidencialidad.

Referencias Bibliográficas

[1] J.G. Ulloa, " Auditoría informática aplicando la metodología COBIT en el Gobierno Autónomo Descentralizado Municipal de San Cristóbal de Patate", 2018. [online], Disponible en: http://repositorio.uta.edu.ec/jspui/handle/123456789/26932, [Accedido: Feb.12, 2020 2020].

[2] R.A. GUEVARA, "Sistema de Gestión de Seguridad de la información basado en la Norma ISO/IEC 27001 para el Departamento de Tecnologías de la Información y Comunicación del Distrito 18D01 de Educación", 2017. [online], Disponible en: http://repositorio.uta.edu.ec/jspui/handle/123456789/26932, [Accedido: Feb.12, 2020 2020].

[3] S.M. Criollo, "Análisis e Implantación de la norma ISO/IEC 27002:2013 para el departamento informático del Gobierno Autónomo Descentralizado Municipal del Cantón Salcedo", 2017 [online]. Disponible en: http://repositorio.uta.edu.ec/jspui/handle/123456789/26537, [Accedido: Feb.12, 2020 2020].

[4] A.L. Mesquid, A. Mas, E. Amengual, I. Cabestrero, "Sistema de Gestión Integrado según las normas ISO 9001, ISO/IEC 20000 e ISO/IEC 27001. REICIS". Revista Española de Innovación, Calidad e Ingeniería del Software, [En línea]. Disponible en:<http://www.redalyc.org/articulo.oa?id=92218768002> ISSN

[5] M. X. Núñez Velasco, "SiRetrieved" , [online], Disponible en https://s3.amazonaws.com/academia.edu.documents/36974512/NOV_DOC_Tabla_AEN_22994_1.pdf?AWSAccessKeyId=AKIAIWOWYYGZ2Y53UL3A&Expires=1550719525&Signature=7ujHvX3FWis91JQg3%2F2wNr7IkFA%3D&response-content-disposition=inline%3B%20filename%3DNOV_DOC_Tabla_AEN_22994_1.pdf

[6] D.L. Fernández, " Fases de un Ataque Informático", Jul, 2019, [online]. Disponible en: https://recordandoeinnovando.wordpress.com/2014/07/29/las-5-fases-o-etapas-de-un-ataque-informatico/.

[7] J. J. Cano, " Inseguridad Informática: Un concepto dual ·en seguridad informática ", 2004. [online], Disponible en: https://webcache.googleusercontent.com/search?q=cache:TLg9fLP7JRkJ:https://ojsrevistaing.uniandes.edu.co/ojs/index.php/revista/article/download/437/640+&cd=1&hl=es&ct=clnk&gl=ec.

[8] J. H. MAZZINGHI, " Gestión del riesgo en la seguridad informática: el nuevo escenario del control ", Febrero 2011, [online]. Available: http://webcache.googleusercontent.com/search?q=cache:s_BoACRkLP8J:www.cidemconsult.cl/biblioteca/doc/40/raw+&cd=13&hl=es-419&ct=clnk&gl=ec.

[9] C. Lara Ponce, 2020. " Estudio de una auditoría en seguridad informática aplicando la Norma Internacional de calidad total ISO 27001 para la Empresa Maint de la ciudad de Guayaquil ", [online], Disponible en: <http://repositorio.ug.edu.ec/handle/redug/6978> [Accedido May.20, 2020].

[10] Repositorio.ug.edu.ec. [online] Disponible en: <http://repositorio.ug.edu.ec/bitstream/redug/24302/1/B-CISC-PTG.1412.Y%C3%A9pez%20Chil%C3%A1n%20Walter%20Enrique.pdf> [Accedido 14 Mar.21, 2020].

[11] J. Naranjo Camacho y J, Reyes Lucas, " Auditoría informática dirigida al Centro de Cómputo de la Carrera de Ingeniería en Sistemas Computacionales de la Universidad de Guayaquil con base en las Normas ISO 27001 y 27002 " , [online] Repositorio.ug.edu.ec. Disponible en: <http://repositorio.ug.edu.ec/handle/redug/48923> [Accessed 18 July 2020].

[12] Iso.org. [online] Disponible en: <https://www.iso.org/files/live/sites/isoorg/files/archive/pdf/en/fast_forward-es.pdf> [Accedido Jul.23, 2020].

[13] Software ISO, " ISO 27001 - Software ISO 27001 de Sistemas de Gestión". [online] Disponible en: <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001> [Accedido Jul. 24, 2020].

[14] C. Lara Ponce, "Estudio de una auditoría en seguridad informática aplicando la Norma Internacional de calidad total ISO 27001 para la Empresa Maint de la ciudad de Guayaquil", [online] Repositorio.ug.edu.ec. Available at: <http://repositorio.ug.edu.ec/handle/redug/6978> [Accessed 23 August 2020].

[15] R. Hernández, "Auditoría Informática: Un Enfoque Metodológico y Practico", México: Continental, 2009, [Accedido: May. 20, 2020].

[16] F. Freire Zapata, " IMPLEMENTACIÓN DEL MODELO DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN APLICANDO ISO 27000 EN LA EMPRESA COKA TOURS, AMBATO – ECUADOR", [online] Dspace.uce.edu.ec. Disponible en: <http://www.dspace.uce.edu.ec/bitstream/25000/4244/1/T-UCE-0011-55.pdf> [Accedido Jul.18, 2020].

[17] C. Burgos Gordón, "Plan de contingencia informático para el área de TI en base a la norma de calidad ISO 27001:2013 para la Fundación Cultural y Educativa Ambato - Unidad Educativa Atenas". [online] Repositorio.uta.edu.ec. Disponible en: <https://repositorio.uta.edu.ec/jspui/handle/123456789/31307> [Accedido Oct.20, 2020].

[18] O. Muñoz Pinto, "Sistema de gestión de seguridad de la información basado en las normas ISO/IEC 27001, en el Departamento de Tecnologías de la Información en la Cooperativa de Ahorro y Crédito Indigena SAC", [online] Repositorio.uta.edu.ec. Disponible en: <https://repositorio.uta.edu.ec/jspui/handle/123456789/31305> [Accedido Ene, 20, 2021].

[19] A.K. Bohórquez Rodríguez, "IMPLEMENTACIÓN DE SOLUCIONES EN UNA INSTITUCIÓN UNIVERSITARIA PARA MITIGAR LA PÉRDIDA Y/O ALTERACIÓN DE LA INFORMACIÓN POR FALENCIAS EN LOS CONTROLES DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD FÍSICA", 2018. [online], Disponible en: . https://alejandria.poligran.edu.co/bitstream/handle/10823/1258/trabajo%20angie%20katerine%20bohorquez.pdf?sequence=1&isAllowed=y.

ANEXOS

ANEXO 1. - ENCUESTA

UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE SAN PEDRO DE PELILEO

1. ¿El departamento de Gestión Tecnológica cuenta con políticas de seguridad para la gestión de información?

   Si ( ) No ( )

   Cuales

   ---

2. ¿El personal del GAD San Pedro de Pelileo tiene conocimientos de las políticas de seguridad existentes?

   Si ( ) No ( )

3. ¿Cada empleado tiene responsabilidades asignadas del uso de los recursos de la institución?

   Si ( ) No ( )

4. ¿Se lleva un control adecuado del acceso del personal para que personas no autorizadas no puedan acceder a los equipos y sistema del GAD San Pedro de Pelileo?

   Si ( ) No ( )

5. ¿Se tiene establecido los debidos controles de usuarios con las debidas restricciones de acuerdo al perfil de cada uno?

   Si ( ) No ( )

6. ¿El sistema al momento de ingresar una contraseña solicita que esta tenga letras números y caracteres especiales?

Si ( ) No ( )

7. ¿Se lleva a cabo periódicamente el mantenimiento correctivo y preventivo de los equipos de la institución?

   Si ( ) No ( )

Indique cada cuanto tiempo

a) 2 meses

b) 3 meses

c) 6 meses

d) cada ano

8. ¿Qué hace el departamento de Gestión Tecnológica cuando el sistema tiene algún fallo?

---

9. Se realizan monitoreo constantemente al sistema para evitar cualquier eventualidad.

Si ( ) No ( )

10. Cuentan con un sistema de inventario de recursos informáticos de la institución

Si ( ) No ( )

11. ¿El departamento cuenta con personal que tengan amplios conocimientos en seguridad de la información?

Si ( ) No ( )

12. ¿Cada Departamento del GAD San Pedro de Pelileo tiene asignada políticas de seguridad?

    Si ( ) No ( )

13. ¿Cuenta el Departamento con algún tipo de política de confidencialidad de la información en el caso de que un empleado abandone el cargo se le supriman todos los accesos al sistema?

    Si ( ) No ( )

14. ¿Se revisa periódicamente el cableado en todos los departamentos de la institución?

    Si ( ) No ( )

15. ¿Se realizan copias de seguridad de la información?

    Si ( ) No ( )

Cada cuanto tiempo

ANEXO 2. FOTOGRAFÍAS

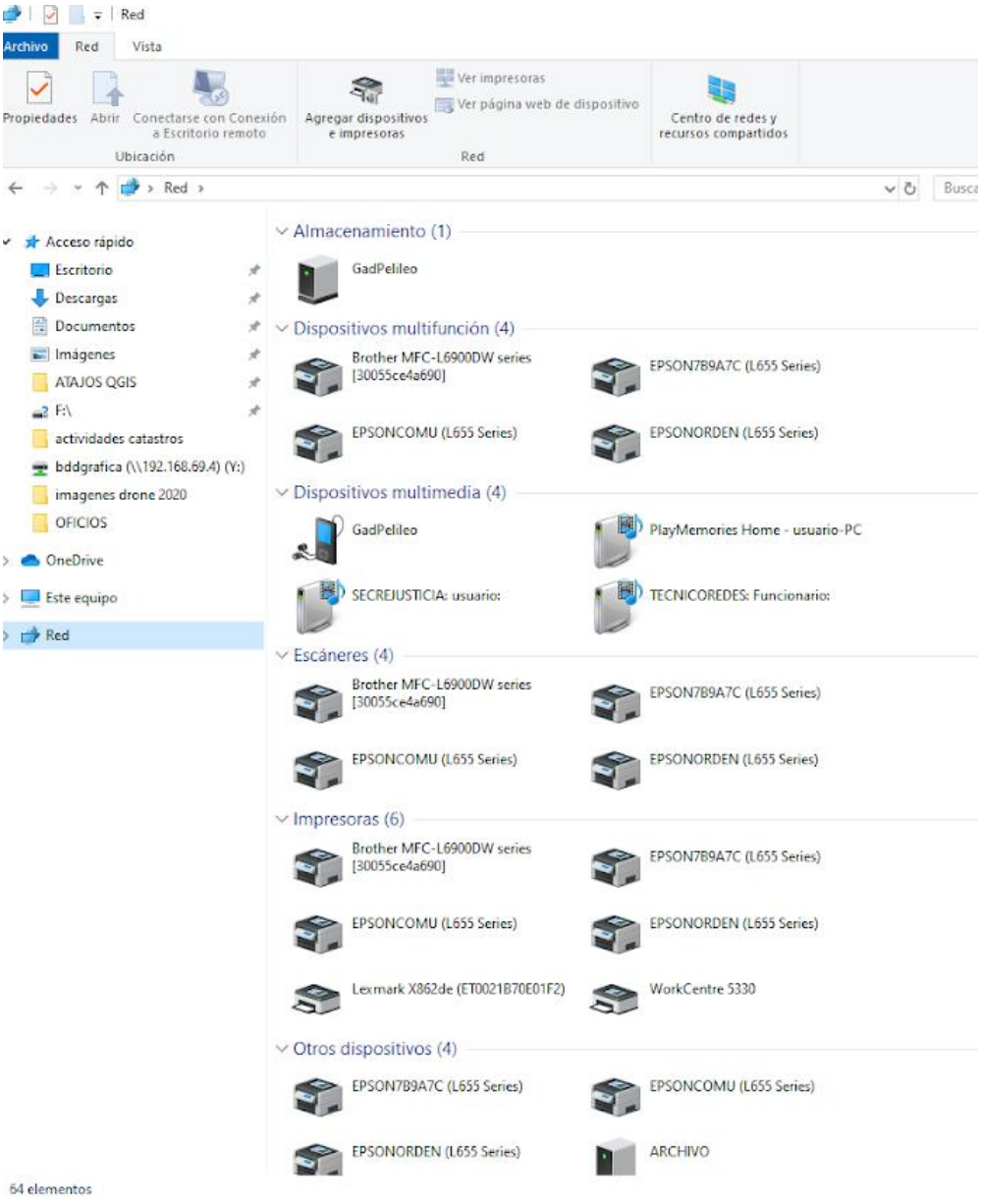


Figura 34. Recursos compartidos

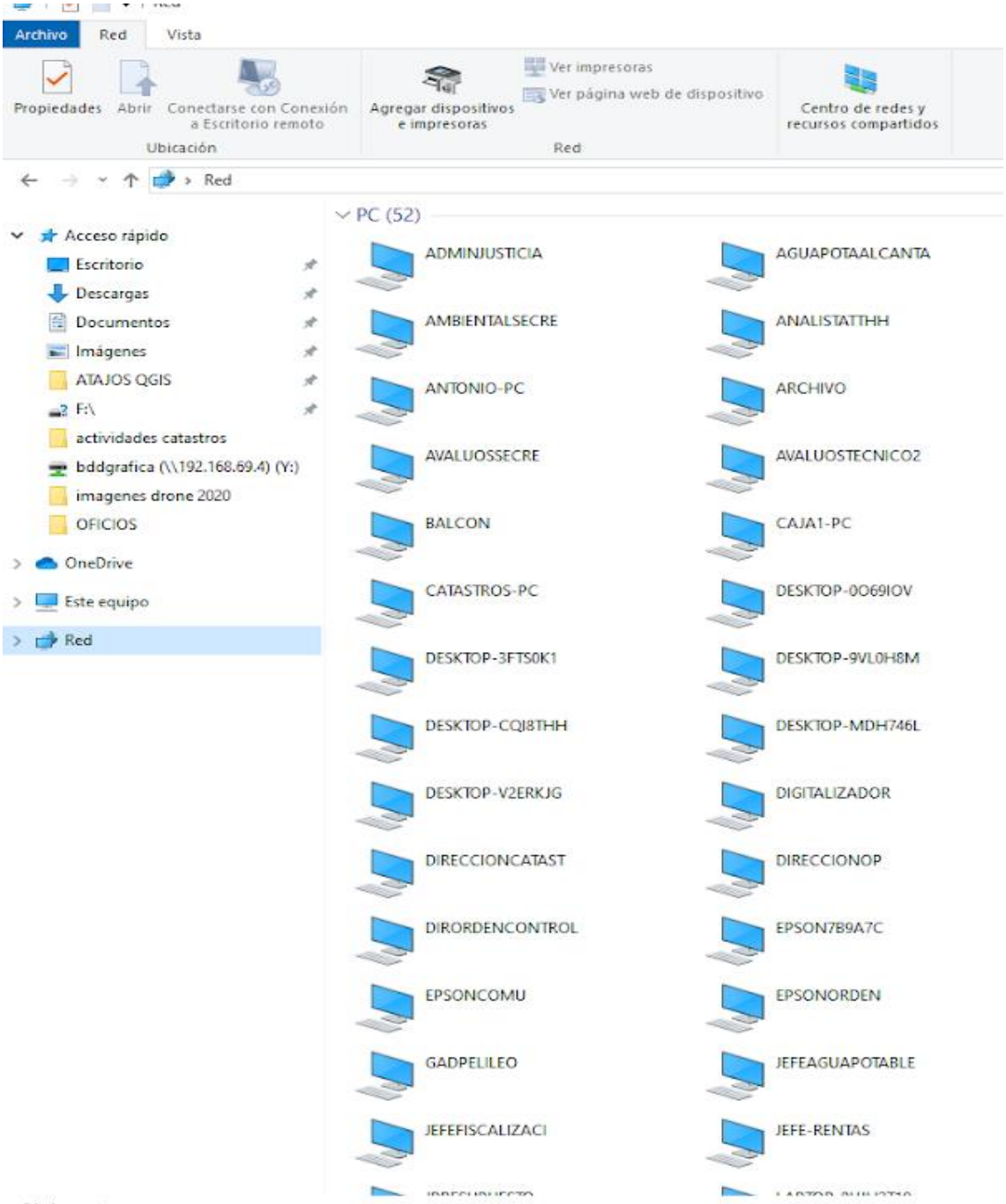


Figura 35. Equipos conectados a la red

Figura 36. Acceso al sistema

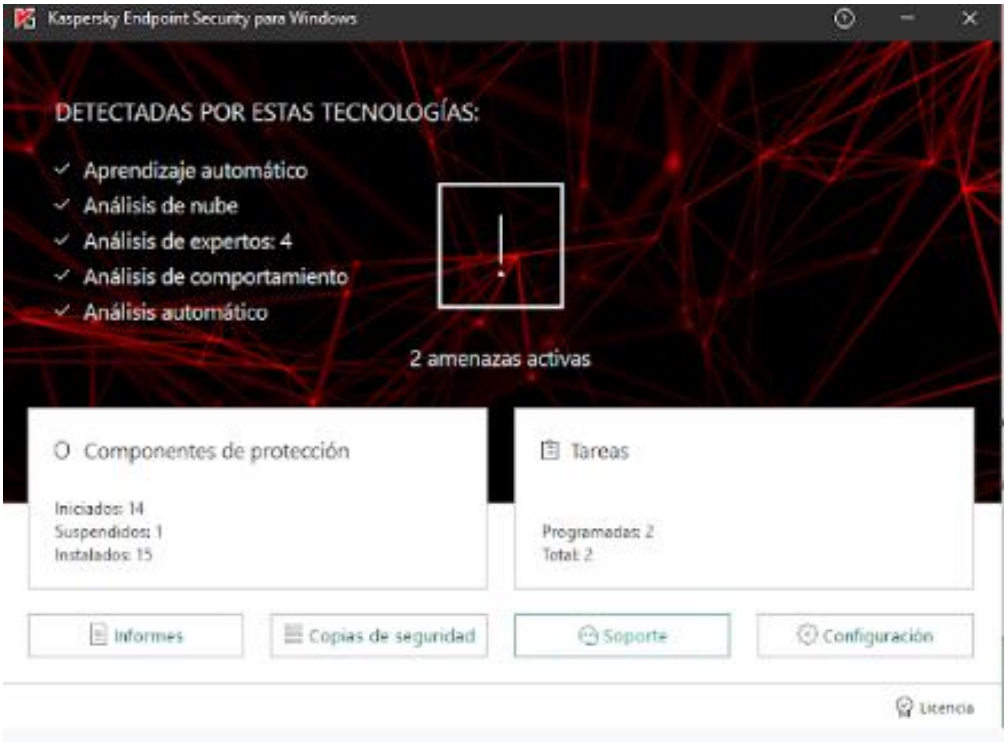


Figura 37. Antivirus en la municipalidad

Figura 38. Jefe de la Unidad de Gestión Tecnológica

Figura 39. Reunión con el jefe de la Unidad de Gestión Tecnológica

Figura 40. Técnico de servidores de la Unidad de Gestión Tecnológica

Figura 41. Cuarto de servidores

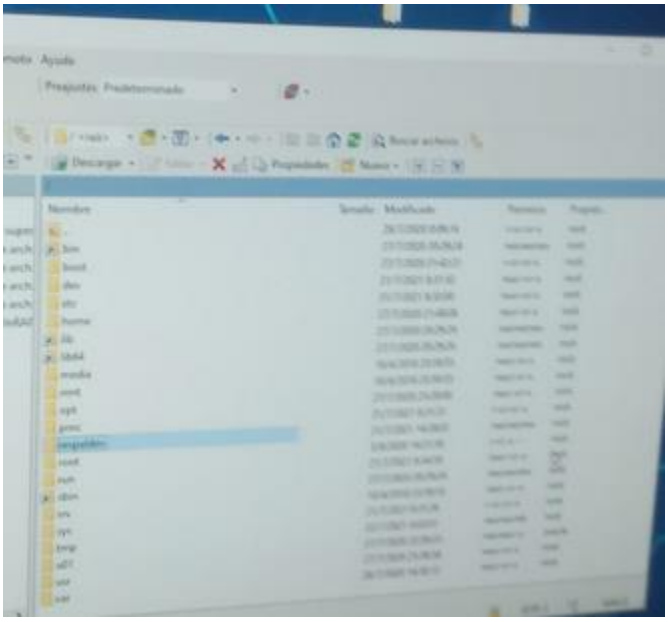


Figura 42. Carpeta donde se guardan los respaldos

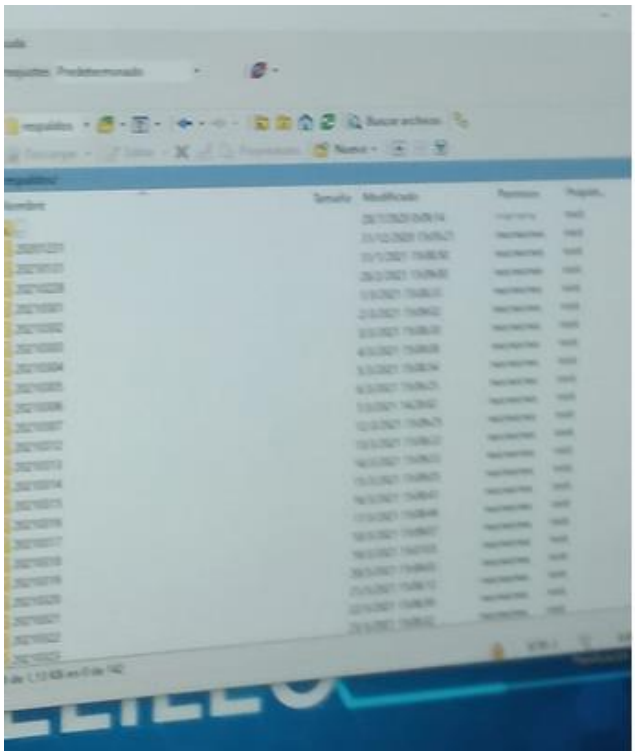


Figura 43. Respaldos almacenados en el servidor