UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

CARRERA DE INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES

PROYECTO DE INVESTIGACIÓN

PROPUESTA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE ACUERDO A LAS ISO 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PANGUA.

AUTORAS:

Cruz Caiza Carla Cristina

Gaibor Gavilanez Mónica Lisseth

TUTOR:

Ing. MSc. Llano Casa Alex Christian

LATACUNGA - COTOPAXI

Septiembre – 2020

UNIVERSIDAD TÉCNICA DE COTOPAXI

Ingeniería Informatica Y Sistemas Computacionales

DECLARACIÓN DE AUTORÍA

Yo **CRUZ CAIZA CARLA CRISTINA** y **GAIBOR GAVILANEZ MÓNICA LISSETH**, declaramos ser autoras del presente proyecto de investigación: "**PROPUESTA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE ACUERDO A LAS ISO 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PANGUA.**", siendo Ing. Llano Casa Alex Christian tutor del presente trabajo; y eximo expresamente a la Universidad Técnica de Cotopaxi y a sus representantes legales de posibles reclamos o acciones legales.

Además, certifico que las ideas, conceptos, procedimientos y resultados vertidos en el presente trabajo investigativo, son de mi exclusiva responsabilidad.

Latacunga, 18 de septiembre del 2020

.....

Cruz Caiza Carla Cristina
C.I. 120679976-7

.....

Gaibor Gavilanez Mónica Lisseth
C.I. 050356128-4

UNIVERSIDAD TÉCNICA DE COTOPAXI

Ingeniería Informatica Y Sistemas Computacionales

AVAL DEL TUTOR DE PROYECTO DE TITULACIÓN

En calidad de Tutor del Trabajo de Investigación sobre el título:

"PROPUESTA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE ACUERDO A LAS ISO 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PANGUA", de **CRUZ CAIZA CARLA CRISTINA** y **GAIBOR GAVILANEZ MÓNICA LISSETH**, de la carrera de Ingeniería en Informática y Sistemas Computacionales, considero que dicho Informe Investigativo cumple con los requerimientos metodológicos y aportes científico-técnicos suficientes para ser sometidos a la evaluación del Tribunal de Validación de Proyecto que el Consejo Directivo de la Facultad de Ciencias de la Ingeniería y Aplicadas de la Universidad Técnica de Cotopaxi designe, para su correspondiente estudio y calificación.

Latacunga, Septiembre, 2020

TUTOR INSTITUCIONAL
Ing. MSc. Llano Casa Alex Christian
050258986-4

UNIVERSIDAD TÉCNICA DE COTOPAXI

Ingeniería Informatica Y Sistemas Computacionales

APROBACIÓN DEL TRIBUNAL DE TITULACIÓN

En calidad de Tribunal de Lectores, aprueban el presente Informe de Investigación de acuerdo a las disposiciones reglamentarias emitidas por la Universidad Técnica de Cotopaxi, y por la FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS ; por cuanto, las postulantes: Cruz Caiza Carla Cristina y Gaibor Gavilanez Mónica Lisseth, con el título de Proyecto de titulación: "**PROPUESTA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE ACUERDO A LAS ISO 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PANGUA**", han considerado las recomendaciones emitidas oportunamente y reúne los méritos suficientes para ser sometido al acto de Sustentación de Proyecto.

Por lo antes expuesto, se autoriza realizar los empastados correspondientes, según la normativa institucional.

Latacunga, Septiembre 2020

Para constancia firman:

(Presidente)
PhD. Gustavo Rodríguez Bárcena
CC: 175700135-7

Lector 2
Ing. Mg. Manuel Villa Quishpe
CC: 180338695-0

Lector 3
Ing. MSc. Verónica Tapia Cerda
CC: 050205369-7

El Corazón, 25 de noviembre del 2 019

CARTA DE ACEPTACIÓN

Por medio de la presente hago constar que las Srtas: GAIBOR GAVILANEZ MÓNICA LISSETH portadora de la C.I. 050356128-4 y CRUZ CAIZA CARLA CRISTINA portadora de la C.I. 120679976-7, estudiantes de la carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, han sido aceptadas en nuestra institución Gobierno Autónomo Descentralizado del cantón Pangua, para realizar el tema de tesis "Propuesta de Políticas de Seguridad Informática de acuerdo a las ISO 27001 en el Gobierno Autónomo Descentralizado del cantón Pangua".

Atentamente,

Lcdo. Sául Mejía P.
ALCALDE DEL GADMUPAN

Calle Sucre y Ramón Campaña 268-4156 / 268-4090 / 268-4443
Telefax Secretaría: 268-4157 www.pangua.gob.ec
Pangua · Cotopaxi · Ecuador

UNIVERSIDAD TÉCNICA DE COTOPAXI

El corazón, 21 de Agosto del 2020

Estimado

Ing. Herman Ortiz
ENCARGADO DE LA UNIDAD DE SISTEMAS INFORMÁTICOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE PANGUA.

Presente.

De mi consideración.

Por medio de la presente hago entrega del Proyecto de Investigación titulado **"PROPUESTA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE ACUERDO A LAS ISO 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PANGUA"**, realizado por las estudiantes **CRUZ CAIZA CARLA CRISTINA**, portadora de la cedula de identidad **120679976-7** y **GAIBOR GAVILANEZ MÓNICA LISSETH**, portadora de la cedula de identidad **050356128-4**, en el cual hace mención a las siguientes políticas:

- ✓ **PO-1A** Control de acceso a recursos computacionales.
- ✓ **PO-1B** Administración de políticas de Active Directory.
- ✓ **PO-1C** Control de Activos de TI.
- ✓ **PO-1F** Resguardo de Información.
- ✓ **PO-1D** Seguridad a componentes informáticos.
- ✓ **PO-1E** Uso adecuado del Internet.

Firma

AGRADECIMIENTO

El presente trabajo de tesis primeramente me gustaría agradecer a ti Dios por brindarme salud, esfuerzo para poder llegar hasta donde he llegado con dedicación y amor a este sueño tan anhelado.

A mi querido padre Ermel Cruz por ese apoyo incondicional, por su paciencia, amor, comprensión y por toda su enseñanza que me ha brindado a pesar de mis problemas él nunca me ha dejado y siempre ha estado ahí durante toda mi carrera profesional. A mi amada madre Carmen Caiza por ser esa mujer luchadora y un ejemplo a seguir quien siempre me dio su cariño cuando más lo necesite. A mis hermanos: Silvana, Edison y Karen.

Agradezco a mi tutor de tesis el Ing. Alex Llano por haberme brindado la oportunidad de recurrir a su capacidad y conocimiento científico, así como también por haberme tenido toda la paciencia del mundo para guiarme durante todo este proceso de desarrollo de tesis.

A mis ingenieros por la enseñanza, mis compañeros de clase por la amistad y a mí querida Universidad por haberme abierto las puertas.

Carla Cruz

AGRADECIMIENTO

Primeramente, gracias a Dios que me brindo el conocimiento, fuerza y salud para seguir adelante, me tendió su mano para ayudarme a levantar y llegar a cumplir uno de mis más grandes sueños.

Agradezco a mis padres Héctor Gaibor y Julieta Gavilanez por estar conmigo, por enseñarme a crecer y a que si caigo debo levantarme, por guiarme, aconsejarme y apoyarme en mis estudios, pues gracias a su sacrificio, paciencia y perseverancia me ayudaron a culminar este ciclo de mi vida y me ayudaron a convertirme en una profesional, gracias también a mis hermanos Marco Gaibor y Elizabeth Villacres por todos los consejos y palabras de aliento, por estar pendientes de mi a pesar de la distancia en la que me encontraba.

Finalmente quiero agradecer a mi tutor al Ing. Alex Llano por depositar en mí todos sus conocimientos, gracias por la paciencia y consejos, pues en el transcurso de mi carrera se convirtió en un gran amigo, gracias por ser una excelente persona y un excelente profesional.

Mónica Gaibor

DEDICATORIA

Esta tesis de grado al igual que al resto del trabajo realizado dedico especialmente a mi angelito, quien es mi mayor motivación para nunca rendirme y poder llegar a ser un ejemplo para ella, para mi hermana y mis sobrinos quienes siguen el mismo proceso de estudio.

A mis padres y hermanos por su sacrificio y esfuerzo por darme una carrera para mi futuro y por creer en mi capacidad de poder llegar hacer una Ingeniera, aunque hemos pasado momentos muy difíciles, pero siempre han estado brindándome su esfuerzo, cariño, amor y sobre todo un "tú puedes hija no te rindas" en el transcurso de cada año de mi carrera Universitaria.

A mi familia en general, especialmente a mis tíos Carmen, Rosana y Gonzalo por brindarme su apoyo incondicional y por compartir buenos y malos momentos.

Carla Cruz

DEDICATORIA

Mi tesis va dedicada a mi Dios, quien me brindo salud, concentración, perseverancia y me guio en cada paso, en cada decisión en el transcurso de mi carrera.

Con mucho cariño la dedico a mis Padres y Hermanos que creyeron en mí, que con su apoyo, sacrificio y apoyo incondicional se hizo realidad esta meta, gracias por todo, no me va alcanzar la vida para agradecerles todo lo que han hecho por mí, los amo mucho.

Finalmente quiero dedicar a todas las personitas que estuvieron durante este proceso, que dejaron huellas en mi vida, brindándome su amistad y cariño, apoyándome, dándome animo en todo momento, en las buenas y las malas, diciéndome "Ya vez te lo dije" cuando superaba cada obstáculo.

Mónica Gaibor

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

UNIVERSIDAD TÉCNICA DE COTOPAXI

FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

TEMA: PROPUESTA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE ACUERDO A LAS ISO 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PANGUA.

AUTORAS: Cruz Caiza Carla Cristina

Gaibor Gavilanez Mónica Lisseth

RESUMEN

En el presente proyecto de investigación se analizó la ausencia de controles y procedimientos de la seguridad que gestionan las TICs del Gobierno Autónomo Descentralizado Municipal de Pangua, en virtud de ello se procedió a levantar información por medio de instrumentos de investigación, como es la entrevista que se realizó al encargado de sistemas informáticos obteniendo información acerca de ciertas ausencias, de igual forma al encontrar ciertas anomalías mediante la observación de los procedimientos, por tal razón se optó sustentar con fuentes bibliográficas acerca de empresas que aplicaron políticas de seguridad informática mediante la ISO 27001 y al percibir los resultados, se generó un modelo diverso de políticas que cumple con los estándares de la ISO además que se acoplen a las necesidades del GAD, para que tomen en consideración implementarlas en el futuro. Como resultado de la investigación se generó una propuesta para la implementación de documentos de gestión informática, con el fin de administrar, evaluar y proteger las TICs, estas políticas de seguridad informática deben ser asumidas asimismo ejecutadas por los miembros del departamento de Sistemas Informáticos apoyados por las demás unidades de la municipalidad, con el propósito de minimizar las amenazas y riesgos de pérdidas de datos o ser víctimas de ataques cibernéticos. Además, permitió a la dirección de la organización, tener una visión necesaria para definir metodologías de mejora continua que aporte al óptimo cumplimiento de los objetivos y servicios de la municipalidad.

Palabras Claves: Políticas de seguridad informática, amenazas, TICs, Confidencialidad, Disponibilidad,Integridad.

TECHNICAL UNIVERSITY OF COTOPAXI

FACULTY OF ENGINEERING AND APPLICATION SCIENCES

THEME: PROPOSED COMPUTER SECURITY POLICIES IN ACCORDANCE WITH ISO 27001 IN THE DECENTRALIZED AUTONOMOUS GOVERNMENT OF PANGUA CANTON.

ABSTRACT

The present research project analyzed security controls absence and procedures managed by TICs of Municipal Decentralized Autonomous Government of Pangua, thus proceeding to collect information through investigative instruments, such as interview that was conducted with computer system manager obtaining information about certain absences, similarly finding certain anomalies by procedures observing, for this reason it was decided to support with bibliographic sources about companies that implemented computer security policies through ISO 27001 and results, generated a diverse model of policies that meets ISO standards in addition to meet GAD'S needs to implement them in the future. As a result of the research, a proposal was generated for its management documents implementation in order to direct, evaluate and protect TICs, these computer security policies should also assume to implement them by members of Computer Systems Department supported by the other units of the municipality, in order to minimize threats and risks of data loss or to be victims of cyberattacks. In addition allowed organization's management to have a necessary vision to define methodologies of continuous improvement that contributes to optimal fulfillment of institution objectives and services.

Keywords: Computer Security Policies, Threats, TICs, Confidentiality, Availability, Integrity.

Universidad Técnica de Cotopaxi

CENTRO DE IDIOMAS

AVAL DE TRADUCCIÓN

En calidad de Docente del Centro de Idiomas de la Universidad Técnica de Cotopaxi; en forma legal **CERTIFICO** que: La traducción del resumen de tesis al Idioma Inglés presentado por los señores estudiantes egresados de la Carrera de **INGENIERÍA EN INFORMÁTICA Y SISTEMAS COMPUTACIONALES** de la **FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS: CRUZ CAIZA CARLA CRISTINA Y GAIBOR GAVILANEZ MÓNICA LISSETH**, cuyo título versa: **"PROPUESTA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE ACUERDO A LAS ISO 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PANGUA"**, lo realizaron bajo mi supervisión y cumple con una correcta estructura gramatical del idioma.

Es todo cuanto puedo certificar en honor a la verdad y autorizo a las peticionarias hacer uso del presente certificado de la manera ética que estimen conveniente.

Latacunga, septiembre del 2020.

Atentamente,

.....

Lic. Marcelo Pacheco Pruna Mg.
DOCENTE CENTRO DE IDIOMAS
C.C. 050261735-0

UNIVERSIDAD TÉCNICA DE COTOPAXI LATACUNGA - ECUADOR

CENTRO DE IDIOMAS

1. INFORMACIÓN GENERAL

Título del Proyecto:

Propuesta de Políticas de Seguridad Informática de acuerdo a las ISO 27001 en el Gobierno Autónomo Descentralizado del cantón Pangua.

Fecha de inicio: Mayo del 2020.

Fecha de finalización: Septiembre del 2020.

Lugar de ejecución:

Calle Ramón Campaña y Sucre (Centro) El Corazón – Cantón Pangua – Cotopaxi – Zona 3 – Gobierno Autónomo Descentralizado Municipal de Pangua.

Facultad que auspicia:

Facultad de Ciencias de la Ingeniería y Aplicadas.

Carrera que auspicia:

Carrera de Ingeniería en Informática y Sistemas Computacionales.

Proyecto de investigación vinculado:

Equipo de Trabajo:

- **Tutor de Titulación**

Ing. Llano Casa Alex Christian.

- **Coordinadoras del Proyecto**

Cruz Caiza Carla Cristina.

Gaibor Gavilanez Mónica Lisseth.

Área de Conocimiento:

Tecnologías de Información y Comunicación.

Sub líneas de investigación de la Carrera:

Sublínea 1: Diseño, Implementación y configuración de redes y seguridad computacional, aplicando normas y estándares internacionales.

2. RESUMEN DEL PROYECTO

El proyecto de investigación analizó las necesidades y riesgos del GAD de Pangua, que nos permitió diseñar políticas de seguridad informáticas que ayude a su buena gestión, así mismo que hagan uso de las buenas prácticas de la ISO 27001. Para analizar las necesidades se requirió realizar una investigación de campo, para extraer datos e información de la realidad haciendo uso de herramientas como la entrevista, de igual forma se planteó la investigación bibliográfica para sustentar acerca de instituciones que hacen uso de las normas ISO 27001. Como resultado de esta investigación se identificó los riesgos existentes en la municipalidad dando como solución un modelo de políticas diverso a cada problemática, consecuentemente se realizó la inducción y entrega de políticas de seguridad informática.

3. JUSTIFICACIÓN DEL PROYECTO

El proyecto de investigación tiene como propósito el diseñar las políticas de seguridad informática aplicando las normas ISO 27001, para la protección de la información y los recursos informáticos de la Municipalidad de Pangua, identificando los riesgos que puedan ir en contra de la confidencialidad, integridad y disponibilidad de la información que afecten a las actividades, pues al carecer de políticas de seguridad informática, la información que administra el cantón Pangua puede verse afectada al ser víctimas de ataques cibernéticos como de robo de información. De este modo es primordial, que la institución considere implementar en un futuro las políticas de seguridad informática como buenas prácticas para gestionar la información de una manera segura evitando pérdidas y permitiendo que el Municipio precautele el uso adecuado de todos los servicios informáticos, para que brinden sus funciones con total normalidad a la ciudadanía. Al proponer las políticas que se creen adecuadas para las necesidades de la Municipalidad, se aporta con la seguridad de la información de los habitantes del cantón Pangua y los bienes informáticos de la Municipalidad. Lo que beneficia a toda la ciudadanía Pánguense y a la institución en general pues optimizará su seguridad y por ende sus actividades.

4. BENEFICIARIOS DEL PROYECTO

4.1. Beneficiarios Directos

Los Beneficiarios directos del presente proyecto de Investigación es el Gobierno Autónomo Descentralizado Municipal de Pangua.

4.2. Beneficiarios Indirectos

Ciudadanía, Administradores y Empleados del Municipio.

5. PROBLEMA DE INVESTIGACIÓN

Según (Colonia Hernández, 2019), menciona que "en la Municipalidad Distrital de Buena Vista Alta – Casma, la problemática es la inseguridad de la información, en tal virtud ha propuesto como objetivo realizar la propuesta de un sistema de gestión de seguridad de la información con normas ISO 27001 de tal forma minimice la pérdida de información. La investigación fue desarrollada cuantitativamente bajo el diseño descriptivo de transcripción no experimental, la línea de investigación Implementación de Tecnologías de Información y Comunicación (TIC), para la mejora continua de la calidad en organizaciones en Perú, de la Escuela Profesional de Ingeniería de Sistemas de la Universidad Católica los Ángeles de Chimbote."

Según (Aguilar Carrión, 2017) alude que "en el Gobierno Autónomo Descentralizado Cantonal de Pastaza ofrece servicios públicos a la ciudadanía de la cabecera cantonal y parroquias aledañas. En visitas realizadas han podido apreciar dificultades relacionadas con el área informática como la pronta saturación de la conectividad a los diferentes Wireless, los equipos informáticos de la institución están siendo utilizados por diferentes departamentos sin el debido control de los funcionarios de TICs, no existe seguridad en el área determinada para los servidores ni en los puestos de trabajo, mencionando que la institución tiene un problema relacionado con el área de tecnología lo que respecta con la seguridad de la información, haciendo uso de la modalidad de investigación Cualitativa y el método Inductivo/Deductivo."

Según (Paguay Lema & Zamora Arana, 2017) menciona que "se desarrollará un plan de seguridad de la información basándose en la norma INEN ISO/IEC 27001 para el GAD Municipal de Milagro, puesto que esta norma detalla cómo gestionar la seguridad de la información de una entidad, ya sea pública o privada. En este contexto, existe una metodología formal de Análisis y Gestión de Riesgos denominada MAGERIT, que permite recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos."

Para la presente investigación a través de una entrevista al Gobierno Autónomo Descentralizado Municipal del cantón Pangua se evidenció la carencia de Políticas de Seguridad Informática, lo cual es perjudicial para la entidad pues puede verse afectada por

ataques cibernéticos o por robo de información, debido que presentan ausencia de controles y procedimientos de la seguridad que gestionan las TICs, por ende facilita el ingreso a cualquier persona y así podrán manipular la información ocasionando pérdidas de la disponibilidad, confidencialidad e integridad de los datos, disminuyendo que brinden sus servicios con total normalidad a la ciudadanía.

6. OBJETIVOS

6.1. Objetivo General

Diseñar políticas de seguridad informática aplicando normas ISO 27001 para la gestión de la información y las herramientas informáticas en el Gobierno Autónomo Descentralizado Municipal del Cantón Pangua.

6.2. Objetivo Específicos

- ✓ Analizar la situación actual de las herramientas y equipos informáticos del Gobierno Autónomo Descentralizado Municipal de Pangua para verificar su operación.
- ✓ Identificar los riesgos que puedan ir en contra de la confidencialidad, integridad y disponibilidad de la información que afecten las actividades del GAD de Pangua.
- ✓ Crear modelos de documentos que permitan dar seguimiento al cumplimiento de los objetivos del departamento de TI.

7. ACTIVIDADES Y SISTEMA DE TAREAS EN RELACIÓN A LOS OBJETIVOS PLANTEADOS

Tabla 1: Sistema de tareas en relación a los objetivos planteados.

OBJETIVO	ACTIVIDADES (TAREAS)	RESULTADO DE LA ACTIVIDAD	MEDIOS DE VERIFICACIÓN
Objetivo Especifico 1: Analizar la situación actual de las herramientas y equipos informáticos del Gobierno Autónomo Descentralizado Municipal de Pangua para verificar su operación	**Tarea 1:** Entrevistar al Alcalde del GAD del cantón Pangua para indagar sobre las actividades. **Tarea 2:** Dialogar con el Área de Servicios Informáticos para percibir la manera con la que se maneja la información. **Tarea 3:** Realizar una visita por las instalaciones para comprender el proceso que se maneja en el GAD del cantón Pangua.	Se pudo apreciar la acogida por parte del Sr. Alcalde Prof. Saúl Mejía, para propuesta de Políticas de Seguridad Informática en el GAD, como también mediante un diálogo la necesidad de las mencionadas Políticas.	
Objetivo Especifico 2: Identificar los riesgos que puedan ir en contra de la confidencialidad, integridad y disponibilidad de la información que afecten las actividades del GAD de Pangua. .	**Tarea 1:** Percibir si se maneja limitaciones al acceso de información para el personal de otras áreas. **Tarea 2:** Verificar la seguridad que se lleva con respecto a la información de los habitantes del cantón Pangua.	Entrevista con el Ingeniero encargado del departamento Informático. Apreciar ciertas carencias que en un futuro puede perjudicar el buen funcionamiento del GAD del cantón Pangua. Levantamiento de la información que contribuya para la investigación.	Audio de la entrevista y entrevista redactada, que será adjuntada al documento.
Objetivo Especifico 3: Crear modelos de documentos que permitan dar seguimiento al cumplimiento de los objetivos del departamento de TI.	**Tarea 1:** Investigar sobre las ISO para aplicar estándares que garanticen y ayuden al buen funcionamiento. **Tarea 2:** Generar documentos adecuados que permitan en un futuro verificar su adecuado cumplimiento.	Diseño de las Políticas de Seguridad Informática. Diseño de Anexos y Registros que contarán el cumplimiento de las Políticas.	Documentación de Políticas de Seguridad redactada.

Fuente: Grupo Investigador.

8. FUNDAMENTACIÓN CIENTÍFICO TÉCNICA

8.1. ANTECEDENTES

En el 2005 el 15 de octubre fue publicado la ISO 27001, con el fin de implementar, opera, establecer, mantener, supervisar y mejorar SGSI aplicable para toda tipo de empresas u organizaciones proporcionando esta norma con niveles altos de seguridad sobre temas altamente confidenciales (Cordero Torres, 2015). Consiste en la confidencialidad, integridad y disponibilidad de la información o procedimientos en diversas organizaciones estas pueden ser públicas o privadas ya sean grandes o pequeñas y estas pueden ser con o sin fines de lucro (Nieves, 2017). El objetivo fundamental es proteger la información para que no caiga en manos incorrectas o esta se pierda para siempre.

El estándar de la ISO 27001 es certificable, es decir cualquier organización que tenga implementado un SGSI según este modelo, puede solicitar una auditoría y dependiendo del éxito de esta auditoría puede adquirir una certificación ISO 27001.

La ISO es la constante reevaluación de controles y políticas que se adopta con el fin de garantizar la información y sistemas informáticos asegurando la sostenibilidad de la información a través del tiempo realizando auditorías o revisiones periódicas (Oidor González, 2016).

8.1.1. Clasificación de las normas

El objetivo principal de las normas ISO es el de orientar, coordinar, simplificar y unificar a nivel internacional el intercambio comercial e industrial, para obtener una mayor eficiencia y productividad en todos los campos de la actividad económica, en la normalización se puede establecer la siguiente clasificación general de las normas (Magaña Herrera, 2012).

a) Ámbito de la aplicación

Nacional: Conjunto de organismos internacionales de normalización.

- ✓ Normas para el sector industrial.
- ✓ Normas para las empresas.
- ✓ Normas para los organismos nacionales.

- Internacional: conjunto de organismos internacionales de normalización.

b) Contenido

Científico

- ✓ Definiciones de magnitudes.
- ✓ Designaciones de la simbología matemática
- ✓ Designaciones de notaciones científicas

Industrial

- ✓ Normas de calidad: definen las características de un producto o proceso.
- ✓ Normas dimensionales: definen las dimensiones tolerancias, formas, etc., de un producto.
- ✓ Normas orgánicas: afectan a sus aspectos generales (color de las pinturas, dibujos, acotaciones, etc.)

c) Forma de la aplicación

- ✓ Obligatorias
- ✓ Voluntarias

8.1.2. Beneficios de las normas internacionales ISO

Según (Díaz Romero & Rodríguez Rojas, 2017), nos relata que "las normas internacionales de la ISO contribuyen a beneficiar a los consumidores, empresas, Gobiernos y sociedad en general" de las siguientes maneras:

Para los consumidores: la conformidad de los productores y servicios con estándares internacionales ofrece garantía a los consumidores sobre la calidad, la seguridad y la confidencialidad de estos productos y servicios.

Para las empresas: en la adopción de normas técnicas internacionales, los proveedores pueden llevar a cabo el desarrollo de sus proveedores y servicios sobre la base de las especificaciones que han sido de amplia aceptación en su sector, lo que facilita la contratación y organización de los bienes y producto. Esto a su vez significa que las empresas internacionales que utilizan normas, técnicas son cada vez más libres de competir en muchos más mercados en todo el mundo.

Para todos: las normas técnicas internacionales pueden contribuir a la calidad de vida en general, por garantizar que los modos de transporte, maquinaria y herramienta que utilizamos sean seguros.

Por el planeta: las normas técnicas internacionales en aire, el agua, la calidad del suelo, sobre las emisiones de gases y la radiación, pueden contribuir a los esfuerzos por preservar el medio ambiente.

Es importante aplicar estos beneficios dado que cumplen una significativa función de instaurar la normativa a nivel internacional. De esta forma sirve como patrón de referencia para obtener una gestión de calidad en cualquier otra empresa.

8.1.3. Misión de la ISO 27001

La misión de la ISO es comenzar la estandarización con actividades relacionadas con facilitar el intercambio de servicios y bienes para así promover la cooperación tecnológica y económica, todos los trabajos realizados por la ISO resultan acuerdos internacionales que son publicados como Estándares Internacionales.

8.1.4. Visión de la ISO 27001

La visión de la ISO 27001 es un enfoque sistemático para implementar, establecer, monitorear, revisar, operar y mejorar la seguridad de la información de una Institución y ayudarle a lograr sus objetivos comerciales.

8.1.5. Cuadro comparativo de resultados de la norma ISO 27001 ante COBIT e ITIL

Tabla 2: Cuadro comparativo de resultados de la norma ISO ante COBIT e ITIL.

CUADRO COMPARATIVO					
ISO 27001		**COBIT**		**ITIL**	
PRONACA C.A (Morales, 2015)	Con el desarrollo de la propuesta expuesta se logrará mantener la confidencialidad, disponibilidad y seguridad de la información de la Procesadora Nacional de Alimentos, obteniendo altos niveles de seguridad con recomendaciones de estándares internacionales de las normas ISO 27001 E 27002.	**Corporación Jarrín Herrera Cía. Ltda. JAHER** (GUAPULEMA MARTÍNEZ, 2017)	La propuesta de dotar al comercial JAHER de la ciudad de Babahoyo del Sistema COBIT5 como herramienta para detectar errores y señalar los fallos en los procesos de auditoría informática es certificada y validada por dos profesionales expertos en ramas similares, los cuales se encargaron de la revisión y aprobación de la misma ellos afirmaron que es un aporte útil, valioso y adaptable a la empresa JAHER. Por lo cual se efectuaron las validaciones pertinentes con la finalidad de comprobar que los requerimientos que se analizaron para el desarrollo de la investigación son los correctos y que la propuesta cumple con las necesidades estipuladas por la institución.	**Corporación Educativa Virgen del Perpetuo Socorro, Tumbes.** (Palacios Marchan, 2018)	Nivel de factibilidad de implementación de procesos basados en ITIL, en la Tabla N° 28 se observa que el 88% indicaron que SI es factible la implementación de ITIL en su organización, esté resultado es similar a García y Gavilanes (1), obteniendo de las personas encuestadas un resultado del 100% que si es factible la implementación de ITIL, obteniendo una similitud entre ambas organizaciones.
GAD Municipal de Milagro. (Paguay Lema & Zamora Arana, 2017)	La norma ISO 27001 es más rentable debido que es más barata, a su vez cuenta con tres factores de suma importancia que son la disponibilidad, confidencialidad y la integridad, teniendo en cuenta que la Norma ISO 27001 cuenta con las políticas y planes de acciones que ayudarán a tener más segura la información del GAD Municipal de Milagro.	**GESTIÓN DE LA TI EN LA EIS** (Vargas García, 2015)	Según el análisis realizado por los estudiantes el 25% se está aplicando COBIT 5 en las Tecnologías de la EIS y el 75% se mejora aplicando la metodología desarrollada fundada en COBIT. Se logra un gran paso en la victoria de las brechas de la administración de las Tecnologías de la Información basándose en estándares y normas de calidad, con un buen beneficio de las tecnologías a disponibilidad de los usuarios TI en la EIS.	**Departamento de sistemas de la Universidad Politécnica Salesiana SEDE Guayaquil** (García Correa & Gavilanes Balarezo, 2015)	La situación inicial contra la situación actual en la medida que se haya dado mejoras a través de la revisión de los resultados de los indicadores de Gestión implementados. Comprende la revisión de resultados en: Mejorar el desempeño de la Organización, Aumentar la satisfacción del cliente, Generar cultura de calidad en la organización, Mantener los procesos actualizados y constantes mejoras.

Fuente: Grupo Investigador.

Mediante la investigación realizada sobre las empresas que utilizaron las diferentes normas ISO, COBIT e ITIL, se realizó un cuadro comparativo de los resultados obtenidos al accionar una gestión, y hemos percibido que la ISO 27001 es una norma efectiva para aplicar, que ayudaría a cumplir a cabalidad con los requerimientos.

Así mismo podemos decir que, al comparar los modelos de políticas de seguridad informáticas de las empresas antes mencionadas, que utilizaron la norma ISO 27001 y al percibir sus resultados, según nuestra perspectiva hemos visto conveniente generar un tipo de modelo diverso, de política de seguridad informática que cumpla con las necesidades.

8.2. MARCO REFERENCIAL (PRT)

Según (Cristancho Lopez, 2018)el Municipio de Guachetá – Cundunamarca, basado en la norma ISO/IEC 27001:2013, menciona que "La información de la entidad está expuesta y a base de eso utilizaron como metodología de análisis de riesgo MAGERIT V3. Se generó un formulario de riesgo, teniendo presente la frecuencia y el impacto que genera las amenazas hacia los activos de la información de la entidad, donde actualmente arroja un riesgo intransigente de los activos de información lo que lleva acabo a la aplicación de los controles de una norma ISO 27001:2013, para así implementar políticas de seguridad para salvaguardar además de proteger la información y los activos informáticos, aprobando la confidencialidad, disponibilidad e integridad de la información".

La finalidad de las políticas ISO 27001 es proteger los activos de la información contra las amenazas que puedan ocurrir y así no pierdan la confidencialidad e integridad de las empresas.

Según (Zura Chala, 2015) relata que "En el Municipio de Otavalo abarca un diseño de modelo de seguridad de multicapa, también conocido como defensa a profundidad, para lo cual será aplicado en tres niveles: donde el primer nivel de usuario ayudará a elaborar un Manual de Normas y Procedimientos de seguridad de información en relación con la Norma ISO/IEC 27002 el cual está socializado con el administrador de red hacia los usuarios, en otro punto está el nivel de red la cual posee un nivel jerárquico. De igual forma en la red perimetral por tanto esta herramienta sirve para el descubrimiento de intrusos basados en motores Suricata bajo una plataforma unida llamada SELKS de esta manera podremos utilizar algunas de las siguientes sugerencias que nos detalla dicho autor siguiendo la

metodología OSSTMM 3.0 de análisis de riesgos utilizando métricas operacionales de seguridad".

La norma ISO está orientadas a ordenar la gestión de una empresa en sus distintos ámbitos, donde están compuestas por estándares, guías y herramientas que ayudan a proteger la información de las organizaciones.

Según (Briñez Bautista, 2017) señala que "La Alcaldía Municipal de Jugua de Ibérico mediante la metodología MAGERIT, describe el diseño metodológico para la implementación de la seguridad informática para construir un proceso de implementación la cual exige cambios como cultura y la organización de la entidad. Esta opción es primordial para proteger la información, pues tiene como objetivo principal proteger dicho activo a través de controles y políticas de seguridad".

El manejo de la metodología MAGERIT minimiza los riesgos del uso de las tecnologías de información por la cual permite saber cuánto valor está en juego para poder ayudar a proteger.

Según (Fernández Villacrés & Martínez Campaña, 2017) alude que "En el GAD cantonal de Pastaza utilizaron una herramienta proporcionada por Microsoft denominada Herramienta de Evaluación de Seguridad de Microsoft (MSAT). Finalmente, dicha herramienta es utilizada en todo mundo para la gestión de riesgos informáticos, relacionada con los parámetros de la norma ISO 27001, 27002, y 27005 visto que con dicho resultado se ha logrado generar el Plan de Seguridad de la Información, para lo cual ayudo a mejorar los controles internos de la entidad relacionada con la seguridad informática. Esto aplicando la metodología PDCA, Planificación - Ejecución - Evaluación – Actuación (en inglés, PDCA de Plan-DO-Check-Act) es una secuencia cíclica de actuaciones que se hacen a lo largo del ciclo de vida de un servicio o producto para planificar su calidad".

La herramienta MSAT analiza las debilidades o puntos de mejora en el ámbito de seguridad de cualquier empresa, de esta forma el MSAT examina los riesgos, en diferentes áreas realizando así un análisis de defensa a profundidad.

Según (Montealegre Alvarez, 2018) menciona que "la alcaldía Municipal de Tame tuvo el propósito de crear políticas de seguridad en vista que cuenta con un sistema de información, pero no cuenta cómo protegerla y esta podría perderse siendo el activo más importante de una empresa."

Actualmente las políticas de seguridad normas y directrices que permiten garantizar la seguridad de la información de las organizaciones.

Según (Diaz Coral, 2015) indica que "el Municipio de Pasto expone que no cuenta con la implementación de un sistema de gestión de seguridad de la información, de modo que sea han propuesto como su principal objetivo identificar las vulnerabilidades, riesgos y amenazas a las que pueden estar expuestos el Municipio y afecte su buen funcionamiento esto con la ayuda de la metodología MAGERIT, para concientizar a los responsables de la información que pueden existir riesgos y poder preparar a la organización para un proceso de auditoría, acreditación o certificación según sea el caso."

MAGERIT ayuda a resolver todas las gestiones de riegos que presentan en las empresas mediante un análisis sistemático para mejorar la calidad y excelencia de las empresas tanto públicas como privadas.

Según (Almeida Suarez, 2017) alude que "la Cooperativa de Ahorro y Crédito "San Antonio" de la Unión se evidenció la falta de evaluación de riesgos, que se basó en dos tipos de investigaciones tales como de campo y la bibliográfica. Por lo cual se aplicó la metodología de las Normas ISO 27001, puesto que es un papel muy importante que abarca a todas las empresas u organizaciones que permite salvaguardar la integridad, privacidad y la confidencialidad de la información."

La norma ISO 27001 nos habla de cómo evaluar los riesgos de la información que puede estar impresa o en digital por ende puede ser confidencial, restringida, etc., de esta manera ayuda a mejorar la gestión de riesgos de seguridad de la información de las organizaciones.

Según (Palacios Portilla, 2015) menciona que "la Cooperativa del magisterio de Túquerres, se evidenció la falta de las políticas además de mecanismos que ayuden a proteger su integridad, disponibilidad y confidencialidad, por tanto es muy perjudicial pues poseen 7.000 asociados en constante crecimiento lo que implica tomar medidas para evitar posibles riesgos y no cause grandes pérdidas económicas, con ello también daño a su reputación y potencial. Por esta razón se plantean como solución, el diseño de un sistema de gestión de seguridad de la información en el área de informática de la Cooperativa del magisterio de Túquerres, con la metodología de la norma ISO 27001:2013."

En las instituciones públicas o privadas la Norma ISO 27001, es importante dado que minimiza los riesgos de pérdida de información o ataques cibernéticos, de esta forma algunas

empresas aplican políticas de seguridad informática para optimizar la privacidad de la información.

Según (Ruiz Peña, 2018) menciona que "la Cooperativa Multiactiva ubicada en Bogotá, el personal de Sena encuentra ausencia de mecanismos para proteger la información, de modo que se diseñó políticas de seguridad a fin de generar comprensión y conciencia, del valor e importancia que posee la información que se maneja en la Cooperativa, por ende en COOPSENA las políticas se las diseñara bajo la metodología del estándar ISO/IEC 27001:2013 cuyo resultado permiten optimizar el tiempo para establecer las salvaguardas destinadas a minimizar, controlar y evitar un impacto potencial en el futuro además facilita el proceso de gestión de riesgos."

La ISO 27001 es la norma que establece la implementación de los sistemas de gestión de la seguridad de información, debido que esta norma permite certificar al conocer si cumple con todos los requisitos de seguridad de la información.

Según (Alcivar, 2017) alude que "la Cooperativa La Benéfica Ltda., no se rigen a estándares internacionales que forman los sistemas de gestión de seguridad de la información, en consecuencia tienen carestía en las medidas de un plan de seguridad de la información basada a las buenas prácticas como es la metodología ISO 27001, como resultado menciona que la puesta en funcionamiento de un SGSI garantiza la ejecución del conjunto de procesos que gestionen la accesibilidad de la información."

En los SGSI se define como un proceso sistémico, organizado y documentado que sirve para implementar y gestionar la seguridad de la información en una organización buscando mantener la confidencialidad, integridad y disponibilidad.

Según (Gallegos Montero, 2015) alude que "la Cooperativa de Ahorro y Crédito Nuevos Horizontes de la ciudad de Machala, presentaba varios problemas relacionados con el área de seguridad de la información tales como falta de controles y procedimientos para el aseguramiento de los datos y los equipos de soporte. De forma empírica se trataba de dar solución a las deficiencias que se presentaban en la organización, pero a su vez quedaban expuestos a los procesos y activos de la información a una serie de amenazas y vulnerabilidades. Con lo expuesto surge la necesidad de analizar, diseñar e implementar un Plan de Gestión de la Seguridad de la Información utilizando la norma ISO 27001 y la metodología de mejora continua PDCA (Planificar, Hacer, Verificar y Actuar). Con la

realización de dicho proyecto de titulación se logró mitigar los riesgos de pérdida, robo o corrupción de información; también se estableció un documento guía de buenas prácticas aplicadas en beneficio de toda la organización para los procesos, usuarios y clientes de la entidad."

La norma ISO 27001 y el PDCA sirve para mejorar la calidad y la productividad en cualquier nivel jerárquico en una organización, esta norma ISO 27001 permite el fortalecimiento de la confidencialidad e integridad de la información de las organizaciones.

Según (Villegas Chiliquinga, 2017) menciona que "la Dirección de Aviación civil del Ecuador (DGAC), ha generado una evaluación y análisis de la información obtenida para verificar la vulnerabilidad existente en la red de datos, así como también evidencia la falla en los procesos que se generan en dicha institución. Basado en las normas de la ISO/IEC 27001, para describir la Política de Protección de la Información, basada en la seguridad de los datos y que en las instituciones no deben trabajar personas que no tengan registros de identificación, así como también cada administrador de red debe poseer claves de acceso para la protección de la infraestructura de datos y de la comunicación."

Las vulnerabilidades en las empresas ocasionan perdidas de la información y daño a la integridad de la institución en virtud a esto las normas ISO 27001, son aptas para toda institución la cual ayuda a prevenir robo de la información o ataques que dañen a las organizaciones.

8.3. ASPECTOS TEÓRICOS CONCEPTUALES

8.3.1. Active Directory

El uso del Active Directory por parte de las empresas en una práctica muy habitual hoy en día. "Es un repositorio de red donde se puede obtener información acerca de lo encontrado en la red como puede ser usuarios, permisos, asignación de recursos y políticas de acceso, surge con la necesidad de validar los usuarios que están en la red, esto con el fin de ofrecer el servicio solamente a usuarios autorizados de hecho, el directorio es una lista de usuarios y recursos de red donde indica a los autorizados a utilizar. Este directorio activo acepta numerosos atributos para cada clase de objeto que se utiliza para recopilar gran cantidad de información. Al tener una sola fuente de información hace el proceso más eficiente y accesible" (Castro Ortega, 2015).

Active Directory básicamente posee una base de datos que está estructurada jerárquicamente, la cual está compuesta de carpetas que permite seguir expandiendo y accede a trabajar con muchas carpetas más que estén formadas por dominios.

8.3.1.1. Estructura Lógica del Active Directory

Según (Ocampo Vélez, Encalada Vivanco, & Ing. Jaramillo Castro, 2015), menciona: "La estructura lógica del Active Directory brinda seguridad ante el almacenamiento de la información acerca de sus clientes y estos mismos pueden presentar entidades u objetos en la estructura lógica, a continuación mostramos en la Figura 1, los componentes de la estructura" (pág. 5).

La parte lógica es la estructura de las unidades organizativas, de un sitio donde se encuentran la representación de los dominios. Esta estructura comprende de los siguientes componentes:

a. Objetos

Es considerado como un objeto intangible, (Ocampo Vélez et al., 2015) indica "Se denominan como los componentes más básicos de esta estructura lógica, cada clase de objetos están definidos mediante un grupo de atributos donde definen los posibles valores a asociar y cada objeto tiene una combinación única de valores de atributos"(pág. 5).

Posteriormente objetos nos permiten representar la estructura de red física como lo son: controlador de dominio, grupos, unidades organizativas, etc., mediante este pilar se trabaja con active directory.

b. Unidades organizativas

Pueden usarse para organizar cientos de objetos, (Ocampo Vélez et al., 2015) alude "Mediante la estructura de los objetos por unidades organizativas facilita su localización y administración, como también se puede delegar la autoridad administrativa a una unidad organizativa"(pág. 5).

Las unidades organizativas son las que representan departamentos internos o los objetos en el directorio dentro de unidades administrativas de las empresas.

c. Dominio

(Reina Tovar, 2016) Determina que: “Es la unidad funcional central de la estructura lógica del Active Directory, que comparten una base de datos y conjunto de objetos definidos, directivas de seguridad y relaciones de confianza comunes con otros dominios” (pág. 72).

Dentro del análisis el dominio es una palabra, texto o el identificativo único para cada uno de las webs, de esta forma los dominios pueden tener diferentes terminaciones como: .com, .net, etc., algunos dominios son para posicionarse en determinados países como .es, .mx.

d. Árboles de dominio

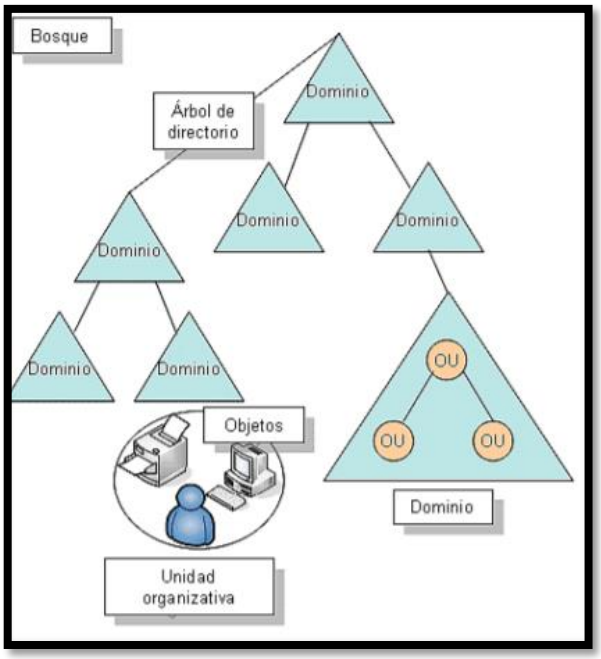
“Árboles de dominio es la recopilación jerárquica de los dominios, los comparten un espacio para nombres común. Es decir cuando se añade un registro a un árbol existente, el nuevo es un dominio hijo por lo cual existe un padre y a su vez se establece automáticamente una relación de confianza” (Vera Castro & Zambrano Zambrano, 2017).

Los árboles de dominios son uno o más dominios que comparten un espacio de nombres DNS contiguo, es decir que cuando se crea diferentes dominios dentro de un mismo árbol automáticamente se genera una confianza entre padres e hijos por lo cual se puede ingresar sin ningún problema.

e. Bosques

Consta de uno o varios árboles es considera como una instancia completa de Active Directoy, es un árbol que se recomienda a la mayoría de organizaciones pues tiene dos niveles y todos los dominios secundarios se convierten en dominio raíz para formar un árbol adyacente. El nombre de ese dominio hace referencia al bosque por ejemplo nwtraders.msft (Gómez Gómez, 2015).

Figura 1: Imagen de Bosques.



Fuente: Lenin Sebastián Ocampo Vélez, Paúl Henry Encalada Vivanco, & Ing. Carlos Miguel Jaramillo Castro, 2015.

Finalmente se menciona que el bosque es una colección de uno o más dominios y por ende posee un único esquema, donde cuentan con relaciones de confianza automática de dos vías y transitivas.

8.3.1.2. Estructura física del Active Directory

"Se usa para configurar y administrar el tráfico de red, además es un componente del Active Directory para así entender los componentes de la estructura física es importante, para optimizar el tráfico de red y el proceso de login" (Vera Castro & Zambrano Zambrano, 2017).

Esta estructura se divide en los siguientes temas importantes:

a. Sitios

"Consiste en la forma que se replicara la información de directorio y como tratar las solicitudes del servicio de equipos los que son estipulados a sitios, esto mediante la combinación de una o más subredes IP conectadas a alta velocidad" (Hernández Mendoza, Martínez González, & Martín Jaime, 2016).

Un sitio indica el método de configuración de las topologías y de las replicaciones con el directorio activo, para así obtener todas las características de la Red Física.

b. Controlador de dominio

Consiste del lugar donde almacena una copia del directorio, almacenan datos, administran las interacciones entre el usuario y el dominio, autenticación, los procesos de inicio de sesión igualmente las búsquedas de directorio como los cambios del directorio asimismo los replica a otros controladores de dominio que sean del mismo dominio (Hernández Mendoza et al., 2016).

A pesar de todo, los controladores de dominio son los sistemas operativos de Windows que guarda las contraseñas en los archivos de SAM, dicho esto el controlador es el eje central de un dominio de Windows.

8.3.2. Acceso a internet

Según (LACNIC FRIDA, 2020), menciona que "el uso de internet en América Latina y el Caribe posee un aproximado de un tercio de la población que sigue sin tener acceso a internet", en una investigación realizada se evidencio que en el año 2019 el porcentaje de las personas que utilizan el internet aumento a un 3,3 puntos porcentuales a nivel nacional (INEC, 2020), esto quiere decir que la sociedad ecuatoriana está evolucionando en términos de consumo de internet, como también compra y manejo de medios digitales.

El acceso a internet es la conexión entre un computador, dispositivos móviles, red de computadoras o hacia otros tipos de dispositivos que sirven para conectarse a internet.

Figura 2: Uso de las personas que utilizan internet.

Fuente: Elaboración propia, con base en los datos de la Encuesta de Calidad de Vida 2012-2019. Instituto Nacional de Estadística (INEC).

8.3.3. Respaldos

A continuación, se describirá los tipos de respaldos que son en gran mayoría altamente indispensables en una organización.

a. Respaldos completos.
b. Respaldos incrementales.
c. Respaldos diferentes.

8.3.3.1. Respaldos completos

Según (Morales Choez, 2016), este tipo de respaldo se caracteriza por que cada uno de los archivos son escritos o almacenados a medida en que se vaya ejecutando los respaldos (pág. 22).

Los respaldos son la copia total de toda la información que se realiza de los ordenadores que poseen las entidades.

8.3.3.2. Respaldos incrementales

(Morales Choez, 2016) menciona: “En este tipo de respaldo se caracteriza por que proceden a comparar en primer lugar la fecha de modificación del activo reciente fue diferente a la que registra como última modificación y a continuación procede actualizar y modificar el registro” (pág. 22).

Los respaldos incrementales son las copias de informaciones creadas y modificadas por las personas desde la última elaboración, las cuales se puede realizar respaldos tanto incrementales como completos.

8.3.3.3. Respaldos diferenciales

Este tipo de respaldo es semejante al incrementar, puesto que copian archivos que han sido modificados, (Morales Choez, 2016) afirma: “este se caracteriza también por ser acumulativo lo que significa que este contiene todos los archivos modificados desde el último respaldo completo” (pág. 23).

Se recomienda para la propuesta SyncBack que es un software que sincroniza y copia las carpetas y archivos, haciendo seguro y sencillo la forma de respaldar la información. Trabaja mediante perfiles o trabajos, ofrece ciertas reglas para evitar conflictos con nombres pre existentes y ofrece Mirror que es una operación uni direccional que crea una copia de

seguridad idéntica del directorio de destino del director fuentes, cuenta con una función de filtro que permite limitar que archivos son copiados.

8.3.4. Privilegios de las cuentas de usuarios

Según (Collazo Linares, 2017), cualquier usuario con privilegio es vulnerable al contagio de algún virus informático, lo que se intenta es aplicar privilegios para minimizar la infección y propagación de los virus, con estos privilegios también se desea poner límites al acceso a la información, ya sea para editar la información y configuración de los usuarios a veces guardan la información en accesos públicos, siendo una debilidad en la seguridad de la información.

En definitiva, el privilegio de cuenta de usuarios es la colección de información que muestra al sistema operativo a realizar acciones como crear carpetas en un directorio, acceder a un dispositivo o para poder leer o borrar archivos.

8.3.5. Delitos informáticos

Los delitos informáticos según (Chungata Cabrera, 2015) relata que "se realizan con la ayuda de los sistemas informáticos, pero tiene como objeto el injusto la información en sí misma, por ende se determina como delito informático al comportamiento antijurídico, no ético o no autorizado". pág. 20.

Los delitos informáticos es aquella persona propia o ajena a la institución, que ingresa a la información con intensiones maliciosas y alteran o borran dicha información. Existen otras maneras en las que, mediante aplicaciones u archivos, ingresan a los ordenadores para robar la información o para eliminarla.

8.3.6. Tipos de delitos informáticos

Existen diversos tipos de delitos informáticos, en la que influyen factores como la imaginación de autor y su capacidad técnica para poder elaborar estrategias con un fin.

8.3.6.1. Caballo de Troya (Manipulación de Programas)

El autor (Acurio Del Pino, 2016), menciona que "Este delito consiste en modificar los programas existentes en el sistema de computadoras o en insertar nuevos programas o rutinas, el método común es insertar instrucciones de computadoras de una forma encubierta en un programa informático". pág. 23.

Este delito informático debe tener gran conocimiento en programación, pues este insertara rutinas o instrucciones en el ordenador de manera encubierta disfrazado de un programa, esta situación a menudo pasa inadvertida.

8.3.6.2. Pishing

Según (López Sánchez, 2019) el "phishing es la estafa en la que se hace el uso de los métodos de la ingeniería social para traicionar a los usuarios con el fin de lograr la información o algún beneficio de manera ilícita y rápida".

El phishing es obra de las formas en las que personas mal intencionadas mediante ventanas emergentes en las páginas web, diseñadas para robar la información de un usuario como puede ser contraseñas e información de cuentas o de otros datos personales.

8.3.6.3. Bombas lógicas

Según (Chungata Cabrera, 2015) menciona que "Logic Bombs se produce a través de la introducción de un programa que se ejecuta en un momento o fecha específica consecutivamente, al cumplirse las determinadas condiciones alterando el funcionamiento de los sistemas ya sea destruyendo o modificando la información". pág. 36.

Para la construcción de estas bombas lógicas se requieren conocimientos en programación, estas bombas cuando explotan causan gran daño, de modo que piden rescate a cambio de dar a conocer donde se encuentra esta bomba antes que ocasione grandes daños.

8.3.6.4. Gusanos

El autor (Chungata Cabrera, 2015), menciona que "los gusanos son parecidos a los virus pero tienen la diferencia que su finalidad es infiltrarse en programas para así modificarlos o destruir los datos contenidos en el mismo posteriormente su cometido no puede multiplicarse ni infectar otros archivos como los virus". pág. 36.

Este gusano se forma semejante a un virus y el daño que ocasiona es la modificación de datos o su destrucción, en ciertos casos estos gusanos dan instrucciones de transferencias continuas de dinero a una cuenta ilegal.

8.3.6.5. Fuga de datos

(Chungata Cabrera, 2015), nos relata que "la fuga de datos consiste en la lectura, sustracción o copiado de información confidencial o de datos reservados". pág. 38.

Es la propaganda de información que maneje en una organización, esto se ocasiona cuando no existen restricciones de acceso en el personal, de este modo es importante definir y controlar el acceso a cierta información que suele ser confidencial. Una forma sencilla para proteger es la criptografía, la seguridad física en los departamentos y la seguridad en los ordenadores donde se encuentra alojada la información.

8.3.6.6. Hackers o Piratas informáticos

Según (Villavicencio Terreros, 2014), menciona que "son personas dedicadas, por afición u otro interés, a violar programas y sistemas supuestamente impenetrables, conocido como delincuentes silencioso o tecnológico". pág. 7.

Los Hackers son personas que realizan los ataques en un lugar externo, aprovechando las vulnerabilidades de seguridad para obtener acceso, se hacen pasar por usuarios del sistema y emplean contraseñas.

8.3.7. Por qué tener políticas Escritas

Las políticas de seguridad informáticas son medidas que toman una organización o institución para proteger la disponibilidad, confidencialidad e integridad de sus datos. Es por eso cuando la institución requiera una certificación, demanda tener esta documentación con el propósito de controlar lo que suceda en la Gestión de Seguridad de la Información, por esta razón necesitan conocer a detalle. En las cláusulas de la ISO 27001 menciona los objetivos entre los más relevantes es que sean medibles, puesto que debe tener los principios claves como:

Confidencialidad: Es decir solo las personas autorizadas pueden conocer y hacer uso de la información.

Integridad: La información que maneja la institución debe estar completa, sin alteraciones, veras y exacta.

Disponibilidad: Debe estar siempre accesible para las personas autorizadas además conocen el compromiso de cuidar, hacer buen uso y garanticen su protección.

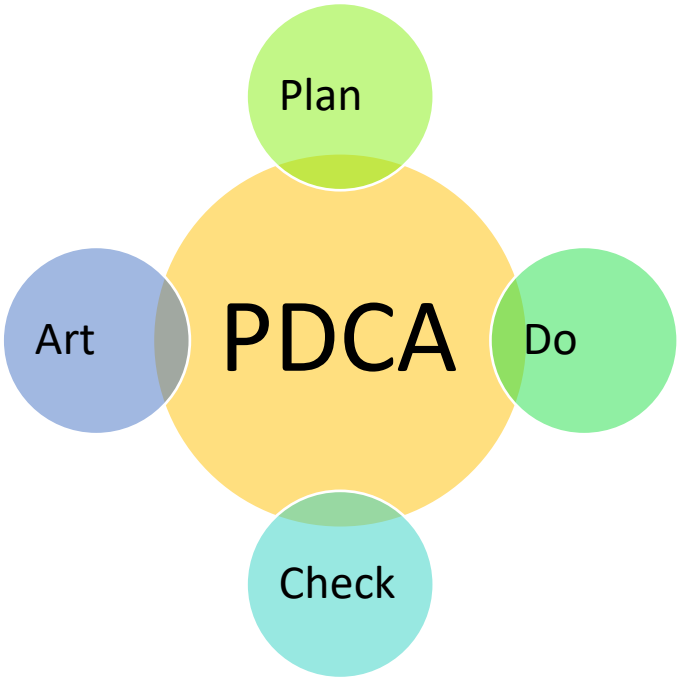
8.3.8. Sistema de Gestión de la Seguridad de la información SGSI

Para (ICA, 2018), el concepto de SGSI menciona "el ICA trabaja permanentemente en pos de implementar el SGSI siguiendo los lineamientos del Modelo de Seguridad y Privacidad

de la información – MSPI es la Estrategia de Gobierno Digital en vista que tiene como privilegio preservar la integridad, confidencialidad, disponibilidad y privacidad de la información".

SGSI sirve para asegurar la calidad como también el manejo de los activos con el fin de proteger de los ataques y amenazas durante la gestión de la información, dado que una organización debe garantizar la confidencialidad, integridad y disponibilidad. A fin de poder implementar el modelo conocido como PDCA este modelo es indispensable con la participación de todo el personal. Consta de 4 etapas con un periodo de 6 meses a 1 año.

Figura 3: Seguridad de la Información Modelo PDCA.



Fuente: Grupo Investigador.

PLAN (Planeación): Diagnostica la seguridad, toma medidas de solución y minimiza los riesgos.

DO (Ejecución): Posee una implementación, informa al personal y minimiza los riesgos.

CHECK (Mejora): Toma medidas como correctivas, preventivas y de mejora.

ACT (Seguimiento): Evalúa el éxito y posee indicadores de resultados.

8.3.9. Implementación del sistema de gestión de seguridad informática SGSI

Como implementación de un SGI se compone de los siguientes: (Mercader, 2018)

✓ Visión global define las políticas de seguridad de la información que conforman las bases del resto del SGSI.

✓ Establecimiento de una metodología de gestión de la seguridad clara y estructurada.

✓ Implicación de la organización para poder llevar a cabo un SGSI donde se requiere la implicación de toda organización desde la Dirección, hasta el usuario final.

✓ Gestión global se define los requisitos para la gestión de la seguridad de la información desde un punto de vista global.

✓ Solución viva son series de medidas o controles para gestionar el riesgo de una organización.

✓ Mejora continua permite determinar una planificación para alcanzar los objetivos en diferentes iteraciones.

✓ Control y seguimiento permite colocar una metodología de medida y evaluación mediantes indicadores, que permite evaluar los resultados obtenidos frente a los objetivos establecidos.

8.3.10. Beneficios de la implementación de un SGSI

Según (Mercader, 2018) indica que podemos citar algunos aspectos positivos de la implementación de un SGSI que aporta a las organizaciones como lo son:

Visión Global: Son las políticas de seguridad informáticas que deberán ser conocidas, aprobadas y promovidas por la dirección.

Implicación de la organización: Con el propósito de llevar a cabo un SGSI se requiere la implicación de toda la organización, desde la Dirección hasta el usuario final.

Gestión Global: Son los requerimientos para la gestión de la información, desde un punto de vista global, siguiendo criterios comunes y procedimientos homogéneos.

Solución Viva: Un SGSI no finaliza con la implementación de una serie de lineamientos para gestionar el riesgo, pues más bien es un proceso de constante revisión y actualización.

Mejora continua: Es la incorporación de nuevas iteraciones aprendida y se implementa las mejoras justificadas, esto permite su evolución paso a paso.

Control y seguimiento: Permite disponer de una metodología de medida de evaluación a fin de verificar el cumplimiento de los objetivos establecidos, para posteriormente mantener informada a la Dirección.

8.3.11. Amenazas

Menciona (Solarte, Rosero, & Benavides, 2015) el autor que “las amenazas están relacionadas con la posibilidad de que algún tipo de evento se puede presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial sobre los activos informáticos y sistemas de información”.

Es la probabilidad de que una amenaza se produzca en un equipo de trabajo, este riesgo permite la toma de decisiones para proteger la información y recursos informáticos.

Estas amenazas se pueden clasificar en función del daño, intervención o tipo de alteración que puede sufrir la información, estas pueden ser:

Modificación: A más de que personas o programas que no autorizados acceden a la información, estos realizaran alteraciones en la misma retrasando las actividades de la Institución.

Interpretación: Es decir que personas, programas o equipos obtendrá información relevante y confidencial de la organización, así como a programas.

Interrupción: Tienen como principal objetivo deshabilitar el acceso a la información, como bloquear el acceso a los datos.

Fabricación: Es agregar datos fabricados o falsos, a la información del sistema de una Institución.

Estas amenazas también se pueden clasificar según su origen, estas pueden ser accidentales o intencionales.

Accidentales: Es decir ante un incendio, fallos de los equipos, software, errores humanos, entre otros.

Intencionales: Cuando la acción humana es con fines maliciosos, esta introduce malware, software malicioso o intrusión informática.

8.3.12. Seguridad informática

El autor (Romero Castro et al., 2018), menciona que “La seguridad informática se encomienda de la seguridad del medio informático, según diferentes autores la informática

es la ciencia comisionada de los procesos, técnicas y métodos que buscan procesar, almacenar y transferir la información."

Desde el punto de vista la seguridad informática con sus diferentes estrategias lleva a cabo la detección de usuarios o programas no autorizados de un sistema informático, para cumplir con su objetivo principal que es proteger la información.

8.3.12.1. Tipos de seguridad informática

Activa: Es el conjunto de medidas que se toman, con la finalidad de controlar el acceso a información confidencial o privada que se maneje en una organización.

Pasiva: Son las medidas que se toma una vez producido el incidente de seguridad, con el fin de minimizar su repercusión y facilitar la recuperación.

8.3.13. Importancia de la seguridad informática

La importancia de la seguridad informática abarca tanto para los directivos en vista que tienen una gran responsabilidad de generar la política y así minimizar la prevención de todos los procesos informativos y tecnológicos (García Pierrat & Vidal Ledo, 2017).

En términos generales la importancia de la seguridad informática en las organizaciones cumple un papel significativo que sirve para proteger la información y los datos.

8.3.14. Seguridad de la información

Para (ISOTools Excellence, 2017), la ilustración de seguridad de la información contribuye a un método "que se encarga de la implementación técnica de la protección de la información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando dicha información es el activo que se encuentra en riesgo o amenaza."

Actualmente la seguridad de la información puede tomar medidas preventivas como reactivas para las organizaciones, asimismo sistemas tecnológicos que ayudarán a resguardar y proteger la información de la empresa.

8.3.15. Mecanismo de seguridad

Se clasifican según la función que desempeñe los mecanismos de seguridad, estos son:

Preventivos: Actúan antes que se produzca un ataque, su misión es evitar que ocurran.

Detectores: Actúa cuando el ataque se ha producido y opera antes que cause graves daños al sistema.

Correctores: Actúa cuando el ataque ya se dio, tiene como misión corregir los daños causados.

Estos son los mecanismos más habituales, la selección de estos mecanismos corresponde de cada sistema de información y de las posibilidades económicas.

8.3.16. Seguridad lógica

Según (Carrillo Jiu, 2014) menciona que "La seguridad lógica se refiere a la manera de generar la seguridad en el uso del software y los sistemas, a la protección de los datos, procesos y programas, así como la del acceso a los ordenadores y autorizaciones del usuario a la información". pág. 11.

Estos mecanismos y herramientas de seguridad tienen como objetivo salvaguardar digitalmente la información de una forma directa.

Control de acceso: El manejo de usuarios y contraseñas.

Cifrado de datos: Es el cifrado de datos con una clave especial donde el emisor y receptor son conocedores y cuando llega el mensaje se produce el descifrado.

Antivirus: Para la detección de virus u otro software malicioso, permitiendo eliminar y corregir daños.

Cortafuegos: Conforma de uno o varios dispositivos de hardware y software que restringen el acceso al sistema, protegiendo la integridad de la información.

Firma digital: Se utiliza para identificar de manera segura al responsable de mensajes telemáticos o documentos electrónicos, permitiendo proteger la integridad y confidencialidad de la información.

Certificados digitales: Son documentos digitales mediante una entidad autorizada, garantiza ser quien dice ser, ratificada por la verificación de su clave pública, de esta forma se protege la integridad y confidencialidad de la información.

8.3.17. Seguridad física

"Es el área de seguridad física posee acciones para proteger las propiedades tanto de los personales como de los activos de las organizaciones". (Cerrar, 2019)

Se dividen en dos fases las cuales son:

Humano: Su principal objetivo es realizar pruebas de seguridad para controlar la concienciación respecto a las responsabilidades y seguridad personal.

Físico: Tiene como objetivo realizar pruebas para intentar romper las barreras físicas y lógicas de las organizaciones.

8.3.18. Activos de la información

El propósito del activo son los bienes, derechos y otros patrimonios que cuenta la empresa por ejemplo: muebles, construcciones, aplicaciones, software del sistema, servicios informáticos, equipos de comunicación, equipos informáticos o derechos de cobro de servicios prestados o venta de bienes a clientes (Figueroa Pérez & Malagón Sáenz, 2017).

Esto indica que también se cercarían aquellos de los que se espera conseguir un beneficio económico en el futuro, donde las organizaciones poseen información valiosa que desean proteger contra las amenazas o riesgos.

De este modo se menciona que son recursos que utiliza un sistema de gestión de la seguridad de la información para que las organizaciones funcionen correctamente y así obtener los objetivos que se formulan por la alta dirección.

Los activos se encuentran asociados, de forma directamente o indirectamente, con las demás entidades (Argüezo Ramirez, 2019).

Posteriormente un proyecto de seguridad tiene como propósito controlar la seguridad de dichos activos de información que se genera por el dominio en el estudio de proyectos. De esta forma el conjunto de los activos del dominio no impide la consideración de las relaciones en materia de seguridad de los activos informáticos de dicho entorno. A pesar de esto el paso principal es que la entidad debe adaptarse a la norma ISO 27001 a fin de poder llevar a cabo un inventario de los activos de la información. Los activos de la información poseen un valor para la empresa y que quedan dentro del alcance de SGSI. Puede parecer un

poco tedioso para el principalmente, por los activos que se van identificando. Es por este motivo que se decide comenzar por clasificar de alguna manera.

Los activos de información son variables, pues mañana pueden ser que la situación sean diferentes o distintas en algunas semanas, meses o años. Es por esto que es recomendable, mantener vivo el inventario de los activos que se realice. Por lo cual se debe incluir al reconocimiento del Sistema de Gestión de Seguridad de la Información. Por ello es necesario actualizar los procesos como parte de la mejora continua.

8.3.18.1. Activos de la información pura

Los activos de información pura mencionan en su investigación (Argüezo Ramirez, 2019), son todos aquellos activos de información que posee algún valor para la organización por lo cual están dentro del alcance del SGSI como mencionamos a continuación:

Tabla 3: Activos de Información - Pura.

Datos digitales	Activos tangibles	Software de aplicación	Sistemas operativos
× Personales × Financieros × Legales × Investigación y desarrollo × Comerciales × Correo electrónico × Base de datos × Unidades lógicas × Copias de seguridad	× Personal × Financieros × Legales × Investigación y desarrollo × Comerciales × Correo electrónico × Otros materiales de copia de seguridad × Llaves de oficinas × Otros medios de almacenamiento	× Propietario desarrollo por la organización × Cliente × Planificación de recursos empresariales. × Gestión de la información × Utilidades × Herramientas de base de datos	× Servidores × Ordenadores de sobremesa × Ordenadores centrales × Dispositivos de red × Dispositivos de mano e incrustados

Fuente: Grupo Investigador.

8.3.18.2. Activos físicos

Los activos físicos según (Díaz Fonseca & Ramírez Rodríguez, 2015), define a todo objeto o un bien material las cuales posee la entidad para manipular de manera óptima y sostenible sus activos.

Tabla 4: Activos de Información - Físicos.

Infraestructura de TI	Controles de entorno TI	Hardware de TI	Activos de servicios de TI
× Edificios × Centros de datos × Habitaciones de equipos y servidores × Oficinas × Armarios de red × Escritorios × Cajones × Archivadores × Salas de almacenamiento de medios físicos × Cajas de seguridad × Dispositivos de identificación × Autentificación × Control de acceso al personal	× Equipos de alarma × Supresión contra incendio × Sistema de alimentación ininterrumpida × Alimentación de potencia × Acondicionadores × Filtros × Supresores de potencia × Des humificadores × Refrigeradores × Alarmas de aire × Alarmas de agua	× Dispositivos de almacenamiento × Ordenadores de mesa × Estaciones de trabajo × Ordenadores portátiles × Equipos de mano × Servidores × Módems × Líneas de terminación de red × Dispositivos de comunicaciones × Equipos multifunción	× Servicios de autenticación de usuarios × Administración de procesos × Enlaces × Cortafuegos × Servidores proxy × Servidores de red × Servicios inalámbricos × Anti-spam × Virus × Spyware × Detección y prevención de intrusiones × Teletrabajo × Seguridad × Correo electrónico × Mensajería instantánea × Servicios web × Contratos de soporte × Mantenimiento de software

Fuente: Grupo Investigador.

8.3.18.3. Activos humanos

Según (INCIBE-CERT, 2016) menciona que los activos humanos son todas aquellas personas contratadas que tengan acceso a las organizaciones.

Tabla 5: Activos de Información - Humanos.

Empleados	Externos
× Personal y directivos × Participar los que tienen roles de gestión como altos cargos × Arquitectos de software y desarrolladores × Administración de sistemas × Administración de seguridad × Operadores × Abogados × Auditores × Usuarios con poder × Expertos en general	× Trabajadores temporales × Consultores externos × Asesores especialistas × Contratistas especialistas × Proveedores × Socios

Fuente: Grupo Investigador.

8.3.19. Vulnerabilidad

Desde el punto de vista la vulnerabilidad es el punto débil de la seguridad informática. Esto indica que a través de esta se pueden presentar amenazas que pongan en riesgo la confidencialidad e integridad de la información, para ello se realizó un análisis con el fin de identificar el tipo y el nivel de cada vulnerabilidad que poseen las organizaciones.

8.3.19.1.Tipos de vulnerabilidades

Física: Es la que afecta la infraestructura de la organización de manera física (Romero Castro et al., 2018), esto indica que tiene la eventualidad de acceder al sistema directamente desde cualquier equipo para extraerle información, alterarlo o destruirlo.

Natural: En cuando a la vulnerabilidad natural permite estimar la posibilidad de que el sistema sufra daños por causas del ambiente o de desastres naturales como: incendios, terremotos, inundaciones, tormentas, etc. (Romero Castro et al., 2018).

Software: También destacada como bugs (error de software), donde tiene la posibilidad de que el sistema sea comprensible debido a daños en el diseño de software que puede tener las empresas (Romero Castro et al., 2018).

Humana: En este literal como error humano los administradores y usuarios del sistema poseen una vulnerabilidad dado que tienen acceso a una red y a los equipos de las instituciones (Romero Castro et al., 2018).

8.3.20. Estimación de riesgo

Según (Guanoluisa Huertas & Maldonado Soliz, 2015), nos relata que "permite determinar cuáles serán los factores de riesgo que potencialmente tendrá un impacto significativo dentro de la organización". Finalmente, una vez que se haya identificado los activos sus vulnerabilidades y las amenazas a las que están expuestos como siguiente paso es estimar el riesgo, esto permitirá determinar los controles que se debe implementar en el sistema.

De esta forma el riego es una probabilidad a que una amenaza explote alguna vulnerabilidad y ocasione algún tipo de daño en los activos para los cuales existen 3 tipos de métodos para estimarlo como:

- ✓ Cuantitativos: Asignan un valor numérico y por lo tanto fácilmente medible.
- ✓ Cualitativos: Describe el riesgo con palabras.
- ✓ Semicuantitativos: Clasifican los riesgos con adjetivos: altos, medios y bajo.

De esta manera se puede utilizar dos métodos las cuales son: cuantitativos y semicuantitativos, pues generan un análisis más detallado y por lo tanto más confiable para las empresas. Se puede usar también un método cualitativo solo cuando no se puede hacer un análisis detallado o cuando no se pueda cuantificar la amenaza por falta de tiempo.

8.3.21. Controles de seguridad

El presente menciona que se establece las acciones técnicas implementadas en la infraestructura tecnológica y sistemas de información (Benjamín, 2017), donde se basa en un sistema de gestión de información y eventos de seguridad (SIEM) de tal manera que posibilita aumentar la efectividad de los controles implementados disminuir la complejidad de la gestión de la seguridad de la información.

Es esencial que todas las empresas conozcan cómo proteger su información en contra de ataques informáticos.

Por estas razones los controles de seguridad tienen como objetivo acciones que se utilizan para minimizar el riego (Bermúdez Molina & Bailón Sánchez, 2015), de filtrar datos y de organización a través del cuidado de accesos, cifrado, telecomunicaciones además operativos con estos controles se puede decir que la información está segura contra ataques autorizados.

a. Control de acceso: Este tipo de control utiliza procedimientos que sirve para la asignación de accesos y privilegios al personal autorizado a un área específica validando la identificación por medio de diferentes tipos de lectura, a su vez controlando el recurso de la empresa (Mora Pérez, 2016). pág. 13. De igual forma la asignación se realiza a través de los siguientes:

- ✓ Información confidencial para la autentificación del sistema.
- ✓ Gestión de contraseñas del usuario.
- ✓ Uso de software para la administración de los sistemas.
- ✓ Gestión de los privilegios de los usuarios.

b. Control de cifrado: Según (Guerra Guzmán, 2019) dice que está diseñada para proteger la confidencialidad e integridad de la información mediante del lenguaje convenido utilizando claves o cifras numéricas, esta ciencia enseña a realizar cifrados también conocidos como códigos secretos fundados por los criptógrafos. pág. 24.

Actualmente existen programas que encriptan el contenido la base de datos con el fin de que no sean entendibles por atacantes en caso de que puedan acceder a la información de las entidades públicas y privadas. Finalmente, solo aquellos usuarios que tengan el código de encriptación podrán ver los contenidos.

c. Control de telecomunicaciones: (Cortéz Rodríguez & Santiago Cueva, 2018) menciona que parte de la base de datos la mayoría de los intercambios de información y de datos en distintas escalas que se llevan a cabo mediante las redes sociales, garantiza la seguridad además protege de forma adecuada los medios de transmisión. pág. 37

Este control permite proteger la información que se comunica por las redes telemáticas que gestionan el flujo de datos a través de lo siguiente como:

- ✓ Control de red.
- ✓ Acuerdos de intercambio.

- ✓ Protección de la mensajería electrónica.

De esta forma existen software que monitorean la red: LAN, WAN que informan al sistema cualquier flujo no autorizado. Un ejemplo de este tipo de controles son los cortos fuegos, que prohíben el acceso de páginas web no autorizadas y que utilizan la red para extraer la información confidencial de las empresas.

d. Control de operación: Tiene un marcado componente técnico entra de en todos los aspectos disponibles como la protección malicioso, copias de seguridad, control de software en explotación, etc. (Cortéz Rodríguez & Santiago Cueva, 2018) pág. 37.

Las empresas cuando se requiere cambios en el sistema, de este modo verifican los cambios y gestiona la copia de seguridad de la información de la empresa. Para funcionar adecuadamente el control hace uso de los siguientes recursos como:

- ✓ Gestión de cambios.
- ✓ Separación de entornos de desarrollo prueba y producción.
- ✓ Detección de código malicioso.
- ✓ Respaldo del sistema.

Para realizar un cambio en el sistema es necesario respaldar la información para recuperarla posteriormente, en caso de perder la información, dicho esto el control ayudará a recuperarla y evitará así acciones legales que afecte a la empresa.

9. VALIDACIÓN DE LAS PREGUNTAS CIENTÍFICAS O HIPÓTESIS

Si se diseña Políticas de Seguridad Informática de acuerdo al estándar ISO 27001, entonces se podrá apoyar a la gestión de la seguridad de la información.

10. METODOLOGÍA Y DISEÑO EXPERIMENTAL

10.1. Tipos de Investigación

10.1.1. Investigación de campo

La investigación de campo nos ayudó a diagnosticar y ratificar la problemática expuesta inicialmente, extrayendo los datos directamente de la realidad a través de la entrevista realizada al encargado de Sistemas Informáticos, comprendiendo las vulnerabilidades y necesidades a la que está expuesta.

10.1.2. Investigación Bibliográfica

Mediante la investigación bibliográfica permitió revisar y recopilar información por medio de la lectura, asimismo la crítica de documentos como libros, artículos o tesis, a fin de poder sustentar nuestra investigación con el fin de obtener las bases necesarias para el desarrollo de la investigación de políticas de seguridad informáticas mediante las ISO 27001.

En virtud de lo expresado acerca de la investigación de campo y bibliográfica se puede indicar que para generar la información se realizó una entrevista, en el cual la municipalidad de Pangua colaboró con total normalidad, ayudando a resolver las inquietudes que poseíamos para la realización de la propuesta de políticas de seguridad informática. Por ende, se ejecutó la observación, esta investigación nos facilitó conocer la factibilidad en la que se encuentra la seguridad del municipio, igualmente analizar las diferentes vulnerabilidades y amenazas que podrían poseer, causando que los activos de la información no trabajen al 100%, de este modo ambas metodologías nos ayudan a mejorar la investigación.

10.2. Enfoque

10.2.1. Cualitativa

Para lograr un mayor conocimiento y poder cumplir con el objetivo de la investigación se utilizó la modalidad cualitativa, en vista que se realizó una entrevista al Ingeniero encargado de Sistemas Informáticos, logrando conocer la gestión de la información y control de los activos de la municipalidad.

10.3. Métodos de Investigación

10.3.1. Inductivo – Deductivo

Se empleó este método, puesto que la base de conceptos empleados en el marco teórico, permitió conocer a profundidad el impacto positivo que tendrá las políticas, si el GAD de Pangua considera implementar nuestra propuesta en un futuro.

10.3.2. Hipotético – deductivo

Al recurrir a este método, accederá a una teoría que comprobará que la hipótesis realizada fue verdadera o falsa, ayudando a la eficiencia de la investigación.

10.4. Técnicas de Investigación

10.4.1. La Entrevista

Para el presente proyecto de investigación fue necesario realizar la entrevista como técnica fundamental para la obtención de información de primera mano, al departamento de Sistemas Informáticos, donde se obtuvo la colaboración del encargado del departamento que proporciono información real y verídica (**Ver Tabla15**).

Lo que ha permitido conocer las necesidades de la institución, que permitirá desarrollar la propuesta de políticas de seguridad que se recomendará al Gobierno Autónomo Descentralizado Municipal de Pangua, para que tengan en consideración implementarlo en el futuro, para que ayude en el progreso de sus actividades.

10.4.2. Observación

Se realizaron observaciones en el lugar donde se va a realizar nuestra propuesta, con el fin de obtener más conocimiento acerca de ausencias existentes, a fin de poder desarrollar de mejor manera las políticas de seguridad informática (**Ver Tabla17**).

11. ANÁLISIS Y DISCUSIÓN DE LOS RESULTADOS

11.1. Análisis de riesgos en el Gobierno Autónomo Descentralizado Municipal del cantón Pangua.

11.1.1. Aplicación práctica de la investigación

Para el diseño del plan de mitigación se ha analizado los diferentes riesgos, tanto internos como externos de la institución, lo que ha permitido conocer las necesidades más allá de lo que se puede apreciar a simple vista.

11.1.2. Riesgos Internos

a) Control de acceso a equipos:

Los equipos no cuentan con solicitud de usuario y contraseña para ingresar a realizar sus actividades, por ende, tampoco tiene protector de pantalla que bloquee el acceso después de un tiempo de 3 minutos.

b) Respaldo a los equipos:

No se respalda la información de los equipos, si no existe una disposición que indique lo realice.

c) Navegación en Internet:

Algunos equipos no cuentan con restricción a ciertas páginas de internet, que no compete a sus actividades laborales, como a Facebook, WhatsApp, YouTube, entre otras.

d) Correo Electrónico:

Los funcionarios no hacen uso de su correo electrónico corporativo, el destino de la información laboral es su correo electrónico personal.

e) Datacenter:

La municipalidad no cuenta con un Datacenter, los servidores se encuentran alojados en el departamento de sistemas informáticos.

f) Seguridad física en equipos de cómputo:

Las portátiles propiedad de la institución, no cuentan con un candado cuando estas no están siendo ocupadas por los responsables.

11.1.3. Riesgos Externos

a) Control de salida e ingreso de equipos:

No se controla el acceso de equipos por parte de los visitantes, así como de los funcionarios que ingresan a laborar con sus equipos personales o equipos propiedad del municipio.

11.2. Identificación de FODA mediante Banco de preguntas

Para continuar con el plan de mitigación, se procede a realizar el análisis del FODA para identificar Fortalezas, Oportunidades, Debilidades y Amenazas, esto mediante el banco de preguntas.

Tabla 6: Cuestionario de Factores Internos y Externos.

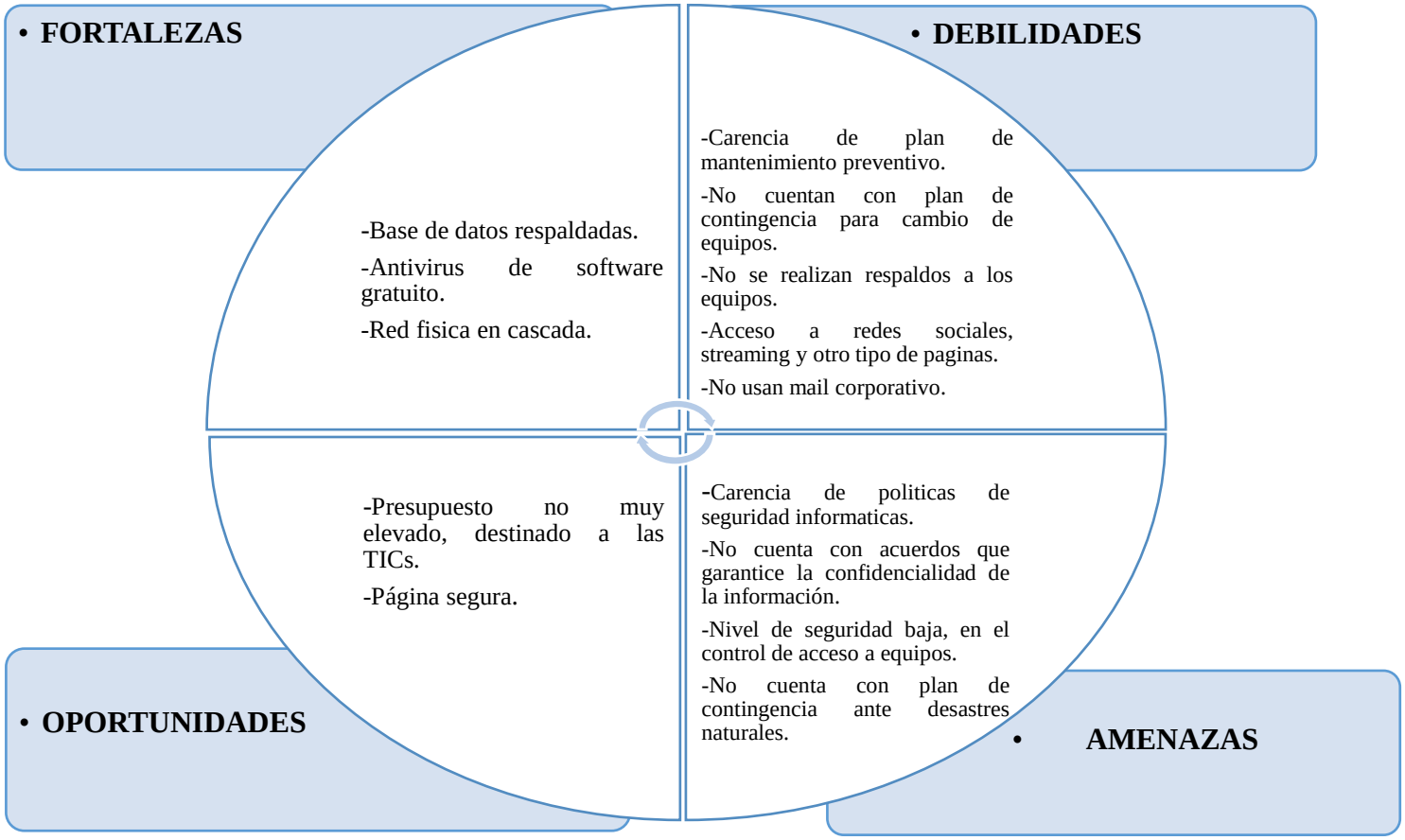
GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE PANGUA			
Entrevistado: Ing. Herman Ortiz			
Cargo: Sistemas Informáticos			
REF.	**PREGUNTAS**	**ALTERNATIVA**	**OBSERVACIONES, COMENTARIOS, ACLARACIONES**
FORTALEZAS			
1	¿Se realizan respaldos de las bases de datos?	SIEMPRE	
2	¿Cuenta con un antivirus?	SIEMPRE	Son software gratuito
3	¿Cuenta con una red física estructurada?	SIEMPRE	Cascada
DEBILIDADES			
1	¿Cuentan con plan de mantenimiento preventivo?	NUNCA	
2	¿Cuenta con un plan de contingencia para cambiar los equipos (computadoras, laptop, servidores)?	NUNCA	
3	¿Se realizan respaldos de los equipos?	CASI NUNCA	
4	¿Cuentan con listas de acceso para navegación en internet?	CASI SIEMPRE	Cuenta con restricciones, pero ciertas maquina aún tienen acceso.

5	¿Usan el dominio de email corporativo?	NUNCA	
OPORTUNIDADES			
1	¿Existe presupuesto destinado a TICs?	SIEMPRE	Existe, pero el valor no es muy elevado
2	¿La página del municipio es un sitio seguro?	SIEMPRE	
AMENAZAS			
1	¿Cuentan con políticas de seguridad informáticas?	NUNCA	
2	¿Cuentan con un acuerdo de confidencialidad de información para empleados?	NUNCA	
3	¿Cuenta con control de acceso a los equipos de cómputo?	CASI NUNCA	
4	¿Cuenta con un plan de contingencia por desastres naturales?	NUNCA	

Fuente: Grupo Investigador.

11.3. Elaboración de Matriz FODA

Figura 4: Matriz FODA.



Fuente: Grupo Investigador.

11.4. Matriz de factores Interno y Externo

Continuando como parte del proceso de la investigación realizada, se procede a realizar una matriz a los factores interno y externos, concordando con la matriz del FODA. Este proceso ayudará también a la elaboración del plan de mitigación de riesgos.

Para realizar la matriz de factores (López Carranza, 2015) explica la asignación del campo valor que corresponde al impacto que ese factor tiene, se acerca a 1 si es muy importante y 0 es de poca importancia. Así mismo el campo clasificación que corresponde al tipo de respuesta que la empresa está en capacidad de dar, va de 1 a 4, siendo 4 el nivel en el que mejor preparado se encuentra, dando valor como lo indica el siguiente cuadro:

Tabla 7: Tabla de rango de calificación de factores internos y externos.

		CLASIFICACIÓN
FACTORES INTERNOS	FORTALEZAS	ENTRE 3-4
	DEBILIDADES	ENTRE 1-2
FACTORES EXTERNOS	OPORTUNIDADES	ENTRE 3-4
	AMENAZAS	ENTRE 1-2

Fuente: (López Carranza, 2015).

Para sacar el total del valor ponderado (Yi Min Shum, 2018) menciona que se suma los valores, estos valores deben estar entre 1.0 y 4.0. Donde 1 es el valor más bajo, 4 el valor más alto y 2.5 es el valor promedio ponderado. Si el valor ponderado está por debajo de la media, significa que la marca es débil internamente, mientras si el valor ponderado está por encima, señala fortaleza.

Tabla 8: Factores Internos.

FACTORES INTERNOS			
FORTALEZAS	**VALOR**	**CLASIFICACIÓN**	**VALOR PONDERADO**
Base de datos respaldadas	0,17	4	0,68
Antivirus de software gratuito	0,15	3	0,45
Red física en cascada	0,15	3	0,45
DEBILIDADES			
Carencia de plan de mantenimiento preventivo	0,09	1	0,09
No cuenta con plan de contingencia para cambio de equipos	0,09	1	0,09
No se realizan respaldos a los equipos	0,17	2	0,34
Acceso a redes sociales, streaming y otras páginas.	0,18	1	0,18
TOTAL	**1,00**		**2,28**

Fuente: Grupo Investigador.

Análisis de la tabla 8 Factores Internos

El valor ponderado de los factores internos es de 2,28 se puede deducir que la situación no es tan favorable pues está por debajo del valor ponderado, lo que quiere decir que la empresa no tiene una fuerte posición interna. Pero se puede decir que los factores externos más relevantes y que pueden hacer una diferencia son: Los respaldos semanales a las bases de datos asimismo el contar con antivirus, estos factores internos pueden hacer competitividad.

Tabla 9: Factores Externos.

FACTORES EXTERNOS			
OPORTUNIDADES	**VALOR**	**CLASIFICACIÓN**	**VALOR PONDERADO**
Presupuesto no muy elevado, destinado a TICs	0,18	3	0,54
Página segura	0,16	3	0,48
AMENAZAS			
Carencia de políticas de seguridad informática.	0,18	1	0,18
No cuenta con acuerdos que garantice la confidencialidad de la información.	0,16	1	0,16
Nivel de seguridad baja, en el control de acceso a equipos.	0,16	1	0,16
No cuenta con plan de contingencia ante desastres naturales.	0,16	1	0,16
TOTAL	**1**		**1,68**

Fuente: Grupo Investigador.

Análisis de la tabla 9 Factores Externos

El valor ponderado la tabla de factores es externa es de 1,68 valor aún más por debajo de media ponderada, que da por conclusión que existe debilidad de igual forma en los factores externos. Existen mayores oportunidades que amenazas estos factores como el presupuesto y la página segura, puede hacer la diferencia ante otras instituciones.

11.5. Matriz para el análisis de riesgos

Según (Cárdenas Posada, Fernández Vásquez, & Hernández Aros, 2018), indica que “la matriz de riesgo se trata de una herramienta ampliamente utilizada como un proceso en la descripción organizada y calificada de sus actividades o rubros para permitir un apoyo al seguimiento y/o gerenciamiento de los riesgos.” pág. 12.

La matriz de riesgo evaluar el riesgo de una institución, por ende, se realiza un diagnostico objetivo de la situación de la institución, se calcula utilizando la formula **Riesgo= Probabilidad de Amenaza x Magnitud de Daño**.

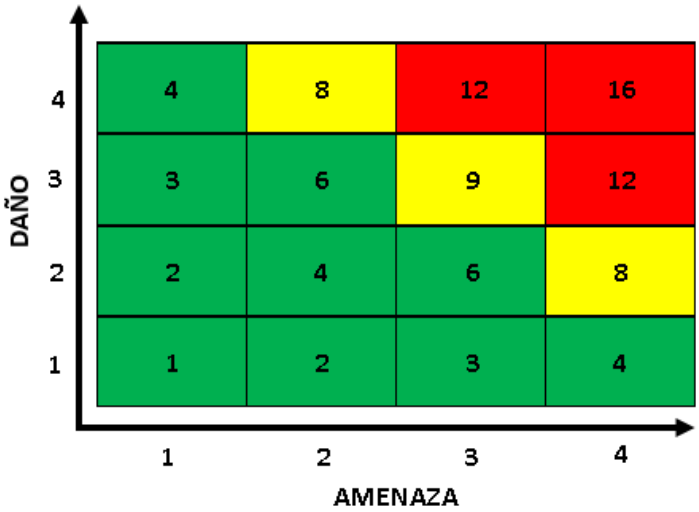
En virtud de esto, se debe realizar la identificación de las actividades principales además de los riesgos a la que puede estar expuesta. Seguidamente desde su concepción metodológica las matrices se componen de dos vectores, uno de impacto y otro de probabilidad, cuya combinación define el riesgo de un factor en particular. Estos vectores tienen valores que están en un rango de 1 a 4, en la que 1 es insignificante, 2 baja, 3 media y 4 alta, tanto para la magnitud de daño como para la probabilidad de amenaza, al multiplicar estos rangos dan como resultado el valor del riesgo que significa:

Bajo Riesgo: 1 – 6 (verde).

Medio Riesgo: 8 - 9 (amarillo).

Alto Riesgo: 12 – 16 (rojo).

Figura 5: Grafo de Riesgo.



Fuente: (Econ.Guillen Fernandez, 2017).

11.5.1. Clasificación y valoración de "Magnitud de Daño"

Clasificación: se marca con una "x", una o varias opciones a la lista, caso que no aplique se deja en blanco.

Magnitud de Daño: Se realiza la valoración según la siguiente escala:

Tabla 10: Valoración magnitud de daño.

Calificación de la probabilidad	Significado de la magnitud de daño
Insignificante	No causa ningún tipo de impacto o daño a la organización.
Bajo	Causa daño aislado, es decir que no perjudica a ningún componente de la organización.
Mediano	Provoca la desarticulación de un componente de la institución. Si no atiende a tiempo, a largo plazo puede provocar la desarticulación de la organización.
Alto	Es decir que en el corto plazo desmoviliza o desarticula a la organización.

Fuente: (Markus Erb, n.d.).

11.5.2. Valoración de "Probabilidad de Amenaza"

Consiguientemente se valora la probabilidad de amenaza que podría causar perjuicio a la confidencialidad, integridad, disponibilidad y autenticidad de la información de la institución. La tabla 7 muestra la valoración según la escala:

Tabla 11: Valoración de probabilidad de amenaza.

Calificación de la probabilidad	Significado de probabilidad de Amenaza
Insignificante	No existen condiciones que impliquen riesgo o ataque.
Bajo	Existen condiciones que hacen muy lejana la posibilidad del ataque.
Mediano	Existen condiciones que hacen probable un ataque en el corto plazo, pero que no son suficientes para evitarlo en el largo plazo.
Alto	La realización del ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

Fuente: (Markus Erb, n.d.).

En virtud de lo investigado acerca de la matriz de análisis de riesgo, se procede a realizar la matriz tomando en consideración la información que se tiene acerca del GAD de Pangua.

Tabla 12: Matriz de análisis de riesgo de datos e Información.

Matriz de Análisis de Riesgo		**Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]**																								
Sistemas de Información	**Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]**	**Actos originados por la criminalidad común y motivación política**									**Sucesos de origen físico**								**Sucesos derivados de la impericia, descuido de usuarios/as y decisiones institucionales**								
		Allanamiento (ilegal, legal)	**Sabotaje (ataque físico y electrónico)**	**Daños por vandalismo**	**Extorsión**	**Fraude / Estafa**	**Robo / Hurto (físico)**	**Robo / Hurto de información**	**Virus / Ejecución no autorizado de programas**	**Violación a derechos de autor**	**Incendio**	**Inundación / deslave**	**Sismo**	**Polvo**	**Falta de ventilación**	**Sobrecarga eléctrica**	**Falla de corriente (apagones)**	**Falla de sistema / Daño disco duro**	**Falta de inducción, capacitación y sensibilización sobre riesgos**	**Utilización de programas no autorizados / software 'pirateado'**	**Perdida de datos**	**Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas, BD centralizada)**	**Compartir contraseñas o permisos a terceros no autorizados**	**Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)**	**Transmisión de contraseñas por teléfono**	**Falta de mantenimiento físico (proceso, repuestos e insumos)**	**Falta de actualización de software (proceso y recursos)**	**Ausencia de documentación**
		3	3	3	3	3	4	4	3	3	3	1	3	3	3	3	4	3	4	3	4	4	4	4	4	3	3	3
Datacenter	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	9	9	9
Seguridad física en equipos de cómputo (Candado en Portátiles, otros)	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	9	9	9

Control de acceso a equipos de cómputo (login)	4	12	12	12	12	12	16	16	12	12	12	4	12	12	12	12	16	12	16	12	16	16	16	16	16	12	12	12
Correo electrónico	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	9	9	9
Cableado estructurado de datos	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	9	9	9
Respaldos de la información	4	12	12	12	12	12	16	16	12	12	12	4	12	12	12	12	16	12	16	12	16	16	16	16	16	12	12	12
Uso del servicio de internet	3	9	9	9	9	9	12	12	9	9	9	3	9	9	9	9	12	9	12	9	12	12	12	12	12	9	9	9
Control de salida e ingreso de equipos	4	12	12	12	12	12	16	16	12	12	12	4	12	12	12	12	16	12	16	12	16	16	16	16	16	12	12	12

Fuente: Grupo Investigador.

11.6. Análisis de riesgo promedio

La valoración de la probabilidad de amenaza según sus resultados es la siguiente:

Baja: Es decir que existen condiciones que hacen muy lejana la posibilidad de un ataque.

Mediana: Sostiene que existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo en largo plazo.

Alta: El ataque es inminente. No existen condiciones internas y externas que impidan el desarrollo del ataque.

Tabla 13: Análisis de riesgo promedio.

		Probabilidad de Amenaza		
		Criminalidad	**Sucesos de origen físico**	**Institucional**
Magnitud de Daño	**Sistemas de Información**	**10.9**	**9.7**	**12.2**

Fuente: Grupo Investigador.

Como resultado del análisis de riesgo, se percibe una probabilidad de riesgo alto con relación a criminalidad y al área de la institución, es decir que el ataque es inminente, no existen condiciones internas y externas que impidan el desarrollo del ataque. La probabilidad de amenaza en sucesos de origen físico es medio lo que significa que existen condiciones que hacen poco probable un ataque en corto plazo, pero no son suficientes para evitarlo en largo plazo. En virtud de ello se puede decir que las políticas de seguridad informáticas, son necesarias y se recomendaría al municipio tome en consideración implementarlas en un futuro, para que sus actividades no se vean afectadas.

11.7. Análisis de tráfico en la red con NethServer.

Para poder sustentar el riesgo y falta de control de acceso a las páginas de internet en horas laborables, se muestra las gráficas donde se puede apreciar el reporte de ingreso a internet de varios equipos, acerca del último mes mediante NethServer donde dicha distribución se destaca por brindar una solución modular para las expansiones rápidas de los servidores ya sea en pequeñas oficinas o medianas empresas.

Se ha visto prudente que por cuestiones de profesionalismo y con el fin de no afectar a nadie, se procedió a cubrir la IP del equipo que se realizó el reporte. Se puede apreciar que, en este equipo tiene muchos ingresos a mega.

Figura 6: Resultados de Análisis de NethServer.

User:	10.10.
Date:	Whole MONTH - 2020 Sep

Total			2.3 G	
#	Accessed site	Connect	Bytes	Cu
1	mus6.djxd.tk:443	86	242.9 M	
2	mus7.djxd.tk:443	42	112.2 M	
3	gfs204n135.userstorage.mega.co.nz:443	9	96.2 M	
4	gfs206n101.userstorage.mega.co.nz:443	11	96.2 M	
5	gfs214n124.userstorage.mega.co.nz:443	10	96.2 M	
6	gfs270n223.userstorage.mega.co.nz:443	8	96.2 M	
7	gfs208n125.userstorage.mega.co.nz:443	7	96.2 M	
8	gfs208n112.userstorage.mega.co.nz:443	6	89.9 M	
9	gfs204n122.userstorage.mega.co.nz:443	5	89.9 M	
10	gfs262n304.userstorage.mega.co.nz:443	5	89.9 M	
11	gfs302n112.userstorage.mega.co.nz:443	5	89.9 M	
12	gfs270n117.userstorage.mega.co.nz:443	3	89.9 M	
13	gfs302n103.userstorage.mega.co.nz:443	11	85.5 M	
14	gfs208n103.userstorage.mega.co.nz:443	6	84.4 M	
15	gfs206n121.userstorage.mega.co.nz:443	5	84.4 M	
16	gfs214n103.userstorage.mega.co.nz:443	4	84.4 M	
17	gfs204n113.userstorage.mega.co.nz:443	4	84.4 M	
18	r6---sn-jou-0pvs.gvt1.com	21	62.1 M	
19	mus5.djxd.tk:443	16	42.2 M	
20	gfs208n109.userstorage.mega.co.nz:443	5	39.4 M	

En este segmento del reporte perteneciente al equipo anterior, se puede observar ingreso a redes sociales y el ingreso a streaming.

45	web.whatsapp.com:443	8	3.9 M
46	mobile.pipe.aria.microsoft.com:443	579	3.7 M
47	image.tmdb.org:443	28	3.4 M
48	s.pinimg.com:443	14	3.0 M
49	pa1.narvii.com:443	3	3.0 M
50	www.sri.gob.ec:443	24	2.9 M
51	mmg-fna.whatsapp.net:443	14	2.8 M
52	ups.analytics.yahoo.com:443	390	2.4 M
53	aka-cdn.adtechus.com:443	27	2.3 M
54	download1472.mediafire.com:443	1	2.3 M
55	mus4.djxd.tk:443	1	2.3 M
56	safe-toclick.com:443	3	2.2 M
57	www.openpelis.com:443	2	2.1 M
58	www.giztab.com:443	6	1.8 M
59	www.foxdisco.info:443	29	1.7 M
60	www.pelisplay.co:443	4	1.7 M
61	urban-spartan.com	55	1.6 M
62	pm1.narvii.com:443	11	1.5 M
63	bajalogratis.com	118	1.5 M
64	static.a-ads.com	15	1.4 M
65	eckjf.dioxinsolutions.info	111	1.3 M
66	katfile.com:443	3	1.3 M
67	crowdsignal.com:443	5	1.3 M
68	miguelmart.com:443	2	1.3 M
69	pelismega.net:443	15	1.1 M
70	ads.contactociudadano.gob.ec:443	3	1.1 M
71	geo.yahoo.com:443	218	1.0 M
72	cdn.runative-syndicate.com	21	1.0 M
73	www.compudescarga.com:443	10	1 018 503
74	a.vdo.ai:443	9	992 682
75	pps.whatsapp.net:443	6	991 935
76	mega.nz:443	36	960 262
97	pelishouse.com:443	6	496 643
98	adserver.adtech.advertising.com:443	66	488 917
99	1millionbot.com:443	7	484 450
100	offerimage.com:443	7	466 075
101	iir.ai:443	8	461 176
102	signup.dainesnow.com:443	1	445 566
103	www.bajarpelisgratis.com	51	442 918
104	storage.googleapis.com	14	442 893
105	pelis24.gratis:443	6	436 417

Fuente: Programa NethServer.

En el reporte de los presentes equipos mediante NethServer, se puede observar el acceso a varias redes sociales muy populares.

Figura 7: Resultados de Análisis de NethServer.

User:	10.10.
Date:	Whole MONTH - 2020 Sep

Total			1.2 G	
#	Accessed site	Connect	Bytes	C
156	player.daznservices.com:443	10	242 635	
157	trc-events.taboola.com:443	49	237 220	
158	linkmaker.itunes.apple.com:443	72	234 864	
159	www.facebook.com:443	72	233 712	
160	dmd.metaservices.microsoft.com	100	232 400	

Fuente: Programa NethServer

Figura 8: Resultados de Análisis de NethServer.

User:	10.10.
Date:	Whole MONTH - 2020 Sep

Total			3.1 G	
#	Accessed site	Connect	Bytes	Cumula
1	updates-http.cdn-apple.com	13	1.1 G	1
2	media.fuio15-1.fna.whatsapp.net:443	854	662.3 M	1
3	mus.djcristiano.tk:443	138	170.2 M	1
4	r8---sn-jou-btxl.gvt1.com:443	5	129.8 M	2
5	global-max.opera-mini.net:443	275	119.2 M	2
6	r7---sn-jou-0pvs.gvt1.com	80	63.6 M	2
7	r6---sn-jou-0pvs.gvt1.com	36	63.5 M	2
8	sf16-webcast.tiktokcdn.com:443	6	61.7 M	2
9	v16m.tiktokcdn.com:443	65	54.7 M	2
10	r1---sn-jou-btxl.gvt1.com:443	8	47.0 M	2
11	mmg.whatsapp.net:443	137	43.0 M	2
12	r2---sn-jou-0pvs.gvt1.com:443	3	41.5 M	2
13	www.gestiondocumental.gob.ec:443	123	38.1 M	2
14	web.whatsapp.com:443	196	34.8 M	2
15	freefiremobile-a.akamaihd.net:443	23	33.0 M	2
16	mmg-fna.whatsapp.net:443	50	26.0 M	2
17	r6---sn-jou-0pvs.gvt1.com:443	6	23.8 M	2
18	pps.whatsapp.net:443	70	23.4 M	2
19	media-mia3-1.cdn.whatsapp.net:443	262	23.1 M	2
20	r3---sn-jou-0pvs.gvt1.com:443	5	14.7 M	2
21	botonpagosuniandes.edu.ec:443	332	14.7 M	2

Fuente: Programa NethServer.

En el presente reporte se puede apreciar que el equipo tiene acceso a navegación, redes sociales, mensajería y streaming.

Figura 9: Resultados de Análisis de NethServer.

User:	10.10. [redacted]
Date:	Whole MONTH - 2020 Sep

Total			3.I
#	Accessed site	Connect	Byte
1	doc-00-c8-docs.googleusercontent.com:443	1	1.5
2	trial2.autodesk.com:443	2	775.0
3	images.adsttc.com:443	45	64.7
4	r6---sn-jou-0pvs.gvt1.com	2	63.5
5	download.ccleaner.com:443	5	59.2
6	r6---sn-jou-btxl.gvt1.com:443	1	57.0
7	sdlc-esd.oracle.com:443	3	43.8
8	mmg-fna.whatsapp.net:443	1	28.3
9	accounts.google.com:443	178	26.4
10	ogs.google.com:443	26	21.1
11	omextemplates.content.office.net:443	58	21.1
12	fonts.gstatic.com:443	154	20.6
13	www.google.com:443	93	16.9
14	crl3.digicert.com	3	13.0
15	www.startmenux.com:443	1	12.8
16	ssl.gstatic.com:443	191	12.1
17	hangouts.google.com:443	3	10.0
18	drive.google.com:443	88	9.8
19	www.gstatic.com:443	74	9.4
20	web.whatsapp.com:443	30	8.7
21	lh3.googleusercontent.com:443	30	7.6
22	cloud.google.com:443	2	7.1
23	nuistatic.avcdn.net	47	6.2
24	www.fundeu.es:443	2	5.9
25	safebrowsing.googleapis.com:443	64	5.8
26	pangua.gob.ec:443	5	5.2
27	neufert-cdn.archdaily.net:443	34	5.2
28	cio.com.mx:443	6	5.1
29	ukproxy.vpnbook.com:443	11	4.3
30	docs.google.com:443	58	4.2
31	tpc.googlesyndication.com:443	55	4.1
32	storage.googleapis.com	38	4.1
33	mail.google.com:443	10	4.0
34	outlook-1.cdn.office.net:443	15	3.6
35	cdn.bannersnack.com:443	1	3.4
36	allcalidad.la:443	2	3.4

Fuente: Programa de NethServer.

En los presentes reportes, se puede apreciar el acceso de dos equipos diferentes a jugos en línea, como también a páginas de mensajería y streaming

Figura 10: Resultados de Análisis de NethServer.

User:	10.10.
Date:	Whole MONTH - 2020 Sep

Total			3.7 G	
#	Accessed site	Connect	Bytes	Cumulative
107	b.config.skype.com:443	6	34 722	3.7 G
108	geo.prod.do.dsp.mp.microsoft.com:443	14	34 675	3.7 G
109	cdn.adnxs.com:443	1	34 124	3.7 G
110	www.googletagmanager.com:443	1	31 879	3.7 G
111	candycrushsoda.king.com:443	9	29 358	3.7 G
112	bubblewitch3mobile.king.com:443	9	29 358	3.7 G

Fuente: Programa de NethServer.

Figura 11 : Resultados de Análisis de NethServer.

User:	10.10.
Date:	Whole MONTH - 2020 Sep

Total	
#	
1	media.fuio15-1.fna.whatsapp.net:443
2	whatsapp.com:443
3	secak-fota-dn.samsungdm.com
4	pps.whatsapp.net:443
5	v16m.tiktokcdn.com:443
6	download.cdn.mozilla.net
7	media-mia3-1.cdn.whatsapp.net:443
8	mmg.whatsapp.net:443
9	tlu.dl.delivery.mp.microsoft.com
10	samsappsbn.vo.llnwd.net
11	r2---sn-jou-0pvs.gvt1.com:443
12	r7---sn-jou-0pvs.gvt1.com
13	r8---sn-jou-btxl.gvt1.com:443
14	mail-attachment.googleusercontent.com:443
15	gfs262n302.userstorage.mega.co.nz
16	gfs208n110.userstorage.mega.co.nz
17	gfs204n120.userstorage.mega.co.nz
18	r1---sn-jou-btxl.gvt1.com:443
19	gfs270n113.userstorage.mega.co.nz
20	gfs302n110.userstorage.mega.co.nz
21	elepcosa.com.ec:443
22	mmg-fna.whatsapp.net:443
23	media.fuio6-1.fna.whatsapp.net:443

Fuente: Programa de NethServer.

Finalmente, en el reporte del equipo se puede apreciar acceso a páginas de compra y venta, redes sociales, mensajería y otras.

Figura 12: Resultados de Análisis de NethServer.

User:	10.10.
Date:	Whole MONTH - 2020 Sep

Total			1.1 G	
#	Accessed site	Connect	Bytes	Cu
1	413e2ebcbb0e842a.apache-iv.com:443	4 446	302.4 M	
2	6a5b77ed48a894ca.apache-iv.com:443	4 143	282.2 M	
3	cache-man01i.cdn.yandex.net:443	5	120.5 M	
4	930575505d572782.apache-iv.com:443	1 789	45.4 M	
5	mail.google.com:443	229	32.3 M	
6	sine.dinardap.gob.ec:443	1 462	32.1 M	
7	pps.whatsapp.net:443	16	21.5 M	
8	http2.mlstatic.com:443	4	19.8 M	
9	download.cdn.mozilla.net	4	18.7 M	
10	ec-static.imgskk.com:443	25	16.3 M	
11	apollo-virginia.akamaized.net:443	44	16.3 M	
12	drive.google.com:443	4	15.4 M	
13	web.whatsapp.com:443	34	12.8 M	
14	www.google.com:443	77	10.1 M	
15	mail.dinardap.gob.ec:443	27	7.9 M	
16	ssl.gstatic.com:443	41	6.5 M	
17	www.olx.com.ec:443	10	6.3 M	
18	nuistatic.avcdn.net	47	6.2 M	
19	z1346165.avi18.u.avcdn.net	47	5.6 M	
20	mmg-fna.whatsapp.net:443	17	5.2 M	
21	www.gstatic.com:443	46	4.9 M	
22	mercadolibre.com.ec:443	1	4.7 M	
23	tpc.googlesyndication.com:443	36	4.6 M	
24	ec.skokka.com:443	10	4.4 M	
25	accounts.google.com:443	30	3.9 M	
26	hangouts.google.com:443	15	3.7 M	
27	pq.biess.fin.ec:443	82	3.3 M	
28	download3.operacdn.com:443	8	3.3 M	
29	su.ff.avast.com	407	2.9 M	

Fuente: Programa de NethServer.

11.8. Análisis de tráfico de red mediante Wireshark.

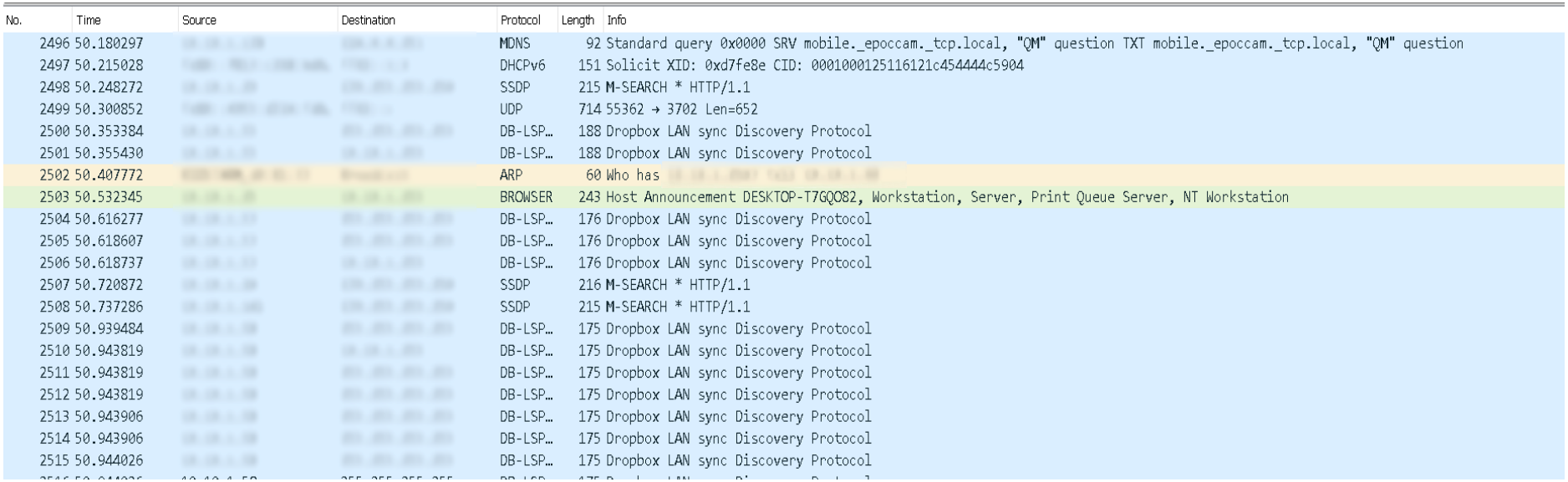
De igual forma mediante la ayuda del software Wireshark, que es un programa gratuito que permite analizar y solucionar el tráfico de red de comunicaciones en tiempo real. Con esta herramienta ayudo a detectar los datos y los protocolos que se realizaba en el GAD de Pangua.

11.9. Análisis de los archivos PCAPNG mediante NetworkMiner

Esta herramienta permite analizar paquetes y a su vez protocolos de esta manera nos facilitó conocer más a detalle que paginas han visitado los usuarios del GAD de Pangua a través de capturas de paquetes llamados archivos PCAPNG, este programa también puede ser combinado con Wireshark que analiza los paquetes de red y el tráfico de tiempo real.

Análisis del equipo N° 1: Ejecución del programa Wireshark

Figura 13: Salvapantalla de programa Wireshark equipo N° 1.



No.	Time	Source	Destination	Protocol	Length	Info
2496	50.180297	[redacted]	[redacted]	MDNS	92	Standard query 0x0000 SRV mobile._epoccam._tcp.local, "QM" question TXT mobile._epoccam._tcp.local, "QM" question
2497	50.215028	[redacted]	[redacted]	DHCPv6	151	Solicit XID: 0xd7fe8e CID: 00010001251161121c454444c5904
2498	50.248272	[redacted]	[redacted]	SSDP	215	M-SEARCH * HTTP/1.1
2499	50.300852	[redacted]	[redacted]	UDP	714	55362 → 3702 Len=652
2500	50.353384	[redacted]	[redacted]	DB-LSP…	188	Dropbox LAN sync Discovery Protocol
2501	50.355430	[redacted]	[redacted]	DB-LSP…	188	Dropbox LAN sync Discovery Protocol
2502	50.407772	[redacted]	[redacted]	ARP	60	Who has [redacted]
2503	50.532345	[redacted]	[redacted]	BROWSER	243	Host Announcement DESKTOP-T7GQO82, Workstation, Server, Print Queue Server, NT Workstation
2504	50.616277	[redacted]	[redacted]	DB-LSP…	176	Dropbox LAN sync Discovery Protocol
2505	50.618607	[redacted]	[redacted]	DB-LSP…	176	Dropbox LAN sync Discovery Protocol
2506	50.618737	[redacted]	[redacted]	DB-LSP…	176	Dropbox LAN sync Discovery Protocol
2507	50.720872	[redacted]	[redacted]	SSDP	216	M-SEARCH * HTTP/1.1
2508	50.737286	[redacted]	[redacted]	SSDP	215	M-SEARCH * HTTP/1.1
2509	50.939484	[redacted]	[redacted]	DB-LSP…	175	Dropbox LAN sync Discovery Protocol
2510	50.943819	[redacted]	[redacted]	DB-LSP…	175	Dropbox LAN sync Discovery Protocol
2511	50.943819	[redacted]	[redacted]	DB-LSP…	175	Dropbox LAN sync Discovery Protocol
2512	50.943819	[redacted]	[redacted]	DB-LSP…	175	Dropbox LAN sync Discovery Protocol
2513	50.943906	[redacted]	[redacted]	DB-LSP…	175	Dropbox LAN sync Discovery Protocol
2514	50.943906	[redacted]	[redacted]	DB-LSP…	175	Dropbox LAN sync Discovery Protocol
2515	50.944026	[redacted]	[redacted]	DB-LSP…	175	Dropbox LAN sync Discovery Protocol

Fuente: Programa Wireshark 3.2.6.

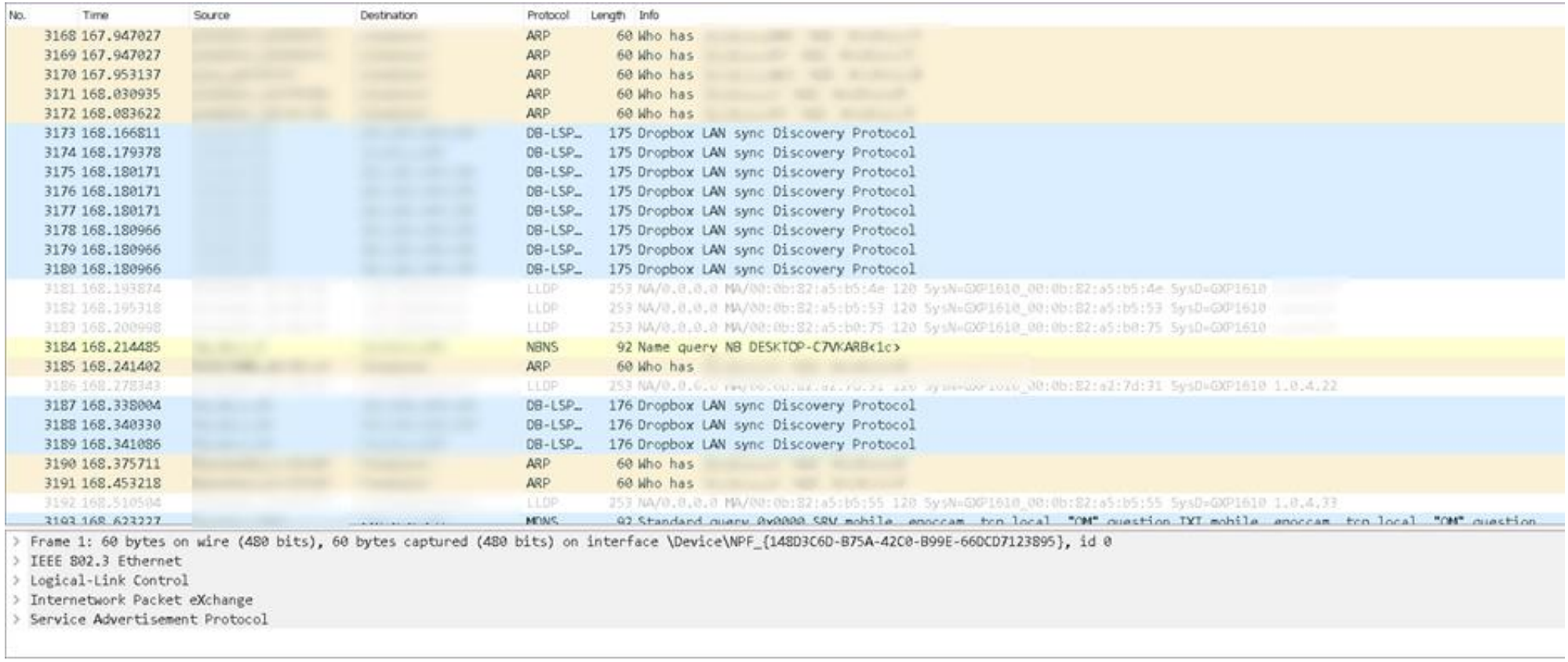
Figura 14: Resultados de Análisis NetworkMiner del Equipo N°1.

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host
40647	Microsoft Secure Server CA 2[8].cer	cer	1 756 B	settingsfd-geo.trafficmanager.net] [settings-win.data....	TCP 443	
40693	google.com.cer	cer	2 420 B	lients.l.google.com] [clients2.google.com] (Linux)	TCP 443	
40693	GTS CA 1O1.cer	cer	1 102 B	lients.l.google.com] [clients2.google.com] (Linux)	TCP 443	
53431	settings-win.data.microsoft.[9].cer	cer	1 517 B	settingsfd-geo.trafficmanager.net] [settings-win.data....	TCP 443	
53431	Microsoft Secure Server CA 2[9].cer	cer	1 756 B	settingsfd-geo.trafficmanager.net] [settings-win.data....	TCP 443	
59146	www.bing.com[1].cer	cer	3 582 B	www.bing.com] [dual-a-0001.a-msedge.net] [a-0001...	TCP 443	
59146	Microsoft IT TLS CA 2[1].cer	cer	1 464 B	www.bing.com] [dual-a-0001.a-msedge.net] [a-0001...	TCP 443	
66921	smartscreen.microsoft.com.cer	cer	3 319 B	[wd-prod-ss-br-south-1-fe.brazilsouth.cloudapp.azur...	TCP 443	
66921	Microsoft IT TLS CA 1.cer	cer	1 464 B	[wd-prod-ss-br-south-1-fe.brazilsouth.cloudapp.azur...	TCP 443	
66962	smartscreen.microsoft.com[1].cer	cer	3 319 B	[wd-prod-ss-br-south-1-fe.brazilsouth.cloudapp.azur...	TCP 443	
66962	Microsoft IT TLS CA 1[1].cer	cer	1 464 B	[wd-prod-ss-br-south-1-fe.brazilsouth.cloudapp.azur...	TCP 443	
67717	events.data.microsoft.com.cer	cer	1 863 B	ypedataprdcolwus11.cloudapp.net] [global.asimov....	TCP 443	
67717	Microsoft Secure Server CA 2.cer	cer	1 756 B	ypedataprdcolwus11.cloudapp.net] [global.asimov....	TCP 443	
69016	login.live.com.cer	cer	1 665 B	ww.tm.lg.prod.aadmsa.akadns.net] [login.msa.msiden...	TCP 443	
69016	DigiCert SHA2 Secure Server .cer	cer	1 176 B	ww.tm.lg.prod.aadmsa.akadns.net] [login.msa.msiden...	TCP 443	
69066	login.live.com[1].cer	cer	1 665 B	ww.tm.lg.prod.aadmsa.akadns.net] [login.msa.msiden...	TCP 443	
69066	DigiCert SHA2 Secure Server [1].cer	cer	1 176 B	ww.tm.lg.prod.aadmsa.akadns.net] [login.msa.msiden...	TCP 443	
69134	storecatalogrevocation.store.cer	cer	2 278 B	0198.b.akamaiedge.net] [storecatalogrevocation.sto...	TCP 443	
69134	Microsoft IT TLS CA 5.cer	cer	1 464 B	0198.b.akamaiedge.net] [storecatalogrevocation.sto...	TCP 443	
69240	slscr.update.microsoft.com.cer	cer	942 B	.row.update.microsoft.com.akadns.net] [sls.update....	TCP 443	
69240	Microsoft ECC Update Secure .cer	cer	1 126 B	.row.update.microsoft.com.akadns.net] [sls.update....	TCP 443	
69326	arc.msn.com.cer	cer	2 133 B	arc.msn.com.nsatc.net] [arc.msn.com] (Linux)	TCP 443	
69326	Microsoft Azure TLS Issuing .cer	cer	1 527 B	arc.msn.com.nsatc.net] [arc.msn.com] (Linux)	TCP 443	
98849	settings-win.data.microsoft.[10].cer	cer	1 517 B	settingsfd-geo.trafficmanager.net] [settings-win.data....	TCP 443	
98849	Microsoft Secure Server CA 2[10].cer	cer	1 756 B	settingsfd-geo.trafficmanager.net] [settings-win.data....	TCP 443	
102097	google.com[1].cer	cer	2 420 B	lients.l.google.com] [clients2.google.com] [clients5.g...	TCP 443	
102097	GTS CA 1O1[1].cer	cer	1 102 B	lients.l.google.com] [clients2.google.com] [clients5.g...	TCP 443	
102111	licensing.md.mp.microsoft.co[1].cer	cer	2 184 B	eap.licensing.md.mp.microsoft.com.akadns.net] [lice...	TCP 443	
102111	Microsoft Azure TLS Issuing [1].cer	cer	1 527 B	eap.licensing.md.mp.microsoft.com.akadns.net] [lice...	TCP 443	
102112	wns.windows.com[1].cer	cer	2 107 B	bn3p.wns.notify.windows.com.akadns.net] [america...	TCP 443	
102112	Microsoft IT TLS CA 4[1].cer	cer	1 464 B	bn3p.wns.notify.windows.com.akadns.net] [america...	TCP 443	
102734	events.data.microsoft.com.cer	cer	1 863 B	ypedataprdcolweu02.cloudapp.net] [global.asimov.e...	TCP 443	
102734	Microsoft Secure Server CA 2.cer	cer	1 756 B	ypedataprdcolweu02.cloudapp.net] [global.asimov.e...	TCP 443	
116244	settings-win.data.microsoft.[11].cer	cer	1 517 B	settingsfd-geo.trafficmanager.net] [settings-win.data....	TCP 443	
116244	Microsoft Secure Server CA 2[11].cer	cer	1 756 B	settingsfd-geo.trafficmanager.net] [settings-win.data....	TCP 443	
125066	smartscreen.microsoft.com[1].cer	cer	3 319 B	martscreen.microsoft.com] [wd-prod-ss-br-south-2-fe....	TCP 443	
125066	Microsoft IT TLS CA 1[1].cer	cer	1 464 B	martscreen.microsoft.com] [wd-prod-ss-br-south-2-fe....	TCP 443	

Fuente: NetworkMiner.

Análisis del equipo N° 2: Ejecución del programa Wireshark

Figura 15: Salvapantalla de programa Wireshark equipo N° 2.



Fuente: Programa Wireshark 3.2.6.

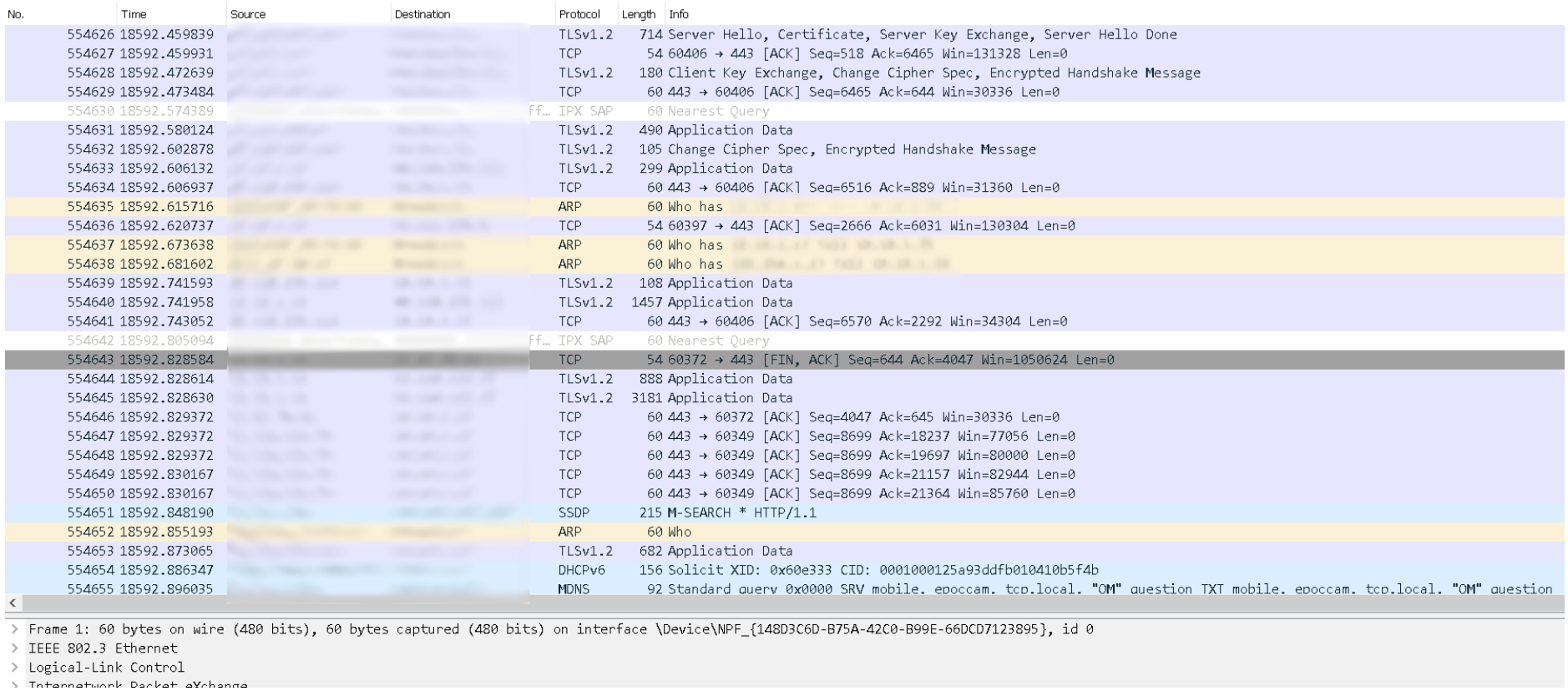
Figura 16: Resultados de Análisis NetworkMiner del Equipo N°2.

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Protocol
324387	google.com[2].cer	cer	2 420 B	[youtube-ui.l.google.com] [www.youtube.co...	TCP 443			
324387	GTS CA 1O1[2].cer	cer	1 102 B	[youtube-ui.l.google.com] [www.youtube.co...	TCP 443			
324929	avast.com[7].cer	cer	1 518 B	ux)	TCP 443			
324929	DigiCert SHA2 High Assurance[7].cer	cer	1 205 B	ux)	TCP 443			
327510	ncc.txt[18].html	html	26 B	4 [a122.dscd.akamai.net] [acroipm2.adobe....	TCP 80			
336346	avast.com[7].cer	cer	1 518 B	inux)	TCP 443			
336346	DigiCert SHA2 High Assurance[7].cer	cer	1 205 B	inux)	TCP 443			
338873	avast.com[8].cer	cer	1 518 B	inux)	TCP 443			
338873	DigiCert SHA2 High Assurance[8].cer	cer	1 205 B	inux)	TCP 443			
340184	avast.com[8].cer	cer	1 518 B	inux)	TCP 443			
340184	DigiCert SHA2 High Assurance[8].cer	cer	1 205 B	inux)	TCP 443			
341837	ncc.txt[16].html	html	26 B	7 [a1488.dscd.akamai.net] [ncc.avast.com....	TCP 80			
345949	telemetry.mozilla.org[2].cer	cer	1 766 B	[pipeline-incoming-prod-elb-149169523.us-w...	TCP 443			
345949	DigiCert SHA2 Secure Server [2].cer	cer	1 176 B	[pipeline-incoming-prod-elb-149169523.us-w...	TCP 443			
346565	success[3].txt	txt	8 B	7 [a1488.dscd.akamai.net] [ncc.avast.com....	TCP 80			
346771	success.txt.E6EE03DF[3].txt	txt	8 B	7 [a1488.dscd.akamai.net] [ncc.avast.com....	TCP 80			
346788	push.services.mozilla.com.cer	cer	1 783 B	[autopush.prod.mozaws.net] [push.services....	TCP 443			
346788	DigiCert SHA2 Secure Server .cer	cer	1 176 B	[autopush.prod.mozaws.net] [push.services....	TCP 443			
346799	index.html[18].ocsp-response	ocsp-response	471 B	s9.wac.phicdn.net] [ocsp.digicert.com] (Linux)	TCP 80			
346821	alvlaskuri.fi[4].cer	cer	2 786 B	7 [alvlaskuri.fi] [calcularіva.es] (Linux)	TCP 443			
346821	Let's Encrypt Authority X3[4].cer	cer	1 174 B	7 [alvlaskuri.fi] [calcularіva.es] (Linux)	TCP 443			
346972	gts1o1core[5].ocsp-response	ocsp-response	471 B	pki-goog.l.google.com] [ocsp.pki.goog] (Linux)	TCP 80			
346849	index.html[2].ocsp-response	ocsp-response	527 B	6 [a771.dscq.akamai.net] [ocsp.int-x3.letsen...	TCP 80			
349066	index.html[19].ocsp-response	ocsp-response	471 B	s9.wac.phicdn.net] [ocsp.digicert.com] (Linux)	TCP 80			
349097	gts1o1core[6].ocsp-response	ocsp-response	472 B	pki-goog.l.google.com] [ocsp.pki.goog] (Linux)	TCP 80			
349101	gts1o1core[7].ocsp-response	ocsp-response	471 B	pki-goog.l.google.com] [ocsp.pki.goog] (Linux)	TCP 80			
349400	telemetry.mozilla.org.cer	cer	1 766 B	2 [pipeline-incoming-prod-elb-149169523.us-...	TCP 443			
349400	DigiCert SHA2 Secure Server .cer	cer	1 176 B	2 [pipeline-incoming-prod-elb-149169523.us-...	TCP 443			
349441	index.html[20].ocsp-response	ocsp-response	471 B	s9.wac.phicdn.net] [ocsp.digicert.com] (Linux)	TCP 80			
349668	gts1o1core[8].ocsp-response	ocsp-response	472 B	pki-goog.l.google.com] [ocsp.pki.goog] (Linux)	TCP 80			
349934	gts1o1core[9].ocsp-response	ocsp-response	471 B	pki-goog.l.google.com] [ocsp.pki.goog] (Linux)	TCP 80			
349935	gts1o1core[10].ocsp-response	ocsp-response	471 B	pki-goog.l.google.com] [ocsp.pki.goog] (Linux)	TCP 80			
349959	gts1o1core[11].ocsp-response	ocsp-response	472 B	pki-goog.l.google.com] [ocsp.pki.goog] (Linux)	TCP 80			
350481	Outlook.live.com[4].cer	cer	2 015 B	l-0002.l-msedge.net] [outlook-live-com.l-0002...	TCP 443			
350481	DigiCert Cloud Services CA-1[4].cer	cer	1 174 B	l-0002.l-msedge.net] [outlook-live-com.l-0002...	TCP 443			
350977	res.outlook.com[28].cer	cer	2 319 B	e1875.dscg.akamaiedge.net] [ow2.res.office...	TCP 443			
350977	Microsoft IT TLS CA 2[28].cer	cer	1 464 B	e1875.dscg.akamaiedge.net] [ow2.res.office...	TCP 443			

Fuente: NetworkMiner.

Análisis del equipo N° 3: Ejecución del programa Wireshark

Figura 17: Salvapantalla de programa Wireshark equipo N° 3.



No.	Time	Source	Destination	Protocol	Length	Info
554626	18592.459839			TLSv1.2	714	Server Hello, Certificate, Server Key Exchange, Server Hello Done
554627	18592.459931			TCP	54	60406 → 443 [ACK] Seq=518 Ack=6465 Win=131328 Len=0
554628	18592.472639			TLSv1.2	180	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
554629	18592.473484			TCP	60	443 → 60406 [ACK] Seq=6465 Ack=644 Win=30336 Len=0
554630	18592.574389		ff…	IPX SAP	60	Nearest Query
554631	18592.580124			TLSv1.2	490	Application Data
554632	18592.602878			TLSv1.2	105	Change Cipher Spec, Encrypted Handshake Message
554633	18592.606132			TLSv1.2	299	Application Data
554634	18592.606937			TCP	60	443 → 60406 [ACK] Seq=6516 Ack=889 Win=31360 Len=0
554635	18592.615716			ARP	60	Who has
554636	18592.620737			TCP	54	60397 → 443 [ACK] Seq=2666 Ack=6031 Win=130304 Len=0
554637	18592.673638			ARP	60	Who has
554638	18592.681602			ARP	60	Who has
554639	18592.741593			TLSv1.2	108	Application Data
554640	18592.741958			TLSv1.2	1457	Application Data
554641	18592.743052			TCP	60	443 → 60406 [ACK] Seq=6570 Ack=2292 Win=34304 Len=0
554642	18592.805094		ff…	IPX SAP	60	Nearest Query
554643	18592.828584			TCP	54	60372 → 443 [FIN, ACK] Seq=644 Ack=4047 Win=1050624 Len=0
554644	18592.828614			TLSv1.2	888	Application Data
554645	18592.828630			TLSv1.2	3181	Application Data
554646	18592.829372			TCP	60	443 → 60372 [ACK] Seq=4047 Ack=645 Win=30336 Len=0
554647	18592.829372			TCP	60	443 → 60349 [ACK] Seq=8699 Ack=18237 Win=77056 Len=0
554648	18592.829372			TCP	60	443 → 60349 [ACK] Seq=8699 Ack=19697 Win=80000 Len=0
554649	18592.830167			TCP	60	443 → 60349 [ACK] Seq=8699 Ack=21157 Win=82944 Len=0
554650	18592.830167			TCP	60	443 → 60349 [ACK] Seq=8699 Ack=21364 Win=85760 Len=0
554651	18592.848190			SSDP	215	M-SEARCH * HTTP/1.1
554652	18592.855193			ARP	60	Who
554653	18592.873065			TLSv1.2	682	Application Data
554654	18592.886347			DHCPv6	156	Solicit XID: 0x60e333 CID: 0001000125a93ddfb010410b5f4b
554655	18592.896035			MDNS	92	Standard query 0x0000 SRV mobile, epoccam, tcp.local, "QM" question TXT mobile, epoccam, tcp.local, "QM" question

> Frame 1: 60 bytes on wire (480 bits), 60 bytes captured (480 bits) on interface \Device\NPF_{148D3C6D-B75A-42C0-B99E-66DCD7123895}, id 0
> IEEE 802.3 Ethernet
> Logical-Link Control
> Internetwork Packet eXchange

Fuente: Programa Wireshark 3.2.6.

Figura 18: Resultados de Análisis NetworkMiner del Equipo N°3.

Frame nr.	Filename	Extension	Size	Source host	S. port	Destination host	D. port	Pr
554626	ipm-klca.kaspersky.com[1].cer	cer	2 276 B	3 [waws-prod-bay-011.sip.azurewebsites.win...	TCP 443			
554626	Kaspersky Lab UCP Service Ce[1].cer	cer	1 868 B	3 [waws-prod-bay-011.sip.azurewebsites.win...	TCP 443			
554626	Kaspersky Lab Public Service[1].cer	cer	1 873 B	3 [waws-prod-bay-011.sip.azurewebsites.win...	TCP 443			
556079	AN_ZIMPy33w0N-lq3s8Th-s[6].html	html	489 B	youtube-ui.l.google.com] [www.youtube.com...	TCP 80			
556148	AN_ZIMP[7].octet-stream	octet-stream	26 B	[r8.sn-jou-btxl.gvt1.com] [r8---sn-jou-btxl.gvt1...	TCP 80			
556300	apis.skype.com[16].cer	cer	2 258 B	[apis.skype.com] (Linux)	TCP 443			
556300	Microsoft IT TLS CA 2[16].cer	cer	1 464 B	[apis.skype.com] (Linux)	TCP 443			
556310	trouter.skype.com[4].cer	cer	2 187 B	8 (Linux)	TCP 443			
556310	Microsoft IT TLS CA 5[4].cer	cer	1 464 B	8 (Linux)	TCP 443			
556660	apis.skype.com[17].cer	cer	2 258 B	[apis.skype.com] (Linux)	TCP 443			
556660	Microsoft IT TLS CA 2[17].cer	cer	1 464 B	[apis.skype.com] (Linux)	TCP 443			
556669	apis.skype.com[18].cer	cer	2 258 B	[apis.skype.com] (Linux)	TCP 443			
556669	Microsoft IT TLS CA 2[18].cer	cer	1 464 B	[apis.skype.com] (Linux)	TCP 443			
556674	apis.skype.com[19].cer	cer	2 258 B	[apis.skype.com] (Linux)	TCP 443			
556674	Microsoft IT TLS CA 2[19].cer	cer	1 464 B	[apis.skype.com] (Linux)	TCP 443			
556680	apis.skype.com[20].cer	cer	2 258 B	[apis.skype.com] (Linux)	TCP 443			
556680	Microsoft IT TLS CA 2[20].cer	cer	1 464 B	[apis.skype.com] (Linux)	TCP 443			
556693	apis.skype.com[21].cer	cer	2 258 B	[apis.skype.com] (Linux)	TCP 443			
556693	Microsoft IT TLS CA 2[21].cer	cer	1 464 B	[apis.skype.com] (Linux)	TCP 443			
557828	AN_ZIMPy33w0N-lq3s8Th-s[7].html	html	473 B	youtube-ui.l.google.com] [www.youtube.com...	TCP 80			
557841	AN_ZIMP[8].octet-stream	octet-stream	3 383 B	[r8.sn-jou-btxl.gvt1.com] [r8---sn-jou-btxl.gvt1...	TCP 80			
557882	AN_ZIMPy33w0N-lq3s8Th-s[8].html	html	473 B	youtube-ui.l.google.com] [www.youtube.com...	TCP 80			
557889	AN_ZIMP[9].octet-stream	octet-stream	9 231 B	[r8.sn-jou-btxl.gvt1.com] [r8---sn-jou-btxl.gvt1...	TCP 80			
557910	AN_ZIMPy33w0N-lq3s8Th-s[9].html	html	473 B	youtube-ui.l.google.com] [www.youtube.com...	TCP 80			
557915	AN_ZIMP[10].octet-stream	octet-stream	4 847 B	[r8.sn-jou-btxl.gvt1.com] [r8---sn-jou-btxl.gvt1...	TCP 80			
558119	trap.skype.com[1].cer	cer	2 351 B	trap.skype.com] (Linux)	TCP 443			
558119	Microsoft IT TLS CA 1[1].cer	cer	1 464 B	trap.skype.com] (Linux)	TCP 443			
558128	prod.registrar.skype.com.cer	cer	2 147 B	0 [prod.registrar.skype.com] (Linux)	TCP 443			
558128	Microsoft IT TLS CA 2.cer	cer	1 464 B	0 [prod.registrar.skype.com] (Linux)	TCP 443			
562089	blocked.nethserver.org[8].cer	cer	1 383 B	[edge-web.dual-gslb.spotify.com] [spclient.w...	TCP 443			
562089	Let's Encrypt Authority X3[8].cer	cer	1 174 B	[edge-web.dual-gslb.spotify.com] [spclient.w...	TCP 443			
566902	ieonlinews.microsoft.com.cer	cer	2 120 B	ieonlinews.trafficmanager.net] [ieonlinews.mi...	TCP 443			
566902	Microsoft IT TLS CA 5.cer	cer	1 464 B	ieonlinews.trafficmanager.net] [ieonlinews.mi...	TCP 443			
567029	adnxs.com.cer	cer	1 322 B	(Linux)	TCP 443			
567029	DigiCert ECC Secure Server C.cer	cer	944 B	(Linux)	TCP 443			
574341	preinstall.FC40352A[9].xml	xml	4 230 B	15 [e15275.g.akamaiedge.net] [wildcard.we...	TCP 80			
574707	cdn.onenote.net[7].cer	cer	2 257 B	[e1553.dspg.akamaiedge.net] [cdn.onenote...	TCP 443			

Fuente: NetworkMiner.

11.10. Plan de mitigación de riesgos

Tabla 14: Plan de mitigación de riesgos.

OBJETIVO	RIESGO	ACCIONES A TOMAR	RESPONSABLE	TIEMPO DE MITIGAR EL RIESGO
Incrementar la seguridad de la información en los equipos, para estar listos ante cualquier eventualidad.	F. Interno: Respaldo a los equipos	ANEXO-1F Listado de usuarios para Backups siendo el medio de verificación de este documento el RE-1F Bitácora de respaldos de usuarios.	Encargado de sistemas informáticos.	6 meses luego de la implementación
	F. Externo: No cuenta con acuerdos que garantice la confidencialidad de la información.	RE-1A Carta de aceptación de políticas de seguridad informática, documento que compromete a cumplir a los empleados con los lineamientos de confidencialidad de información enlistados en la carta.	Encargado de sistemas informáticos.	6 meses luego de la implementación

Controlar los equipos que ingresen a la institución además de reducir la saturación de la red por mal uso del internet.	F. Interno: Acceso a redes sociales, streaming y otras páginas.	ANEXO-1E Listado de categorías de acceso a internet, enuncia a las categorías de accesos según las funciones de cada departamento.	Encargado de sistemas informáticos.	7 meses luego de la implementación
	F. Externo: Nivel de seguridad baja, en el control de acceso a equipos.	RE-2A Solicitud de creación de nuevos usuarios de red, en el cual se crearán usuarios y contraseñas. De igual forma se da seguimientos a la actualización con la RE-3A Bitácora de actualización de contraseñas.	Personal de seguridad y Bodega	8 meses luego de la implementación

Diseñar políticas de seguridad informática para proteger los activos del municipio.	F. Interno: Carencia de plan de mantenimiento preventivo.	ANEXO-2C Cronograma para mantenimiento preventivo de equipos, dando seguimiento con el RE-4C Bitácora de mantenimiento preventivo de equipos.	Encargado de sistemas informáticos.	6 meses luego de la implementación
	F. Externo: Carencia de políticas de seguridad informática.	PR-01 Sistemas de Información, que aplica lineamiento para protección de la información como de los recursos informáticos.	Encargado de sistemas informáticos.	8 meses luego de la implementación

Fuente: Grupo Investigador.

11.11. Estructura del documento de políticas de seguridad informática

Antes de explicar la estructura de las políticas de seguridad informática, se requiere dar a conocer que para el desarrollo de las políticas de seguridad se ha percibido conveniente englobar a todas las políticas de seguridad informática dentro de un proceso, el cual se ha denominado PR-01 Sistemas de Información, para su gestión deben cumplir con las siguientes actividades:

- ✓ Mantener y administrar las redes.
- ✓ Prestar soporte técnico a usuarios en todo lo referente a la plataforma computacional.
- ✓ Supervisar todo el proyecto informático.
- ✓ Generar propuestas para facilitar el acceso y uso de la tecnología.
- ✓ Velar por la integridad y la seguridad de la información.
- ✓ Desarrollar, investigar y adaptar nuevas técnicas para mejorar la gestión interna y externa de la municipalidad.

De acuerdo a la investigación realizada, la manera más adecuada de generar la documentación, para la gestión de información es la siguiente:

Encabezado: Al lado izquierdo de la tabla se destina el logo de la Institución para quien va dirigido el diseño de las políticas de seguridad; intermedio de la tabla se especifica el nombre de la política; al lado derecho se define el código de la política, seguido de la versión y finalmente en el último recuadro el número de página.

Objetivo: Posee un conjunto de metas que se propone alcanzar según el tema o referencia de la política.

Alcance: Define a las personas que se verán involucradas acatar las políticas descritas.

Definiciones: Es un glosario de palabras que se asume el usuario desconozca, pretendiendo mejorar la comprensión de lectura de las políticas a los usuarios.

Documentos de referencia: Son documentos que se recomienda utilizar a fin de acatar las políticas, estos documentos pueden ser registros o anexos, se recomienda llamarla o identificarla de la siguiente forma: para registros se identifica anticipando el RE, seguido del código y finalmente el nombre del registro (RE-1A Carta de Aceptación de políticas de seguridad) y para los anexos se recomienda anticipar ANEXO, seguido del código y el nombre del anexo (ANEXO-1A Cronograma de mantenimiento preventivo de equipos).

Descripción de la política Aquí abarca los lineamientos que se propone según las necesidades de la institución, para mejorar la calidad de la seguridad informática, se detalla lo más claro posible de forma que sea comprensible para el lector.

Registros: Puede ser representada mediante una tabla que contiene:

- ✓ **Código** que es el nombre del documento.
- ✓ **Nombre** es el título del documento.
- ✓ **Responsable** será la persona encargada de llevar esta documentación.
- ✓ **Ubicación** es el lugar donde se pueda alojar el documento.
- ✓ **Archivos** especifica la fecha en la que ha sido aprobado.
- ✓ **Actualización** indica la fecha del tiempo que estará vigente el modelo del anexo o registro, pasado el tiempo estipulado se podrá realizar los cambios que se crean convenientes.
- ✓ **Retención** es el tiempo que se estima, se tendrá los documentos impresos.
- ✓ **Destino final** habitualmente los registros van hacer los documentos físicos.
- ✓ **Acceso** es quien va a poder ver, revisar o administrar las políticas físicas.

Anexos: Indica el listado de documentos en los que ya está estipulada cierta información, se vuelve a ubicar los anexos descritos en Documentos de Referencia, en caso que la política no requiera anexos, no hay que dejar el espacio vacío se debe usar N/A (No aplica).

Cabe aclarar que los registros tanto como los anexos pueden ser llamados en otras políticas de acuerdo a la necesidad.

Pie de Página: Posee las firmas de quienes son los responsables de gestionar la política y de quien aprueba para su ejecución.

Finalmente, esta documentación se debe imprimir asimismo reposar en cada uno de los departamentos para cualquier auditoría ya sea informática, auditoría de calidad, auditoría de procedimientos, entre otras.

11.12. ANÁLISIS DE LA ENTREVISTA APLICADA

A continuación, se muestra los datos obtenidos de la entrevista ejecutada al Encargado del Departamento de Sistemas Informáticos del Gobierno Autónomo Descentralizado Municipal de Pangua. Es importante mencionar que el criterio de la persona entrevistada, es muy

significativa, pues posee el nivel de conocimiento sobre los procesos que se llevan a cabo en la Municipalidad.

Tabla 15: Análisis de la entrevista aplicada.

FICHA DE ENTREVISTA	
Objetivo:	Analizar las vulnerabilidades y necesidades que tiene el Gobierno Autónomo Descentralizado Municipal de Pangua para el desarrollo de políticas de seguridad informáticas de acuerdo a las ISO 27001
Datos Informativos:	
Entrevistado:	Ing. Herman Ortiz
Lugar:	Gobierno Autónomo Descentralizado Municipal de Pangua
Entrevistador:	Cruz Caiza Carla Cristina Gaibor Gavilanez Mónica Lisseth
Pregunta	**Respuesta**
¿Cuenta con un antivirus?	Si, con software gratuito como Kaspersky y AVG que se utilizan a la par.
¿La página del Municipio es un sitio seguro?	La página de la Municipalidad fue proporcionada por AME, quienes tienen convenio con una empresa, el GAD de Pangua se encarga de pagar el dominio y el hosting.
¿Cuentan con un plan de contingencia para cambiar los equipos (computadoras, cables, laptops, servidores)?	No cuenta.
¿Cuenta con un DATACENTER adecuado (piso, ventilación, seguridad)?	No cuenta con DATACENTER.
¿Cuenta con un UPS para evitar daños en los equipos?	Si cuenta.
¿Cómo manejan los privilegios de los usuarios?	Tiene restricción, que no permite que nadie tenga acceso solo el encargo de TI.
¿Existe una persona responsable de la seguridad de autenticación de acceso?	Nadie tiene acceso solo el encargo de TI.

¿Cada que tiempo cambian las contraseñas de su equipo?	Los equipos a responsabilidad del encargado de TI se cambian cada 3 meses. Los demás equipos, pocos hacen uso de autenticación, en su gran mayoría tienen acceso libre, con la finalidad de que, en ausencia del responsable del equipo, si necesitase cierta información, cualquier otro empleado puede ingresar y facilitarle lo solicitado.
¿Cada que tiempo se realiza capacitaciones para el uso de las herramientas dentro de la Municipalidad?	Se las realiza solo cuando vienen nuevos funcionarios, acerca de las aplicaciones propias de cada departamento, en especial de cobros de impuestos, tesorería, recaudación, rentas y el sistema de contabilidad para el departamento financiero, o en caso la aplicación se haya actualizado y suceda algún cambio en ciertos aspectos, en esas situaciones se realiza la capacitación, puesto que el resto de funcionarios están constante labor y conocen las herramientas.
¿Cómo comparten información dentro del municipio?	Por la red, con carpetas compartidas.
¿Cuentan con comunicación telefónica IP?	Si.
¿Cuentan con un plan de contingencia por desastres naturales?	No, no tiene.
¿Periodo de tiempo que se realizan los respaldos la base de datos o sistemas?	Cada semana.
¿Si tienen una red física estructurada y de qué tipo?	Si, recién se hizo un tablero estructurado (**Ver**), tenemos 3 pisos hecho las conexiones en cascada y la parte principal está arriba que se conecta a todo el Municipio.
¿Cuentan con un informe de registros de nuevos equipos y nuevos softwares?	Bodega lleva el control.

¿Constan con un documento de vida útil del equipo?	Bodega lleva ese control, pero hay un sistema que registra cuando ingreso y lleva el control de la vida útil. Pero es difícil la adquisición de un nuevo equipo, cuando un equipo ha llegado a su tiempo, este es reemplazado en otros departamentos.
¿Cuentan con un presupuesto para las TICs?	No es mucho el presupuesto, pero si hay presupuesto
¿Cuentan con un software para registrar las actividades de los empleados?	No se registra
¿Cuentan con un contrato de confidencialidad de información para empleados?	No,
¿Cuentan con un espacio en la nube para guardar la información de la empresa?	Si, dos departamentos cuentan.
¿Cuentan con dominios propios de la empresa como Gmail, hotmail?	Se tiene creadas las cuentas de correo institucional con dominio pangua.gob.ec pero no la utilizan, el departamento administrativo tiene la información de eso al igual que las cuentas de equipos, pero los funcionarios están acostumbrados a trabajar solo con correos personales.
¿Cuál es la estructura del departamento de TICs?	Solo es un funcionario.
¿Cuál es la estructura organizacional de la Municipalidad?	Si cuenta, se Anexa (**Ver**) la estructura organizacional del Municipio.
¿Los empleados tienen restricciones a redes sociales?	Si a todas, Facebook. Twitter, Instagram, WhatsApp web, radio, videos en YouTube entre otras, se tiene una VPN para eso.
¿Cada que tiempo bloquea o apaga la pantalla del ordenador?	Cada 30 min se apaga la pantalla del ordenador.

¿Qué servicio presta o que actividades realiza el departamento de TI?	Cuando se requiere aplicaciones bajo Windows en Visual Studio.
¿Cada que tiempo se realiza mantenimiento a los equipos?	Mensualmente.
¿Tiene un cronograma con el cual se organiza para realizar mantenimiento?	Hace tiempo tubo uno, pero ya no lo ocupa pues no está actualizado.
¿Qué pasa con la información que es manejada, por un funcionario que será despedido?	Se realiza respaldos días antes, en un disco duro que está a custodia del encargado del TI.

Fuente: Grupo Investigador.

11.13. RESULTADO DE LA ENTREVISTA

A continuación, se presenta la interpretación a los resultados obtenidos de la entrevista realizada al Departamento de Sistemas Informáticos del Gobierno Autónomo Descentralizado Municipal de Pangua.

Tabla 16: Resultado de la entrevista.

FICHA DE ENTREVISTA	
Objetivo:	Analizar las vulnerabilidades y necesidades que tiene el Gobierno Autónomo Descentralizado Municipal de Pangua para el desarrollo de políticas de seguridad informáticas de acuerdo a las ISO 27001
Datos Informativos:	
Entrevistado:	Ing. Herman Ortiz
Lugar:	Gobierno Autónomo Descentralizado Municipal de Pangua
Entrevistador:	Cruz Caiza Carla Cristina Gaibor Gavilanez Mónica Lisseth
RESULTADOS	
¿Cuenta con un antivirus? La Municipalidad es un sitio en el que protege sus ordenadores con software gratuito.	
¿La página del Municipio es un sitio seguro?	

La página del Municipio es visiblemente segura, a más de tener un convenio con una empresa que debe garantizar su seguridad.
¿Cuentan con un plan de contingencia para cambiar los equipos (computadoras, cables, laptops, servidores)? En la entrevista se mencionó que es difícil la posibilidad de cambiar a nuevos equipos, pero cuando dejan de ser útiles en un departamento, es cambiado a otro departamento que lo requiera.
¿Cuenta con un DATACENTER adecuado (piso, ventilación, seguridad)? No cuenta con DATACENTER y los servidores no cuentan con un espacio en donde se alojen de forma segura y con las condiciones adecuadas, pero se encuentra ubicado en la oficina de Sistemas Informáticos donde solo el encargado de TI tiene acceso.
¿Cuenta con un UPS para evitar daños en los equipos? Si cuenta con UPS ciertos equipos.
¿Cómo manejan los privilegios de los usuarios? Ningún usuario puede acceder o manipular los servidores.
¿Existe una persona responsable de la seguridad de autenticación de acceso? No porque solo tiene acceso el responsable de TI.
¿Cada que tiempo cambian las contraseñas de su equipo? Existen ciertos funcionarios que no hacen uso de contraseñas, pero el encargado de TI que si hace uso de ellas la renueva cada 3 meses.
¿Cada que tiempo se realiza capacitaciones para el uso de las herramientas dentro de la Municipalidad? No se realizan a menos que sea por el ingreso de un nuevo funcionario.
¿Cómo comparten la información dentro del municipio? La información es compartida por medio de una carpeta en red.
¿Cuentan con comunicación telefónica IP? La Municipalidad si hace uso.
¿Cuentan con un plan de contingencia por desastres naturales? No cuentan con un plan de contingencia que les ayude a actuar ante un desastre natural, tanto para su bienestar como para los activos de la Municipalidad.
¿Periodo de tiempo que se realizan los respaldos la base de datos o sistemas? Se las realizan de las bases de datos, cada semana.

¿Si tienen una red física estructurada y de qué tipo? La Municipalidad es un edificio de 3 pisos, que tiene una red física en cascada.
¿Cuentan con un informe de registros de nuevos equipos y nuevos softwares? Se pudo apreciar que almacenan información respecto a los equipos, pero dicha información no está actualizada.
¿Constan con un documento de vida útil del equipo? Los equipos tienen un documento que especifica información al ingresar a la Municipalidad, pero manifestaron existe un sistema que se encarga de controlar la vida útil de cada equipo.
¿Cuentan con un presupuesto para las TICs? El departamento cuenta con un presupuesto que ha sido asignado para TICs, aunque según el encargado de TI, no es un valor elevado.
¿Cuentan con un software para registrar las actividades de los empleados? No cuentan.
¿Cuentan con un contrato de confidencialidad de información para empleados? Según manifiesta el entrevistado, por el momento no hay documento de confidencialidad firmado por cada empleado del Municipio.
¿Cuentan con un espacio en la nube para guardar la información de la empresa? La municipalidad si cuenta, según manifiesta el entrevistado, desconoce de la capacidad de almacenamiento, pero se da uso de este recurso.
¿Cuentan con dominios propios de la empresa como Gmail, hotmail? La municipalidad cuenta con un dominio pangua.gob.ec, pero los funcionarios no hacen uso de estas cuentas de correo, lo que causa inconvenientes cuando un funcionario es despedido, pues toda la información se la lleva en su cuenta personal de correo.
¿Cuál es la estructura del departamento de TICs? El departamento de TI, es un departamento pequeño que se encarga de dirigir una sola persona, en este caso el entrevistado.
¿Cuál es la estructura organizacional de la Municipalidad? Esta estructura fue solicitada en un departamento, la cual adjuntamos en los anexos.
¿Los empleados tienen restricciones a redes sociales?

El encargado de Sistemas Informáticos, puso restricciones en el uso del internet para las redes sociales, pero se pudo apreciar que ciertos equipos a pesar de ello siguen teniendo acceso.
¿Cada que tiempo bloquea o apaga la pantalla del ordenador? Los ordenadores de la Municipalidad se apagan cada 30 min, solo ciertos ordenadores de funcionarios se bloquean.
¿Qué servicio presta o que actividades realiza el departamento de TI? El encargado de Sistemas Informáticos, se encarga del mantenimiento de los equipos, respaldos de información, desarrollo de aplicaciones, entre otras.
¿Cada que tiempo se realiza mantenimiento a los equipos? Mediante la organización del entrevistado, realiza mantenimiento mensual de los equipos.
¿Tiene un cronograma con el cual se organiza para realizar mantenimiento? Existe uno que necesita de actualizaciones, por tal motivo no hace uso de este.
¿Qué pasa con la información que es manejada, por un funcionario que será despedido? Esta información importante es respaldada en un disco duro, que está en custodia del encargado de Sistemas Informáticos.

Fuente: Grupo Investigador.

11.14. ANÁLISIS DE OBSERVACIÓN

Tabla 17 Análisis de Observación.

FICHA DE OBSERVACIÓN	
Elaborado:	Cruz Caiza Carla Cristina Gaibor Gavilanez Mónica Lisseth
Lugar:	Gobierno Autónomo Descentralizado Municipal de Pangua
Fecha:	25 de Noviembre del 2019
Aspectos	**Observación**
¿Cuenta con un datacenter?	No se observó un DATACENTER y los servidores no estaban alojados en un lugar con seguridad además de condiciones que no se consideran favorables.

¿Cuenta con autenticación en los equipos?	Se pudo apreciar los ordenadores de las diferentes unidades y se evidencio que muchas de ellas no cuentan con bloqueo en sus computadoras.
¿Los equipos cuentan con todos sus accesorios?	Se pudo palpar que por motivos que se desconoce, un ordenador no estaba con mouse.
¿Dan uso al correo corporativo?	No los funcionarios hacen uso de su correo personal, para asuntos laborales.
¿Tiene restricción para el acceso a internet?	Si cuenta en especial para redes sociales.
¿Uso compartido de impresoras?	Se observó que hacen uso de impresoras compartidas con funcionarios del mismo departamento.
¿Respaldan la información?	Respalda la base de datos.
¿Administran documentación impresa?	La municipalidad aun hace uso de documentación física, dependiendo sus funciones.
¿Lleva un registro detallado de los bienes del Municipio y quien está a su cargo?	Se evidencio, que la información acerca de los bienes del Municipio no es actualizada.
¿Cuenta con servidores?	Si cuenta con servidores.
¿Los servidores se encuentran alojados en una zona con seguridad?	No se encuentran en una zona segura.
¿Es permitido el uso de laptop que no son propiedad de la Municipalidad?	Si, ciertos funcionarios ingresan con sus laptops para laborar.
¿Poseen los equipos papel tapiz corporativo, al bloquearse?	No cuenta con un papel tapiz con un diseño basado en la Municipalidad.
¿Cuentan con políticas de seguridad informáticas?	El Municipio no cuenta con políticas de Seguridad Informáticas.
¿Posee con una red física estructurada?	Si posee y es en cascada

Fuente: Grupo Investigador.

11.15. Análisis de los problemas

Como consecuencia de los resultados obtenidos de la entrevista y la observación, hemos analizado los siguientes inconvenientes:

- ✓ No poseen control de acceso a los equipos del municipio (login).
- ✓ No se controla el ingreso y salida de equipos.
- ✓ No posee un Datacenter.
- ✓ Los servidores no se encuentran alojados en un lugar adecuado.
- ✓ No todas las maquinas tienen restricciones a streaming y redes sociales.
- ✓ Los equipos no poseen cobertor anti polvos.
- ✓ No hacen uso del correo corporativo.
- ✓ No realizan respaldos periódicos de los equipos.

En vista de lo expuesto se procedió a elaborar políticas de seguridad informática, que se propone al municipio tome en consideración implementar en el futuro, para que ayude ante los diferentes problemas que se pudo palpar, por ende a continuación detallamos detenidamente cuando usarlas, como funcionan y el responsable de ejecutar cada una de las políticas.

11.16. DISEÑO DEL MODELO DE POLÍTICAS DE SEGURIDAD INFORMÁTICA

Como consecución de la investigación, análisis y levantamiento de cada una de las actividades de este proceso además basándonos a la estructura ya especificada, hemos generado las siguientes políticas:

- ✓ **PO-1A** Control de acceso a recursos computacionales.
- ✓ **PO-1B** Administración de políticas de Active Directory.
- ✓ **PO-1C** Control de Activos de TI.
- ✓ **PO-1F** Resguardo de Información.
- ✓ **PO-1D** Seguridad a componentes informáticos.
- ✓ **PO-1E** Uso adecuado del Internet.

Es importante destacar que para no alterar la estructura del cuerpo de la tesis, se presenta las políticas sin encabezado y pie de página, el formato completo se lo presenta en los Anexos, por ende hemos cumplido con estándares, por lo cual hemos colocado las políticas de la siguiente manera.

La presente política esta propuesta para ser utilizada cuando un nuevo funcionario ingresa a trabajar y necesite acceso a los recursos computacionales para laborar.

Nombre de la Política: PO-1A Control de Acceso a recursos computacionales.

1. Objetivo

Brindar lineamientos para el acceso a los recursos de información importante del Gobierno Autónomo Descentralizado Municipal de Pangua mediante el buen uso de los mecanismos de acceso a los recursos computacionales de la Institución.

2. Alcance

Aplica a todos los miembros de la comunidad del Gobierno Autónomo Descentralizado Municipal de Pangua, incluyendo empleados, contratistas, consultores y visitantes.

3. Definiciones:

Recursos Informáticos: Es un componente físico o virtual incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.

Mecanismos de acceso: Es un mecanismo que permite controlar y conceder el acceso a un computador principal.

Reforzar: Puede tratarse de aquello que se emplea para brindarle resistencia o solidez a algo.

Lineamientos: Es una tendencia, una dirección o un rasgo característico sobre algo.

Password: O contraseña es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa.

4. Documentos de referencia

RE-1A Carta de aceptación de políticas de seguridad informáticas.

RE-2A Solicitud de creación de nuevos usuarios de red.

RE-3A Bitácora de actualización de contraseñas.

5. Descripción de la Política

Por ningún motivo el empleado recibirá el acceso a los recursos computacionales si no ha firmado y a aceptación el documento RE-1A Carta de aceptación de políticas de seguridad.

Para el acceso a los recursos computacionales se asignarán claves y se crearán usuarios de red RE-2A Solicitud de creación de nuevos usuarios de red.

Los recursos informáticos y la información pueden ser usados solo para propósitos autorizados y en cumplimiento con las metas y objetivos del GAD.

A continuación, se considera las siguientes recomendaciones a ser cumplidas por el usuario

✓ Los usuarios y contraseñas son de uso exclusivo por el usuario, deben ser utilizadas únicamente para cuestiones de trabajo, el usuario no podrá usarlas para ningún otro fin, fuera del Municipio.

✓ Las actividades realizadas por estas credenciales son responsabilidad del usuario.

✓ La Municipalidad puede realizar seguimiento de las actividades y uso de las credenciales mediante auditorías periódicas para evaluar su uso adecuado.

✓ El usuario debe comunicar inmediatamente si tiene sospecha que alguien está haciendo mal uso de ellas.

✓ Confidencialidad: Por ningún motivo el usuario debe divulgar las credenciales o claves, estas son intransferibles.

✓ El usuario debe limitarse a ingresar contraseñas cuando estén personas a su alrededor.

✓ Por seguridad de la información si el usuario llegara a perder su contraseña este debe notificar de manera inmediata para ser dado de baja la contraseña del sistema.

✓ La contraseña que elija el usuario deberá ser robusta es decir esta debe contener letras, números y símbolos.

✓ Impedir que personal no autorizado tenga acceso a la información importante de la empresa para que no exista alteraciones o pérdidas ya sea intencionales o accidentalmente.

✓ El usuario deberá cambiar su contraseña cada 3 Meses.

✓ El usuario deberá solicitar ayuda al personal encargado en caso que olvide su contraseña.

✓ El usuario no debe elegir contraseñas antiguas.

✓ Seguridad: El usuario no deberá anotar la contraseña en un lugar físico.

✓ Cualquier persona que, de incumplimiento a las disposiciones señaladas en esta política, puede ser sujeta a una acción disciplinaria según el Reglamento Interno de Trabajo

5.1. Equipos de Cómputo

El inicio de sesión deberá bloquearse cuando haya excedido el límite de 3 intentos.

El usuario debe elegir contraseñas que tenga un mínimo de siete caracteres constituidos de letras, números y símbolos.

5.2. Sistemas informáticos

Configurar para que solicite un inicio de sesión para el ingreso a los recursos computacionales.

Se recomienda implementar un software para generar la cuenta de los empleados (responsable, nombre de equipo, área, contraseña).

Generar un documento de seguimiento de actualización de contraseñas RE-3A Bitácora de actualización de contraseñas.

5.3. Del área de Recursos Humanos

Realizar la selección adecuada del personal para que maneje los accesos de la empresa.

Cuando un empleado es despedido o renuncia se solicitará que su cuenta sea inhabilitada antes que deje el cargo.

6. Registros.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-1A	Carta de aceptación de políticas de seguridad informáticas	Técnico de Servicios Informáticos.	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-2A	Solicitud de creación de nuevos usuarios de red	Técnico de Servicios Informáticos.	Oficina Sistemas área de Soporte a usuarios	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-3A	Bitácora de actualización de contraseñas	Técnico de Servicios Informáticos	Oficina Sistemas área de Soporte a usuarios	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno

7. Anexos.

N/A

El presente registro es el RE-1A o carta de aceptación de políticas de seguridad informáticas, debe ser firmado por el empleado junto con su contrato laboral, este documento hace referencia a que el empleado se compromete a cumplir a cabalidad todos los lineamientos propuestos en las políticas listadas.

RE-1A - CARTA DE ACEPTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICAS

El corazón, (00) de (Mes) del (Año)

Yo, **APELLIDOS Y NOMBRES DEL SOLICITANTE**, portadora de la cédula de identidad **Número,** usuario del Departamento **(Nombre del departamento**), una vez leído y comprendido mis obligaciones, acepto y me comprometo a cumplir las políticas de seguridad informáticas del Gobierno Autónomo Descentralizado Municipal de Pangua.

PO-1A Control de acceso a recursos computacionales.
PO-1B Administración de políticas de Active Directory.
PO-1C Control de Activos de TI.
PO-1F acceso de Información.
PO-1D Seguridad a componentes informáticos.
PO-1E Uso adecuado del Internet.

Atentamente,

APELLIDOS Y NOMBRES DEL SOLICITANTE
C.I.: **Número de cédula**

El presente registro RE-2A o solicitud de creación de nuevos usuarios de red, debe ser solicitado por el funcionario para que les proporcionen acceso a los recursos computacionales, carpetas y archivos a los que puede tener acceso.

Información del usuario solicitante, estos datos son para identificar al funcionario y el área en la que trabajará, con el fin de evaluar sus necesidades laborales y aprobar los requerimientos solicitados.

Información del jefe inmediato, para identificar quien otorgo los accesos, al nuevo funcionario.

Acceso a recursos solicitados, para constar e indicar a los accesos que tiene permitido.

Aprobación, una vez analizado los accesos se firmará como constancia de validez del documento y conformidad de las dos partes.

Para uso de TICs, se debe especificar el nombre del usuario de red generado y finalmente el nombre de quien genero este usuario con firma y fecha de creación para su validez.

El formulario señalado debe contener toda la información solicitada de forma clara, sin correcciones ni enmendaduras, firmado y sellado. Si alguno de los funcionarios no posee todos los requisitos señalados, el trámite será devuelto al funcionario y no se procesará la creación solicitada.

RE-2A - SOLICITUD DE CREACIÓN DE NUEVOS USUARIOS DE RED

1. **Información del usuario solicitante**

Código del empleado: _____

Nombre y Apellido: _____

Departamento: _____

Cargo: _____

2. **Información del jefe inmediato**

Código del empleado: _____

Nombre y Apellido: _____

Cargo: _____

3. **Acceso a recursos solicitados**

Mail:

Interno ☐ Externo ☐

Internet:

Parcial ☐ Total ☐

Tipo de cuenta:

Administrador ☐ Estándar ☐ Invitado ☐

Equipo de cómputo:

PC ☐

Laptop ☐ Justificación: _____

Telefonía IP:

Interno ☐ Local ☐ Nacional ☐ Internacional ☐

4. **Aprobación**

Solicitante: _____ Firma: _____ Fecha: _____

Jefe inmediato: _____ Firma: _____ Fecha: _____

5. **Para uso de TICs**

User Creado: _____(Ejemplo: j_p de Juan Perez)

Entregado por: _____ (Nombre de quien creo cuenta) Firma: _____

Fecha de creación: _____

A continuación, el registro RE-3A Bitácora de actualización de contraseñas, se debe llenar de forma manual toda la información solicitada y firmar, esto como constancia de cumplimiento en caso de una auditoría. Este proceso es muy importante pues el cambio de contraseña asegura la confidencialidad, integridad y disponibilidad de la información que maneja.

RE-3A - BITÁCORA DE ACTUALIZACIÓN DE CONTRASEÑAS

BITÁCORA DE ACTUALIZACIÓN DE CONTRASEÑAS					
CEDULA	**NOMBRE Y APELLIDO**	**DEPARTAMENTO**	**NOMBRE EQUIPO**	**FECHA**	**FIRMA**

La presente política se recomienda utilizar para administrar los inicios de sesión de equipos conectados a red.

Nombre de la Política: PO-1B Administración de políticas Active Directory.

1. Objetivo

Definir políticas de controlador de dominio, reglas de control de acceso a servicios de la red de la Municipalidad para gestionar los sistemas informáticos utilizados por el usuario final.

2. Alcance

Aplica al servidor de dominio, a todas las unidades organizativas, los usuarios y equipos de cómputo dentro de la red del GAD cantonal.

3. Definiciones:

Controlador de dominio: Es un conjunto de ordenadores agrupados que ciñen a unas reglas de seguridad y autenticación comunes.

Unidad Organizativa: Es la que permite crear la jerarquía de nuestra organización, su fin es crear una estructura de carpetas que administrativamente organice una empresa u organización.

Active Directory: Es un servicio establecido de uno o varios servidores en donde se crean objetos como usuarios, grupos con el fin de administrar los inicios de sesión y políticas en toda la red.

4. Documentos de referencia:

ANEXO-1B Asignación de políticas de AD

ANEXO-2B Cronograma de cambio de fondo de pantalla

5. Descripción de la Política

Establecer las buenas prácticas para la gestión de servicios de tecnologías de la información en todos los niveles que se participa para entregar el servicio al cliente. Es necesario contar con herramientas y procesos de gestión de red para controlar posibles fallas o degradaciones en los servicios de red que soportan los servicios de TI utilizando un directorio activo, para una buena administración que ayude en la eficiencia de los empleados durante sus jornadas de acuerdo al ANEXO-1B Asignación de políticas de AD.

6. Registros.

N/A

7. Anexos.

1B Asignación de políticas de AD

2B Cronograma de cambio de fondo de pantalla

El siguiente Anexo-1B Asignación de políticas AD, muestra políticas del Active Directory, que se deben cumplir a cabalidad para proteger la información de la Municipalidad, el departamento de sistemas informáticos será el encargo de poner en marcha estos lineamientos especificados.

ANEXO-1B - ASIGNACIÓN DE POLÍTICAS AD

N°	NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	NO APLICA	APLICA
1	Auditoría	Genera registros de inicios y salida de sesiones tanto exitosas como fallidas en el equipo de cómputo.		X
2	Mensaje de inicio de sesión	Va a indicar un mensaje de inicio.		X
3	Papel tapiz	Despliega un fondo de pantalla.		X
4	Renombrar administrador	Renombrar el usuario administrador local.	X	
5	Regedit	Permite editar el registro del sistema operativo Windows este registro es la base de datos donde se guardan las preferencias del usuario en materia de configuraciones.	X	
6	Prohibir a drivers	Evita accesos a unidades USB.	X	
7	Seguridad	La contraseña del usuario va a caducar cada 3 meses.		X
8	Framework	El usuario no podrá desactivar los framework del antivirus.		X
9	Bloqueo de pantalla	Una vez que se bloquea va a presentar el protector de pantalla para nuevamente activar el usuario o poner el uso donde va a pedir la contraseña.		X

10	Programas de espías	Está prohibida la utilización de “sniffers”, “keylogguers” o cualquier otro software espía en cualquier red o equipo de cómputo.		X
11	Instalación de programas	No podrá instalar ningún software adicional en el equipo que sea asignado.	X	
12	Antivirus	Bloquear el acceso a la administración		X
13	Usuarios locales	Establecer cuentas locales para el acceso a la administración de los equipos de cómputo.		X

El sucesivo Anexo-2B Cronograma de cambio de fondos de pantalla, propone fondos de bloqueo de equipos, según fechas especiales del Cantón o de celebración Mundial para que sea un ambiente de trabajo más interactivo, pero sin perder la formalidad de la Institución.

CRONOGRAMA DE CAMBIO DE FONDOS DE PANTALLA

ANEXO-2B

	MES											
DEPARTAMENTOS	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**
Fondo de Año Nuevo utilizando el logo del Municipio	X											
Fondo del Carnaval Panguense con logo del Municipio		X										
Fondo Normal y Formal con el logo del Municipio			X									
Fondo de Provincialización de Cotopaxi con logo del Municipio				X								
Fondo de Parroquialización de Ramón Campaña, día del trabajo u otro con logo del Municipio.					X							

Fondo de Cantonización utilizando el logo del Municipio						X						
Fondo Normal y Formal con el logo del Municipio							X					
Fondo del Reencuentro Panguense utilizando el logo del Municipio								X				
Fondo de las fiestas de la Virgen de la Merced utilizando el logo del Municipio									X			
Fondo Normal y Formal con el logo del Municipio										X		
Fondo Normal y Formal con el logo del Municipio											X	
Fondo Navideño utilizando el logo del Municipio												X

Esta política se utiliza cuando los funcionarios del municipio descritos en el alcance, recibirán un activo fijo, o este se transferirá de un departamento, con el fin de dar seguimiento a los recursos informáticos del municipio, a su vez los lineamientos propuestos en esta política ayuda a la conservación y buen funcionamientos de los recursos informáticos pues propone cronogramas a seguir, respecto a mantenimientos tanto de datacenter como de equipos, a su vez modelos de bitácoras que respalden su cumplimiento en caso de auditorías informáticas.

Nombre de la Política: PO-1C Administración de activos de TI.

1. Objetivo

Gestionar el ciclo de vida de los activos de la empresa mediante lineamiento e inventarios para la toma de decisiones del Gobierno Autónomo Descentralizado Municipal de Pangua.

2. Alcance

Aplicar a todos los activos fijos tecnológicos de la organización del Gobierno Autónomo Descentralizado Municipal de Pangua, incluyendo empleados, contratistas, consultores y visitantes.

3. Definiciones:

Activos de TI: Son los activos informáticos, su gestión permite alcanzar un manejo adecuado y mejora su eficiencia y rendimiento de la organización.

Datacenter: Es una construcción de gran tamaño donde se alberga los equipos electrónicos necesarios para mantener una red de computadoras.

Hardware: Es la parte física de un ordenador o la parte tangible como CPU (Unidad Central de Procesamiento), la memoria RAM, el disco duro, el monitor, la tarjeta gráfica, el teclado, el ratón, la unidad de disquete, la unidad de CD o DVD, la impresora, el escáner, el disco duro rígido, los altavoces, etc.

Software: Son los programas del computador o la parte intangible que permite realizar multitareas.

Mantenimiento Preventivo: Consiste en la revisión en el software y hardware de la PC u ordenador lo que permite al usuario poseer un equipo fiable para intercambiar información a una máxima velocidad con respecto a la configuración del sistema.

4. Documentos de referencia

RE-1C Inventario de los activos de TI (nombre de equipo, usuario, marca, modelo, tipo, sistema operativo, office, microprocesador, ram, disco duro, monitor).

RE-2C Acta de entrega y recepción de equipo.

RE-3C Bitácora del mantenimiento preventivo del datacenter.

RE-4C Bitácora del mantenimiento preventivo de equipos.

RE-5C Bitácora del mantenimiento correctivo de equipos.

RE-6C Bitácora de acceso al datacenter.

RE-7C Documento de transferencia de activos fijos.

RE-8C Documento de baja a los activos fijos.

ANEXO-1C Cronograma para mantenimiento preventivo del datacenter.

ANEXO-2C Cronograma para mantenimiento preventivo de equipos

ANEXO-3C Cronograma para mantenimiento correctivo de equipos.

5. Descripción de la Política

Todos los activos de TI (RE-1C Inventarios de activos de TI) de la Municipalidad están a cargo del área de TI quien es el responsable hasta que los equipos sean asignados a los usuarios del GAD, los equipos de cómputo se gestionaran así:

5.1. Asignación de activo de TI

Generar documento para que asigne equipos a nuevos empleados, equipos que demande para realizar sus funciones laborales para ello se requiere el RE-2A Solicitud de creación de nuevos usuarios de red. Como también esta política permite supervisar cuántos y cuáles son

los recursos tecnológicos que realmente cuenta el Municipio y posteriormente controlar la fase y el tiempo de los activos para la renovación según su estado.

El área de TI debe tener la capacidad de asignar equipos.

5.2. Asignación de Sistemas Informáticos

El usuario responsable por su equipo deberá firmar un acta de entrega.

Se evaluará el rendimiento del equipo para su uso, cabe mencionar que es recomendable cambiar cada seis a ocho años.

5.3. Transferencia de activos de TI

El usuario responsable de la asignación de equipos es el encargado de departamento de sistemas, en caso de trasferencias de equipos entre empleados, deberá llenar el RE-7C Documento de transferencia de activos.

5.4. Baja de activos de TI

Los equipos que superen los 5 años de vida funcional deben ser dados de baja por su bajo rendimiento RE-8C Documento de baja de activos fijos.

5.5. Mantenimiento de Datacenter

Data Center

La puerta de ingreso al cuarto del Datacenter deberá estar permanentemente cerrada con llave.

El usuario debe controlar que la temperatura del Datacenter este de 18 a 25 Grados Centígrados.

El usuario responsable del Departamento de Sistemas podrá efectuar el mantenimiento se realizará mensual ANEXO 1C Cronograma de mantenimiento preventivo del Datacenter finalizada la actividad llenar la bitácora RE-3C Bitácora de mantenimiento preventivo del Datacenter.

El usuario no podrá consumir alimentos, bebidas o fumar dentro del data center.

Realizar la selección adecuada de la seguridad de la data center es preferible que esta sea cerradura electrónica.

Está prohibido la acumulación y almacenamiento de material inflamables (cartón, papel).

No se puede proveer información sobre la ubicación del Datacenter.

Mantenimiento de PC’s

Realizar manteamiento a todos los equipos cada 6 meses de acuerdo al ANEXO 2C Cronograma para mantenimiento preventivo de equipos finalizado el mantenimiento se debe llenar la bitácora RE-4C Bitácora de mantenimiento preventivo de equipos.

Para el mantenimiento correctivo deberá seguir basándonos en el ANEXO 3C Cronograma para mantenimiento correctivo de equipos de igual forma finalizado la actividad se deberá llenar la bitácora RE-5C Bitácora de mantenimiento correctivo de equipos.

Solo el técnico encargado estará autorizado en sacar los equipos fuera de la empresa.

Solo el técnico encargado tendrá la autorización de realizar instalaciones en los equipos.

Los cables deben estar protegidos por canaletas

Las credenciales de usuario son personal e intransferible.

5. Registros.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-1C	Inventario de los activos de TI	Analista de sistemas informáticos	Oficina Sistemas área de Soporte a equipos	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-2C	Acta de entrega y recepción del equipo	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-3C	Bitácora de mantenimiento preventivo del Datacenter	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-4C	Bitácora de mantenimiento preventivo de equipos	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-5C	Bitácora de mantenimiento correctivo de equipos	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno

RE-6C	Bitácora de acceso al Datacenter	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-7C	Documento de transferencia de activos fijos	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-8C	Documento de baja a los activos fijos	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno

5.1. Anexos.

1C Cronograma para mantenimiento preventivo del datacenter.

2C Cronograma para mantenimiento preventivo de equipos

3C Cronograma para mantenimiento correctivo de equipos.

El sucesivo Registro-1C Inventarios de activos de TI, propone un listado para controlar los recursos informáticos del GAD de Pangua que especifique información real y actualizada. Para ello en la nómina se propone que debe contener:

Código del equipo: Son los códigos que poseen los equipos de cómputo electrónicos que tienen los diferentes departamentos de la municipalidad.

Fecha de entrega: Aquí va la fecha del día en que se entrega el equipo al funcionario del GAD de Pangua.

Responsable: Es importante para dar seguimiento a un equipo registrar a la persona que tiene a responsabilidad el recurso informático, esta información debe ser actualizada en caso de renuncia, despido o algún otro motivo cause el abandono del lugar del trabajo.

Departamento o Unidad: Son los departamentos que posee la Municipalidad de Pangua con sus respectivos equipos, es por ello que se considera necesario una gran organización al conocer el departamento en la que se encuentra cada uno de los equipos.

Dominio: El dominio es el nombre único que se identifica a la red de los equipos de la municipalidad.

Nombre de la PC: Se especifica el nombre de la PC la cual está asignada para el usuario.

Nombre de usuario: Aquí se especifica el nombre de la persona encargada del equipo asignado por el municipio.

Tipo del equipo: Es el modelo de equipo que es propiedad del municipio, estos pueden ser laptop, escritorio o cualquier otro, dependiendo de las necesidades de cada departamento o unidad.

Marca: En este segmento se debe especificar la marca de la Laptop o CPU en caso de Escritorio.

Modelo: Se especifica el modelo de la de las laptops, computadoras de escritorio que posee los departamentos.

Serie CPU: Es la cadena de caracteres único que identifica la CPU.

Serie Laptop: Es la cadena de caracteres único, que lleva especificada las laptops por lo general donde se ubica la batería.

Serie Servidor: Es la cadena de caracteres único, que identifica de un servidor a otro.

Procesador: Se detalla las características del procesador que posee el equipo propiedad de la Municipalidad.

RAM: Se especifica la capacidad que posee el equipo, de igual forma esta información ayuda para la toma de decisiones en un futuro.

Disco Duro: Se puntualiza la capacidad del dispositivo, para en el futuro ayudar en la toma de decisiones para su reemplazo.

Marca del Monitor: Se detalla la marca del monitor en caso de equipo de escritorio, para laptop se recomienda llenar esta característica con N/A (No Aplica).

Marca del Teclado: Se define la marca como constancia que el escritorio posee este accesorio, en caso de laptop si no hace uso de un teclado externo, se propone escribir en esta característica N/A (No Aplica).

Marca del Mouse: Se detalla la marca del accesorio, en caso que no se haga uso en laptop se recomiendo utiliza N/A (No Aplica).

Adaptador laptop: Se especifica la serie que posee el cargador de la laptop.

Accesorio: Se menciona todos los materiales que posee las laptops como; maleta, audífonos, etc., esto sirve para llevar seguimiento de cada uno de los accesorios.

Candado: Especifica si se entrega este accesorio que sirve para dar seguridad a las laptops del municipio.

Sistema Operativo: Se detalla el sistema operativo que esté instalado en el equipo, esto porque ya sea con licencia o libre, ayuda a la toma decisiones al encargado de Sistemas informáticos.

Office: Se detalla el office que lleva los equipos de cómputo de la entidad.

RE-1C INVENTARIO DE LOS ACTIVOS DE TI

INVENTARIO DE LOS ACTIVOS DE TI																							
N°	CÓDIGO DEL EQUIPO	FECHA DE ENTREGA	RESPONSABLE	DEPARTAMENTO	DOMINIO	NOMBRE DEL PC	NOMBRE DEL USUARIO	TIPO DEL EQUIPO	MARCA	MODELO	SERIE			POCESADOR	RAM	DISCO DURO	MONITOR	TECLADO	MOUSE	ADAPTADOR LAPTOP (cargador)	ACCESORIO (Maletas)	CANDADO	SISTEMA OPERATIVO	OFFICE
											CPU	LAPTOP	SERVIDOR				MARCA	MARCA	MARCA					

A continuación, el RE-2C Acta de entrega y recepción del equipo, propone un documento que será llenado como constancia que se entrega el equipo a un funcionario y este equipo se encuentra en buen estado, se debe firmar el documento por parte del funcionario que recibe el equipo y del encargado para sellar la constancia y a partir de ese momento la persona que recibe el equipo, es responsable mientras labore en el municipio.

Activo fijo: Se detalla en caso de proporcionar al funcionario algún activo fijo, caso contrario se redacta Ninguno o N/A, no es recomendable dejar estos espacios en blanco.

Nombre del Equipo: Se especifica el nombre del equipo que será entregado al empleado.

Usuario: Se puntualiza a la persona a quien se le entrega el equipo.

Marca: Se escribe la marca del equipo a entregar.

Modelo: Se describe el modelo de fábrica del equipo.

Tipo: Se detalla si es laptop o escritorio.

Serie: Se detalla la serie que es característica propia del equipo a entregar.

Sistema Operativo: Describe el sistema operativo con el que se entrega instalado al empleado.

RAM: Capacidad del equipo a entregar.

Disco duro: Especifica la capacidad del disco duro a entregar.

Microprocesador: Se detalla la información acerca del microprocesador del equipo.

Monitor: La marca y serie del monitor que se entrega.

Mouse: Se escribe la marca y serie del accesorio, en caso de no entregar se escribe ninguno o N/A (No Aplica).

Teclado: Detallar la marca y serie del accesorio, en caso de no entregar se escribe ninguno o N/A (No Aplica).

Nota: Es un segmento en el que se puede describir algún otro accesorio a entregar, o en caso exista alguna anomalía respecto al equipo o accesorio.

RE-2C ACTA DE ENTREGA Y RECEPCIÓN DEL EQUIPO

A los _____ días del mes de _____ del año _____se procede a realizar la entrega y recepción de los equipos que se detallaran, al Departamento de _____ del Gobierno Autónomo Descentralizado Municipal de Pangua.

Activo fijo	Nombre de equipo	Usuario	Marca	Modelo	Serie	Tipo	S.O	RAM	Disco Duro	Microprocesador	Monitor	Mouse	Teclado

Nota:_____
_____

Como constancia de que los equipos se entregaron en buen estado, se procede a la firma de recibido.

_____ _____

APELLIDOS Y NOMBRES DE RECIBIDO
C.I.: **Número de cédula**

APELLIDOS Y NOMBRES DEL ENCARGADO
C.I.: **Número de cédula**

El siguiente RE-3C Bitácora de mantenimiento preventivo de Datacenter, se propone un modelo de bitácora a llenarse ante el cumplimiento del cronograma ANEXO-1C Cronograma para mantenimiento preventivo del Datacenter, esto cuando en el futuro el municipio adquiera Datacenter proporcione un buen trato y extienda su vida útil.

Departamento: Detalla el departamento que está ubicado el Datacenter que se realizó el mantenimiento.

Fecha: En vista que en el cronograma se propone por mes en este segmento se debe especificar con día, mes y año en el que realizo el mantenimiento.

Descripción de Mantenimiento: En este segmento se describe la reparación que se haya realizado dentro del Datacenter.

Firma: Debe ser firmada por el encargado de TI, esta es la constancia que el mantenimiento fue realizado.

RE-3C BITÁCORA DE MANTENIMIENTO PREVENTIVO DE DATACENTER

BITÁCORA DE MANTENIMIENTO PREVENTIVO DE DATACENTER			
DEPARTAMENTO	**FECHA**	**DESCRIPCIÓN DE MANTENIMIENTO**	**FIRMA**

A continuación, el registro RE-4C Bitácora de Mantenimiento preventivo de equipos, se propone una bitácora que se debe llenar una vez cumplido el mantenimiento especificado en el ANEXO-2C Cronograma para mantenimiento preventivo de equipos, el encargado de TI debe llenar los campos solicitados, estos campos son:

Departamento: Es el nombre del departamento donde proviene el equipo, con esta información se puede conocer al equipo que ya se realizó el mantenimiento.

Nombre de Equipo: Es el nombre que se proporcionó al equipo para identificarlo del resto.

Fecha: Se describe el día, mes y año en el que se realizó el mantenimiento preventivo del equipo.

Hora: Se detalla la hora en la que se realizó mantenimiento al equipo.

Problema: Se describe los inconvenientes encontrados en el equipo y lo que se hizo para solventar el inconveniente.

Firma: Debe firmar la persona que realizo el mantenimiento en este caso el encargado de Sistemas Informáticos, como constancia que el mantenimiento fue realizado.

RE-4C BITÁCORA DE MANTENIMIENTO PREVENTIVO DE EQUIPOS

BITÁCORA DE MANTENIMIENTO PREVENTIVO DE EQUIPOS					
DEPARTAMENTO	**NOMBRE EQUIPO**	**FECHA**	**HORA**	**PROBLEMA**	**FIRMA**

El siguiente Registro es el RE-5C Bitácora de mantenimiento correctivo de equipos, se propone utilizar para hacer constancia que el mantenimiento fue realizado, esto debe ser llenado y firmado por el encargado de Sistemas Informáticos de la siguiente manera:

Departamento: Se especifica el nombre de la unidad que proviene el equipo, con esta información se puede identificar al equipo que ya se realizó el mantenimiento.

Nombre de Equipo: Se puntualiza el nombre que se proporcionó al equipo, para identificarlo del resto.

Fecha: Se describe el día, mes y año en el que se realizó el mantenimiento preventivo del equipo.

Hora: Se detalla la hora en la que se realizó las correcciones al equipo.

Problema: Se describe las correcciones necesarias que se le hizo al equipo, para que funcione con total normalidad y sin inconvenientes.

Firma: Debe firmar la persona que realizo el mantenimiento en este caso el encargado de Sistemas Informáticos, como constancia que el mantenimiento fue realizado.

RE-5C BITÁCORA DE MANTENIMIENTO CORRECTIVO DE EQUIPOS

BITÁCORA DE MANTENIMIENTO CORRECTIVO DE EQUIPOS					
DEPARTAMENTO	**NOMBRE EQUIPO**	**FECHA**	**HORA**	**PROBLEMA**	**FIRMA**

A continuación, se presenta el Registro RE-6C Bitácora de acceso al Datacenter, el documento se propone debe reposar fuera del Datacenter y debe llenarse cuando personal autorizado ingresa al Datacenter a realizar alguna diligencia, es importante llevar este control, puesto que es un lugar muy importe y caso llegará a darse algo inusual, se dará seguimiento mediante la bitácora. Esta bitácora debe ser llenada y firmada únicamente por la persona autorizada que ingresa, se debe llenar de la siguiente forma:

Fecha de ingreso: Se especifica el día, mes y año que ingresa al Datacenter.

Hora de ingreso: La hora debe ser real, debe ser el memento en el que va a ingresar.

Firma de ingreso: Es la constancia de que no es otra persona suplantando su identidad.

Nombre: Debe ingresar Nombres y Apellidos completos de forma clara, sin tachones ni enmendaduras.

Actividad realizada: se debe especificar el motivo por el cual desea ingresar al Datacenter.

Hora de salida Se debe especificar la hora exacta que la persona autorizada esta fuera del Datacenter.

Firma de Salida: Es la constancia que la persona afirma haber ya salido a la hora especificada y se encuentra fuera del Datacenter.

RE-6C BITÁCORA DE ACCESO AL DATACENTER

BITÁCORA DE ACCESO AL DATACENTER						
Fecha Ingreso	**Hora Ingreso**	**Firma Ingreso**	**Nombre**	**Actividad Realizada**	**Hora Salida**	**Firma Salida**

El presente registro es el RE-7C Documento de transferencia de activos fijos, se propone utilizar cuando un activo fijo pasara a manos de otra persona ya sea del mismo departamento o no, según nuestra investigación esto es muy importante para dar seguimiento al equipo, deslindando de su responsabilidad al antiguo custodio. Contiene los siguientes campos que se propone debe especificar así:

En el segmento del párrafo se propone deberá llenar día, mes y año verídico en que se realizó la transferencia, esto sin tachones ni enmendaduras.

Activo Fijo: Se debe detallar el activo fijo a transferir, caso que sea ninguno este campo no debe ir vacío, se deberá llenar utilizando N/A (No aplica) o Ninguno.

Descripción: Detalla el motivo por el que será transferido el equipo a otro departamento.

Serie, modelo y marca: como su campo lo pide, se deberá escribir las características exactas del equipo a transferir.

Departamento del anterior custodio: Se describe el nombre de la unidad actual a la que pertenece el equipo.

Departamento del nuevo custodio: Se detalla el nombre de la unidad a la que va a ser transferida el equipo.

Anterior custodio: Se detalla el nombre y apellido de la persona que estaba a cargo del equipo a transferir.

Nuevo custodio: Se especifica el nombre y apellido de la persona a la que se le dará a cargo el equipo.

Firmas: Las firmas son partes esenciales como constancia que la información proporcionada en el documento es verídica, debe firmar el anterior custodio, nuevo custodio y director de finanzas.

RE-7C DOCUMENTO DE TRANSFERENCIA DE ACTIVOS FIJOS

En el cantón Pangua a los __días del mes de_____ del año _____, se procede a la **Transferencia de activos** el equipo que se especifica a continuación con los respectivos empleados:

ACTIVO FIJO	DESCRIPCIÓN	SERIE, MODELO Y MARCA	DEPARTAMENTO DEL ANTERIOR CUSTODIO	DEPARTAMENTO DEL NUEVO CUSTODIO	ANTERIOR CUSTODIO	NUEVO CUSTODIO

De acuerdo a lo anterior se hace constar que el equipo se encuentra en normal funcionamiento

Anterior Custodio	Nuevo Custodio	Director de Finanzas
_____	_____	_____
NOMBRE Y FIRMA	**NOMBRE Y FIRMA**	**NOMBRE Y FIRMA**

A continuación, muestra la propuesta de RE-8C Documentos de baja a los activos fijos, formulario que según nuestra investigación es importante cuando la vida útil de algún activo fijo llegue a su límite, es un documento de respaldo si necesita conocer que paso con un activo en especial. Es por eso que se explica cómo debe llenarse.

Acta N°: Es el número de acta, este debe ir en orden según se vaya dando de baja los activos.

Fecha: Se debe especificar día, mes y año que se está dando de baja el activo.

Nombre del responsable: Es el nombre del funcionario que está responsable del activo fijo.

Departamento: Es la unidad en la que estaba funcionando el equipo.

Equipo de cómputo: Se especifica el nombre del equipo.

Activo fijo: Se especifica la descripción del activo fijo a dar de baja.

Detalle: Se detalla el estado del activo fijo a dar de baja.

Marca: En este segmento ingresa información verídica de la marca del equipo

Modelo: Redacta el modelo exacto del equipo.

Serie: Especifica el número de serie con el que se identifica al equipo.

Valor de adquisición: Se debe escribir el precio que se adquirió el equipo, se debe anexar la factura donde indica el costo.

Valor depreciado: Es el valor que cuesta actualmente el equipo según su estado y años de uso.

Fecha de compra: Se detalla el día, mes y año que se adquirió el equipo.

Causa de baja: Se explica por qué se da de baja el activo fijo y se anexa un documento que justifique la baja.

Observaciones: Se detalla alguna situación o alguna información adicional con respecto la baja de activos.

Firmas: Firman como constancia de la baja del activo, los departamentos asignados se los propuso porque según investigaciones ellos están involucrados en dar seguimiento a estos activos.

RE-8C DOCUMENTO DE BAJA A LOS ACTIVOS FIJOS

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE PANGUA

INFORME DE BAJA DE BIENES

ACTA N°:_____
FECHA:
_____

NOMBRE DEL RESPONSABLE: _____

DEPARTAMENTO: _____

EQUIPO DE COMPUTO: _____

CARACTERÍSTICAS

Activo Fijo	Detalle	Marca	Modelo	Serie	Valor de adquisición	Valor depreciado	Fecha compra

CAUSA DE BAJA: _____

(Documentación anexa para verificación física documental)

DOCUMENTACIÓN INTEGRANTE AL REVERSO

OBSERVACIONES:_____

_____

_____ _____

SISTEMAS INFORMÁTICOS DIRECCIÓN FINANCIERA

_____

DIRECCIÓN ADMINISTRATIVA

El siguiente Anexo se trata del Cronograma para mantenimiento preventivo del Datacenter, en la que se propone realizarlo en las fechas estipuladas, no hemos designado un día exacto, para que el encargado de Sistemas informáticos lo pueda cumplir cualquier día del mes, de igual forma se ha propuesto ciertos elementos del Datacenter que pueden darse mantenimiento, esto para mantener el lugar en condiciones óptimas y garantice la seguridad de los equipos dentro del mismo.

Las firmas propuestas son el compromiso y aceptación de cumplir el cronograma propuesto.

ANEXO-1C CRONOGRAMA PARA MANTENIMIENTO PREVENTIVO DEL DATACENTER

	MES											
DATACENTER	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiem.**	**Octubre**	**Noviem.**	**Diciemb**
Equipos de Networking					x							x
Servidores					x							x
Iluminación					x							x
Climatización (motores, aire acondicionado, temperatura, etc.)					x							x
Control de incendio (extintores, sensores)					x							x
UPS					x							x
Control de acceso (cámaras, tarjetas, etc.)					x							x
Piso					x							x

_____ _____

FIRMA DE ENCARGADO DE TI **FIRMA DEL ALCALDE**

C.I.: NÚMERO DE CEDULA **C.I.: NÚMERO DE CEDULA**

El presente ANEXO-2C Cronograma para mantenimiento preventivo de equipos, se propone para organizar el mantenimiento preventivo de los equipos de cada departamento, de igual forma se propone el mes con la finalidad que pueda realizar cualquier día del mes.

ANEXO-2C CRONOGRAMA PARA MANTENIMIENTO PREVENTIVO DE EQUIPOS

	MES											
DEPARTAMENTOS	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiem**	**Octubre**	**Noviem**	**Diciemb**
MIES	X											
UNIDAD DE CULTURA	X											
PROMOCIÓN COMUNITARIA		X										
SERVICIOS GENERALES		X										
PLANIFICACIÓN Y DESARROLLO			X									
ASESORÍA DE ALCALDÍA			X									
UNIDAD TÉCNICO DE GESTIÓN DE RIESGOS			X									
UNIDAD DE TALENTO HUMANO				X								
ADMINISTRACIÓN DE PLAZAS Y MERCADOS				X								
COMISARIA MUNICIPAL					X							
SECRETARIA EJECUTIVA DE LA NIÑEZ Y ADOLESCENCIA DEL CANTÓN PANGUA					X							
CONSEJO CANTONAL DE PROTECCIÓN DE DERECHOS						X						

DIRECCIÓN FINANCIERA						X						
UNIDAD DE ATENCIÓN A GRUPOS VULNERABLES							X					
REGISTRO DE LA PROPIEDAD							X					
SECRETARIA GENERAL								X				
UNIDAD TÉCNICO DE INFRAESTRUCTURA Y DISEÑO DE PROYECTOS								X				
UNIDAD DE FISCALIZACIÓN									X			
VIALIDAD Y EQUIPO CAMINERO									X			
AGUA POTABLE Y ALCANTARILLADO									X			
OBRAS PÚBLICAS										X		
RECAUDACIÓN										X		
OFICINA DE RENTAS										X		
TESORERO											X	
ORDENAMIENTO TERRITORIAL											X	
SISTEMAS INFORMÁTICOS											X	
SINDICATURA												X
AVALÚOS Y CATASTROS												X
BODEGA												X

_____ _____

FIRMA DE ENCARGADO DE TI
C.I.: Número de cédula

FIRMA DE ALCALDE
C.I.: Número de cédula

A continuación, se presenta el ANEXO-3C Cronograma para mantenimiento correctivo de equipos, se propone el cronograma con la finalidad de mejorar el rendimiento de los equipos de la municipalidad, indicando el mes para que pueda realizar las correcciones de los equipos cualquier día del mes.

ANEXO-3C CRONOGRAMA PARA MANTENIMIENTO CORRECTIVO DE EQUIPOS

	MES											
DEPARTAMENTOS	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiem.**	**Octubre**	**Noviem.**	**Diciemb**
MIES	X			X			X			X		
UNIDAD DE CULTURA	X			X			X			X		
PROMOCIÓN COMUNITARIA	X			X			X			X		
SERVICIOS GENERALES	X			X			X			X		
PLANIFICACIÓN Y DESARROLLO	X			X			X			X		
ASESORÍA DE ALCALDÍA	X			X			X			X		
UNIDAD TÉCNICO DE GESTIÓN DE RIESGOS	X			X			X			X		
UNIDAD DE TALENTO HUMANO	X			X			X			X		
ADMINISTRACIÓN DE PLAZAS Y MERCADOS	X			X			X			X		
COMISARIA MUNICIPAL	X			X			X			X		

SECRETARIA EJECUTIVA DE LA NIÑEZ Y ADOLESCENCIA DEL CANTÓN PANGUA	X			X			X			X		
CONSEJO CANTONAL DE PROTECCIÓN DE DERECHOS	X			X			X			X		
DIRECCIÓN FINANCIERA	X			X			X			X		
UNIDAD DE ATENCIÓN A GRUPOS VULNERABLES	X			X			X			X		
REGISTRO DE LA PROPIEDAD	X			X			X			X		
SECRETARIA GENERAL	X			X			X			X		
UNIDAD TÉCNICO DE INFRAESTRUCTURA Y DISEÑO DE PROYECTOS	X			X			X			X		
UNIDAD DE FISCAIZACIÓN	X			X			X			X		
VIALIDAD Y EQUIPO CAMINERO	X			X			X			X		
AGUA POTABLE Y ALCANTARILLADO	X			X			X			X		
OBRAS PÚBLICAS	X			X			X			X		
RECAUDACIÓN	X			X			X			X		
OFICINA DE RENTAS	X			X			X			X		
TESORERO	X			X			X			X		
ORDENAMIENTO TERRITORIAL	X			X			X			X		

SISTEMAS INFORMÁTICOS	X			X			X			X		
SINDICATURA	X			X			X			X		
AVALÚOS Y CATASTROS	X			X			X			X		
BODEGA	X			X			X			X		

_____ _____

FIRMA DE ENCARGADO DE TI
C.I.: Número de cédula

FIRMA DE ALCALDE
C.I.: Número de cédula

La presente política propuesta hace referencia a los respaldos de la información que maneja la municipalidad, se utiliza al momento de querer respaldar la información importante, para que siempre esté integra, disponible y confiable, de forma que no detenga sus actividades.

Nombre de la Política: PO-1F Resguardo de información

1. Objetivo

Definir e implementar lineamientos para respaldar la información relevante en todos los niveles de la Municipalidad.

2. Alcance

Aplica a todos los miembros de la comunidad del Gobierno Autónomo Descentralizado Municipal de Pangua. Definida en el ANEXO-1F Listado de usuarios para backup**.**

3. Definiciones:

SyncBack: Es un programa gratuito que sincroniza y hace copias de seguridad de los archivos, carpetas, directorios entre otros.

4. Documentos de referencia:

ANEXO-1F Listado de usuarios para backup

RE-1F Bitácora de respaldos de usuarios.

5. Descripción de la Política

Evitar la pérdida de la información dentro de la empresa en caso de que existan eventos fortuitos con el fin de garantizar la disponibilidad de la información.

5.1. Responsabilidad de los Usuarios

El usuario debe almacenar su información laboral dentro de la carpeta llamada RESPALDOS que va estar alojada en la unidad D si no tiene una partición se creara una carpeta dentro de la partición.

El usuario debe dar acceso de su información cuando el personal de tecnología de información lo requiera.

5.2. Responsabilidad del área de Sistemas Informáticos

El departamento de sistemas debe crear una carpeta para que los usuarios almacenen ahí su información y se haga el debido respaldo (Ejemplo: D:\respaldos), caso que el usuario no acate la disposición de almacenar en esa carpeta la información, el encargado de Sistemas Informáticos no se hará responsable de la pérdida de dicha información.

Implementar un software específico que ayude a generar respaldos periódicamente.

Asignar espacios de almacenamiento específico de acuerdo a la posición que desempeñe el usuario final.

Generar el control de acuerdo al RE-1F Bitácora de respaldos de usuarios.

Disponer con una segunda herramienta para respaldos de información.

5.3. Responsabilidad del área de Recursos Humanos

Proporcionar información de la salida de personal con tiempo suficiente (48 horas) para la planificación de respaldos de información.

6. Registros.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-1F	Bitácora de respaldos de usuarios.	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno

7. Anexos.

ANEXO-1F Listado de usuarios para Backups

A continuación, se propone el registro RE-1F Bitácora de respaldos de usuarios, es un listado en que lleva el control de la fecha en que realizo el respaldo. Los campos deben llenarse de la siguiente manera:

Cargo: Es el cargo u ocupación que tiene el empleado en municipio, este campo debe estar sin tachones ni enmendaduras.

Nombre de equipo: Se describe el nombre que identifica al equipo.

Meses: Se señala con una x el mes que fue realizado el respaldo de la información.

RE-1F BITÁCORA DE RESPALDOS DE USUARIOS

N°	CARGO	NOMBRE EQUIPO	MESES											
			ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
1														
2														
3														
4														
5														
6														
7														
8														
9														
10														

El siguiente es el ANEXO-1F Listado de usuarios para backup, se propone este documento para ser utilizado como un registro de los usuarios a los que se debe generar el respaldo, especificando cierta información como:

Nombre de equipo: Es el nombre que se reconoce al equipo, se sugiere vaya con abreviaciones de palabras, un nombre que contenga la ubicación del municipio, tipo de equipo, el departamento a la que pertenece el equipo, seguido del número según su prioridad siendo 01 la más alta.

Cargo: Es la unidad a la que pertenece el equipo.

Periodo de respaldo: Especifica el tiempo estimado, que se debe realizar el respaldo.

ANEXO-1F LISTADO DE USUARIOS PARA BACKUP

LISTADO DE USUARIOS PARA BACKUP			
N°	**NOMBRE DE EQUIPO**	**CARGO**	**PERÍODO DE RESPALDO**
1	Panpcfin-01	Dirección Financiera	Semanal
2	Panpcalc-02	Asesoría de Alcaldía	Semanal
3	Pannbsis-03	Gerente de Sistemas	Semanal
4	Panpcplaymer-04	Administración de plazas y mercados	Semanal
5	Panpcrec-05	Recaudación	Semanal
6	Panpctes-06	Tesorero	Semanal
7	Panpcsecg-07	Secretaria general	Semanal
8	Panpcregpro-08	Registro de la propiedad	Semanal

La presente política de seguridad informática se emplea para controlar y verificar los activos del municipio, debido que por diversos factores que se presenten puede surgir la necesidad de sacar los activos fijos del GAD, por ello los lineamientos propuestos hace énfasis que no es recomendable realizar el acto a menos que sea por cuestiones urgentes, entonces al darse el caso se trata dar seguimiento al equipo con la finalidad de cuidar los activos y evitar pérdidas.

Nombre de la Política: PO-1D Seguridad de componentes informáticos.

1. Objetivo

Generar lineamientos para proteger y resguardar los componentes informáticos del Gobierno Autónomo Descentralizado Municipal de Pangua.

2. Alcance

Aplica a toda la infraestructura del Gobierno Autónomo Descentralizado Municipal de Pangua.

3. Definiciones:

Componente informático: Son el conjunto de equipos y programas que conforman un computador o sistema informático.

4. Documentos de referencia:

RE-1D Bitácora de registro de salida e ingreso de equipos.

RE-2D Bitácora de control de ingreso y salida de equipos de visitas.

ANEXO1D- Listado de personas autorizadas.

5. Descripción de la Política

El departamento de sistemas informáticos es el encargado de proteger, planificar y dar seguimiento a los lineamientos de seguridad establecidos:

- ✓ Protección de los equipos.
- ✓ Ingreso de equipos y dispositivos externos, que no son propios de la institución.

5.1. Responsabilidad del Departamento de Sistemas Informáticos

Debe proporcionar e instalar un antivirus garantizado su adecuado funcionamiento, cortafuegos para bloquear el acceso no autorizado a la red con el fin de evitar virus, gusanos, ataques, robo de datos, etc.

Debe actualizar los programas que regulan la seguridad (Antivirus, licencias, sistemas operativos).

5.2. Acceso a servidores

TI tiene la responsabilidad de asignar los permisos adecuados para el acceso a los servidores, para que el especialista analice su estado y funcionamiento.

No se puede ingerir alimentos en el área de servidores pues cualquier derrame podría ocasionar pérdidas del activo.

5.3. Protección de equipos

Implementar Antivirus en los equipos con sus debidas actualizaciones.

Es recomendable instalar un Sistema Operativo con licencias autorizadas y que estén acorde con las características de la computadora, se recomiendan versiones a partir de Windows 8.1 pro hasta Windows 10.

Los equipos deben tener un cobertor anti polvos para alargar el tiempo de vida útil.

No se puede ingerir alimentos ante los activos, pues cualquier derrame podría ocasionar pérdidas del activo.

5.4. Ingreso y salida de equipos

Los dispositivos de red son propiedad de la empresa, por lo que ningún empleado puede hacer uso externo de él.

Para el ingreso de equipos externos, debe tener un documento de autorización y llevar un control de acuerdo al RE-1D Bitácora de registro de salida e ingreso de equipos, en caso de empleados.

Para el ingreso de equipos de personas visitantes, debe llevar control el personal encargado de la seguridad, mediante la RE-2D Bitácora de control de ingreso y salida de equipos de visitas.

Las laptops del Municipio deben tener candado.

Los empleados que deben llevarse los equipos deben tener una autorización previa ANEXO1D- Listado de personas autorizadas.

6. Registros.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-1D	Bitácora de registro de salida e ingreso de equipos	Analista de sistemas	Oficina Sistemas área de análisis de sistemas	23/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-2D	Bitácora de control de ingreso y salida de equipos de visitas.	Personal encargado de la seguridad(guardia)	Ingreso al edificio	23/08/2020	Anual	2años	Reciclaje de papel	Uso interno

7. Anexos.

ANEXO1D- Listado de personas autorizadas

A continuación, se muestra la propuesta de registro RE-1D Bitácora de registro de salida e ingreso de equipos, con este documento se trata llevar el control de la persona que por cuestiones que debe aclarar, saco el equipo de la municipalidad. La bitácora solicita ciertos campos que deben ser llenados de forma clara, sin tachones y enmendaduras.

Responsable: Se detalla el nombre y apellido de la persona a cargo del equipo que saldrá de la municipalidad.

Cargo: Es la unidad a la que pertenece el equipo.

Motivo: Se debe especificar de forma clara, directa y sin tachones el motivo por el cual el equipo saldrá del municipio, seguido del nombre del equipo, marca y serie.

Hora de salida: Es la hora exacta en la que el equipo saldrá.

Firma: El campo es obligatorio de llenar una vez llenado la hora de salida, como constancia que el funcionario afirma ser quien estipulo la hora en la bitácora, la firma debe ser la utilizada en la cédula de ciudadanía.

Hora de ingreso: La hora exacta en la que el equipo ingresa al municipio, este proceso debe ser acompañado del guardia quien controlara la presencia del equipo.

Firma: Se debe firmar de manera obligatoria al ingresar el equipo, como constancia y compromiso que el equipo ingreso al municipio. La firma debe ser la misma de la cédula de ciudadanía.

RE-1D BITÁCORA DE REGISTRO DE SALIDA E INGRESO DE EQUIPOS

BITÁCORA DE REGISTRO DE SALIDA E INGRESO DE EQUIPOS						
RESPONSABLE	**CARGO**	**MOTIVO**	**HORA DE SALIDA**	**FIRMA**	**HORA DE INGRESO**	**FIRMA**

A continuación, se muestra la propuesta de registro RE-2D Bitácora de control de ingreso y salida de equipos de visitas, este documento tiene la finalidad de controlar el ingreso y salida de equipos propiedad de las personas que ingresan como visitantes al municipio, este documento debe gestionar el encargado de la seguridad (guardia) del GAD, por ende debe reposar en el ingreso al edificio.

Responsable: Es el nombre de la persona quien ingresa con su equipo y debe llenar con sus respectivos nombres completos.

Marca: Es la marca del equipo de cómputo que está ingresando a la institución.

Modelo: Es el modelo de equipo de cómputo que ingresa.

Serie: Es la serie que posee el equipo de cómputo de la persona que ingresa al municipio.

Fecha: Aquí va la fecha que visita a la institución para llevar un registro adecuado.

Hora de ingreso: Aquí específica la hora de ingreso a la entidad.

Hora de salida: Aquí específica la hora de salida a la entidad.

Firma: Por último, se especifica la firma de salida de la persona que ingreso a la institución.

RE-2D BITÁCORA DE CONTROL DE INGRESO Y SALIDA DE EQUIPOS DE VISITAS

BITÁCORA DE CONTROL DE INGRESO Y SALIDA DE EQUIPOS DE VISITAS								
N°	**NOMBRE DEL RESPONSABLE**	**MARCA**	**MODELO**	**SERIE**	**FECHA**	**HORA DE INGRESO**	**HORA DE SALIDA**	**FIRMA**

A continuación, se presenta el ANEXO-1D Listado de personas autorizadas, se propone este listado para que el encargado de la Unidad de Sistemas Informáticos quien está a cargo de los equipos del municipio, sea el responsable de enlistar a las personas que por motivos laborales en verdad requieran sacar los equipos fuera del GAD y por ende autoriza hacer uso de la RE-1D Bitácora de registro de salida e ingreso de equipos, para seguimiento del equipo.

Se propone sea obligatorio e importante llenar todos los campos solicitados, para tener la información correcta en caso de seguimiento del equipo.

Código: Aquí se especifica el código de las laptops que existe en la municipalidad que va a salir.

Tipo: Se detalla el tipo de equipo de cómputo que posee la entidad a entregar al usuario que va a salir.

Activo Fijo: Debe detallar el nombre del activo fijo que está autorizado a salir.

Responsable: Se debe escribir los Nombres y Apellidos completos de la persona quien está a cargo del equipo.

Cargo: Es la unidad o departamento donde labora o pertenece el equipo.

Modelo: Es el modelo de fábrica que identifica al equipo.

Serie: Es la designación que tiene el equipo para identificarlo del resto.

ANEXO-1D LISTADO DE PERSONAS AUTORIZADAS

CÓDIGO	TIPO	RESPONSABLE	CARGO	MARCA	MODELO	SERIE
1.4.1.01.07.013.003	Laptop	Ing. Luis Guzmán	Director de saneamiento ambiental	DELL	CPDCBD6P03	CN-OCK6DB-CMC00-9B6-0005
1.4.1.01.07.001.001.051	Laptop	Ing. Manuel Coronel	Gestión de Riesgos	HP	NOTEBOOK	5CG6441WY
1.4.1.01.07.001.002.17	Laptop	Dra. Gabriela Rivera	Saneamiento ambiental	HP	NOTEBOOK	5CG6441R54
1.4.1.01.07.001.002.009	Laptop	Ing. Ingrid Torres	Tesorero Municipal	HP	Z800K15	CND3510HQR
1.4.1.01.07.001.002.15	Laptop	Sra. Jenny Domínguez	Recaudadora, Dirección Financiera	ACER	E5-471	NXMN2AL00342809897600
1.4.1.01.07.001.002.012	Laptop	Ing. Henry Tana	Administración de Plazas y Mercados	TOSHIBA	SATELIT	S4E1265312C
1.4.1.01.07.001.002.011	Laptop	Ing. Washington Palacios	Dirección Financiera	HP	ETILE K8470P CORE I7	CNU415BK1H
	Laptop	Ing. Marco Zurita	Director de Obras Públicas	HP	15-AY016LA	CND71357KP

La presente política se propone a utilizar para controlar el tráfico de red del municipio de Pangua, a su vez aplica restricciones al acceso de ciertas páginas de internet, proporcionando solo las necesarias que requiera según sus funciones, de esta forma no exista distracciones en horas laborables.

Nombre de la Política: PO-1E Uso adecuado del internet.

1. Objetivo

Definir las reglas y categorías para el acceso al internet por el usuario para que no existan distracciones en las horas laborables.

2. Alcance

Aplica a todos los usuarios que constituyen la lista de distribución del servidor de dominio del Gobierno Autónomo Descentralizado Municipal de Pangua, incluyendo contratistas, consultores y visitantes.

3. Definiciones:

Webfilter: Es un software diseñado para restringir los sitios web que pueden ser visitados por el usuario en su equipo.

Categoría de Navegación: Es la clasificación de sitios web donde los usuarios conectados a una red pueden ingresar.

Malware: Es un término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

4. Documentos de referencia:

ANEXO-1E Listado de categorías de acceso a internet.

5. Descripción de la Política

Buenas prácticas para el uso adecuado del internet.

Regular con un webfilter el acceso a internet.

Evitar distracciones por parte de los usuarios que laboran en la Institución.

Prevenir la saturación del ancho de banda por el uso de páginas de gran consumo de recursos como: Descargas, Streaming y Redes Sociales.

5.1. Restricciones

Queda estrictamente prohibido el uso de servicio de internet para las siguientes páginas:

Acceso a los sitios web para descargar información ajena a la actividad laboral.

El uso de sitios de videos, streaming en línea o en tiempo real. (YouTube, Spotify, etc.).

Ingresar a contenidos obscenos, agresivos, pornográficos, amenazadores, inmorales u ofensivos.

Uso de Juegos “online” en la red.

Acceso a sitios inseguros que comprometan la confidencialidad e integridad de la información.

Instalación y uso de aplicativos para intercambios de archivos.

Instalación de aplicativos de mensajería instantánea (WhatsApp, Messenger, etc.).

Nota: Si el empleado requiere trabajar con una de estas, deberá pedir autorización al Jefe Inmediato.

5.2. Accesos a categorías

El acceso a internet que proporciona al GAD de Pangua está relacionado con nombre y usuario para inicio de sesión en el equipo de cómputo.

La empresa está en la capacidad de monitorear todos los accesos a internet de acuerdo a las categorías asignadas según el ANEXO-1E Listado de categorías de acceso a internet.

5.3. Penalizaciones

Cualquier usuario que no se ajuste a los lineamientos detallados en las políticas será sujeto a toma de decisiones de acuerdo al reglamento interno de trabajo.

6. Registros.

N/A

7. Anexos.

ANEXO-1E Listado de categorías de acceso a internet.

A continuación, se propone el ANEXO-1E Listado de categorías de acceso a internet, el cual especifica el acceso a internet que van a tener según se considera las necesidades de cada departamento, se ha marcado con una "x" las categorías a las que tendrán acceso.

Gubernamentales: Son paginas como su nombre lo dice del gobierno, con extensiones de dominio .gob.ec, como: Instituto Ecuatoriano de Seguridad Social: www.iess.gob.ec, Ministerio del Ambiente: www.ambiente.gob.ec, Ministerio de Cultura: www.cultura.gob.ec, Secretaria de Gestión de Riesgos: www.gestionderiesgo.gob.ec, entre otras.

Educación: Son páginas que destina el Ministerio de Educación como: Instituto de tecnologías educativas: www.ite.educacion.es o el Ministerio de Educación: www.educacion.gob.ec.

Financieros: Son sitios web financieros que el funcionario requiera utilizar como la página del Ministerio de Finanzas: www.finanzas.gob.ec

Investigación: Acceso al buscador de Google para los empleados que requieran según sus funciones laborables.

Redes Sociales: Son sitios y aplicaciones que operan permitiendo el intercambio de información entre persona y/o empresas, las más comunes Facebook, WhatsApp, Instagram, etc.

Streaming: Son páginas que permiten la ejecución de audio o video en línea.

TICs: Aplicaciones que tienen que ver directamente a tecnología como TeamViewer, entre otras.

LISTADO DE CATEGORÍAS DE ACCESO A INTERNET

ANEXO-1E

	CATEGORÍAS DE ACCESO						
DEPARTAMENTO	**Gubernamental**	**Educación**	**Financieros**	**Investigación**	**Redes Sociales**	**Streaming**	**TICs**
DIRECTORIO	X	X	X	X	X		X
MIES	X	X	X	X			
UNIDAD DE CULTURA	X	X		X	X		
PROMOCIÓN COMUNITARIA	X	X					
SERVICIOS GENERALES	X			X			
PLANIFICACIÓN Y DESARROLLO	X						
ASESORÍA DE ALCALDÍA	X	X	X		X		X
UNIDAD TÉCNICO DE GESTIÓN DE RIESGOS	X						
UNIDAD DE TALENTO HUMANO	X	X	X				
ADMINISTRACIÓN DE PLAZAS Y MERCADOS	X		X				
COMISARIA MUNICIPAL	X						
SECRETARIA EJECUTIVA DE LA NIÑEZ Y ADOLESCENCIA DEL CANTÓN PANGUA	X	X		X			
CONSEJO CANTONAL DE PROTECCIÓN DE DERECHOS	X						
DIRECCIÓN FINANCIERA	X		X				

UNIDAD DE ATENCIÓN A GRUPOS VULNERABLES	X						X
REGISTRO DE LA PROPIEDAD	X			X			
SECRETARÍA GENERAL	X						
UNIDAD TÉCNICO DE INFRAESTRUCTURA Y DISEÑO DE PROYECTOS	X			X			
UNIDAD DE FISCALIZACIÓN	X						
VIALIDAD Y EQUIPO CAMINERO	X						
AGUA POTABLE Y ALCANTARILLADO	X						
OBRAS PÚBLICAS	X						
RECAUDACIÓN	X		X				
OFICINA DE RENTAS	X		X				
TESORERO	X		X				
ORDENAMIENTO TERRITORIAL	X						
SISTEMAS INFORMÁTICOS	X	X		X			
SINDICATURA	X		X				
AVALÚOS Y CATASTROS	X						
BODEGA	X						

12. IMPACTOS (TÉCNICOS, SOCIALES, AMBIENTALES O ECONÓMICOS)

Mediante el desarrollo de las políticas de seguridad informáticas a proponer, se consigue los siguientes impactos:

12.1. Impacto tecnológico

El impacto tecnológico a contribuir será el desarrollo de políticas de seguridad informáticas mediante la ISO 27001, que aporte a las necesidades de la municipalidad con la finalidad infundir las buenas prácticas mediante herramientas del SGSI.

12.2. Impacto económico

Si el Gobierno Autónomo Descentralizado Municipal de Pangua, toma en consideración implementar las políticas de seguridad informática mediante las ISO 27001 en el futuro, se está ahorrando un valor estimado mediante consultoría, de 10.000 dólares.

12.3. Impacto Social

El impacto social a contribuir, es la persuasión al uso de buenas prácticas que se ha indagado en el trascurso de la investigación, para que ayuden a la gestión y buen funcionamiento del GAD de Pangua.

13. PRESUPUESTO PARA LA PROPUESTA DEL PROYECTO

En el presente se procede a enlistar los costos para el diseño de las políticas de seguridad de la información, para lo cual se ostentará gastos directos como los indirectos y el gato total.

13.1. Gastos directos

Tabla 18: Estimación de costos de Gastos Directos.

Recursos	**PRESUPUESTO PARA LA ELABORACIÓN**			
	Cantidad	**Unidad**	**V. Unitario**	**Valor Total**
			$	**$**
Equipos (detallar)				
Laptop.	2		0	0

Impresora.	1		0	200
Grabadora de Audio (Teléfono celular)	1		0	0
Pendrive	1		10.00	10.00
Transporte y salida de campo (detallar)				
Movilización al GAD de Pangua Autor Cruz ($30.50) Autor Gaibor ($24.50)	2		55.00	55.00
Materiales y suministros (detallar)				
Esferos.	4		0.40	1.60
Resma de Papel.	3		0	0
Carpeta.	2		0.50	1.00
Material Bibliográfico y fotocopias. (detallar)				
42 Hojas de políticas de seguridad.	2	0.15	0	0
80 Hojas de documentación de tesis.	1	0.15	0	0
Libro ISO	1		50.00	50.00
Total				**317.6**

Fuente: Grupo Investigador.

13.2. Gastos indirectos

Tabla 19: Estimación de costos de Gastos Indirectos.

Recursos	PRESUPUESTO PARA LA ELABORACIÓN			
	Cantidad	Unidad	V. Unitario $	Valor Total $
Gastos Varios (detallar)				
Llamadas Telefónica.	1		3.00	3.00
Total				**3.00**

Fuente: Grupo Investigador.

13.3. Gasto total

Tabla 20: Estimación de costo General.

Gastos directos	317.6
Gastos indirectos	3.00
Gastos totales	320.6
Gastos de imprevisto 12%	38.472
Sub Total	358.472
10%	35.8472
TOTAL	**394.3192**

Fuente: Grupo Investigador.

14. CONCLUSIONES

Se concluye que se pudo analizar a cabalidad la situación en la que se encontraba la institución acerca de las operaciones con las herramientas y equipos informáticos.

Se identificó los riesgos que puedan ir contra la confidencialidad, integridad y disponibilidad de la información, garantizando a la Municipalidad que, si cumple a cabalidad estas políticas de seguridad informática, sus actividades no se verán afectadas ante actos inescrupulosos de personas propias o externas de la Institución.

Se logró diseñar modelos de documentos de políticas de seguridad informáticas adecuadas, siguiendo los estándares de la ISO 27001 para ayudar a la Municipalidad a permanecer con la información confiable, integra y disponible.

15. RECOMENDACIONES

Se recomienda elaborar un Plan de Contingencia ante desastres naturales, para que empleados de la Municipalidad tenga conocimiento de cómo actuar ante estas situaciones.

Se recomienda que para el correcto funcionamiento de las políticas de seguridad informática es primordial estar al día de la aparición de nuevas técnicas que amenazan a la seguridad de los equipos informáticos del Municipio, para tratar de evitarlas o de dar una solución al problema.

Para el futuro se recomienda realizar más políticas de seguridad para monitorear el cumplimiento de seguridad de la información del Municipio para así un mejorar la integridad.

16. BIBLIOGRAFÍA

Acurio Del Pino, S. (2016). *Delitos informáticos: generalidades*. Guadalajara, Jalisco, México. Retrieved from http://148.202.167.116:8080/xmlui/handle/123456789/599

Aguilar Carrión, M. R. (2017). *"PLAN DE SEGURIDAD INFORMÁTICA BASADO EN ESTÁNDAR ISO-IEC 27001 PARA PROTEGER LA INFORMACIÓN Y ACTIVOS DEL GAD CANTONAL DE PASTAZA.* Ambato - Ecuador. Retrieved from http://dspace.uniandes.edu.ec/bitstream/123456789/6508/1/PIUAMIE007-2017.pdf

Alcivar, S. B. (2017). *PLAN DE SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO/IEC 27001 PARA CUMPLIMIENTO DE LA RESOLUCIÓN DE LA JUNTA BANCARIA NRO. JB-2014-3066 EN LA COOPERATIVA DE AHORRO Y CRÉDITO "LA BENEFICA" LTDA*. Retrieved from http://dspace.uniandes.edu.ec/handle/123456789/7795

Almeida Suarez, S. L. (2017). ANALISIS DE LA SEGURIDAD INFORMATICA EN LA COOPERATIVA DE AHORRO Y CREDITO "SAN ANTONIO" DE LA UNION. Retrieved from http://dspace.utb.edu.ec/handle/49000/2385

Argüezo Ramirez, E. D. (2019). *PROPUESTA DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE INFORMACIÓN PARA LA PROTECCIÓN DE ACTIVOS DE INFORMACIÓN BASADO EN LA NORMA ISO 27001 EN EL ÁREA DE INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE HUÁNUCO*. Huánuco - Perú. Retrieved from http://200.37.135.58/bitstream/handle/123456789/2084/ARGÜEZO RAMIREZ%2C EDUARDO DANIEL.pdf?sequence=3&isAllowed=y

Briñez Bautista, M. L. (2017). *DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA PARA LA ALCALDÍA MUNICIPAL DE LA JAGUA DE IBIRICO-CESAR BASADO EN LA NORMA ISO 27001:2013*. Valledupar. Retrieved from https://repository.unad.edu.co/handle/10596/14253

Cárdenas Posada, K., Fernández Vásquez, J. D., & Hernández Aros, L. (2018). Matriz de riesgos en el desarrollo del encargo, 22. Retrieved from https://repository.ucc.edu.co/bitstream/20.500.12494/5166/1/Matriz de riesgo en el desarrollo del encargo %282%29.pdf

Carrillo Jiu, J. A. (2014). *FUNDAMENTOS DE SEGURIDAD LÓGICA* . UNIVERSIDAD NACIONAL DE AMAZONIA PERUANA, IQUITOS-PERÚ. Retrieved from http://repositorio.unapiquitos.edu.pe/bitstream/handle/UNAP/4487/Jose_Tesis_Titulo_2014.pdf?sequence=1&isAllowed=y

Castro Ortega, J. (2015). IMPLEMENTACIÓN DE UNA PLATAFORMA QUE PERMITA LA INTEGRACIÓN DE ACTIVE DIRECTORY Y GOOGLE APP CONTACTS SOPORTADO POR LA PLATAFORMA ANYWHERE PARA LA EMPRESA TMTEK DE COLOMBIA. Retrieved from repositorio.ufpso.edu.co:8080/dspaceufpso/handle/123456789/742

Chungata Cabrera, A. M. (2015). *EL FRAUDE COMO DELITO INFORMÁTICO*. Cuenca - Ecuador. Retrieved from http://dspace.ucuenca.edu.ec/bitstream/123456789/21321/1/TESIS.pdf

Collazo Linares, A. (2017). *Sistema para la gestión y control de cuentas de usuario en la UCLV*. Santa Clara. Retrieved from https://dspace.uclv.edu.cu/bitstream/handle/123456789/7867/Adrian Collazo Linares.pdf?sequence=1&isAllowed=y&fbclid=IwAR3ajV4848zBAjhLerwQX662rkedZ3alagMz8oCDSAOWtLYiEwaiB2yc770

Colonia Hernández, P. J. (2019). *UNIVERSIDAD CATÓLICA ÁNGELES CHIMBOTE FACULTAD DE INGENIERÍA ESCUELA PROFESIONAL DE SISTEMAS*. *Universidad Católica Los Ángeles de Chimbote*. Chimbote-Peru: Universidad Católica los Ángeles de Chimbote.

Cordero Torres, G. (2015). *Estudio comparativo entre las metodologías MAGERIT y CRAMM, utilizadas para Análisis y Gestión de Riesgos de Seguridad de la Información*. Cuenca - Ecuador.

Cortéz Rodríguez, A. I., & Santiago Cueva, W. J. (2018). *PLAN DE SEGURIDAD INFORMÁTICA BASADO EN LA NORMA ISO 27002 PARA MEJORAR LA GESTIÓN TECNOLÓGICA DEL COLEGIO CARMELITAS – TRUJILLO*. UNIVERSIDAD NACIONAL DE TRUJILLO, TRUJILLO - PERÚ. Retrieved from http://dspace.unitru.edu.pe/bitstream/handle/UNITRU/11066/CORTÉZ RODRÍGUEZ%2C AMELIA IVON%2C SANTIAGO CUEVA%2C WILFREDO JHONATAN.pdf?sequence=1&isAllowed=y

Cristancho Lopez, E. F. (2018). *PROPUESTA DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION PARA LA ALCALDIA MUNICIPAL DE GUACHETACUNDINAMARCA, BASADO EN LA NORMA ISO/IEC 27001:2013*. Bogota - Colombia. Retrieved from https://repository.unad.edu.co/handle/10596/20410

Diaz Coral, R. A. (2015). *Apoyo al proceso de implementación de un Sistema de Gestión de la seguridad de la información basado en la Norma ISO 27001:2013 en la Alcaldía de Pasto*. San Juan de Pasto. Retrieved from http://biblioteca.udenar.edu.co:8085/atenea/biblioteca/91045.pdf

Díaz Romero, C. C., & Rodríguez Rojas, Y. L. (2017). Beneficios e impactos de la implementación de normas técnicas en las organizaciones: una revisión sistemática. *SIGNOS - Investigación En Sistemas de Gestión*, *8*(2), 133. https://doi.org/10.15332/s2145-1389.2016.0002.07

Econ.Guillen Fernandez, R. E. (2017). *MEDICIÓN DEL RIESGO DE LIQUIDEZ EN LAS PEQUEÑAS Y MEDIANAS COMPAÑÍAS DEDICADAS A LA FABRICACIÒN DE MUEBLES DE MADERA EN CUENCA, DURANTE EL PERIODO 2014-2015*. CUENCA. Retrieved from http://dspace.uazuay.edu.ec/bitstream/datos/7477/1/13373.pdf

Fernández Villacrés, G. E., & Martínez Campaña, C. E. (2017). *Plan de seguridad informática basado en estándares ISO-IEC 27001 para proteger la información y activos del GAD cantonal de Pastaza*. Ambato - Ecuador. Retrieved from http://dspace.uniandes.edu.ec/handle/123456789/6508

Figueroa Pérez, O., & Malagón Sáenz, N. E. (2017). *Propuesta de Políticas de Seguridad de la Información para la institución Educativa de Educación Básica y Media del departamento de Boyacá, basadas en la norma ISO 27001:2013. instname:Universidad Nacional Abierta y a Distancia*. Colombia: Universidad Nacional Abierta y a Distancia UNAD. Retrieved from http://repository.unad.edu.co/handle/10596/11881

Gallegos Montero, J. A. (2015). Análisis , diseño e implementación de un plan de gestión de seguridad de la información basados en la norma ISO/IEC 27001 para la Cooperativa de Ahorro y Crédito Nuevos Horizontes. Retrieved from http://repositorio.utmachala.edu.ec/handle/48000/6058

García Correa, J. B., & Gavilanes Balarezo, M. A. (2015). *ANÁLISIS Y PROPUESTA DE IMPLEMENTACIÓN DE LAS MEJORES PRÁCTICAS DE ITIL EN EL DEPARTAMENTO DE SISTEMAS DE LA UNIVERSIDAD POLITÉCNICA SALESIANA SEDE GUAYAQUIL.* Guayaquil. Retrieved from http://dspace.ups.edu.ec/handle/123456789/10305

García Pierrat, G., & Vidal Ledo, M. J. (2017). La informática y la seguridad. Un tema de importancia para el directivo. *Infodir (Revista de Información Para La Dirección En Salud)*, *13*(25), 26–36. Retrieved from https://www.researchgate.net/publication/303541468_La_informatica_y_la_seguridad_Un_tema_de_importancia_para_el_directivo

Gómez Gómez, M. A. (2015). *Diseño e implementación del servicio de directorio activo en la red de la gobernación y esquematización del direccionamiento IP en la red de datos departamental.* Universidad Católica de Pereira. Retrieved from http://repositorio.ucp.edu.co/handle/10785/3051

Guanoluisa Huertas, J. E., & Maldonado Soliz, I. F. (2015). *ANÁLISIS DE RIESGOS Y DISEÑO DE UN PLAN DE SEGURIDAD DE LA INFORMACIÓN PARA EL CONSEJO NACIONAL DE IGUALDAD DE DISCAPACIDADES "CONADIS".* Quito. Retrieved from https://bibdigital.epn.edu.ec/bitstream/15000/10499/1/CD-6217.pdf

GUAPULEMA MARTÍNEZ, M. G. (2017). *UNIVERSIDAD REGIONAL AUTÓNOMA DE LOS ANDES UNIANDES FACULTAD DE SISTEMAS MERCANTILES CARRERA SISTEMAS PROYECTO DE INVESTIGACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO*. BABAHOYO – ECUADOR. Retrieved from http://dspace.uniandes.edu.ec/bitstream/123456789/8396/1/TUBSIS005-2017.pdf

Guerra Guzmán, D. E. (2019). *ASEGURAMIENTO DEL INTERCAMBIO DE DATOS ENTRE UNA APLICACIÓN MÓVIL ADROID Y UNA APLICACIÓN WEB JAVA MEDIANTE CÓDIGOS QR, EN BASE AL ESTÁNDAR ISO/IEC 27002.* UNIVERSIDAD TÉCNICA DEL NORTE BIBLIOTECA UNIVERSITARIA, IBARRA-ECUADOR. Retrieved from http://repositorio.utn.edu.ec/bitstream/123456789/9539/2/04 ISC 528 TRABAJO GRADO.pdf

Hernández Mendoza, Y., Martínez González, M., & Martín Jaime, E. M. (2016). FREE ACTIVE DIRECTORY MANAGER (FADMANAGER). *3C TIC Cuadernos de Desarrollo Aplicados a Las TIC*, *5*(1), 39–53. https://doi.org/10.17993/3ctic.2016.51.39-53

ICA. (2018). *Manual del Sistema de Gestión de Seguridad de la Información SGSI AGOSTO 2018 El presente Manual es parte integral del Manual del Sistema de Gestión Oficina Tecnologías de la Información*. Colombia. Retrieved from https://www.ica.gov.co/getattachment/Modelo-de-P-y-G/Eficiencia-Administrativa/Procesos-y-Procedimientos/ManualSGSI-Agosto-2018.pdf.aspx?lang=es-CO

INEC. (2020). Tecnologías de la Información y Comunicación-TIC |. Retrieved August 19, 2020, from https://www.ecuadorencifras.gob.ec/tecnologias-de-la-informacion-y-comunicacion-tic/

ISOTools Excellence. (2017, January 26). ¿Seguridad informática o seguridad de la información? Retrieved July 28, 2020, from https://www.pmg-ssi.com/2017/01/seguridad-de-la-informacion/

LACNIC FRIDA. (2020, May 22). Acceso a Internet. Retrieved August 19, 2020, from https://programafrida.net/acceso-a-internet

López Carranza, K. E. (2015). *DISEÑO DE UN PLAN DE MITIGACIÓN DE RIESGOS EMPRESARIALES IDENTIFICANDO LOS RIESGOS INTERNOS Y EXTERNOS DE COMERCIAL NOVEDADES LEYDI EN EL CANTÓN LA TRONCAL DEL AÑO 2014.* Retrieved from http://186.5.103.99/handle/reducacue/7293

López Sánchez, J. (2019). *Métodos y técnicas de detección temprana de casos de phishing*. Universitat Oberta de Catalunya, España. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/89225/6/jlopezsanchez012TFM0119memoria.pdf

Magaña Herrera, P. P. (2012). NORMALIZACION Y NORMAS ISO, 1–13. Retrieved from https://www.emagister.com/uploads_courses/Comunidad_Emagister_38542_Microsoft_Word_-_38541.pdf

Markus Erb, C. F. H. A. C. A. K. D. S. G. (n.d.). Gestión de Riesgo en la Seguridad Informática. Retrieved September 6, 2020, from https://protejete.wordpress.com/about/

Mercader, E. M. (2018). *TFM-SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN INTEGRADOR X*. España. Retrieved from http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81186/6/emunozmerTFM0618memoria.pdf

Montealegre Alvarez, Z. H. (2018). *Implementación de una auditoria en seguridad de la información e infraestructura de red bajo los lineamientos de las normas iso/iec 27001 y 11801, a la alcaldia del municipio de Tame, departamento de Arauca. Alcaldia municipal de Tame-Arauca. (s.f.). Mision y vision. Recuperado de http://www.tame-arauca.gov.co/NuestraAlcaldia/Paginas/Mision-y-Vision.aspx.* Arauca: Universidad Cooperativa de Colombia - Arauca Facultad de Ingeniería de Sistemas. Retrieved from https://repository.ucc.edu.co/handle/20.500.12494/8031

Mora Pérez, A. (2016). *GESTIÓN DE LA PREVENCIÓN. CONTROL DE ACCESOS MASTER PREVENCIÓN DE RIESGOS LABORALES TRABAJO FINAL DE MASTER 2016 AUTORA: ARANTXA MORA PEREZ UNIVERSIDAD POLITÉCNICA DE CARTAGENA*. Colombia. Retrieved from https://repositorio.upct.es/bitstream/handle/10317/5636/tfm-mor-ges.pdf?sequence=3&isAllowed=y

Morales Choez, A. I. (2016). *Sistema De Respaldos Inrementales Monitoreado A Partir Del Uso De Herramientas OPEN SOURCE*. Guayaquil: Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería en Sistemas Computacionales. Retrieved from http://repositorio.ug.edu.ec/handle/redug/16502

Morales, R. F. (2015). *DISEÑO PARA LA IMPLEMENTACIÓN DE TRES DOMINIOS DE UN SISTEMA DE GESTIÓN EN LA SEGURIDAD DE LA INFORMACIÓN BASADA EN LA NORMA ISO 27001 E ISO 27002, PARA EL ÁREA DE SOFTWARE DE LA PROCESADORA NACIONAL DE ALIMENTOS PRONACA*. Sangolqui. Retrieved from http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/9804/T-ESPE-048423.pdf?sequence=1&isAllowed=y

Nieves, A. C. (2017). DISEÑO DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADOS EN LA NORMA ISO/IEC 27001:2013. Retrieved July 30, 2020, from http://repository.poligran.edu.co/bitstream/handle/10823/994/Trabajo Final.pdf?sequence=1&isAllowed=y

Ocampo Vélez, L. S., Encalada Vivanco, P. H., & Ing. Jaramillo Castro, C. M. (2015). *"Implementación de Active Directory aplicando el estándar 802.1x, dentro de la red LAN y WLAN de la Universidad Nacional de Loja."* Loja. Retrieved from https://s3.amazonaws.com/academia.edu.documents/60317580/Ocampo_Velez__Lenin_Sebastian__Vivanco_Encalada__Henry_Paul20190817-79403-3vebxx.pdf?response-content-disposition=inline%3B filename%3DUNIVERSIDAD_NACIONAL_DE_LOJA_Implementac.pdf&X-Amz-Algorithm=

Oidor González, J. C. (2016). DISEÑO DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION-SGSI BAJO LA NORMA ISO/IEC 27001:2013 PARA LA EMPRESA "EN LINEA FINANCIERA" DE LA CIUDAD DE CALI-COLOMBIA. Retrieved June 5, 2019, from https://repository.unad.edu.co/bitstream/10596/11907/1/76041068.pdf

Paguay Lema, C. K., & Zamora Arana, G. E. (2017). *Auditoría de la Seguridad Informática basado en la ISO 27001 Sistema de Gestión de Seguridad de la Información para el GAD Municipal de Milagro*. Milagro, Ecuador. Retrieved from http://repositorio.unemi.edu.ec/handle/123456789/3845

Palacios Marchan, J. W. (2018). *PROPUESTA DE IMPLEMENTACIÓN DE PROCESOS BASADOS EN ITIL V3 EDICIÓN 2011 PARA LA GESTIÓN DE SERVICIOS DE TI EN LA CORPORACIÓN EDUCATIVA VIRGEN DEL PERPETUO SOCORRO TUMBES; 2018*. PIURA - PERÚ. Retrieved from http://repositorio.uladech.edu.pe/bitstream/handle/123456789/7340/GESTION_DE_SERVICIOS_ITIL_PALACIOS_MARCHAN_JIANKARLO_WASHINGTON.pdf?sequence=1&isAllowed=y

Palacios Portilla, D. O. (2015). Diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de informática de la cooperativa del magisterio de Túquerres bajo la norma ISO 27001: 2013. *Instname:Universidad Nacional Abierta y a Distancia*, 127. Retrieved from https://repository.unad.edu.co/bitstream/10596/3817/1/1085255001.pdf

Reina Tovar, Y. (2016). *CREACION DE POLITICAS ADMINISTRATIVAS Y DE SEGURIDAD PARA EL SISTEMA INFORMATICO Y DE COMUNICACIONES DE LA GOBERNACION*. UNIVERSIDAD SURCOLOMBIANA. Retrieved from http://repositorio.usco.edu.co/handle/123456789/1113

Romero Castro, M. I., Figueroa Moran, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., … Castillo Merino, M. A. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES*. Manabí. Retrieved from https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-informática.pdf

Ruiz Peña, J. H. (2018). Diseño de un sistema de gestión de seguridad de la información (SGSI) bajo la norma ISO/IEC 27001:2013, en la Cooperativa Multiactiva del personal del Sena, en Bogotá., 204. Retrieved from https://repository.unad.edu.co/bitstream/10596/17300/1/80267708.pdf

Vargas García, J. J. (2015). *PROPUESTA TECNOLÓGICA BASADA EN COBIT 5 APLICADA A LA GESTIÓN DE LA TI EN LA EIS*. RIOBAMBA - ECUADOR. Retrieved from http://dspace.espoch.edu.ec/bitstream/123456789/4397/1/18T00602.docx.pdf

Vera Castro, J. B., & Zambrano Zambrano, J. A. (2017). *SERVICIO DE DIRECTORIO BASADO EN CÓDIGO ABIERTO EN EL GADM DEL CANTÓN JUNÍN*. Calceta-Manabí. Retrieved from http://repositorio.espam.edu.ec/bitstream/42000/663/1/TC115.pdf?fbclid=IwAR0CXG1kMB9gjFWH6qFMuBINcu4LZr339f8dcj1KkJBInzcjY-57kLVF204

Villegas Chiliquinga, W. E. (2017). Diseño de las buenas prácticas del sistema de gestión de la seguridad de la información basado en normas ISO 27001 para la dirección general de Aviación Civil. Retrieved from http://dspace.udla.edu.ec/handle/33000/7650

Yi Min Shum. (2018). Matriz de evaluación de factores internos (Matriz EFI - MEFI). Retrieved September 7, 2020, from https://yiminshum.com/matriz-evaluacion-factores-internos-mefi/

Zura Chala, A. Y. (2015). *DISEÑO DEL MODELO DE SEGURIDAD DE DEFENSA EN PROFUNDIDAD EN LOS NIVELES DE USUARIO, RED INTERNA Y RED PERIMETRAL, APLICANDO POLÍTICAS DE SEGURIDAD EN BASE A LA NORMA ISO/IEC 27002 PARA LA RED DE DATOS DEL GAD MUNICIPAL DE OTAVALO*. Ibarra - Ecuador. Retrieved from http://repositorio.utn.edu.ec/handle/123456789/4469

17. ANEXOS

17.1. Ficha de Observación

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE PANGUA

Moraspungo-Pangua-Cotopaxi

FICHA DE OBSERVACIÓN DE PROYECTO DE INVESTIGACIÓN

Nombre:	Ing. Herman Ortiz
Cargo:	Ingeniero en Sistemas
Departamento:	Servicios Informáticos
Fecha:	_____

Objetivo de la Observación:

Palpar las necesidades y problemáticas mediante la observación y una entreviste para proponer políticas de seguridad informáticas adecuadas a sus requerimientos.

	ASPECTOS	ESCALA DE CALIFICACIÓN							
		1	2	3	4	5	SI	NO	OBSERVACION
1	¿Cuenta con un datacenter?							X	
2	¿Cuenta con autenticación en los equipos?				X				La mayoría de equipos no contaban con autenticación.
3	¿Los equipos cuentan con todos sus accesorios?				X				Se pudo observar que un ordenador no poseía mouse.
4	¿Dan uso al correo corporativo?	X							

5	¿Tiene restricción para el acceso a internet?	X							
6	¿Uso compartido de impresoras?						X		
7	¿Respaldan la información?						X		
8	¿Administran documentación impresa?						X		
9	¿Lleva un registro detallado de los bienes del Municipio y quien está a su cargo?				X				
10	¿Cuenta con servidores?						X		
11	¿Los servidores se encuentran alojados en una zona con seguridad?							X	
12	¿Es permitido el uso de laptop que no son propiedad de la Municipalidad?						X		
13	¿Poseen los equipos papel tapiz corporativo, al bloquearse?							X	
14	¿Cuentan con políticas de seguridad informáticas?							X	
15	¿Posee con una red física estructurada?						X		
	TOTAL								

OBSERVACIONES: Se procedió a realizar el levantamiento informático en la Municipalidad sobre las características de los equipos informáticos que posee el GAD de Pangua.

_____ _____

Nombre y firma del observador **Nombre y Firma**

17.2. Ficha de Entrevista

UNIVERSIDAD TÉCNICA DE COTOPAXI
FACULTAD DE CIENCIAS DE LA INGENIERÍA Y APLICADAS

FICHA DE ENTREVISTA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE PANGUA

Objetivo: Analizar las vulnerabilidades y necesidades que tiene el Gobierno Autónomo Descentralizado Municipal de Pangua para el desarrollo de políticas de seguridad informáticas de acuerdo a las ISO/IEC 27001

Datos informativos:

Entrevistado: Ing. Herman Ortiz

Lugar: Gobierno Autónomo Descentralizado Municipal de Pangua

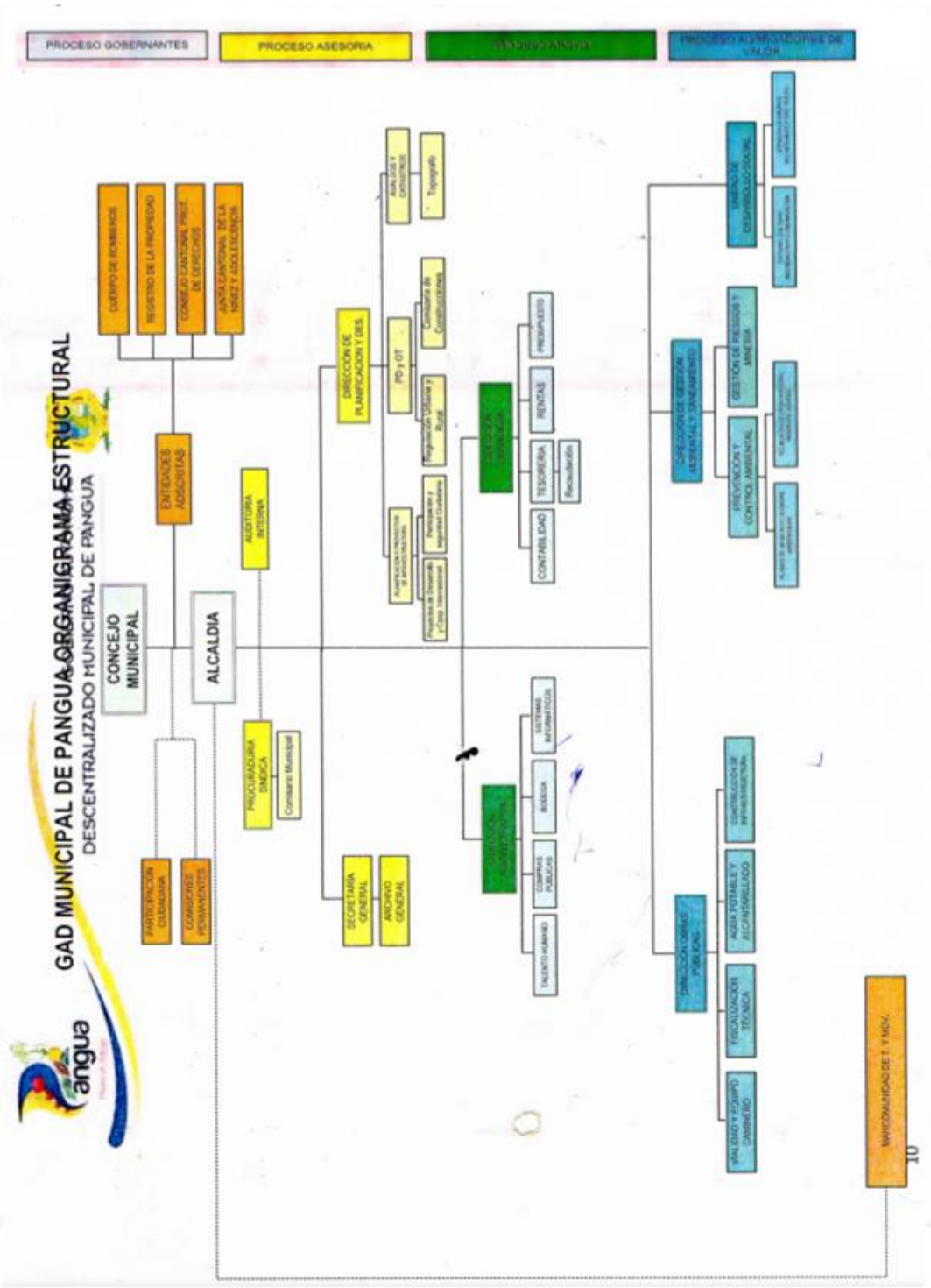
Entrevistador: Cruz Caiza Carla Cristina, Gaibor Gavilanez Mónica Lisseth

Años laborables en la Municipalidad de Pangua:

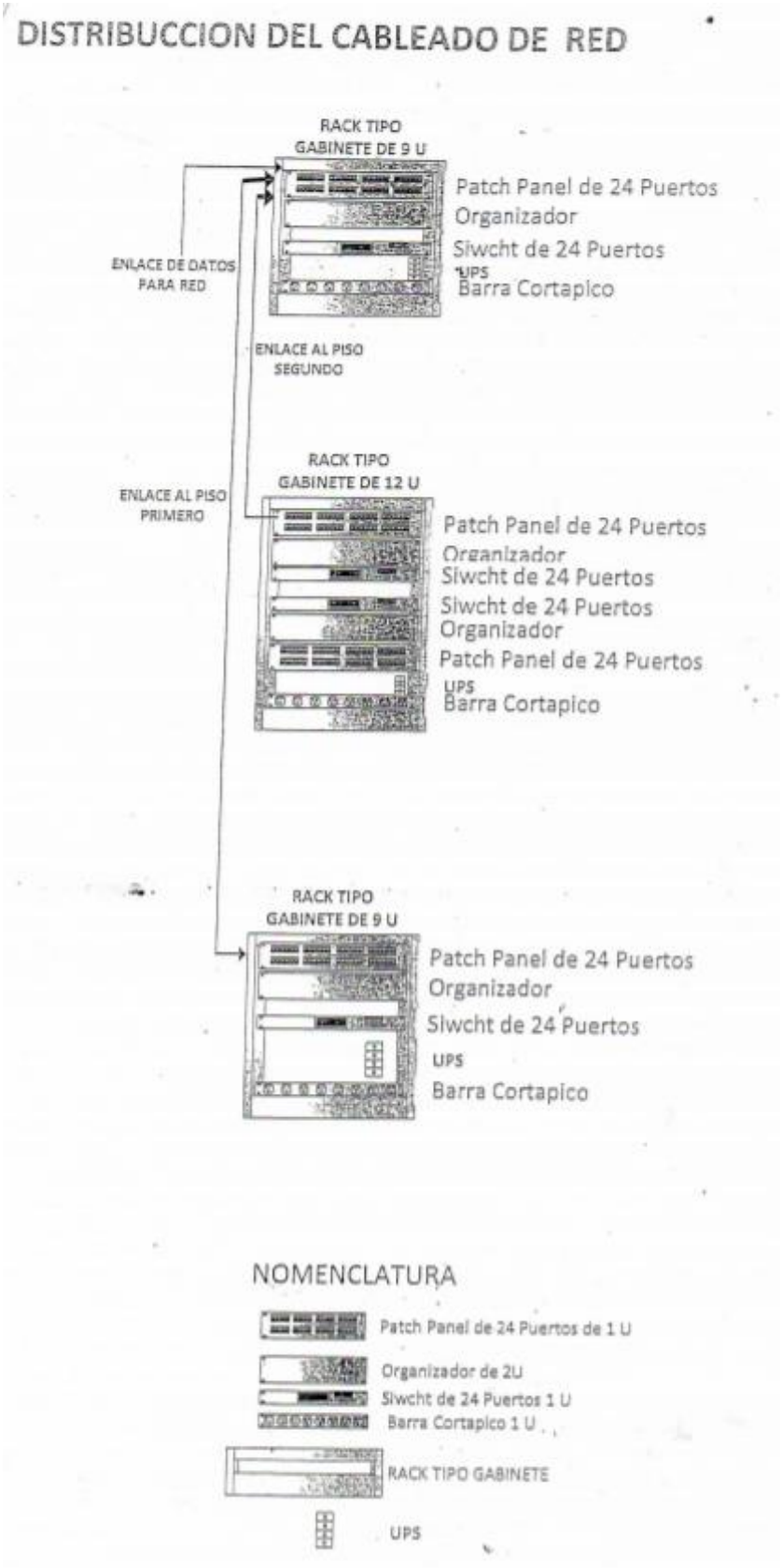
1. ¿Cuenta con un antivirus?
2. ¿La página del Municipio es un sitio seguro?
3. ¿Qué marca de dispositivos cuenta para la red?
4. ¿Cuentan con un plan de contingencia para cambiar los equipos (computadoras, cables, laptops, servidores)?
5. ¿Cuenta con un DATACENTER adecuado (piso, ventilación, seguridad)?
6. ¿Cuenta con un UPS para evitar daños en los equipos?
7. ¿Cómo manejan los privilegios de los usuarios?
8. ¿Existe una persona responsable de la seguridad de autenticación de acceso?
9. ¿Cada que tiempo cambian las contraseñas de su equipo?
10. ¿Cada que tiempo se realiza capacitaciones para el uso de las herramientas dentro de la empresa?
11. ¿Cómo comparten información dentro del municipio?
12. ¿Cuentan con comunicación telefónica IP?
13. ¿Cuentan con un plan de contingencia por desastres naturales?

14. ¿Periodo de tiempo que se realizan los respaldos la base de datos o sistemas?
15. ¿Si tienen una red física estructurada y de qué tipo?
16. ¿Cuentan con un informe de registros de nuevos equipos y nuevos software?
17. ¿Cuentan con un presupuesto para las TICs?
18. ¿Cuentan con un software para registrar las actividades de los empleados?
19. ¿Cuentan con un contrato de confidencialidad de información para empleados?
20. ¿Cuentan con un espacio en la nube para guardar la información de la empresa?
21. ¿Cuentan con dominios propios de la empresa como Gmail, hotmail?
22. ¿Cuál es la estructura del departamento de TICs?
23. ¿Cuál es la estructura organizacional de la empresa?
24. ¿Los empleados tienen restricciones a redes sociales?
25. ¿Constan con un documento de vida útil del equipo?
26. ¿Cada que tiempo renuevan las contraseñas?
27. ¿Qué tipo de políticas de seguridad tienen para las contraseñas?
28. ¿Cuenta con un documento de vida útil de los equipos?

17.3.Estructura Organizacional



17.4.Distribución del cableado de red



17.5.Carta de aceptación

GOBIERNO AUTÓNOMO DESCENTRALIZADO
MUNICIPAL DE PANGUA
ALCALDÍA

El Corazón, 25 de noviembre del 2 019

CARTA DE ACEPTACIÓN

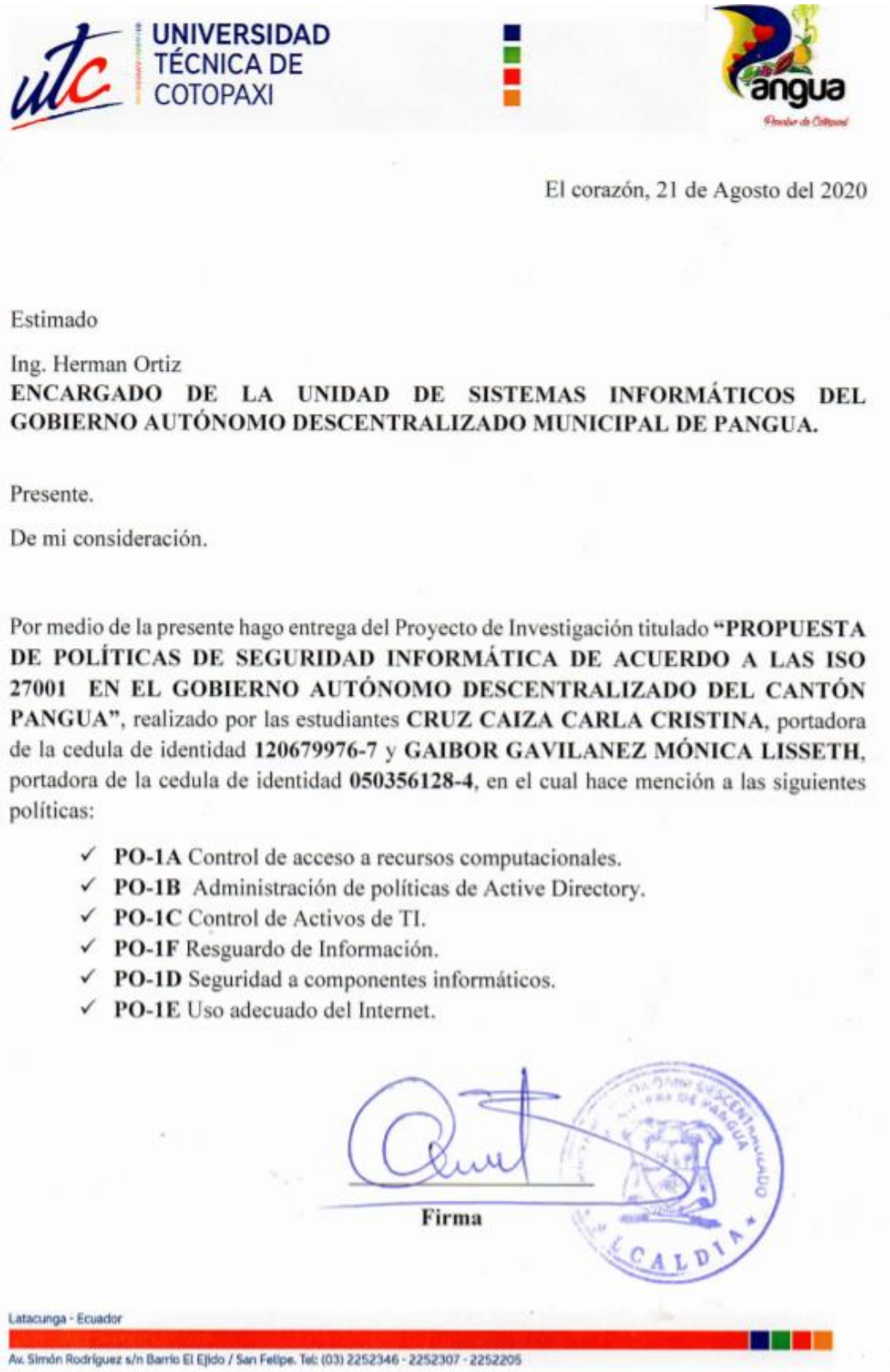
Por medio de la presente hago constar que las Srtas: GAIBOR GAVILANEZ MÓNICA LISSETH portadora de la C.I. 050356128-4 y CRUZ CAIZA CARLA CRISTINA portadora de la C.I. 120679976-7, estudiantes de la carrera de Ingeniería en Informática y Sistemas Computacionales de la Universidad Técnica de Cotopaxi, han sido aceptadas en nuestra institución Gobierno Autónomo Descentralizado del cantón Pangua, para realizar el tema de tesis "Propuesta de Políticas de Seguridad Informática de acuerdo a las ISO 27001 en el Gobierno Autónomo Descentralizado del cantón Pangua".

Atentamente,

Lcdo. Saúl Mejía P.
ALCALDE DEL GADMUPAN

Calle Sucre y Ramón Campaña 268-4156 / 268-4090 / 268-4443
Telefax Secretaría: 268-4157 www.pangua.gob.ec
Pangua - Cotopaxi - Ecuador

17.6.Documento de entrega de Políticas de Seguridad Informáticas



UNIVERSIDAD TÉCNICA DE COTOPAXI

El corazón, 21 de Agosto del 2020

Estimado

Ing. Herman Ortiz
ENCARGADO DE LA UNIDAD DE SISTEMAS INFORMÁTICOS DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE PANGUA.

Presente.

De mi consideración.

Por medio de la presente hago entrega del Proyecto de Investigación titulado **"PROPUESTA DE POLÍTICAS DE SEGURIDAD INFORMÁTICA DE ACUERDO A LAS ISO 27001 EN EL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN PANGUA"**, realizado por las estudiantes **CRUZ CAIZA CARLA CRISTINA**, portadora de la cedula de identidad **120679976-7** y **GAIBOR GAVILANEZ MÓNICA LISSETH**, portadora de la cedula de identidad **050356128-4**, en el cual hace mención a las siguientes políticas:

- ✓ **PO-1A** Control de acceso a recursos computacionales.
- ✓ **PO-1B** Administración de políticas de Active Directory.
- ✓ **PO-1C** Control de Activos de TI.
- ✓ **PO-1F** Resguardo de Información.
- ✓ **PO-1D** Seguridad a componentes informáticos.
- ✓ **PO-1E** Uso adecuado del Internet.

Firma

Latacunga - Ecuador

Av. Simón Rodríguez s/n Barrio El Ejido / San Felipe. Tel: (03) 2252346 - 2252307 - 2252205

Pangua Paraíso de Colibríes	**CONTROL DE ACCESO A RECURSOS COMPUTACIONALES**	PO-1A Ver No. 01 Pág. 1 de 3

1. Objetivo

Brindar lineamientos para el acceso a los recursos de información importante del Gobierno Autónomo Descentralizado Municipal de Pangua mediante el buen uso de los mecanismos de acceso a los recursos computacionales de la Institución.

2. Alcance

Aplica a todos los miembros de la comunidad del Gobierno Autónomo Descentralizado Municipal de Pangua, incluyendo empleados, contratistas, consultores y visitantes.

3. Definiciones:

Recursos Informáticos: Es un componente físico o virtual incluyen medios para entrada, procesamiento, producción, comunicación y almacenamiento.
Mecanismos de acceso: Es un mecanismo que permite controlar y conceder el acceso a un computador principal.
Reforzar: Puede tratarse de aquello que se emplea para brindarle resistencia o solidez a algo.
Lineamientos: Es una tendencia, una dirección o un rasgo característico sobre algo.
Password: O contraseña es una serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa.

4. Documentos de referencia

RE-1A Carta de aceptación de políticas de seguridad informáticas.
RE-2A Solicitud de creación de nuevos usuarios de red.
RE-3A Bitácora de actualización de contraseñas.

5. Descripción de la Política

Por ningún motivo el empleado recibirá el acceso a los recursos computacionales si no ha firmado y a aceptación el documento RE-1A Carta de aceptación de políticas de seguridad.
Para el acceso a los recursos computacionales se asignaran claves y se crearan usuarios de red RE-2A Solicitud de creación de nuevos usuarios de red.
Los recursos informáticos y la información pueden ser usados solo para propósitos autorizados y en cumplimiento con las metas y objetivos del GAD.
A continuación se considera las siguientes recomendaciones a ser cumplidas por el usuario

- Los usuarios y contraseñas son de uso exclusivo por el usuario, deben ser utilizadas únicamente para cuestiones de trabajo, el usuario no podrá usarlas para ningún otro fin, fuera del Municipio.
- Las actividades realizadas por estas credenciales son responsabilidad del usuario.

Responsable: Ingeniero de Sistemas _____ Firma Fecha: 2020-05-29(fecha de entrega)	Aprobación: Alcalde del GAD _____ Firma Fecha: 2019-05-29

- La Municipalidad puede realizar seguimiento de las actividades y uso de las credenciales mediante auditorias periódicas para evaluar su uso adecuado.
- El usuario debe comunicar inmediatamente si tiene sospecha que alguien está haciendo mal uso de ellas.
- Confidencialidad: Por ningún motivo el usuario debe divulgar las credenciales o claves, estas son intransferibles.
- El usuario debe limitarse a ingresar contraseñas cuando estén personas a su alrededor.
- Por seguridad de la información si el usuario llegara a perder su contraseña este debe notificar de manera inmediata para ser dado de baja la contraseña del sistema.
- La contraseña que elija el usuario deberá ser robusta es decir esta debe contener letras, números y símbolos.
- Impedir que personal no autorizado tenga acceso a la información importante de la empresa para que no exista alteraciones o pérdidas ya sea intencionales o accidentalmente.
- El usuario deberá cambiar su contraseña cada 3 Meses.
- El usuario deberá solicitar ayuda al personal encargado en caso que olvide su contraseña.
- El usuario no debe elegir contraseñas antiguas.
- Seguridad: El usuario no deberá anotar la contraseña en un lugar físico.
- Cualquier persona que de incumplimiento a las disposiciones señaladas en esta política, puede ser sujeta a una acción disciplinaria según el Reglamento Interno de Trabajo

5.1 Equipos de Cómputo

El inicio de sesión deberá bloquearse cuando haya excedido el límite de 3 intentos.
El usuario debe elegir contraseñas que tenga un mínimo de siete caracteres constituidos de letras, números y símbolos.

5.2 Sistemas informáticos

Configurar para que solicite un inicio de sesión para el ingreso a los recursos computacionales.
Se recomienda implementar un software para generar la cuenta de los empleados (responsable, nombre de equipo, área, contraseña).
Generar un documento de seguimiento de actualización de contraseñas RE-3A Bitácora de actualización de contraseñas.

5.3 Del área de Recursos Humanos

Realizar la selección adecuada del personal para que maneje los accesos de la empresa.
Cuando un empleado es despedido o renuncia se solicitara que su cuenta sea inhabilitada antes que deje el cargo.

6. Registros.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-1A	Carta de aceptación de políticas de seguridad informáticas	Técnico de Servicios Informáticos.	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-2A	Solicitud de creación de nuevos usuarios de red	Técnico de Servicios Informáticos.	Oficina Sistemas área de Soporte a usuarios	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-3A	Bitácora de actualización de contraseñas	Técnico de Servicios Informáticos	Oficina Sistemas área de Soporte a usuarios	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno

7. Anexos.

N/A

	CARTA DE ACEPTACIÓN DE POLÍTICAS DE SEGURIDAD INFORMÁTICAS	RE-1A
		Ver No. 01
		Pág. 1 de 1

El Corazón, (00) de (Mes) del (Año)

Yo, **APELLIDOS Y NOMBRES DEL SOLICITANTE**, portadora de la cédula de identidad **Número,** usuario del Departamento **(Nombre del departamento**), una vez leído y comprendido mis obligaciones, acepto y me comprometo a cumplir las políticas de seguridad informáticas del Gobierno Autónomo Descentralizado Municipal de Pangua.

PO-1A Control de acceso a recursos computacionales.
PO-1B Administración de políticas de Active Directory.
PO-1C Control de Activos de TI.
PO-1F Resguardo de Información.
PO-1D Seguridad a componentes informáticos.
PO-1E Uso adecuado del Internet.

Atentamente,

APELLIDOS Y NOMBRES DEL SOLICITANTE
C.I.: Número de cédula

	SOLICITUD DE CREACIÓN DE NUEVOS USUARIOS DE RED	RE-2A Ver No. 01 Pág. 1 de 1

1. Información del usuario solicitante

Código del empleado: _____
Nombre y Apellidos: _____
Departamento: _____
Cargo: _____

2. Información del jefe inmediato

Código del empleado: _____
Nombre y apellido: _____
Cargo: _____

3. Acceso a recursos solicitados

Mail:

Interno ☐ Externo ☐

Internet:

Parcial ☐ Total ☐

Equipo de cómputo:

PC ☐

Laptop ☐ Justificación: _____

Telefonía IP:

Interno ☐ Local ☐ Nacional ☐ Internacional ☐

4. Aprobación

Solicitante: _____ Firma: _____ Fecha: _____

Jefe inmediato: _____ Firma: _____ Fecha: _____

5. Para uso de TIC's

User Creado:_____(Ejemplo: j_p de Juan Perez)

Entregado por: _____ (Nombre de quien creo cuenta) Firma: _____

Fecha de creación: _____

BITÁCORA DE ACTUALIZACIÓN DE CONTRASEÑAS					
CÉDULA	**NOMBRES Y APELLIDOS**	**DEPARTAMENTO**	**NOMBRE EQUIPO**	**FECHA**	**FIRMA**

1. Objetivo

Definir políticas de controlador de dominio, reglas de control de acceso a servicios de la red de la Municipalidad para gestionar los sistemas informáticos utilizados por el usuario final.

2. Alcance

Aplica al servidor de dominio, a todas las unidades organizativas, los usuarios y equipos de cómputo dentro de la red del GAD cantonal.

3. Definiciones:

Controlador de dominio: Es un conjunto de ordenadores agrupados que ciñen a unas reglas de seguridad y autenticación comunes.

Unidad Organizativa: Es la que permite crear la jerarquía de nuestra organización, su fin es crear una estructura de carpetas que administrativamente organice una empresa u organización.

Active Directory: Es un servicio establecido de uno o varios servidores en donde se crean objetos como usuarios, grupos con el fin de administrar los inicios de sesión y políticas en toda la red.

4. Documentos de referencia:

ANEXO-1B Asignación de políticas de AD.

ANEXO-2B Cronograma de cambio de fondo de pantalla.

5. Descripción de la Política

Establecer las buenas prácticas para la gestión de servicios de tecnologías de la información en todos los niveles que se participa para entregar el servicio al cliente. Es necesario contar con herramientas y procesos de gestión de red para controlar posibles fallas o degradaciones en los servicios de red que soportan los servicios de TI utilizando un directorio activo, para una buena administración que ayude en la eficiencia de los empleados durante sus jornadas de acuerdo al ANEXO-1B Asignación de políticas de AD.

6. Registros.

N/A

7. Anexos.

1B Asignación de políticas de AD

2B Cronograma de cambio de fondo de pantalla

	ASIGNACIÓN DE POLÍTICAS DE ACTIVE DIRECTORY	ANEXO-1B
		Ver No. 01
		Pág 1 de 1

N°	NOMBRE DE LA POLÍTICA	DESCRIPCIÓN	NO APLICA	APLICA
1	Auditoría	Genera registros de inicios y salida de sesión tanto exitosos como fallidos en el equipo de computo.		X
2	Mensaje de inicio de sesión	Va a indicar un mensaje de inicio.		X
3	Papel tapiz	Despliega un fondo de pantalla.		X
4	Renombrar administrador	Renombrar el usuario administrador local.	X	
5	Regedit	Permite editar el registro del sistema operativo Windows este registro es la base de datos donde se guardan las preferencias del usuario en materia de configuraciones.	X	
6	Prohibir a drivers	Evita accesos a unidades USB.	X	
7	Seguridad	La contrseña del usuario va a caducar cada 3 meses.		X
8	Framework	El usuario no podrá desactivar los framework del antivirus.		X
9	Bloqueo de pantalla	Una vez que se bloquea va apresentar el proctetor de pantalla para nuevamente activar el usuario o poner el uso donde va a pedir la contraseña.		X
10	Programas de espias	Está prohibida la utilización de “sniffers”, “keylogguers” o cualquier otro software espía en cualquier red o equipo de cómputo.		X
11	Instalación de programas	No podrá instalar ningún software adicional en el equipo que sea asignado.	X	
12	Antivirus	Bloquear el acceso a la admintración		X
13	Usuarios locales	Establecer cuentas locales para el acceso a la administración de los equipos de computo.		X

	CRONOGRAMA DE CAMBIO DE FONDOS DE PANTALLA	ANEXO-2B Ver No. 01 Pág. 1 de 1

	MES											
DEPARTAMENTOS	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**
Fondo de Año Nuevo utilizando el logo del Municipio	X											
Fondo del Carnaval Panguense con logo del Municipio		X										
Fondo Normal y Formal con el logo del Municipio			X									
Fondo de Provincialización de Cotopaxi con logo del Municipio				X								
Fondo de Parroquialización de Ramón Campaña, día del trabajo u otro con logo del Municipio.					X							
Fondo de Cantonización utilizando el logo del Municipio						X						
Fondo Normal y Formal con el logo del Municipio							X					
Fondo del Reencuentro Panguense utilizando el logo del Municipio								X				
Fondo de las fiestas de la Virgen de la Merced utilizando el logo del Municipio									X			
Fondo Normal y Formal con el logo del Municipio										X		
Fondo Normal y Formal con el logo del Municipio											X	
Fondo Navideño utilizando el logo del Municipio												X

1. Objetivo

Gestionar el ciclo de vida de los activos de la empresa mediante lineamiento e inventarios para la toma de decisiones del Gobierno Autónomo Descentralizado Municipal de Pangua.

2. Alcance

Aplicar a todos los activos fijos tecnológicos de la organización del Gobierno Autónomo Descentralizado Municipal de Pangua, incluyendo empleados, contratistas, consultores y visitantes.

3. Definiciones:

Activos de TI: Son los activos informáticos, su gestión permite alcanzar un manejo adecuado y mejora su eficiencia y rendimiento de la organización.

Data Center: Es un ambiente acondicionado que contiene computadoras (ordenadores) y otros dispositivos de hardware, conectados en red y equipados con el software necesario para desarrollar el procesamiento de los datos.

Hardware: Es la parte física de un ordenador o la parte tangible como CPU (Unidad Central de Procesamiento), la memoria RAM, el disco duro, el monitor, la tarjeta gráfica, el teclado, el ratón, la unidad de disquete, la unidad de CD o DVD, la impresora, el escáner, el disco duro rígido, los altavoces, etc.

Software: Son los programas del computador o la parte intangible que permite realizar multitareas.

Mantenimiento Preventivo: Consiste en la revisión en el software y hardware de la PC u ordenador lo que permite al usuario poseer un equipo fiable para intercambiar información a una máxima velocidad con respecto a la configuración del sistema.

4. Documentos de referencia

RE-1C Inventario de los activos de TI (nombre de equipo, usuario, marca, modelo, tipo, sistema operativo, office, microprocesador, ram, disco duro, monitor).
RE-2C Acta de entrega y recepción de equipo.
RE-3C Bitácora del mantenimiento preventivo del datacenter.
RE-4C Bitácora del mantenimiento preventivo de equipos.
RE-5C Bitácora del mantenimiento correctivo de equipos.
RE-6C Bitácora de acceso al datacenter.
RE-7C Documento de transferencia de activos fijos.
RE-8C Documento de baja a los activos fijos.
ANEXO-1C Cronograma para mantenimiento preventivo del datacenter.
ANEXO-2C Cronograma para mantenimiento preventivo de equipos
ANEXO-3C Cronograma para mantenimiento correctivo de equipos.

5. Descripción de la Política

Todos los activos de TI (RE-1C Inventarios de activos de TI) de la Municipalidad están a cargo del área de TI quien es el responsable hasta que los equipos sean asignados a los usuarios del GAD, los equipos de cómputo se gestionaran así:

5.1. Asignación de activo de TI

Generar documento para que asigne equipos a nuevos empleados, equipos que demande para realizar sus funciones laborales para ello se requiere el RE-2A Solicitud de creación de nuevos usuarios de red. Como también esta política permite supervisar cuántos y cuáles son los recursos tecnológicos que realmente cuenta el Municipio y posteriormente controlar la fase y el tiempo de los activos para la renovación según su estado.

El área de TI debe tener la capacidad de asignar equipos.

5.2. Asignación de Sistemas Informáticos

El usuario responsable por su equipo deberá firmar un acta de entrega.

Se evaluará el rendimiento del equipo para su uso, cabe mencionar que es recomendable cambiar cada seis a ocho años.

5.3. Transferencia de activos de TI

El usuario responsable de la asignación de equipos es el encargado de departamento de sistemas, en caso de trasferencias de equipos entre empleados, deberá llenar el RE-7C Documento de transferencia de activos.

5.4. Baja de activos de TI

Los equipos que superen los 5 años de vida funcional deben ser dados de baja por su bajo rendimiento RE-8C Documento de baja de activos fijos.

5.5. Mantenimiento de Datacenter

Data Center

La puerta de ingreso al cuarto del Datacenter deberá estar permanentemente cerrada con llave.

El usuario debe controlar que la temperatura del Datacenter este de 18 a 25 Grados Centígrados.

El usuario responsable del Departamento de Sistemas podrá efectuar el mantenimiento se realizara mensual ANEXO 1C Cronograma de mantenimiento preventivo del Datacenter finalizada la actividad llenar la bitácora RE-3C Bitácora de mantenimiento preventivo del Datacenter.

El usuario no podrá consumir alimentos, bebidas o fumar dentro del data center.

Realizar la selección adecuada de la seguridad del data center es preferible que esta sea cerradura electrónica.

Está prohibido la acumulación y almacenamiento de material inflamables (cartón, papel).

No se puede proveer información sobre la ubicación del Datacenter.

1.1. Mantenimiento de PC's

Realizar manteamiento a todos los equipos cada 6 meses de acuerdo al ANEXO 2C Cronograma para mantenimiento preventivo de equipos finalizado el mantenimiento se debe llenar la bitácora RE-4C Bitácora de mantenimiento preventivo de equipos.
Para el mantenimiento correctivo deberá seguir en base al ANEXO 3C Cronograma para mantenimiento correctivo de equipos de igual forma finalizado la actividad se deberá llenar la bitácora RE-5C Bitácora de mantenimiento correctivo de equipos.
Solo el técnico encargado estará autorizado en sacar los equipos fuera de la empresa.
Solo el técnico encargado tendrá la autorización de realizar instalaciones en los equipos.
Los cables deben estar protegidos por canaletas
Las credenciales de usuario son personal e intransferible.

2. Registros.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-1C	Inventario de los activos de TI	Analista de sistemas informáticos	Oficina Sistemas área de Soporte a equipos	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-2C	Acta de entrega y recepción del equipo	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-3C	Bitácora de mantenimiento preventivo del datacenter	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-4C	Bitácora de mantenimiento preventivo de equipos	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-5C	Bitácora de mantenimiento correctivo de equipos	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-6C	Bitácora de acceso al datacenter	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-7C	Documento de transferencia de activos fijos	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno

RE-8C	Documento de baja a los activos fijos	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno

3. Anexos.

1C Cronograma para mantenimiento preventivo del datacenter.
2C Cronograma para mantenimiento preventivo de equipos
3C Cronograma para mantenimiento correctivo de equipos.

	INVENTARIO DE LOS ACTIVOS DE TI	RE-1C
		Ver No. 01
		Pág. 1 de 1

INVENTARIO DE LOS ACTIVOS DE TI

N°	CÓDIGO DEL EQUIPO	FECHA DE ENTREGA	RESPONSABLE	DEPARTAMENTO	DOMINIO	NOMBRE DEL PC	NOMBRE DEL USUARIO	TIPO DEL EQUIPO	MARCA	MODELO	SERIE			PROCESADOR	RAM	DISCO DURO	MONITOR	TECLADO	MOUSE	ADAPTADOR LAPTOP (cargador)	ACCESORIO (Maletas)	CANDADO	SISTEMA OPERATIVO	OFFICE
											CPU	LAPTOP	SERVIDOR				MARCA	MARCA	MARCA					

	ACTA DE ENTREGA Y RECEPCIÓN DEL EQUIPO	RE-2C Ver No. 01 Pág. 1 de 1

A los _____ días del mes de _____ del año _____se procede a realizar la entrega y recepción de los equipos que se detallaran, al Departamento de _____ del Gobierno Autónomo Descentralizado Municipal de Pangua.

ACTIVO FIJO	NOMBRE DE EQUIPO	USUARIO	MARCA	MODELO	SERIE	TIPO	S.O	RAM	DISCO DURO	MICRO PROCESADOR	MONITOR	MOUSE	TECLADO

Nota:_____
_____

Como constancia de que los equipos se entregaron en buen estado, se procede a la firma de recibido.

_____ _____

APELLIDOS Y NOMBRES DE RECIBIDO **APELLIDOS Y NOMBRES DEL ENCARGADO**

C.I.: **Número de cédula** C.I.: **Número de cédula**

	BITÁCORA DE MANTENIMIENTO PREVENTIVO DE DATACENTER	RE-3C Ver No. 01 Pág. 1 de 1

BITÁCORA DE MANTENIMIENTO PREVENTIVO DE DATACENTER			
DEPARTAMENTO	**FECHA**	**DESCRIPCIÓN DE MANTENIMIENTO**	**FIRMA**

	BITÁCORA DE MANTENIMIENTO PREVENTIVO DE EQUIPOS	RE-4C
		Ver No. 01
		Pág. 1 de 1

BITÁCORA DE MANTENIMIENTO PREVENTIVO DE EQUIPOS					
DEPARTAMENTO	**NOMBRE EQUIPO**	**FECHA**	**HORA**	**PROBLEMA**	**FIRMA**

	BITÁCORA DE MANTENIMIENTO CORRECTIVO DE EQUIPOS	RE-5C Ver No. 01 Pág. 1 de 1

BITÁCORA DE MANTENIMIENTO CORRECTIVO DE EQUIPOS					
DEPARTAMENTO	**NOMBRE EQUIPO**	**FECHA**	**HORA**	**PROBLEMA**	**FIRMA**

	BITÁCORA DE ACCESO AL DATACENTER	RE-6C Ver No. 01 Pág. 1 de 1

BITÁCORA DE ACCESO AL DATACENTER						
Fecha Ingreso	**Hora Ingreso**	**Firma Ingreso**	**Nombre**	**Actividad Realizada**	**Hora Salida**	**Firma Salida**

	DOCUMENTO DE TRANSFERENCIA DE ACTIVOS FIJOS	RE-7C Ver No. 01 Pág. 1 de 1

En el cantón Pangua a los __días del mes de_____ del año _____, se procede a la **Transferencia de activos** el equipo que se especifica a continuación con los respectivos empleados:

ACTIVO FIJO	DESCRIPCIÓN	SERIE, MODELO Y MARCA	DEPARTAMENTO DEL ANTERIOR CUSTODIO	DEPARTAMENTO DEL NUEVO CUSTODIO	ANTERIOR CUSTODIO	NUEVO CUSTODIO

De acuerdo a lo anterior se hace constar que el equipo se encuentra en normal funcionamiento

Anterior Custodio	Nuevo Custodio	Director de Finanzas
_____	_____	_____
NOMBRE Y FIRMA	**NOMBRE Y FIRMA**	**NOMBRE Y FIRMA**

GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPAL DE PANGUA

INFORME DE BAJA DE BIENES

ACTA N°:_____
FECHA:_____

NOMBRE DEL RESPONSABLE:_____

DEPARTAMENTO:_____

EQUIPO DE COMPUTO:_____

CARACTERISTICAS

Activo Fijo	Detalle	Marca	Modelo	Serie	Valor de adquisición	Valor depreciado	Fecha compra

CAUSA DE BAJA: _____
(Documentación anexa para verificación física documental)

DOCUMENTACIÓN INTEGRANTE AL REVERSO

OBSERVACIONES:_____
_____

_____ _____
SISTEMAS INFORMÁTICOS DIRECCIÓN FINANCIERA

_____
DIRECCIÓN ADMINISTRATIVA

	CRONOGRAMA PARA MANTENIMIENTO PREVENTIVO DEL DATACENTER	ANEXO-1C Ver No. 01 Pág. 1 de 1

	MES											
DATACENTER	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**
Equipos de networking					x							x
Servidores					x							x
Iluminación					x							x
Climatización (motores, aire acondicionado, temperatura, etc.)					x							x
Control de incendio (extintores, sensores)					x							x
UPS					x							x
Control de acceso (cámaras, tarjetas, etc.)					x							x
Piso					x							x

FIRMA DE ENCARGADO DE TI
C.I.: **Número de cédula**

FIRMA DEL ALCALDE
C.I.: **Número de cédula**

	CRONOGRAMA PARA MANTENIMIENTO PREVENTIVO DE EQUIPOS	ANEXO-2C Ver No. 01 Pág. 1 de 3

	MES											
DEPARTAMENTOS	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**
MIES	X											
UNIDAD DE CULTURA	X											
PROMOCIÓN COMUNITARIA		X										
SERVICIOS GENERALES		X										
PLANIFICACIÓN Y DESARROLLO			X									
ASESORIA DE ALCALDIA			X									
UNIDAD TÉCNICO DE GESTIÓN DE RIESGOS			X									
UNIDAD DE TALENTO HUMANO				X								
ADMINISTRACIÓN DE PLAZAS Y MERCADOS				X								
COMISARIA MUNICIPAL					X							

SECRETARIA EJECUTIVA DE LA NIÑEZ Y ADOLECENCIA DEL CANTÓN PANGUA					X							
CONSEJO CANTONAL DE PROTECCIÓN DE DERECHOS						X						
DIRECCIÓN FINANCIERA						X						
UNIDAD DE ATENCIÓN A GRUPOS VULNERABLES							X					
REGISTRO DE LA PROPIEDAD							X					
SECRETARIA GENERAL								X				
UNIDAD TÉCNICO DE INFRAESTRUCTURA Y DISEÑO DE PROYECTOS								X				
UNIDAD DE FISCAIZACIÓN									X			
VIALIDAD Y EQUIPO CAMINERO									X			
AGUA POTABLE Y ALCANTARILLADO									X			
OBRAS PÚBLICAS										X		

RECAUDACIÓN										X		
OFICINA DE RENTAS										X		
TESORERO											X	
ORDENAMIENTO TERRITORIAL											X	
SISTEMAS INFORMÁTICOS											X	
SINDICATURA												X
AVALÚOS Y CATASTROS												X
BODEGA												X

_____ _____

FIRMA DE ENCARGADO DE TI **FIRMA DE ALCALDE**
C.I.: Número de cédula **C.I.: Número de cédula**

	MES											
DEPARTAMENTOS	**Enero**	**Febrero**	**Marzo**	**Abril**	**Mayo**	**Junio**	**Julio**	**Agosto**	**Septiembre**	**Octubre**	**Noviembre**	**Diciembre**
MIES	X			X			X			X		
UNIDAD DE CULTURA	X			X			X			X		
PROMOCIÓN COMUNITARIA	X			X			X			X		
SERVICIOS GENERALES	X			X			X			X		
PLANIFICACIÓN Y DESARROLLO	X			X			X			X		
ASESORÍA DE ALCANDÍA	X			X			X			X		
UNIDAD TÉCNICO DE GESTIÓN DE RIESGOS	X			X			X			X		
UNIDAD DE TALENTO HUMANO	X			X			X			X		
ADMINISTRACIÓN DE PLAZAS Y MERCADOS	X			X			X			X		
COMISARIA MUNICIPAL	X			X			X			X		

SECRETARIA EJECUTIVA DE LA NIÑEZ Y ADOLECENCIA DEL CANTÓN PANGUA	X			X			X			X		
CONSEJO CANTONAL DE PROTECCIÓN DE DERECHOS	X			X			X			X		
DIRECCIÓN FINANCIERA	X			X			X			X		
UNIDAD DE ATENCIÓN A GRUPOS VULNERABLES	X			X			X			X		
REGISTRO DE LA PROPIEDAD	X			X			X			X		
SECRETARIA GENERAL	X			X			X			X		
UNIDAD TÉCNICO DE INFRAESTRUCTURA Y DISEÑO DE PROYECTOS	X			X			X			X		
UNIDAD DE FISCAIZACIÓN	X			X			X			X		
VIALIDAD Y EQUIPO CAMINERO	X			X			X			X		
AGUA POTABLE Y ALCANTARILLADO	X			X			X			X		
OBRAS PÚBLICAS	X			X			X			X		

RECAUDACIÓN	X			X			X			X		
OFICINA DE RENTAS	X			X			X			X		
TESORERO	X			X			X			X		
ORDENAMIENTO TERRITORIAL	X			X			X			X		
SISTEMAS INFORMÁTICOS	X			X			X			X		
SINDICATURA	X			X			X			X		
AVALÚOS Y CATASTROS	X			X			X			X		
BODEGA	X			X			X			X		

FIRMA DE ENCARGADO DE TI
C.I.: **Número de cédula**

FIRMA DE ALCALDE
C.I.: **Número de cédula**

1. Objetivo

Definir e implementar lineamientos para respaldar la información relevante en todos los niveles de la Municipalidad.

2. Alcance

Aplica a todos los miembros de la comunidad del Gobierno Autónomo Descentralizado Municipal de Pangua. Definida en el ANEXO-1F Listado de usuarios para backup**.**

3. Definiciones:

SyncBack: Es un programa gratuito que sincroniza y hace copias de seguridad de los archivos, carpetas, directorios entre otros.

4. Documentos de referencia:

ANEXO-1F Listado de usuarios para backup.
RE-1F Bitácora de respaldos de usuarios.

5. Descripción de la Política

Evitar la pérdida de la información dentro de la empresa en caso de que existan eventos fortuitos con el fin de garantizar la disponibilidad de la información.

5.1 Responsabilidad de los Usuarios

El usuario debe almacenar su información laboral dentro de la carpeta llamada RESPALDOS que va estar alojada en la unidad D si no tiene una partición se creara una carpeta dentro de la partición.
El usuario debe dar acceso de su información cuando el personal de tecnología de información lo requiera.

5.2 Responsabilidad del área de Sistemas Informáticos

El departamento de sistemas debe crear una carpeta para que los usuarios almacenen ahí su información y se haga el debido respaldo (Ejemplo: D:\respaldos), caso que el usuario no acate la disposición de almacenar en esa carpeta la información, el encargado de Sistemas Informáticos no se hará responsable de la perdida de dicha información.
Implementar un software específico que ayude a generar respaldos periódicamente.
Asignar espacios de almacenamiento específico de acuerdo a la posición que desempeñe el usuario final.
Generar el control de acuerdo al RE-1F Bitácora de respaldos de usuarios.
Disponer con una segunda herramienta para respaldos de información.

5.3. Responsabilidad del área de Recursos Humanos

Proporcionar información de la salida de personal con tiempo suficiente (48 horas) para la planificación de respaldos de información.

5. Registros.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-1F	Bitácora de respaldos de usuarios.	Analista de sistemas informáticos	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno

6. Anexos.

ANEXO-1F Listado de usuarios para backup.

	BITÁCORA DE RESPALDOS DE USUARIOS	RE-1F
		Ver No. 01
		Pág. 1 de 1

N°	CARGO	NOMBRE EQUIPO	MESES											
			ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE

LISTADO DE USUARIOS PARA BACKUP			
N°	**NOMBRE DE EQUIPO**	**CARGO**	**PERÍODO DE RESPALDO**
1	Panpcfin-01	Dirección Financiera	Semanal
2	Panpcalc-02	Asesoría de Alcaldía	Semanal
3	Pannbsis-03	Gerente de Sistemas	Semanal
4	Panpcplaymer-04	Administración de plazas y mercados	Semanal
5	Panpcrec-05	Recaudación	Semanal
6	Panpctes-06	Tesorero	Semanal
7	Panpcsecg-07	Secretaria general	Semanal
8	Panpcregpro-08	Registro de la propiedad	Semanal

1. Objetivo

Generar lineamientos para proteger y resguardar los componentes informáticos del Gobierno Autónomo Descentralizado Municipal de Pangua.

2. Alcance

Aplica a toda la infraestructura del Gobierno Autónomo Descentralizado Municipal de Pangua.

3. Definiciones:

Componente informático: Son el conjunto de equipos y programas que conforman un computador o sistema informático.

4. Documentos de referencia:

RE-1D Bitácora de registro de salida e ingreso de equipos.
RE-2D Bitácora de control de ingreso y salida de equipos de visitas.
ANEXO1D- Listado de personas autorizadas.

5. Descripción de la Política

El departamento de sistemas informáticos es el encargado de proteger, planificar y dar seguimiento a los lineamientos de seguridad establecidos:

- Protección de los equipos
- Ingreso de equipos y dispositivos externos, que no son propios de la institución.

5.1. Responsabilidad del Departamento de Sistemas Informáticos

Debe proporcionar e instalar un antivirus garantizado su adecuado funcionamiento, cortafuegos para bloquear el acceso no autorizado a la red con el fin de evitar virus, gusanos, ataques, robo de datos, etc.
Debe actualizar los programas que regulan la seguridad (Antivirus, licencias, sistemas operativos)

5.2. Acceso a servidores

TI tiene la responsabilidad de asignar los permisos adecuados para el acceso a los servidores, para que el especialista analice su estado y funcionamiento.
No se puede ingerir alimentos en el área de servidores pues cualquier derrame podría ocasionar perdidas del activo.

5.3. Protección de equipos

Implementar Antivirus en los equipos con sus debidas actualizaciones.
Es recomendable instalar un Sistemas Operativos con licencias autorizadas y que estén acorde con las características de la computadora, se recomiendan versiones a partir de Windows 8.1 pro hasta Windows 10.

Los equipos deben tener un cobertor anti polvos para alargar el tiempo de vida útil.
No se puede ingerir alimentos ante los activos, pues cualquier derrame podría ocasionar perdidas del activo.

5.4. Ingreso y salida de equipos

Los dispositivos de red son propiedad de la empresa, por lo que ningún empleado puede hacer uso externo de él.

Para el ingreso de equipos externos, debe tener un documento de autorización y llevar un control de acuerdo al RE-1D Bitácora de registro de salida e ingreso de equipos, en caso de empleados.

Para el ingreso de equipos de personas visitantes, debe llevar control el personal encargado de la seguridad, mediante la RE-2D Bitácora de control de ingreso y salida de equipos de visitas.

Las laptop del Municipio deben tener candado.

Los empleados que deben llevarse los equipos deben tener una autorización previa ANEXO1D- Listado de personas autorizadas.

6. Registros.

Código	Nombre	Responsable	Ubicación	Archivo	Actualización	Retención	Destino Final	Acceso
RE-1D	Bitácora de registro de salida e ingreso de equipos	Analista de sistemas	Oficina Sistemas área de análisis de sistemas	21/08/2020	Anual	2 años	Reciclaje de papel	Uso interno
RE-2D	Bitácora de control de ingreso y salida de equipos de visitas.	Personal encargado de la seguridad(guardia)	Ingreso al edificio	21/08/2020	Anual	2años	Reciclaje de papel	Uso interno

7. Anexos.

ANEXO1D- Listado de personas autorizadas.

BITÁCORA DE REGISTRO DE SALIDA E INGRESO DE EQUIPOS						
RESPONSABLE	**CARGO**	**MOTIVO**	**HORA DE SALIDA**	**FIRMA**	**HORA DE INGRESO**	**FIRMA**

	BITÁCORA DE VISITAS PARA EL CONTROL DE ENTRADA Y SALIDA DE EQUIPOS DE COMPUTO	RE-2D
		Ver No. 01
		Pág 1 de 1

BITÁCORA DE CONTROL DE INGRESO Y SALIDA DE EQUIPOS DE VISITAS								
N°	**NOMBRE DEL RESPONSABLE**	**MARCA**	**MODELO**	**SERIE**	**FECHA**	**HORA DE INGRESO**	**HORA DE SALIDA**	**FIRMA**

LISTADO DE PERSONAS AUTORIZADAS						
CÓDIGO	**TIPO**	**RESPONSABLE**	**CARGO**	**MARCA**	**MODELO**	**SERIE**
1.4.1.01.07.013.003	Laptop	Ing. Luis Guzmán	Director de saneamiento ambiental	DELL	CPDCBD6P03	CN-OCK6DB-CMC00-9B6-0005
1.4.1.01.07.001.001.051	Laptop	Ing. Manuel Coronel	Gestión de Riesgos	HP	NOTEBOOK	5CG6441WY
1.4.1.01.07.001.002.17	Laptop	Dra. Gabriela Rivera	Saneamiento ambiental	HP	NOTEBOOK	5CG6441R54
1.4.1.01.07.001.002.009	Laptop	Ing. Ingrid Torres	Tesorero Municipal	HP	Z800K15	CND3510HQR

1.4.1.01.07.001.002.15	Laptop	Sra. Jenny Domínguez	Recaudadora, Dirección Financiera	ACER	E5-471	NXMN2AL0034280 9897600
1.4.1.01.07.001.002.012	Laptop	Ing. Henry Tana	Administración de Plazas y Mercados	TOSHIBA	SATELIT	S4E1265312C
1.4.1.01.07.001.002.011	Laptop	Ing. Washington Palacios	Dirección Financiera	HP	ETILE K8470P CORE I7	CNU415BK1H
	Laptop	Ing. Marco Zurita	Director de Obras Publicas	HP	15-AY016LA	CND71357KP

1. Objetivo

Definir las reglas y categorías para el acceso al internet por el usuario para que no existan distracciones en las horas laborables.

2. Alcance

Aplica a todos los usuarios que constituyen la lista de distribución del servidor de dominio del Gobierno Autónomo Descentralizado Municipal de Pangua, incluyendo contratistas, consultores y visitantes.

3. Definiciones:

Webfilter: Es un software diseñado para restringir los sitios web que pueden ser visitados por el usuario en su equipo.

Categoría de Navegación: Es la clasificación de sitios web donde los usuarios conectados a una red pueden ingresar.

Malware: Es un término que engloba a todo tipo de programa o código informático malicioso cuya función es dañar un sistema o causar un mal funcionamiento.

4. Documentos de referencia:

ANEXO-1E Listado de categorías de acceso a internet.

5. Descripción de la Política

Buenas prácticas para el uso adecuado del internet.

Regular con un webfilter el acceso a internet.

Evitar distracciones por parte de los usuarios que laboran en la Institución.

Prevenir la saturación del ancho de banda por el uso de páginas de gran consumo de recursos como: Descargas, Streaming y Redes Sociales.

5.1 Restricciones

Queda estrictamente prohibido el uso de servicio de internet para las siguientes páginas:

Acceso a los sitios web para descargar información ajena a la actividad laboral.

El uso de sitios de videos, streaming en línea o en tiempo real. (YouTube, Spotify, etc.).

Ingresar a contenidos obscenos, agresivos, pornográficos, amenazadores, inmorales u ofensivos.

Uso de Juegos “online” en la red.

Acceso a sitios inseguros que comprometan la confidencialidad e integridad de la información.

Instalación y uso de aplicativos para intercambios de archivos.

Instalación de aplicativos de mensajería instantánea (WhatsApp, Messenger, etc.).

Nota: Si el empleado requiere trabajar con una de estas, deberá pedir autorización al Jefe Inmediato.

5.2 Accesos a categorías

El acceso a internet que proporciona al GAD está relacionado con nombre y usuario para inicio de sesión en el equipo de cómputo.
La empresa está en la capacidad de monitorear todos los accesos a internet de acuerdo a las categorías asignadas según el ANEXO-1E Listado de categorías de acceso a internet.

5.3 Penalizaciones

Cualquier usuario que no se ajuste a los lineamientos detallados en las políticas será sujeto a toma de decisiones de acuerdo al reglamento interno de trabajo.

6. Registros.

N/A

7. Anexos.

ANEXO-1E Listado de categorías de acceso a internet.

	CATEGORIAS DE ACCESO						
DEPARTAMENTO	**Gubernamentales**	**Educación**	**Financieros**	**Investigación**	**Redes Sociales**	**Streaming**	**TICs**
DIRECTORIO	X	X	X	X	X		X
MIES	X	X	X	X			
UNIDAD DE CULTURA	X	X		X	X		
PROMOCIÓN COMUNITARIA	X	X					
SERVICIOS GENERALES	X			X			
PLANIFICACIÓN Y DESARROLLO	X						
ASESORIA DE ALCALDIA	X	X	X		X		X
UNIDAD TÉCNICO DE GESTIÓN DE RIESGOS	X						
UNIDAD DE TALENTO HUMANO	X	X	X				
ADMINISTRACIÓN DE PLAZAS Y MERCADOS	X		X				
COMISARIA MUNICIPAL	X						
SECRETARIA EJECUTIVA DE LA NIÑEZ Y ADOLECENCIA DEL CANTÓN PANGUA	X	X		X			
CONSEJO CANTONAL DE PROTECCIÓN DE DERECHOS	X						
DIRECCIÓN FINANCIERA	X		X				
UNIDAD DE ATENCIÓN A GRUPOS VULNERABLES	X						X
REGISTRO DE LA PROPIEDAD	X			X			

SECRETARIA GENERAL	X						
UNIDAD TÉCNICO DE INFRAESTRUCTURA Y DISEÑO DE PROYECTOS	X			X			
UNIDAD DE FISCAIZACIÓN	X						
VIALIDAD Y EQUIPO CAMINERO	X						
AGUA POTABLE Y ALCANTARILLADO	X						
OBRAS PÚBLICAS	X						
RECAUDACIÓN	X		X				
OFICINA DE RENTAS	X		X				
TESORERO	X		X				
ORDENAMIENTO TERRITORIAL	X						
SISTEMAS INFORMÁTICOS	X	X		X			
SINDICATURA	X		X				
AVALÚOS Y CATASTROS	X						
BODEGA	X						