Universidad Científica del Perú - UCP
Registrado en el Asiento Nº A00010 de la Partida Nº 11000318, Personas Jurídicas de Iquitos, Superintendencia de los Registros Públicos - SUNARP

FACULTAD DE CIENCIAS E INGENIERÍA

PROGRAMA ACADEMICO DE INGENIERIA DE SISTEMAS DE INFORMACIÓN

TESIS

ELABORACIÓN DE UN PLAN PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA - 2021

PARA OBTAR EL TITÚLO PROFESIONAL DE

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTORES:

- BACH. HANS JOSÉ MAÚRTUA GUERRA
- BACH. HANS JOSEPH URCIA SABOYA

ASESOR:

ING. CARLOS GONZALEZ ASPAJO, MGR

SAN JUAN BAUTISTA – MAYNAS – LORETO- PERÚ – 2021

DEDICATORIA

A mis padres por brindarme siempre el apoyo que necesito en lo profesional y personal para el logro de mis metas y futuros logros planteados.

Bach. HANS JOSÉ MAÚRTUA GUERRA

El esfuerzo realizado va dedicado a mis padres y hermanos que siempre me brindan el apoyo incondicional ante los nuevos proyectos a los que me enfrento diariamente.

Bach. HANS JOSEPH URCIA SABOYA

AGRADECIMIENTO

Expresamos nuestro agradecimiento al nuestro asesor el Ing. Carlos Gonzales Aspajo por acompañarnos en este proceso de elaboración de nuestra tesis a la Universidad Científica del Perú, por ser nuestra alma mater.

A todos nuestros seres queridos que estuvieron detrás de esta meta planteada y por cumplir para nuestras vidas en especial a nuestros padres quienes estuvieron detrás para que esto sea realidad.

A nuestros padres por ser los principales promotores de nuestros sueños, por confiar y creer en nuestras expectativas, por los consejos, valores y principios que nos han inculcado.

A los maestros por la formación profesional que nos brindaron para lograr de mí una profesional.

A todas las personas que nos apoyaron por hacer de este proyecto una realidad.

BACH. HANS JOSÉ MAÚRTUA GUERRA

BACH. HANS JOSEPH URCIA SABOYA

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

UNIVERSIDAD CIENTÍFICA DEL PERÚ

"Año del Fortalecimiento de la Soberanía Nacional"

CONSTANCIA DE ORIGINALIDAD DEL TRABAJO DE INVESTIGACIÓN

DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP

El presidente del Comité de Ética de la Universidad Científica del Perú - UCP

Hace constar que:

La Tesis titulada:

"ELABORACIÓN DE UN PLAN PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA - 2021"

De los alumnos: **HANS JOSÉ MAÚRTUA GUERRA Y HANS JOSEPH URCIA SABOYA,** de la Facultad de Ciencias e Ingeniería , pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **6% de plagio**.

Se expide la presente, a solicitud de la parte interesada para los fines que estime conveniente.

San Juan, 06 de Setiembre del 2022.

Dr. César J. Ramal Asayag
Presidente del Comité de Ética – UCP

CJRA/ri-a
392-2022

UNIVERSIDAD CIENTÍFICA DEL PERÚ

FACULTAD DE CIENCIAS E INGENIERÍA

"Año del Fortalecimiento de la Soberanía Nacional"

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 551-2021-UCP-FCEI del 31 de agosto del 2021, la FACULTAD DE CIENCIAS E INGENIERÍA DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP designa como Jurado Evaluador de la sustentación de tesis a los señores:

- Ing. Jimmy Max Ramírez Villacorta, Mgr. — Presidente
- Ing. Tonny Eduardo Bardales Tello, Mgr. — Miembro
- Ing. Ángel Alberto Marthans Ruiz, Mgr. — Miembro

Como Asesor: al Ing. Carlos Gonzales Aspajo, Mgr.

En la ciudad de Iquitos, siendo las 08:00 am del día 26 de octubre del 2022, de manera Virtual utilizando la plataforma ZOOM y supervisado por la Secretaria Académica del programa Académico de Ingeniería Ambiental de la Facultad de Ciencias e Ingeniería de la Universidad Científica del Perú, se constituyó el Jurado para escuchar la sustentación y defensa de la Tesis: **"ELABORACIÓN DE UN PLAN PARA MEJORAR LA GESTIÓN DE LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE PUNCHANA-2021".**

Presentado por la sustentante: **HANS JOSE MAURTUA GUERRA y HANS JOSEPH URCIA SABOYA**

Como requisito para optar el título profesional de: **INGENIERO DE SISTEMAS DE INFORMACION**

Luego de escuchar la sustentación y formuladas las preguntas las que fueron: *ABSUELTAS*

El Jurado después de la deliberación en privado llegó a la siguiente conclusión

La sustentación: *APROBADO MAYORIA*

En fe de lo cual los miembros del Jurado firman el acta.

Ing. Jimmy Max Ramírez Villacorta, Mgr.
Presidente

Tonny Eduardo Bardales Tello, Mgr
Miembro

Ing. Ángel Alberto Marthans Ruiz, Mgr.
Miembro

HOJA DE APROBACIÓN

Ing. Jimmy Max Ramirez Villacorta, Mgr

Presidente

Ing. Tonny Eduardo Bardales Lozano, Mgr

Miembro

Ing. Ángel Alberto Marthans Ruiz, Mgr

Miembro

Ing. Carlos Gonzalez Aspajo, Mgr

Asesor

INDICE DEL CONTENIDO

Páginas

INDICE DE TABLAS

Página

INDICE DE GRÁFICOS

Página

INDICE DE FIGURAS

Página

RESUMEN

En la presente tesis titulada Elaboración de un plan para mejorar la seguridad informática de la Municipalidad Distrital de Punchana, se realizó una evaluación en tiempo real respecto al estado situacional de la entidad tomando en consideración la norma internacional ISO/IEC 27002, donde se puedo determinar que en todos los ítems que corresponde la norma, la entidad tiene muchas vulnerabilidades, pudiendo conllevar a que las amenazas puedan ejecutar algún acto perjudicando a la información de la municipalidad y por ende paralizar los servicios informáticos causando molestia tanto a los vecinos o usuarios que van a realizar algún trámite o también a los trabajadores de la municipalidad, en esta investigación se tomó en consideración los siguientes aspectos: Políticas de Seguridad, Gestión de Activos, Seguridad Ligada a los Recursos Humanos, Seguridad Física y del Entorno, Gestión de Comunicaciones y Operaciones, Control de Accesos, Adquisición, desarrollo y mantenimiento de los sistemas informáticos, Gestión de Incidentes de Seguridad de la Información, y Conformidad de los Servicios Informáticos.

Palabras Claves: Plan, Seguridad, Informática, Municipalidad

ABSTRACT

In this thesis entitled Elaboration of a plan to improve the computer security of the District Municipality of Punchana, an evaluation was carried out in real time regarding the situational state of the entity taking into account the international standard ISO / IEC 27002, where it can be determined that in all the items that the standard corresponds to, the entity has many vulnerabilities, which can lead to the threats being able to execute some act harming the information of the municipality and therefore paralyze the computer services causing inconvenience to both the neighbors or users who go to carry out some procedure or also to the workers of the municipality, in this investigation the following aspects were taken into consideration: Security Policies, Asset Management, Security Linked to Human Resources, Physical Security and the Environment, Communications Management and Operations , Access Control, Acquisition, development and maintenance of systems IT Services, Information Security Incident Management, and IT Services Compliance.

Keywords: Plan, Security, Informatics, Municipality

Capítulo I: Marco teórico

1.1 Antecedentes del estudio

Carbajal, Felipe & Vega, Eduin & García Ramon (2020) en su tesis para obtener su título de Ingeniero de Sistemas en la Universidad Cooperativa de Colombia, titulada Diseño de una plan de seguridad informática para el sistema de información del colegio gimnasio los Pinos, cuyo objetivo general es Diseñar una guía de seguridad informática que garantice la confidencialidad, integridad y disponibilidad de los sistemas de información mediante el Modelo de Seguridad y Privacidad de la Información (MSPI) de MINTIC según el instructivo número tres (3) Como parte de la NORMA TECNICA COLOMBIANA ISO 27001, en el Colegio Gimnasio Los Pinos en la ciudad de Bogotá DC., para el desarrollo de esta investigación primero se analizó los posibles riesgos informáticos existentes en la entidad, y para la elaboración del plan de seguridad informática la Norma ISO 27001, teniendo como resultado una evaluación exhaustiva del riego informático existente en la entidad y como propuesta un plan de seguridad informática.

Merchán, Joao (2019) en su tesis para obtener su título de Ingeniero en Sistemas Computacionales en la Universidad Estatal del Sur de Manabí, titulada Diseño de un Plan de Seguridad Informática para la Cooperativa de Ahorro Y Crédito “Por El Pan Y El Agua” De La Ciudad De Jipijapa”, cuyo objetivo general es diseñar un plan de seguridad informática y análisis de riesgos fundamentados en estándares internacionales, con el fin de promover como política institucional para servir como referencia para la toma de decisiones sobre las tecnologías emergentes y sus amenazas, para el desarrollo de esta investigación primero se analizó los posibles riesgos informáticos existentes en la entidad, y para la elaboración del plan de seguridad informática la Norma ISO 27002, teniendo como resultado una evaluación exhaustiva del riego informático existente en la entidad y como propuesta un plan de seguridad informática.

Borja, Yolanda & Sánchez Fanny (2015) en su tesis para obtener su grado de magister en evaluación y auditoria de sistemas tecnológicos en la Universidad de las Fuerzas Armadas – Ecuador, titulada Plan de Seguridad Informática de la ESPE Santo Domingo, cuyo objetivo general es diseñar un plan de seguridad informática y análisis de riesgos fundamentados en estándares internacionales, con el fin de promover como política institucional para servir como referencia para la toma de decisiones sobre las tecnologías emergentes y sus amenazas, para el desarrollo de esta investigación se aplicó la metodología COBIT 5 con la finalidad de analizar los posibles riesgos informáticos existentes en la entidad, y para la elaboración del plan de seguridad informática la Norma ISO 27002 y 27003, teniendo como resultado una evaluación exhaustiva del riego informático existente en la entidad y como propuesta un plan de seguridad informática.

Sota, Luis (2019) en su tesis para obtener su título de Ingeniero de Sistemas en la Universidad Andina del Cusco, titulada "Diseño Del Plan De Seguridad Informática Basado En La NTP ISO/IEC 27001:2014 Para La Municipalidad Del Centro Poblado De Salcedo - Puno", cuyo objetivo general Diseñar un plan de seguridad informática basado en la NTP-ISO/IEC 27001:2014, para que en base a su aplicación se logre la disminución de los niveles de riesgo de seguridad informática en los procesos de negocios de la Municipalidad del Centro Poblado de Salcedo Puno"., con el fin de promover como política institucional para servir como referencia para la toma de decisiones sobre las tecnologías emergentes y sus amenazas, para el desarrollo de esta investigación primero se analizó los posibles riesgos informáticos existentes en la entidad, y para la elaboración del plan de seguridad informática la NTP-ISO/IEC 27001:2014, teniendo como resultado una evaluación exhaustiva del riego informático existente en la entidad y como propuesta un plan de seguridad informática.

Ariasca, Suma & Quispe, Borda (2017), en su tesis titulada "Desarrollo de una Propuesta de Implementación de la NTPISO/IEC 27001:2014, Sistema de Gestión de Seguridad de la Información, para la Oficina Funcional de Informática del Gobierno Regional del Cusco", concluyeron que la aplicación de la NTP ISO/IEC 27001:2014, permite definir los procesos y actividades requeridos para el diseño y planificación del Sistema de Gestión de Seguridad de la Información, así como identificar los activos de información críticos, los riegos asociados a

estos, los propietarios de cada riesgo y así definir los controles de seguridad requeridos para garantizar un nivel de seguridad adecuado para la elaboración del Plan de Tratamiento de Riesgos y así lograr desarrollar y documentar los procesos, procedimientos y actividades del diseño y planificación del Sistema de Gestión de Seguridad de la Información en cumplimiento respecto a la documentación requerida por la norma".

1.2 Bases teóricas

- Plan

  La palabra plan que quiere decir altitud o nivel que proviene del latín "Planus" y puede traducirse como "plano". Un plan es una serie o de pasos o procesamientos que buscan conseguir un objeto o propósito de dirigir a una dirección, el proceso para diseñar un plan se le conoce como planeación o planificación.

  Las características de un plan deben ser coherente, contener objetivos claros, estar contextualizado, ser viable y flexible, estar consensuado, estar organizado, servir de guía y ser evaluable.

- Seguridad Informática

  Para Porto (2018), La seguridad informática es muy importante ya que permite conservar el hardware y el software de una organización en buenas condiciones, también permite asegurarse que el uso de los recursos sea seguro respecto a los usuarios o personas acreditadas para hacerlo.

  La ISO Tools (2010), señala que la seguridad informática está relacionada con la Seguridad de la Información la cual consiste en asegurar que los recursos informáticos de una organización o empresa se utilicen de la forma más adecuada con políticas estructuradas de seguridad y acceso de información, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites establecidos de la autorización.

La seguridad informática tiene como objetivo la protección de los activos de información de la organización los principales elementos que se considera en la seguridad informática son: La Información: es el objeto de mayor valor para la empresa, los equipos: suelen ser software, hardware y la propia organización y por ultimo los Usuarios: que son las personas que usan la tecnología de la organización.

- Plan de Seguridad Informática

Es la representación gráfica de un Sistema de Seguridad basada en los recursos Informáticos, se plasma en un documento donde se establece los principios organizativos y funcionales de la actividad de Seguridad Informática en una organización y recoge claramente las políticas de seguridad y las responsabilidades de cada uno de los participantes en el proceso informático, así como las medidas y procedimientos que permitan prevenir, detectar y responder a las amenazas que gravitan sobre el mismo.

Un Plan de Seguridad Informática es un documento en el que establecen las políticas, y acciones que permiten garantizar la prestación de servicios y asegurar la información contenida en un sistema computacional, considerando los lineamientos para promover la planeación, el diseño y la implementación de un modelo de seguridad en la organización, con el fin de establecer una cultura y conocimientos de la seguridad informática en la organización.

- Norma ISO/IEC 27002

La norma 27002 de la Organización Internacional para la Normalización (ISO) y la Comisión Electrotécnica Internacional (IEC) es un reglamento reconocido a escala internacional que establece buenas prácticas para la seguridad de la información.

También es considerada como un estándar para la seguridad de la información publicado por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional.

ISO/IEC 27002 es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. La seguridad de la Información se define en el estándar como: "la preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran).

- Norma Técnica Peruana NTP ISO/IEC 27001:2014

La Oficina Nacional de Gobierno Electrónico, señala que la norma técnica peruana es una adaptación de la ISO/IEC 27001. Esta fue planteada por la Presidencia del Consejo de ministros a través de la Oficina Nacional de Gobierno Electrónico, hoy en día Secretaría de Gobierno Digital (SeGDi), dispone el uso obligatorio de la Norma Técnica Peruana “NTP–ISO/IEC 27001:2014 EDI, Tecnología de la Información. Técnicas de seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos”

INDECOPI (2014). Señala que la Norma Técnica Peruana ha sido pensada y elaborada para facilitar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información (SGSI). Al mismo tiempo, la adopción de un SGSI es una decisión estratégica para una organización.

El establecimiento e implementación de un SGSI de la organización está directamente vinculada por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización

La NTP-ISO/IEC 27001:2014, presenta la siguiente estructura:

1. Introducción.
2. Objeto y campo de aplicación.
3. Referencias Normativas.
4. Términos y definiciones.
5. Contexto de la organización.
6. Liderazgo.
7. Planificación.
8. Soporte.
9. Operación.
10. Evaluación.
11. Mejora.
12. Lista de controles

- Políticas de Seguridad Informática

Benítez (2013) señala que las políticas de seguridad informática tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de las empresas.

1.3 Definición de términos básicos:

- Vulnerabilidades: Es la probabilidad que existen de que las amenazas existentes en el entorno de las Tecnologías de la Información, se materialice o ejecuten en dé contra un activo informático. Se señala que no todos los activos son vulnerables a la misma amenaza.

- Amenazas: Es la presencia de uno más factores de diversos indoles (Personas, maquinas o sucesos) que pueden tener la oportunidad de realizar un ataque a los sistemas o hardware de una organización, esto puede producir daños.

- Riesgo: Es la posibilidad que se materialice o no la amenaza aprovechando una vulnerabilidad. No constituye riesgo una amenaza cuando no hay vulnerabilidad ni una vulnerabilidad cuando no existe amenaza para la misma.

- Activos: son los elementos que pertenecen al propio sistema de información o que están relacionados con este. La presencia de los activos facilita el funcionamiento de la empresa y la consecución de sus objetivos.

- Políticas de Seguridad: es una lista o descripción donde se establecen las acciones o procedimientos a realizar frente a los riesgos de información, identifican los objetivos de seguridad aceptables y también los mecanismos para lograr estos objetivos.

- Efectividad: La información debe ser relevante y pertinente para los procesos del negocio y debe ser proporcionada en forma oportuna, correcta, consistente y utilizable.

- Eficiencia: Se debe proveer información mediante el empleo óptimo de los recursos (la forma más productiva y económica).

Capítulo II: Planteamiento del problema

2.1. Descripción del problema

La parte operativa y administrativa de toda organización pública esta obligatoriamente a un sometimiento directa o indirecto con la tecnología de la información, ya que gracias a ellos los procesos y el manejo de la información se han automatizado y sistematizado, generando muchos beneficios a los servicios que presta a los ciudadanos, pues en la actualidad sin el uso de las mismas no se puede realizar ningún proceso o mantener un negocio, incluso la informática ha traspasado límites al integrarse al Internet, pues los procesos se vuelven más dinámicos; sin embargo, por la falta de políticas de seguridad, los procedimientos de seguridad en muchas ocasiones no se toman en cuenta.

En el Perú, desde el año 2004 la Secretaría de Gobierno Digital, ha venido publicando normas relacionadas a la seguridad de la información a través de leyes y decretos una de las más importantes fueron las NTP ISO/IEC 17799:2004, NTP ISO/IEC 17799:2007, NTP ISO/IEC 27001:2008 y la NTP ISO/IEC 27001:2014 (que reemplaza a la NTP ISO/IEC 27001:2008), que mediante la implementación de un sistema de gestión de seguridad de la información ayudan a las entidades del estado a resguardar y proteger su información sensible y confidencial, en todas ellas se obliga actualmente las entidades públicas a diseñar e implementar un sistema de gestión de seguridad de la información (SGSI).

Por lo tanto, la Municipalidad Distrital de Punchana no está exceptúa a cumplir con dichas disposiciones, en la actualidad la mencionada entidad no cuenta con un plan de seguridad informática el cual le permita mitigar o disminuir el riesgo existente respecto a los recursos informáticos, los principales problemas existentes que vulneran la seguridad informática son: Constante modificación de la información de sus sistemas informáticos, la conectividad del internet es bastante deficiente, las redes inalámbricas no tiene adecuada seguridad de acceso, no tiene una adecuada infraestructura que brinde la seguridad perimetral de su red de comunicaciones, también existe un desconocimiento sobre la implementación de políticas de seguridad por parte del personal que labora en la unidad de tecnología de la información que esta entidad cuenta,

por esos y muchas razones más en esta investigación se pretende elaborar un documento que permita establecer la ruta y políticas que se debe cumplir para asegurar los activos o recursos informáticos de la Municipalidad Distrital de Punchana.

2.2. Formulación del problema

2.2.1. Problema general

- ✓ ¿Mediante la elaboración de un Plan se logrará mejorar la Seguridad Informática de la Municipalidad Distrital de Punchana?

2.2.2. Problemas específicos

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a las Políticas de Seguridad?

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Activos?

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Seguridad Ligada a los Recursos Humanos?

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Seguridad Física y del Entorno?

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Comunicaciones y Operaciones?

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto al Control de Accesos?

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Adquisición, desarrollo y mantenimiento de los sistemas informáticos?

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Incidentes de Seguridad de la Información?

- ✓ ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Conformidad de los Servicios Informáticos?

2.3. Objetivos.

2.3.1. Objetivo general:

- ✓ Evaluar el estado situacional de la seguridad informática y elaborar de un Plan para mejorar la seguridad informática de la Municipalidad Distrital de Punchana.

2.3.2. Objetivos específicos:

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a las Políticas de Seguridad.

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Activos.

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Seguridad Ligada a los Recursos Humanos.

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Seguridad Física y del Entorno.

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Comunicaciones y Operaciones.

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto al Control de Accesos.

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Adquisición, desarrollo y mantenimiento de los sistemas informáticos.

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Incidentes de Seguridad de la Información.

- ✓ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Conformidad de los Servicios Informáticos.

2.4. Hipótesis

- ✓ Hipótesis General: Mediante la elaboración de un Plan se logrará mejorar la seguridad informática de la Municipalidad Distrital de Punchana en el periodo 2021.

2.5. Variables

2.5.1. Identificación de las variables

- ✓ Variable: Elaboración de un Plan para mejorar la Seguridad Informática de la Municipalidad Distrital de Punchana en el periodo 2021.

2.5.2. Definición conceptual de la Variable

- ✓ Variable General: Elaboración de un plan de seguridad informática, se define como un documento que plasma las políticas y aspectos a cumplir para asegurar los activos informáticos de una entidad.

2.5.3. Operacionalización de la variable

Tabla N°01

Operacionalización de la Variable

Variable	Dimensiones	Indicadores	Instrumento de Recolección de Datos
Elaboración de un Plan de seguridad informática	Políticas de Seguridad	% de Respuestas del Cuestionario	• Ficha de Observación • Revisión documental • Encuesta
	Gestión de Activos		
	Seguridad Ligada a los Recursos Humanos		
	Seguridad Física y del Entorno		
	Gestión de Comunicaciones y Operaciones		
	Control de Accesos		
	Adquisición, desarrollo y mantenimiento de los sistemas informáticos		
	Gestión de Incidentes de Seguridad de la Información		
	Gestión de la Continuidad del Negocio		
	Conformidad de los Servicios Informáticos		

Fuente: Elaboración Propia

Capítulo III: Metodología

3.1. Tipo y diseño de investigación

Tipo de Investigación

- ✓ Descriptiva

Diseño de la Investigación

- El diseño de la investigación es de tipo no experimental: Descriptivo Simple

La representación gráfica es la siguiente:

M -> O

Dónde:
M: Muestra con quien(es) vamos a realizar el estudio.
O: Información (observaciones) relevante o de interés que recogemos de la muestra

3.2. Población y muestra

- Población:

Personal de la unidad de Tecnología de la Información de la Municipalidad Distrital de Punchana:

Tabla N°02
Distribución del Personal de la Unidad de Tecnología de la Información de la Municipalidad Distrital de Punchana

CANTIDAD	CARGO
01	Jefe de Unidad
02	Soporte Técnico
01	Administrador de Redes
01	Administrador de Base de Datos
Total	5 personas

Fuente: Recursos Humanos MDP

- Muestra:

  Para esta investigación se tomará toda la población por ser finita y ello consiste en considerar solo las 5 personas que trabajan en la Unidad de Tecnología de la Información de la Municipalidad Distrital de Punchana.

3.3. Técnicas, instrumentos y procedimientos de recolección de datos

3.3.1. Técnicas

Para la investigación se utilizó las siguientes técnicas para la recolección de datos:

- Análisis Documental
- Encuesta
- Observación Directa

3.3.2. Instrumentos:

- Cuestionario
- Ficha de Observación

3.3.3. Procedimientos de Recolección de Datos

Como procedimiento de recolección de datos se utilizó la encuesta con la escala de Likert, para elaborar cuadros por cada uno de los ítems a evaluar

3.4. Procesamiento y análisis de datos

Para el procesamiento, tabulación y análisis de los datos recopilados se utilizó la SPSS Versión 22.

Capítulo IV. Resultados

- Estadística Descriptiva de la Variable: Plan de seguridad informática

  Dimensión: Políticas de Seguridad

  - Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a las Políticas de Seguridad:

Tabla N°01

1.- ¿Se ha definido una política de seguridad de información en su entidad?

Pregunta01

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Si	1	20,0	20,0	80,0
	No	3	60,0	60,0	60,0
	No Sabe	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°02

2.- ¿De haberse definido una política de seguridad de la información, se están aplicando las políticas de seguridad de la información?

Pregunta02

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	3	60,0	60,0	60,0
	No	1	20,0	20,0	80,0
	No Sabe	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°03

3.- ¿Se hace de conocimiento al personal de la entidad las políticas de seguridad de la información?

Pregunta03

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°04

4.- ¿Existe normativa y procedimientos relativos a la seguridad de los Sistemas de Información?

Pregunta04

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	3	60,0	60,0	60,0
	No	2	40,0	40,0	100,0
	Total	5	100,0	100,0	

Tabla N°05

5.- ¿Se realizan evaluaciones y actualizaciones constantes, en caso las haya, de las políticas de seguridad de la información?

Pregunta05

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°06

6.- ¿Las políticas de seguridad de la información, si en caso las tuvieran, están basadas en algún estándar nacional o Internacional?

Pregunta06

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	2	40,0	40,0	80,0
	No Sabe	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°07

7.- ¿Existe un responsable de las políticas, normas y procedimiento?

Pregunta07

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

❖ **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana no cuenta con Políticas de Seguridad de la Información que permitan proteger la información de posibles peligros que vulneren la confidencialidad, integridad y disponibilidad de los datos de la entidad.

Dimensión: Gestión de Activos

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a la Gestión de Activos:

Tabla N°08

8.- ¿Existe un inventario actualizado de los activos informáticos de la entidad?

Pregunta08

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°09

9.- ¿El inventario contiene activos de datos, software, equipos y servicios?

Pregunta09

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°10

10.- ¿Realizan periódicamente la actualización de su inventario de los activos informáticos?

Pregunta10

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°11

11.- ¿Se dispone de una clasificación de los activos de información de acuerdo a la importancia de los mismos?

Pregunta11

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°12

12.- ¿Existen procedimientos para clasificar la información?

Pregunta12

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	1	20,0	20,0	40,0
	No Sabe	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

- **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana no cuenta con un inventario de los activos de la entidad, solo se tiene como simulación de inventario una lista tipeada en hoja de cálculo y en ella se puede encontrar la relación del hardware y software que tiene la entidad, el cual no se actualiza periódicamente lo cual no garantiza tomar medidas de protección eficaz de los recursos.

Dimensión: Seguridad Ligada a los Recursos Humanos

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a la Seguridad Ligada a los Recursos Humanos:

Tabla N°13

13.- ¿Se tienen definidas responsabilidades y roles de seguridad?

Pregunta13

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°14

14.- ¿Se tiene en cuenta la seguridad en la selección de personal?

Pregunta14

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°15

15.- ¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?

Pregunta15

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Tabla N°16

16.- ¿Reciben los usuarios capacitación actualizada en temas de seguridad de la información?

Pregunta16

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°17

17.- ¿Se identifican los usuarios para poder ingresar a la empresa?

Pregunta17

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°18

18.- ¿Existe algún procedimiento a seguir en caso de algún incidente de seguridad?

Pregunta18

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°19

19.- ¿Se recogen los datos de los incidentes de forma detallada?

Pregunta19

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°20

20.- ¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?

Pregunta20

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°21

21.- ¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?

Pregunta21

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

- **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana no cuenta con los procedimientos adecuados para el reclutamiento y selección del personal idóneo para la unidad de TI de la entidad, trayendo como consecuencia problemas en el manejo de la información respecto a la confidencialidad, integridad o disponibilidad de parte de los trabajadores de la municipalidad.

Dimensión: Seguridad Ligada a la Seguridad Física y del Entorno

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a la Seguridad Física y del Entorno:

Tabla N°22

22.- ¿Existe un perímetro de seguridad física?

Pregunta22

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Tabla N°23

23.- ¿Existe un adecuado control en el acceso físico en el área de informática?

Pregunta23

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°24

24.- ¿El área de informática tiene una oficina independiente de las demás áreas de la empresa?

Pregunta24

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	5	100,0	100,0	100,0

Tabla N°25

25.- ¿Se mantiene un registro de todas las personas que Ingresan y salen del área de informática o de la empresa?

Pregunta25

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°26

26.- ¿Se apagan los servidores en algún momento?

Pregunta26

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	1	20,0	20,0	40,0
	No Sabe	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°27

27.- ¿Las computadoras tienen deshabilitados los dispositivos externos, como la lectora de CD o USBs?

Pregunta27

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°28

28.- ¿La BIOS tiene habilitada una contraseña?

Pregunta28

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°29

29.- ¿Cuentan un plan de mantenimiento preventivo o correctivo tanto para hardware como software en los equipos informáticos?

Pregunta29

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°30

30.- ¿Existe un control sobre los dispositivos que se instalan en las computadoras?

Pregunta30

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°31

31.- ¿Existen protecciones frente a fallos en la alimentación eléctrica?

Pregunta31

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°32

32.- ¿Existen extintores ante posibles incendios?

Pregunta32

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°33

33.- ¿Se cuenta con un Sistema de aire acondicionado?

Pregunta33

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	2	40,0	40,0	40,0
	Si	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°34

34.- ¿Existen planos descriptivos de los puntos de red?

Pregunta34

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°35

35.- ¿Existe vigilancia en el departamento de cómputo las 24 horas?

Pregunta35

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Tabla N°36

36.- ¿Existen políticas de limpieza en el puesto de trabajo?

Pregunta36

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

- **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana la unidad de TI no cuenta con un ambiente adecuado que brinde la seguridad de acceso a personal no autorizado por no existir vigilancia las 24 horas, siendo esta un peligro eminente respecto a la protección de los datos e información que contienen los servidores que se encuentran en este ambiente.

Dimensión: Seguridad Ligada a la Gestión de Comunicaciones y Operaciones

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a la Gestión de Comunicaciones y Operaciones:

Tabla N°37

37.- ¿Cuentan con procedimientos y responsabilidades operativas y documentadas del uso y acceso a los sistemas informáticos?

Pregunta37

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°38

38.- ¿Existe un control para el acceso a Internet?

Pregunta38

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°39

39.- ¿Existen carpetas compartidas en las computadoras de la red?

Pregunta39

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	5	100,0	100,0	100,0

Tabla N°40

40.- ¿Se cuentan con licencias de antivirus para todos los equipos existentes?

Pregunta40

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	1	20,0	20,0	40,0
	No Sabe	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°41

41.- ¿Tienen procedimientos formales a seguir en caso de infección de virus?

Pregunta41

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°42

42.- ¿Se cuentan con licencias correspondientes del software instalado?

Pregunta42

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Tabla N°43

43.- ¿Se realizan copias de seguridad de los archivos, datos y programas de los sistemas de información?

Pregunta43

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°44

44.- ¿Tienen un control documentado de las direcciones IP de las máquinas de los usuarios y de los planos descriptivos de los puntos de la red informática?

Pregunta44

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

- **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana la unidad de TI no cuenta con la documentación adecuada sobre información de las redes de datos, no dispone de licencias tanto de los antivirus como los sistemas operativos, del mismo modo no cuenta con procedimientos para la realización de backup y la recuperación de los datos.

Dimensión: Seguridad Ligada al Control de Accesos

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación al Control de Accesos:

Tabla N°45

45.- ¿Se ha definido el nivel de acceso a los usuarios? ¿Es decir, a qué recursos tienen acceso y a qué recursos no?

Pregunta45

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°46

46.- ¿Los usuarios del sistema tienen asignado una fecha de expiración del password?

Pregunta46

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°47

47.- ¿Es bloqueado el sistema cuando un usuario digita mal la contraseña de ingreso al sistema?

Pregunta47

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	1	20,0	20,0	40,0
	No Sabe	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°48

48.- ¿Existe un procedimiento formal para efectuar las bajas de los empleados de los sistemas?

Pregunta48

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°49

49.- ¿Se tiene en cuenta alguna restricción horaria en el momento de permitir a un usuario el logueo al sistema?

Pregunta49

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°50

50.- ¿El sistema ejecuta alguna acción cuando el usuario permanece un largo periodo de tiempo sin actividad?

Pregunta50

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Tabla N°51

51.- ¿Los servidores permanecen logueados durante las 24 horas del día?

Pregunta51

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°52

52.- ¿Los passwords tienen una longitud mínima requerida por el sistema?

Pregunta52

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

❖ **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana la unidad de TI no cuenta con los procedimientos de seguridad adecuada para acceder a los equipos informáticos de las distintas áreas de la municipalidad, como la creación de usuarios y contraseñas que cumplan con requisitos de seguridad.

Dimensión: Seguridad Ligada a la Adquisición, desarrollo y mantenimiento de los sistemas informáticos

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a la Adquisición, desarrollo y mantenimiento de los sistemas informáticos:

Tabla N°53

53.- ¿Se cuenta con el total de licencias respectivas del sistema operativo de redes y de todas las computadoras, se mantienen actualizado el sistema operativo?

Pregunta53

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°54

54.- ¿Se realizan controles de acceso lógico a la base de datos y a los programas fuente de las aplicaciones que se utiliza en la red de la entidad?

Pregunta54

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No Sabe	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°55

55.- ¿La información tiene asignado un responsable conforme a su clasificación?

Pregunta55

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°56

56.- ¿Existe un adecuado modelamiento de la base de datos por parte del personal del área de sistemas?

Pregunta56

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Tabla N°57

57.- ¿Tienen estándares definidos, procedimientos a seguir y documentación respecto a la instalación y actualización de la Configuración de las computadoras?

Pregunta57

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0

	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Tabla N°58

58.- ¿Los usuarios tienen restricciones con respecto a la instalación de programas en sus respectivos puestos de trabajo?

Pregunta58

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°59

59.- ¿Conocen los usuarios de los sistemas, las funcionalidades al detalle del mismo?

Pregunta59

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	5	100,0	100,0	100,0

Tabla N°60

60.- ¿Existe un plan de desarrollo de sistemas formal durante el ciclo de vida del software?

Pregunta60

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°61

61.- ¿Existe una gestión de configuración o un control de versiones durante el desarrollo?

Pregunta61

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	1	20,0	20,0	40,0
	No Sabe	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°62

62.- ¿Existe documentación referente a los sistemas en operación, se actualiza?

Pregunta62

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°63

63.- ¿Tienen manuales de usuario de los sistemas en operación?

Pregunta63

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

- **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana, cuando adquiere equipos nuevos no los adquieren con licencias de software tanto del sistema operativo, ofimática y utilitarios, tampoco existe un control de versiones cuando se desarrolle algún aplicativo o se adquiera.

Dimensión: Seguridad Ligada a la Gestión de Incidentes de Seguridad de la Información

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a la Gestión de Incidentes de Seguridad de la Información

Tabla N°64

64.- ¿Tienen elaborado planes de contingencia o continuidad de las operaciones informáticas?

Pregunta64

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°65

65.- ¿Están implementadas los planes de continuidad de las operaciones informáticas?

Pregunta65

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°66

66.- ¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones informáticas?

Pregunta66

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

❖ **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana, no tiene elaborado planes de contingencia respecto a la recuperación de desastres en la información, tampoco existe planes que permitan mantener la continuidad de las operaciones en la entidad.

Dimensión: Seguridad Ligada a la Gestión de la Continuidad del Negocio

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a la Gestión de la Continuidad del Negocio

Tabla N°67

67.- ¿Existen procesos para la gestión de la continuidad?

Pregunta67

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°68

68.- ¿Existe un plan de continuidad del negocio y análisis de impacto?

Pregunta68

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	2	40,0	40,0	40,0
	No Sabe	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°69

69.- ¿Existe un diseño, redacción e implantación de planes de continuidad?

Pregunta69

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°70

70.- ¿Existe un marco de planificación para la continuidad del negocio?

Pregunta70

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

Tabla N°71

71.- ¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?

Pregunta71

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	4	80,0	80,0	100,0
	Total	5	100,0	100,0	

- **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana la unidad de TI no cuenta con planes que permitan la continuidad de los servicios que brinda a los pobladores del distrito.

Dimensión: Seguridad Ligada a la Conformidad de los Servicios Informáticos

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación a la Conformidad de los Servicios Informáticos

Tabla N°72

72.- ¿La empresa cuenta con normativa legal respecto a las aplicaciones que utiliza en la empresa y al uso del software licenciado?

Pregunta72

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	4	80,0	80,0	80,0
	Si	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

Tabla N°73

73.- ¿Existe un responsable definido en la estructura de la empresa encargado de mantener actualizada las normas emitidas por la Oficina Nacional de Gobierno Electrónico?

Pregunta73

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°74

74.- ¿Se tiene en cuenta el cumplimiento con la legislación?

Pregunta74

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	No	5	100,0	100,0	100,0

Tabla N°75

75.- ¿Existe una revisión de la política de seguridad y de la conformidad técnica?

Pregunta75

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	1	20,0	20,0	20,0
	No	1	20,0	20,0	40,0
	No Sabe	3	60,0	60,0	100,0
	Total	5	100,0	100,0	

Tabla N°76

76.- ¿Existen consideraciones sobre las auditorías de los sistemas?

Pregunta76

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Respuesta	Si	4	80,0	80,0	80,0
	No	1	20,0	20,0	100,0
	Total	5	100,0	100,0	

- **Resumen de los resultados**:

Según los resultados obtenidos de las respuestas del cuestionario representada en las tablas, en resumen, se pudo determinar que la Municipalidad Distrital de Punchana la unidad de TI no está íntimamente ligado con las normativas y directivas establecidas por la oficina nacional de gobierno electrónico, por lo tanto, no están dando cumplimiento a la legislación vigente respecto a la seguridad informática.

Capítulo V. Discusión, conclusiones y recomendaciones

5.1. Discusiones:

Nuestra tesis coincide con la de Carbajal, Felipe & Vega, Eduin & García Ramon donde realizan el Diseño de una plan de seguridad informática para el sistema de información del colegio gimnasio los Pinos, del mismo modo con la nuestra se analizó los posibles riesgos informáticos existentes en la entidad, y para la elaboración del plan de seguridad informática la Norma ISO 27002, teniendo como resultado una evaluación exhaustiva del riego informático existente en la entidad y como propuesta un plan de seguridad informática.

Nuestra tesis coincide con la de Merchán, Joao donde realiza el diseño de un Plan de Seguridad Informática para la Cooperativa de Ahorro Y Crédito “Por El Pan Y El Agua” De La Ciudad De Jipijapa”, en esta investigación se realiza una evaluación del estado situacional de la entidad respecto a la seguridad, determinando la necesidad de elaborar un plan de seguridad informática tomando en consideración la Norma ISO 27002,

Nuestra tesis coincide con la de Borja, Yolanda & Sánchez Fanny donde elevaron un Plan de Seguridad Informática de la ESPE Santo Domingo, para la evaluación del desarrollo de esta investigación se aplicó la metodología COBIT 5 con la finalidad de analizar los posibles riesgos informáticos existentes en la entidad, y para la elaboración del plan de seguridad informática la Norma ISO 27002 y 27003, teniendo como resultado una evaluación exhaustiva del riego informático existente en la entidad y como propuesta un plan de seguridad informática.

Nuestra tesis coincide con la de Sota, Luis donde relizan el Diseño Del Plan De Seguridad Informática Basado En La NTP ISO/IEC 27001:2014 Para La Municipalidad Del Centro Poblado De Salcedo - Puno”, del mismo modo en

nuestra tesis realizamos lo mismo con el fin de promover como política institucional para servir como referencia para la toma de decisiones sobre las tecnologías emergentes y sus amenazas, para el desarrollo de esta investigación primero se analizó los posibles riesgos informáticos existentes en la entidad, y para la elaboración del plan de seguridad informática la NTP-ISO/IEC 27001:2014

5.2. Conclusiones

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a las Políticas de Seguridad.

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Activos.

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Seguridad Ligada a los Recursos Humanos.

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Seguridad Física y del Entorno.

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Comunicaciones y Operaciones.

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto al Control de Accesos.

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Adquisición, desarrollo y mantenimiento de los sistemas informáticos.

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Incidentes de Seguridad de la Información.

- ✓ Se realizo la evaluación del estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Conformidad de los Servicios Informáticos.

5.3. Recomendaciones:

- ✓ La Oficina de Tecnologías de la Información de la Municipalidad distrital de Punchana debería solicitar la aprobación del Plan de Seguridad Informática de manera urgente puesto que su información se encuentra vulnerable a cualquier peligro.

- ✓ La oficina de Tecnologías de la Información de la Municipalidad distrital de Punchana debería solicitar un presupuesto de manera urgente para la implementación de este Plan de Seguridad Informática para su implementación.

- ✓ La Municipalidad Distrital de Punchana a través del órgano competente debe conformar un comité de vigilancia para realizar la verificación y controles periódicos de la implementación del plan de seguridad informática.

- ✓ Para los demás investigadores de este tipo de tesis, se debería elaborar una nueva metodología tomando como modelos las normas ISO/IEC de seguridad Informática.

Referencias Bibliográficas

- Tesis: Propuesta de un plan para mejorar la gestión de la seguridad informática en los centros desconcentrados de soporte de la Universidad Técnica Nacional Sede Pacifico
  Recuperado de:
  https://hdl.handle.net/10669/79269

- Guzmán, Goyo (2017) Tesis: "Metodología para la Seguridad de Tecnologías de la Información y Comunicaciones en la Clínica Ortega", recuperado de:
  http://repositorio.uncp.edu.pe/handle/UNCP/1478

- Gualppa, Luis (2019) Tesis: "Plan de Seguridad Informática Basada En La Norma ISO 27002 para el Control de Accesos Indebidos a la Red De Uniandes Puyo", recuperado de:
  http://dspace.uniandes.edu.ec/handle/123456789/6762

- Miranda Cairo, Michel, Valdés Puga, Osmany, Pérez Mallea, Iván, Portelles Cobas, Renier, & Sánchez Zequeira, Raúl. (2016). Methodology for the Implementation of Automated Management of Computer Security Controls. Revista Cubana de Ciencias Informáticas, 10(2), 14-26. Recuperado en 23 de marzo de 2022, de http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2227-18992016000200002&lng=es&tlng=en.

- Abalco, David & Ruilova, Romel (2015),Tesis Elaboración de un Plan de Seguridad Para el Fondo de Cesantia y Jubilación del MDMQ
  Recuperado en 23 de marzo de 2022, de
  https://bibdigital.epn.edu.ec/bitstream/15000/10391/1/CD-6182.pdf

- Molano, Rafael (2018) Tesis: Estrategias para implementar un sistema de gestión de la seguridad de la información basada en la norma ISO 27001 en el área de TI para la empresa Market Mix, recuperado de:
  https://repository.ucatolica.edu.co/bitstream/10983/15240

- Merino (2012, P.26): Tesis ""Tecnologías De Información Y Comunicación En La Gestión Municipal Del Distrito De Colcabamba, 2012" recuperado de:
  http://repositorio.unh.edu.pe/bitstream/handle/UNH/706/TP%20-%20UNH.%20%20SIST.%200004.pdf?sequence=1&isAllowed=y

- Pariaton (2018, P.28); Tesis "Nivel De Gestión Del Dominio Planificación Y Organización De Las Tecnologías De Información Y Comunicaciones (Tic) En La Municipalidad Provincial De Piura En El Año 2015. Recuperado de:
  http://repositorio.uladech.edu.pe/bitstream/handle/123456789/793/GESTION_%20TIC_PALACIOS%20_VILLALTA_YIMMY_%20ALI%20.pdf?sequence=1&isAllowed=y

- Gavino (2018); Tesis “Nivel De Gestión Del Dominio Planificación Y Organización De Las Tecnologías De Información Y Comunicaciones (Tic) En La Municipalidad Provincial De Piura En El Año 2015. Recuperado de: http://repositorio.unjfsc.edu.pe/bitstream/handle/UNJFSC/2924/raul-gavino.pdf?sequence=1&isAllowed=y

- Cano (2017), Plan de Seguridad Informática (2017, Pág. 03); Recuperado de: https://juliocanoramirez.files.wordpress.com/2017/02/plan_seguridad.pdf

Anexo 1. Matriz de consistencia

PROBLEMA	OBJETIVOS	HIPOTESIS	VARIABLES	DIMENSIÓN	INDICADORES	METODOLOGIA
Problema General ¿Mediante la elaboración de un Plan se logrará mejorar la Seguridad Informática de la Municipalidad Distrital de Punchana? **Problemas Específicos** ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a las Políticas de Seguridad? ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Activos? ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a	**General** Evaluar el estado situacional de la seguridad informática y elaborar de un Plan para mejorar la seguridad informática de la Municipalidad Distrital de Punchana **Específicos** ❑ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a las Políticas de Seguridad. ❑ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Activos. ❑ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma	**General**: Mediante la elaboración de un Plan se logrará mejorar la seguridad informática de la Municipalidad Distrital de Punchana en el periodo 2021.	Plan de seguridad informática	Políticas de Seguridad Gestión de Activos Seguridad Ligada a los Recursos Humanos Seguridad Física y del Entorno Gestión de Comunicaciones y Operaciones Control de Accesos Adquisición, desarrollo y mantenimiento de los	% de respuestas del cuestionario	Tipo de Investigación Descriptiva El diseño de la investigación es de tipo no experimental: Descriptiva Simple La representación gráfica es la siguiente: M - O Dónde: M: Muestra con quien(es) vamos a realizar el estudio. O: Información (observaciones) relevante o de interés que recogemos de la muestra Población y Muestra 5 trabajadores administrativos de la municipalidad distrital de Punchana Técnica de Recolección de Datos: La Encuesta Instrumento de Recolección de Datos: El Cuestionario Procedimiento de Recolección de Datos: Aplicación de cuestionario Procesamiento y Análisis de Datos La Información será procesada en software estadístico, cuyos resultados serán clasificados en cuadros y gráficos estadísticos.

la Seguridad Ligada a los Recursos Humanos? ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Seguridad Física y del Entorno? ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Comunicaciones y Operaciones? ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto al Control de Accesos? ¿Cuál es el estado situacional de la seguridad Informática en la	ISO/IEC 27002 respecto a la Seguridad Ligada a los Recursos Humanos. ❑ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Seguridad Física y del Entorno. ❑ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Comunicaciones y Operaciones. ❑ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto al Control de Accesos. ❑ Describir el estado situacional de la			sistemas informáticos		

Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Adquisición, desarrollo y mantenimiento de los sistemas informáticos? ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Incidentes de Seguridad de la Información? ¿Cuál es el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Conformidad de los Servicios Informáticos?	seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Adquisición, desarrollo y mantenimiento de los sistemas informáticos. ❑ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Gestión de Incidentes de Seguridad de la Información. ❑ Describir el estado situacional de la seguridad Informática en la Municipalidad Distrital de Punchana, tomando en consideración la Norma ISO/IEC 27002 respecto a la Conformidad de los Servicios Informáticos.					

Anexo 2. Instrumento de recolección de información

INSTRUMENTO DE RECOLECCIÓN DE DATOS

CUESTIONARIO PARA EVALUAR EL ESTADO SITUACIONAL DE LA SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD DISTRITAL DE PUNCHANA, TOMANDO EN CONSIDERACIÓN LA NORMA ISO/IEC 27002

Señor trabajador de la unidad de Tecnologías de la Información de la Municipalidad Distrital de Punchana, marque con un X en el recuadro que corresponda su respuesta:

Dimensión	N°	Pregunta	Si	No	Desconozco
Políticas de Seguridad	1	¿Se ha definido una política de seguridad de información en su entidad?			
	2	¿De haberse definido una política de seguridad de la información, se están aplicando las políticas de seguridad de la información?			
	3	¿Se hace de conocimiento al personal de la entidad las políticas de seguridad de la información?			
	4	¿Existe normativa y procedimientos relativos a la seguridad de los Sistemas de Información?			
	5	¿Se realizan evaluaciones y actualizaciones constantes, en caso las haya, de las políticas de seguridad de la información?			
	6	¿Las políticas de seguridad de la información, si en caso las tuvieran, están basadas en algún estándar nacional o Internacional?			
	7	¿Existe un responsable de las políticas, normas y procedimiento?			
Gestión de Activos	8	¿Existe un inventario actualizado de los activos informáticos de la entidad?			
	9	¿El inventario contiene activos de datos, software, equipos y servicios?			
	10	¿Realizan periódicamente la actualización de su inventario de los activos informáticos?			
	11	¿Se dispone de una clasificación de los activos de información de acuerdo a la importancia de los mismos?			
	12	¿Existen procedimientos para clasificar la información?			
Seguridad Ligada a los Recursos Humanos	13	¿Se tienen definidas responsabilidades y roles de seguridad?			
	14	¿Se tiene en cuenta la seguridad en la selección de personal?			
	15	¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?			
	16	¿Reciben los usuarios capacitación actualizada en temas de seguridad de la información?			
	17	¿Se identifican los usuarios para poder ingresar a la empresa?			
	18	¿Existe algún procedimiento a seguir en caso de algún incidente de seguridad?			
	19	¿Se recogen los datos de los incidentes de forma detallada?			
	20	¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?			

	21	¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?			
Seguridad Física y del Entorno	22	¿Existe un perímetro de seguridad física?			
	23	¿Existe un adecuado control en el acceso físico en el área de informática?			
	24	¿El área de informática tiene una oficina independiente de las demás áreas de la empresa?			
	25	¿Se mantiene un registro de todas las personas que Ingresan y salen del área de informática o de la empresa?			
	26	¿Se apagan los servidores en algún momento?			
	27	¿Las computadoras tienen deshabilitados los dispositivos externos, como la lectora de CD o USBs?			
	28	¿La BIOS tiene habilitada una contraseña?			
	29	¿Cuentan un plan? de mantenimiento preventivo o correctivo tanto para hardware como software en los equipos informáticos?			
	30	¿Existe un control sobre los dispositivos que se instalan en las computadoras?			
	31	¿Existen protecciones frente a fallos en la alimentación eléctrica?			
	32	¿Existen extintores ante posibles incendios?			
	33	¿Se cuenta con un Sistema de aire acondicionado?			
	34	¿Existen planos descriptivos de los puntos de red?			
	35	¿Existe vigilancia en el departamento de cómputo las 24 horas?			
	36	¿Existen políticas de limpieza en el puesto de trabajo?			
Gestión de Comunicaciones y Operaciones	37	¿Cuentan con procedimientos y responsabilidades operativas y documentadas del uso y acceso a los sistemas informáticos?			
	38	¿Existe un control para el acceso a Internet?			
	39	¿Existen carpetas compartidas en las computadoras de la red?			
	40	¿Se cuentan con licencias de antivirus para todos los equipos existentes?			
	41	¿Tienen procedimientos formales a seguir en caso de infección de virus?			
	42	¿Se cuentan con licencias correspondientes del software instalado?			
	43	¿Se realizan copias de seguridad de los archivos, datos y programas de los sistemas de información?			
	44	¿Tienen un control documentado de las direcciones IP de las máquinas de los usuarios y de los planos descriptivos de los puntos de la red informática?			
Control de Accesos	45	¿Se ha definido el nivel de acceso a los usuarios? ¿Es decir, a qué recursos tienen acceso y a qué recursos no?			
	46	¿Los usuarios del sistema tienen asignado una fecha de expiración del password?			
	47	¿Es bloqueado el sistema cuando un usuario digita mal la contraseña de ingreso al sistema?			

	48	¿Existe un procedimiento formal para efectuar las bajas de los empleados de los sistemas?			
	49	¿Se tiene en cuenta alguna restricción horaria en el momento de permitir a un usuario el logeo al sistema?			
	50	¿El sistema ejecuta alguna acción cuando el usuario permanece un largo periodo de tiempo sin actividad?			
	51	¿Los servidores permanecen logeados durante las 24 horas del día?			
	52	¿Los passwords tienen una longitud mínima requerida por el sistema?			
Adquisición, desarrollo y mantenimiento de los sistemas informáticos	53	¿Se cuenta con el total de licencias respectivas del sistema operativo de redes y de todas las computadoras, se mantienen actualizado el sistema operativo?			
	54	¿Se realizan controles de acceso lógico a la base de datos y a los programas fuente de las aplicaciones que se utiliza en la red de la entidad?			
	55	¿La información tiene asignado un responsable conforme a su clasificación?			
	56	¿Existe un adecuado modelamiento de la base de datos por parte del personal del área de sistemas?			
	57	¿Tienen estándares definidos, procedimientos a seguir y documentación respecto a la instalación y actualización de la Configuración de las computadoras?			
	58	¿Los usuarios tienen restricciones con respecto a la instalación de programas en sus respectivos puestos de trabajo?			
	59	¿Conocen los usuarios de los sistemas, las funcionalidades al detalle del mismo?			
	60	¿Existe un plan de desarrollo de sistemas formal durante el ciclo de vida del software?			
	61	¿Existe una gestión de configuración o un control de versiones durante el desarrollo?			
	62	¿Existe documentación referente a los sistemas en operación, se actualiza?			
	63	¿Tienen manuales de usuario de los sistemas en operación?			
Gestión de Incidentes de Seguridad de la Información	64	¿Tienen elaborado planes de contingencia o continuidad de las operaciones informáticas?			
	65	¿Están implementadas los planes de continuidad de las operaciones informáticas?			
	66	¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones informáticas?			
Gestión de la Continuidad del Negocio	67	¿Existen procesos para la gestión de la continuidad?			
	68	¿Existe un plan de continuidad del negocio y análisis de impacto?			
	69	¿Existe un diseño, redacción e implantación de planes de continuidad?			
	70	¿Existe un marco de planificación para la continuidad del negocio?			
	71	¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?			

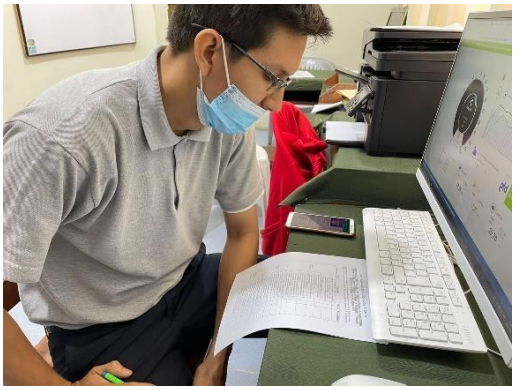
Conformidad de los Servicios Informáticos	72	¿La empresa cuenta con normativa legal respecto a las aplicaciones que utiliza en la empresa y al uso del software licenciado?			
	73	¿Existe un responsable definido en la estructura de la empresa encargado de mantener actualizada las normas emitidas por la Oficina Nacional de Gobierno Electrónico?			
	74	¿Se tiene en cuenta el cumplimiento con la legislación?			
	75	¿Existe una revisión de la política de seguridad y de la conformidad técnica?			
	76	¿Existen consideraciones sobre las auditorías de los sistemas?			

Muchas Gracias por sus respuestas

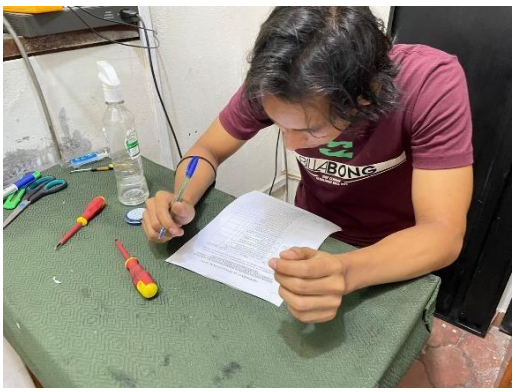
Anexo 3: De la Redacción

Fotografías del personal llenado la encuesta, instalaciones de la unidad de TI y otros.

Figura N°01



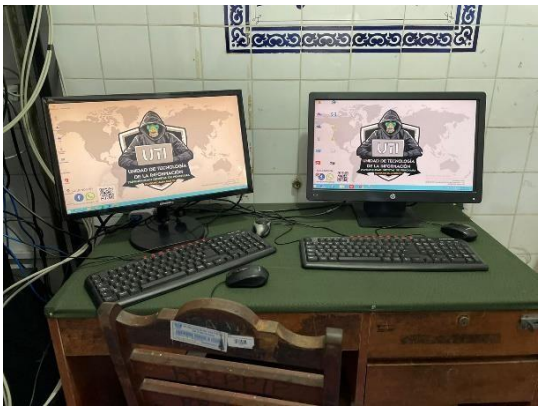
Personal de redes realizando la encuesta



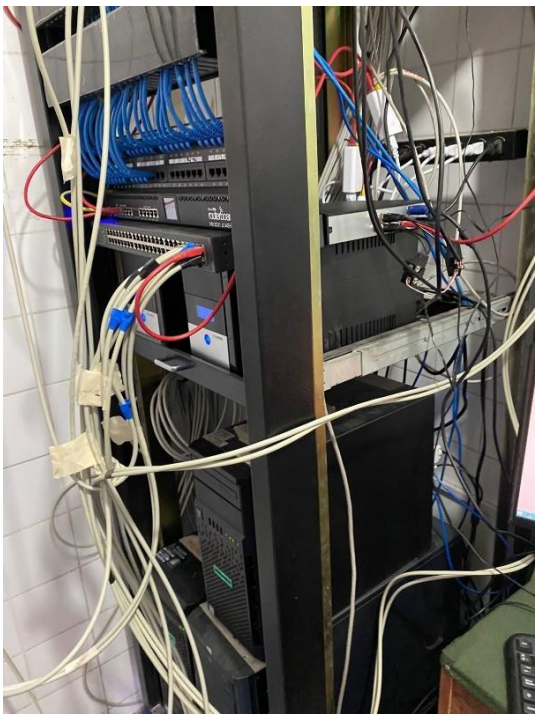
Personal de soporte realizando la encuesta

Figura N°02

Cableado estructurado del área de TI



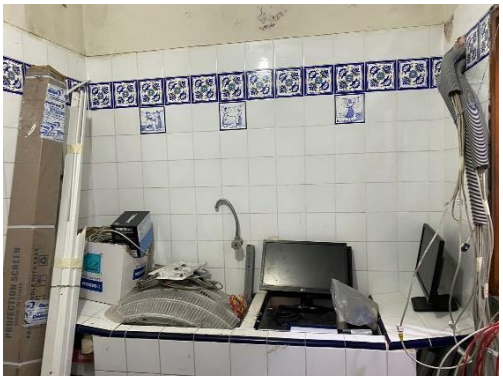
Servidores del área de TI



Servidor general del área de TI

Figura N°03

Área de reparación de máquinas e impresoras



Área de equipos averiados y por reparar

Centro de cómputo y área de TI

Figura N°04

Llenado de encuesta por el personal del área de TI

INSTRUMENTO DE RECOLECCIÓN DE DATOS

CUESTIONARIO PARA EVALUAR EL ESTADO SITUACIONAL DE LA SEGURIDAD INFORMÁTICA EN LA MUNICIPALIDAD DISTRITAL DE PUNCHANA, TOMANDO EN CONSIDERACIÓN LA NORMA ISO/IEC 27002

Señor trabajador de la unidad de Tecnologías de la Información de la Municipalidad Distrital de Punchana, marque con un X en el recuadro que corresponda su respuesta:

Dimensión	N°	Pregunta	Si	No	Desconozco
Políticas de Seguridad	1	¿Se ha definido una política de seguridad de información en su entidad?	X		
	2	¿De haberse definido una política de seguridad de la información, se están aplicando las políticas de seguridad de la información?	X		
	3	¿Se hace de conocimiento al personal de la entidad las políticas de seguridad de la información?	X		
	4	¿Existe normativa y procedimientos relativos a la seguridad de los Sistemas de Información?	X		
	5	¿Se realizan evaluaciones y actualizaciones constantes, en caso las haya, de las políticas de seguridad de la información?	X		
	6	¿Las políticas de seguridad de la información, si en caso las tuvieran, están basadas en algún estándar nacional o Internacional?	X		
	7	¿Existe un responsable de las políticas, normas y procedimiento?			X
Gestión de Activos	8	¿Existe un inventario actualizado de los activos informáticos de la entidad?	X		
	9	¿El inventario contiene activos de datos, software, equipos y servicios?	X		
	10	¿Realizan periódicamente la actualización de su inventario de los activos informáticos?	X		
	11	¿Se dispone de una clasificación de los activos de información de acuerdo a la importancia de los mismos?	X		
	12	¿Existen procedimientos para clasificar la información?	X		
Seguridad Ligada a los Recursos Humanos	13	¿Se tienen definidas responsabilidades y roles de seguridad?	X		
	14	¿Se tiene en cuenta la seguridad en la selección de personal?	X		
	15	¿Se plasman las condiciones de confidencialidad y responsabilidades en los contratos?	X		
	16	¿Reciben los usuarios capacitación actualizada en temas de seguridad de la información?			X
	17	¿Se identifican los usuarios para poder ingresar a la empresa?	X		
	18	¿Existe algún procedimiento a seguir en caso de algún incidente de seguridad?	X		

	19	¿Se recogen los datos de los incidentes de forma detallada?	X		
	20	¿Informan los usuarios de las vulnerabilidades observadas o sospechadas?	X		
	21	¿Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades?	X		
Seguridad Física y del Entorno	22	¿Existe un perímetro de seguridad física?			X
	23	¿Existe un adecuado control en el acceso físico en el área de informática?	X		
	24	¿El área de informática tiene una oficina independiente de las demás áreas de la empresa?	X		
	25	¿Se mantiene un registro de todas las personas que Ingresan y salen del área de informática o de la empresa?	X		
	26	¿Se apagan los servidores en algún momento?	X		
	27	¿Las computadoras tienen deshabilitados los dispositivos externos, como la lectora de CD o USBs?		X	
	28	¿La BIOS tiene habilitada una contraseña?	X		
	29	¿Cuentan un plan? de mantenimiento preventivo o correctivo tanto para hardware como software en los equipos informáticos?	X		
	30	¿Existe un control sobre los dispositivos que se instalan en las computadoras?			X
	31	¿Existen protecciones frente a fallos en la alimentación eléctrica?			X
	32	¿Existen extintores ante posibles incendios?			X
	33	¿Se cuenta con un Sistema de aire acondicionado?	X		
	34	¿Existen planos descriptivos de los puntos de red?			X
	35	¿Existe vigilancia en el departamento de cómputo las 24 horas?			X
	36	¿Existen políticas de limpieza en el puesto de trabajo?	X		
Gestión de Comunicaciones y Operaciones	37	¿Cuentan con procedimientos y responsabilidades operativas y documentadas del uso y acceso a los sistemas informáticos?			X
	38	¿Existe un control para el acceso a Internet?			X
	39	¿Existen carpetas compartidas en las computadoras de la red?	X		
	40	¿Se cuentan con licencias de antivirus para todos los equipos existentes?	X		
	41	¿Tienen procedimientos formales a seguir en caso de infección de virus?	X		
	42	¿Se cuentan con licencias correspondientes del software instalado?			X

	43	¿Se realizan copias de seguridad de los archivos, datos y programas de los sistemas de información?	X		
	44	¿Tienen un control documentado de las direcciones IP de las máquinas de los usuarios y de los planos descriptivos de los puntos de la red informática?	X		
Control de Accesos	45	¿Se ha definido el nivel de acceso a los usuarios? ¿Es decir, a qué recursos tienen acceso y a qué recursos no?	X		
	46	¿Los usuarios del sistema tienen asignado una fecha de expiración del password?		X	
	47	¿Es bloqueado el sistema cuando un usuario digita mal la contraseña de ingreso al sistema?		X	
	48	¿Existe un procedimiento formal para efectuar las bajas de los empleados de los sistemas?			X
	49	¿Se tiene en cuenta alguna restricción horaria en el momento de permitir a un usuario el logeo al sistema?			X
	50	¿El sistema ejecuta alguna acción cuando el usuario permanece un largo periodo de tiempo sin actividad?			X
	51	¿Los servidores permanecen logeados durante las 24 horas del día?			X
	52	¿Los passwords tienen una longitud mínima requerida por el sistema?			X
Adquisición, desarrollo y mantenimiento de los sistemas informáticos	53	¿Se cuenta con el total de licencias respectivas del sistema operativo de redes y de todas las computadoras, se mantienen actualizado el sistema operativo?			X
	54	¿Se realizan controles de acceso lógico a la base de datos y a los programas fuente de las aplicaciones que se utiliza en la red de la entidad?			X
	55	¿La información tiene asignado un responsable conforme a su clasificación?			X
	56	¿Existe un adecuado modelamiento de la base de datos por parte del personal del área de sistemas?	X		
	57	¿Tienen estándares definidos, procedimientos a seguir y documentación respecto a la instalación y actualización de la Configuración de las computadoras?			X
	58	¿Los usuarios tienen restricciones con respecto a la instalación de programas en sus respectivos puestos de trabajo?			X
	59	¿Conocen los usuarios de los sistemas, las funcionalidades al detalle del mismo?			X

	60	¿Existe un plan de desarrollo de sistemas formal durante el ciclo de vida del software?			X
	61	¿Existe una gestión de configuración o un control de versiones durante el desarrollo?	X		
	62	¿Existe documentación referente a los sistemas en operación, se actualiza?			X
	63	¿Tienen manuales de usuario de los sistemas en operación?	X		
Gestión de Incidentes de Seguridad de la Información	64	¿Tienen elaborado planes de contingencia o continuidad de las operaciones informáticas?			X
	65	¿Están implementadas los planes de continuidad de las operaciones informáticas?			X
	66	¿Realizan pruebas, mantenimiento y evaluación constante de los planes de continuidad de las operaciones informáticas?			X
Gestión de la Continuidad del Negocio	67	¿Existen procesos para la gestión de la continuidad?			X
	68	¿Existe un plan de continuidad del negocio y análisis de impacto?			X
	69	¿Existe un diseño, redacción e implantación de planes de continuidad?			X
	70	¿Existe un marco de planificación para la continuidad del negocio?			X
	71	¿Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio?			X
Conformidad de los Servicios Informáticos	72	¿La empresa cuenta con normativa legal respecto a las aplicaciones que utiliza en la empresa y al uso del software licenciado?			X
	73	¿Existe un responsable definido en la estructura de la empresa encargado de mantener actualizada las normas emitidas por la Oficina Nacional de Gobierno Electrónico?			X
	74	¿Se tiene en cuenta el cumplimiento con la legislación?			X
	75	¿Existe una revisión de la política de seguridad y de la conformidad técnica?			X
	76	¿Existen consideraciones sobre las auditorías de los sistemas?			X

Muchas Gracias por sus respuestas

Anexo 4: Plan de Seguridad Informática de la Municipalidad Distrital de Punchana

Etapa I - Gestión de Activos

1.1 Responsabilidad sobre los Activos

1.1.1 Inventario de activos

- Realizar el inventario del Hardware de la Municipalidad considerando los siguientes datos:
  - ✓ Nombre de Equipo
  - ✓ Marca
  - ✓ Modelo
  - ✓ IP Actual
  - ✓ Ubicación
  - ✓ Usuario Responsable
  - ✓ Código Patrimonial

- Realizar el Inventario del Software de la Municipalidad considerando los siguientes datos
  - ✓ Nombre del Software
  - ✓ Plataforma de desarrollo
  - ✓ Versión
  - ✓ Estado de desarrollo
  - ✓ Tipo de Base de datos

1.1.2 Propiedad de los activos

Establecer la existencia de la documentación correspondiente respecto a las responsabilidades de los propietarios (control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos) y la identificación de éstos. Así mismo se realiza una actualización periódica de los activos y sus propietarios cada seis meses.

1.1.3 Uso aceptable de los activos

Se identifica, documenta e implanta convenios con el personal interno y cláusulas en los contratos con terceros sobre el uso aceptable de los activos

1.1.4 Devolución de activos

Se verifica la existencia de una política formalizada de devolución de activos en la cual todos los empleados y usuarios de terceras partes devuelven los activos que estuvieron en su posesión / responsabilidad una vez finalizada el acuerdo, contrato de prestación de servicios o actividades relacionadas con su contrato de empleo en todas las áreas de la entidad.

1.2 Clasificación de la Información

1.2.1 Directrices de clasificación

Se debe utilizar un esquema de clasificación de la información en relación a su valor, requisitos legales, sensibilidad y criticidad para la institución; definiendo el conjunto adecuado de niveles de protección y la necesidad de medidas especiales para su tratamiento.

1.2.2 Etiquetado y manipulado de la información

Se debe establecer un conjunto apropiado de procedimientos para el etiquetado y tratamiento de la información, de acuerdo a un esquema de clasificación de los activos de información, definiendo el conjunto adecuado de niveles de protección.

1.2.3 Manipulación de Activos

Se recomienda establecer y revisar los procedimientos de manipulación de activos, acorde con el esquema de clasificación de activos adoptado por la organización, basado en la norma ISO/IEC 27002.

1.3 Manejo de los Soportes de Almacenamiento

1.3.1 Gestión de soportes extraíbles

Se recomienda el establecimiento de procedimientos formales para proteger los documentos, medios informáticos, datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas a nivel de la entidad y acorde con el esquema de clasificación de activos que se adopta en la institución.

1.3.2 Eliminación de soportes medios

Se recomienda llevar a cabo procedimientos formales para la eliminación segura y sin riesgo de los soportes de medios cuando ya no son requerido para así evitar la divulgación, modificación, retirada o destrucción de activos no autorizada.

1.3.3 Soportes físicos en tránsito

Se recomienda asegurar los soportes y la información en tránsito no solo físico sino electrónico (a través de las redes) y cifrar todos los datos sensibles o valiosos antes de ser transportados

Etapa II - Control de Accesos

2.1. Requisitos de negocio para el Control de Accesos

2.1.1. Política de control de accesos

Toda aplicación a utilizar debe contar con un usuario y una clave de acceso asignada al personal que labora en la Municipalidad.

Cada personal debe tener un determinado perfil para según eso darle acceso a solo funcionalidades que lo competen.

Está terminantemente prohibido hacer uso de usuarios que no le corresponde bajo la responsabilidad del que lo brinda.

Cerrar sesión una vez que este deje de trabajar en el los aplicativos de la municipalidad con la finalidad de que otros usuarios no usen su sesión.

2.1.2 Control de acceso a las redes y servicios asociados

El administrador de red es el encargado de brindar los privilegios correspondientes al personal y a los equipos que usaran tales como impresoras fotocopiadoras, etc.

Estadísticas de cortafuegos, tales como porcentaje de paquetes o sesiones salientes que han sido bloqueadas (por ejemplo: intentos de acceso a páginas web prohibidas; número de ataques potenciales de hacking repelidos, clasificados en insignificantes / preocupantes / críticos).

2.2. Gestión de Acceso de Usuario

2.2.1 Gestión de altas/bajas en el registro de usuarios

El administrador de los aplicativos asigna cada personal un usuario y una contraseña.

Cada personal una vez que este deja de laborar en la Municipalidad se le da de baja su usuario temporalmente por si este en algún momento puede regresar a laborar como también puede servir para una auditoria posterior.

El usuario se da de baja definitivamente si este fallece o ya no volverá a trabajar definitivamente en la municipalidad.

2.2.2 Gestión de los derechos de acceso asignados a usuarios

El personal tiene que autorizar para que el especialista ingrese a su pc remotamente para darle soporte.

Todo personal, dependiendo de su perfil profesional, puede ingresar remotamente a una PC para darle soporte esto.

Queda terminantemente prohibido copiar información o borrar la información de personal que accede a su pc remotamente.

2.2.3 Gestión de los derechos de acceso con privilegios especiales

Se revisa los derechos de acceso de los usuarios a intervalos de tiempo regulares (se recomienda cada seis meses) y después de cualquier cambio como promoción, degradación o término del empleo.

Los derechos de acceso de los usuarios son revisados y reasignados cuando se traslade desde un empleo a otro dentro de la misma organización.

Se revisa más frecuentemente (se recomienda cada tres meses) las autorizaciones de derechos de acceso con privilegios especiales.

Se comprueba las asignaciones de privilegios a intervalos de tiempo regulares para asegurar que no se han obtenido privilegios no autorizados.

Los cambios en las cuentas privilegiadas deben ser registradas para una revisión periódica.

2.2.4 Gestión de información confidencial de autenticación de usuarios

Mediante la autenticación se verifica si dicha persona es la que está accediendo a los aplicativos o a información que le compete sea la persona asignada.

2.2.5 Revisión de los derechos de acceso de los usuarios

Cada cierto periodo de tiempo un encargado del área de tecnología revisa si verdaderamente los usuarios tienen los permisos que se les asignó.

Se verifica cuando este es cambiado de cargo, área o cuando este tiene vacaciones o licencia.

2.2.6 Retirada o adaptación de los derechos de acceso

El administrador es el encargado de retirar los derechos de acceso para todos los empleados, contratistas o usuarios de terceros a la información y, a las instalaciones del procesamiento de información a la finalización del empleo, contrato o acuerdo, o ser revisados en caso de cambio

2.3 Responsabilidades del Usuario

La contraseña es de uso exclusivo del personal de la Municipalidad. Se recomienda establecer una regla en la cual cada cierto tiempo el personal cambie la contraseña y para la sesión una vez finalizado su trabajo para que este no sea utilizado por personal que no le pertenece.

2.3.1 Uso de información confidencial para la autenticación

Acceso solo a personal autorizado y, según el cargo que este tenga debe tener un determinado nivel de acceso a las aplicaciones.

2.4 Control de Acceso a Sistemas y Aplicaciones

Se controla los inicios de sesión mediante un algoritmo de encriptación de contraseñas, con este mecanismo de autenticación, ni el desarrollador sabe cuál es la contraseña del personal y así se controla el diseño de las pantallas de inicio de sesión.

2.4.1 Restricción del acceso a la información

Acceso solo a personal autorizado y, según el cargo que este tenga debe tener un determinado nivel de acceso a las aplicaciones.

2.4.2 Procedimientos seguros de inicio de sesión

Se controla los inicios de sesión mediante un algoritmo de encriptación de contraseñas, con este mecanismo de autenticación, ni el desarrollador sabe cuál es la contraseña del personal y así se controla el diseño de las pantallas de inicio de sesión.

2.4.3 Gestión de contraseñas de usuario

El personal que labora en la Municipalidad tiene la facilidad de cambiar su contraseña en el momento que lo desee.

Si en caso este fuera olvidada el administrador del aplicativo puede resetear y el usuario tendrá que ingresar una contraseña nueva.

Todo usuario debe tener una contraseña compuesta por letras números y caracteres especiales.

2.4.4 Uso de herramientas de administración de sistemas

Se debe usar una herramienta, el cual ayuda a la configuración de sistemas accesible vía web, con él se pueden configurar aspectos internos de muchos sistemas operativos, como usuarios, cuotas de espacio, servicios, archivos de configuración, apagado del equipo, etc.

2.4.5 Control de acceso al código fuente de los programas

Cada analista de sistemas, coordinador etc. tiene un usuario y contraseña al servidor de versiones el cual accede y puede guardar las versiones de las fuentes de los aplicativos

Etapa III - Cifrado

3.1 Controles Criptográficos

3.1.1 Política de uso de los controles criptográficos

Un enfoque de gestión del uso de las medidas criptográficas, incluyendo los principios generales en base a los cuales se debería proteger la información de la Municipalidad.

Basados en la evaluación de riesgos, el nivel requerido de protección debe ser identificado tomando en cuenta el tipo, fuerza y calidad del algoritmo cifrado requerido - El uso de cifrado para la protección de información sensible transportada en medios o dispositivos móviles o removibles y en las líneas de comunicación.

Un enfoque de gestión de claves, incluyendo métodos para tratar la recuperación de la información cifrada en caso de pérdida, divulgación o daño de las claves; Los roles y responsabilidades de cada cual que es responsable de la implementación de la política y la gestión de claves, incluyendo la generación de claves.

Los estándares a ser adoptados para una efectiva implementación a través de la institución (que solución es utilizada para cada proceso del negocio); - Las normas para utilizar información cifrada en controles que confíen en la inspección de contenido (como la detección de virus).

3.1.2 Gestión de claves

El sistema de gestión de claves se debería basar en un conjunto acordado de normas, procedimientos y métodos seguros para:

Generar claves para distintos sistemas criptográficos y distintas aplicaciones

Distribuir claves a los usuarios previstos, incluyendo la forma de activar y recibir las claves.

Almacenar claves, incluyendo la forma de obtención de acceso a las claves por los usuarios

Cambiar o actualizar claves, incluyendo reglas para saber cuándo y cómo debería hacerse en atención a la seguridad requerida y los avances en técnicas de descifrado.

Tratar las claves comprometidas (afectadas).

Revocar claves, incluyendo la forma de desactivarlas o retirarlas, por ejemplo, cuando tienen problemas o el usuario deja la organización (en cuyo caso las claves también se archivan)

Recuperar claves que se han perdido o corrompido como parte de la gestión de continuidad del negocio, por ejemplo, para recuperar la información cifrada.

Archivar claves, por ejemplo, para información archivada o de respaldo; destruir claves.

Etapa IV - Seguridad Física y Ambiental

4.1 Áreas Seguras

4.1.1 Perímetro de seguridad física

> "Los perímetros de seguridad (como paredes, tarjetas de control de entrada a puertas o un puesto manual de recepción) deberían utilizarse para proteger las áreas que contengan información y recursos para su procesamiento.
>
> Lista de chequeo para implementación de políticas"
>
> a) Verifique y documente de que material están constituidas las áreas de trabajo
> b) Documente si existe algún control de ingreso de personal
> c) Documente si existen escaleras de emergencia
> Si existe escalera de emergencia para cualquier sismo
> d) Documente si existen alarmas de seguridad

4.1.2 Controles físicos de entrada

> "Las áreas de seguridad deberían estar protegidas por controles de entrada adecuados que garanticen el acceso únicamente al personal autorizado."
>
> Lista de chequeo para implementación de políticas:
>
> a) Verificar si hay restricciones al área de caja
> b) Verificar si hay restricción centro de computo
> c) Cada visitante que se dirija a todas las áreas debe estar identificado
> d) Revisar los movimientos de ingreso y salida

4.1.3 Seguridad de oficinas, despachos y recursos

> "Se debería diseñar y aplicar un sistema de seguridad física a las oficinas, salas e instalaciones de la organización."
>
> Lista de chequeo para implementación de políticas:
>
> a) Existe políticas de seguridad
> b) Detallar claramente todos los lugares que se encuentran con restricciones de acceso

4.1.4 Protección contra las amenazas externas y ambientales

> "Se debería diseñar y aplicar una protección física contra desastres naturales, ataques maliciosos o accidentes."
>
> Lista de chequeo para implementación de políticas:
>
> a) Se cuenta con un sistema central de incendios
> b) Se han desarrollado simulacros de evacuación con el personal

4.1.5 El trabajo en áreas seguras

"Se deberían diseñar y aplicar procedimientos para el desarrollo de trabajos y actividades en áreas seguras."

Lista de chequeo para implementación de políticas:

a) Verifique si existen directorios públicos que especifican la ubicación de lugares restringidos.
b) Documente que existan cámaras y monitores constantes dentro de áreas seguras
c) Verifique si existe política de toma de foto y grabaciones

4.1.6 Áreas de acceso público, carga y descarga

"Se deberían controlar puntos de acceso a la organización como las áreas de entrega y carga/descarga (entre otros) para evitar el ingreso de personas no autorizadas a las dependencias aislando estos puntos, en la medida de lo posible, de las instalaciones de procesamiento de información."

Lista de chequeo para implementación de políticas:

Hacer un recorrido cada piso para ver si hay acceso para algo adicional, alguna puerta abierta donde esta alguna computadora apagada

4.2 Seguridad de los Equipos

4.2.1 Emplazamiento y protección de equipos

Revisar que todos los equipos de la institución se encuentran protegidos en sus respectivas áreas con una ventilación adecuada para evitar que se sobrecalienten y con seguridad del cableado para evitar que exista alguna ruptura.

4.2.2 Instalaciones de suministro

Verificar que La institución cuente con un generador de energía para mantener los servicios en línea el tiempo que dure el corte de fluido eléctrico que se puede originar en forma imprevista.

4.2.3 Seguridad del cableado

Para la protección del cableado de los equipos se han detectado las siguientes medidas:

a) Utiliza cableado empotrado para evitar daños en su estructura.
b) El cableado pasa por el techo de las instalaciones para las conexiones a computadores.
c) Evita interferencia entre los cables de comunicaciones y energía eléctrica.

4.2.4 Mantenimiento de los equipos

Para prevenir errores en los sistemas lógicos como físicos de las instalaciones el encargado de TI realiza un mantenimiento cíclico y preventivo (limpieza, revisión, ajustes) acorde al uso del equipo.

4.2.5 Salida de activos fuera de las dependencias de la empresa

a) Verificará el estado de los equipos tecnológicos a ser entregados a las áreas, a través de un Formulario de Activos (Equipos), aprobado por el jefe del área de Sistemas, para comprobar su salida y recepción en buen estado.
b) Se deberá otorgar a los activos que serán utilizados fuera de la institución no sea mayor de tres (3) días.
c) El usuario deberá reportar cualquier inconveniente que suceda con los activos que estén fuera de la institución educativa
d) Debe realizar un reporte dentro de las 24 horas que se haya sucedido algún inconveniente con el activo o reportando el estado del activo.

4.2.6 Seguridad de los equipos y activos fuera de las instalaciones

"Se debería aplicar seguridad a los equipos que se encuentran fuera de los locales de la organización considerando los diversos riesgos a los que están expuestos."

Lista de chequeo para implementación de políticas:

a) Indagar con el jefe de Sistemas de la institución educativa, ¿Para que indique si existen seguros de equipos al momento de trasladarlos de un lugar otro?
b) No existen seguros de traslados de equipos. Además, los equipos solo se trasladan cuando se quiere realizar algún servicio técnico.
c) Documentar las políticas y controles físicos para laptops.
d) Consultar si se realizan respaldos de la información de los discos de las computadoras portátiles.
e) Actualmente no se realizan respaldos de la información de los discos, se sugiere implantar una política para que el personal que utilice un computador portátil realice respaldos antes de emprender vacaciones.
f) Consultar si se realizan encriptación de los discos de las computadoras portátiles
g) No se realizan encriptación de los discos.

4.2.7 Reutilización o retirada segura de dispositivos de almacenamiento

Se deberían verificar todos los equipos que contengan medios de almacenamiento para garantizar que cualquier tipo de datos sensibles y software con licencia se hayan extraído o se hayan sobrescrito de manera segura antes de su eliminación o reutilización.

Si este dispositivo lo "extraemos directamente del PC" podríamos dañarlo, perder los datos contenidos en él y en caso extremo, dañar el puerto USB del equipo, por tanto, siempre antes de retirar una unidad externa conectada por USB a nuestro equipo debemos detenerla, utilizando para ello, por ejemplo, la "extracción segura de dispositivos de almacenamiento masivo USB".

Muchas veces los usuarios de las computadoras de la institución educativa no se toman el tiempo para poder realizar una reutilización o retirada segura de dispositivos

de almacenamiento simplemente retiran el dispositivo de la computadora, siendo esto una mala práctica.

4.2.8 Equipo informático de usuario desatendido

Verificar si existen políticas o procedimientos que detallan la protección de sus equipos en su ausencia (Protector de pantalla con clave, desconectarse de las aplicaciones, etc.)

4.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla

Se debería adoptar una política de puesto de trabajo despejado para documentación en papel y para medios de almacenamiento extraíbles y una política de monitores sin información para las instalaciones de procesamiento de información.

Etapa V - Seguridad en las Operaciones

5.1 Responsabilidades y Procedimientos de Operación

5.1.1 Documentación de procedimientos de operación

Se recomienda la documentación de los procedimientos operativos y dejar a disposición de todos los usuarios que los necesiten.

5.1.2 Gestión de cambios

Se recomienda el manejo de control de versiones en los manuales de procedimiento de operación.

5.1.3 Gestión de capacidades

Realizar un monitoreo y ajuste del uso de los recursos, como los servidores, junto a proyecciones necesarias de requisitos de capacidad en el futuro con el objetivo de garantizar el rendimiento adecuado en los sistemas.

5.1.4 Separación de entornos de desarrollo, prueba y producción

El área de TI que es la encargada y responsable de los sistemas que se usan en todo el consorcio y tiene bien marcado los sistemas que son de desarrollo, prueba y de producción el cual se tiene acceso según el perfil y módulos encargados.

Además, existe la documentación de los controles que se tiene para pases de producción

5.2 Protección contra Código Malicioso

5.2.1 Controles contra el código malicioso

La entidad debe contar con antivirus originales actualizados en las computadoras, VMware Workstation o para evitar la propagación de infección de virus mediante memoria o dispositivos externos.

5.3 Copias de Seguridad

5.3.1 Copias de seguridad de la información

Contar con un plan de respaldo de copias de seguridad de forma automática y de forma diaria todo esto perfectamente establecido mediante un plan ya desarrollado.

Dichas copias son almacenadas en un servidor de copias en diferentes puntos por si estos sufran algún accidente operacional o natural. Se aplican técnicas de cifrado a copias de seguridad y archivos.

5.4 Registro de Actividad y Supervisión

5.4.1 Registro y gestión de eventos de actividad

Se realiza periódicamente la producción, mantenimiento y revisión de estos registros de actividad

5.4.2 Protección de los registros de información

Se realiza la protección contra posibles alteraciones y accesos no autorizados a través de actividades de seguimiento de comportamiento irregular y el envío de alertas a los responsables de operación.

5.4.3 Registros de actividad del administrador y operador del sistema

Se realiza el registro de las actividades del administrador y del operador del sistema, tanto su hora de inicio de sesión como las acciones que realizan.

Además de la protección de estos registros, como se menciona en el apartado anterior, así como la revisión regular de éstos.

5.4.4 Sincronización de relojes

Todos los sistemas de procesamiento de información pertinentes en relación a una fuente de sincronización única de referencia.

5.5 Control del Software en Explotación

5.5.1 Instalación del software en sistemas en producción

Implementar procedimientos para controlar la instalación de software en sistemas operacionales mediante una herramienta que permite realizar la gestión de inventario, de cambio y distribución de paquetes de software con el fin de garantizar la integridad de los sistemas operacionales.

5.6 Gestión de la Vulnerabilidad Técnica

5.6.1 Gestión de las vulnerabilidades técnicas

Se realizan periódicamente pruebas de seguridad para vulnerabilidades técnicas y test de intrusión para detección de intrusos tanto en infraestructura, software y base de datos para evaluar el grado de exposición de la municipalidad y tomar las medidas necesarias para abordar los riesgos asociados.

Se clasifican los errores por niveles los cuales en un primer nivel es atendido por el personal Help Desk y si estos son más complejos pasan a un nivel 2 que son analizados por un personal de TI según sea el caso reportado

5.6.2 Restricciones en la instalación de software

Con el fin de evitar la explotación de vulnerabilidades técnicas en los sistemas se recomienda lo siguiente:

Implementar reglas que rijan la instalación de software por parte de personal autorizado y en atención a los términos y condiciones que surjan de la licencia de uso, además de procedimientos formales que garanticen su cumplimiento, y respetando la división de funciones.

Efectuar un análisis de riesgos previo a los cambios en atención al posible impacto por situaciones adversas.

Aplicar los cambios de manera escalonada empezando por los sistemas menos críticos y aplicar medidas de copias de seguridad y puntos de restauración.

Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

Informar a las áreas antes de la implementación de un cambio que pueda afectar sus operaciones y realizar pruebas de aceptación del nuevo estado para los usuarios finales.

Realizar actualización de versiones oportunamente para evitar quedar fuera de soporte por el fabricante.

5.7 Consideraciones de las Auditorías de los Sistemas de Información

5.7.1 Controles de auditoría de los sistemas de información

Con el fin de minimizar el impacto de actividades de auditoría en los sistemas operacionales se hacen las siguientes recomendaciones:

Acordar los requerimientos de auditoría con las áreas correspondientes.

Limitar las verificaciones hechas por los auditores, como permisos de “sólo lectura” en software y aislar y contrarrestar los efectos de modificaciones realizadas al finalizar la auditoría como la revocación de los privilegios otorgados.

Identificar claramente los recursos para llevar a cabo las verificaciones y puestos a disposición de los auditores

Etapa VI - Seguridad en las Telecomunicaciones

6.1 Gestión de la Seguridad en las Redes

6.1.1 Controles de Red

“Se debería mantener y controlar adecuadamente las redes para protegerlas de amenazas y mantener la seguridad en los sistemas y aplicaciones que utilizan las redes, incluyendo la información en tránsito.”

Se puede encontrar información adicional sobre seguridad de redes en ISO/IEC 18028, Tecnología de Información. Técnicas de seguridad. Seguridad de la red de tecnología de la información.

a) Existe una segregación de responsabilidad en el departamento de Sistemas

b) Indagar con el jefe de Sistemas y consultar que controles especiales se tiene para que los datos transmitidos a través de la LAN y WAN, estén protegidos su confidencialidad e integridad, por ejemplo, uso de criptografía

Para prevenir cualquier situación de riesgo, existen medidas de seguridad dentro de la red de la institución.

6.1.2 Mecanismos de seguridad asociados a servicios en red

Obtenga el contrato de Enlaces y extraiga las cláusulas que indiquen los compromisos acordados para gestionar de forma segura la red (Integridad, disponibilidad y confidencialidad).

No se pudo obtener el contrato debido a que son documentos que no están autorizados a entregar a cualquier persona.

6.1.3 Segregación de redes

"Se debería segregar los grupos de usuarios, servicios y sistemas de información en las redes"

6.2 Intercambio de Información con Partes Externas

6.2.1 Políticas y procedimientos de intercambio de información

"Deberían existir políticas, procedimientos y controles formales de transferencia para proteger la información que viaja a través del uso de todo tipo de instalaciones de comunicación."

Lista de chequeo para implantación de políticas:

a) Investigar en los manuales internos que políticas de seguridad especifican intercambio de información.
b) Intercambio de información electrónica.
c) En caso que se intercambie información sensitiva por correo electrónico, este también debe de estar encriptada.

6.2.2 Acuerdos de intercambio

Analice si existe una política que especifique que deberá existir un acuerdo de confidencialidad y buen uso de los recursos de procesamiento de la información, antes de otorgar acceso a un externo

6.2.3 Mensajería electrónica

Se debería proteger adecuadamente la información referida en la mensajería electrónica

6.2.4 Acuerdos de confidencialidad y secreto

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

Etapa VII - Adquisición, Desarrollo y Mantenimiento de los Sistemas de Información

7.1 Requisitos de Seguridad de los Sistemas de Información

7.1.1 Análisis y especificación de los requisitos de seguridad

"Los enunciados de requisitos de los requisitos de negocios para sistemas nuevos o mejoras a sistemas existentes deberían especificar los requisitos de control".

Lista de chequeo para implantación de políticas:

a) Detallar si existen políticas de la adquisición o desarrollo de software según las necesidades de la institución educativa
b) Documentar si existen políticas de pruebas antes de la adquisición o desarrollo de un software
c) Verificar que se cuente con estándares para el desarrollo de software
d) Documentar la existencia de los controles que deberán incluir para la seguridad de la información en los aplicativos de la institución.

Los controles que deberían incluir en todas las aplicaciones de la institución para la seguridad informática serían:

- ✓ Único inicio de sesión.
- ✓ Perfiles de usuario.
- ✓ Para acceso a las bases de datos serán a través de interfases aplicativas.
- ✓ El token o inicio de sesión.
- ✓ Identificación única de la sesión del usuario.

7.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas

Se debe implementar seguridad de las comunicaciones en servicios accesibles por redes públicas, puesto que todo se maneja localmente en la institución.

7.1.3 Protección de las transacciones por redes telemáticas

Se debe implementar protección de las transacciones por redes telemáticas, puesto que no existe un centro de datos propiamente en la institución.