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

PROPUESTA DE UN PLAN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE MAZÁN- 2021

PARA OBTAR EL TITÚLO PROFESIONAL DE

INGENIERO INFORMÁTICO Y DE SISTEMAS

AUTORES:

- **BACH. ALBERTO VEINTEMILLA QUINTEROS**
- **BACH. JHORDAN TORRES TANGOA**

ASESOR:

- **ING. CARLOS GONZALEZ ASPAJO**

SAN JUAN BAUTISTA – MAYNAS – LORETO- PERÚ – 2021

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N°673-2021-UCP-FCEI del 30 de setiembre 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 Lozano, Mgr. — Miembro
- Ing. Ángel Alberto Marthans Ruiz, Mgr. — Miembro

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

En la ciudad de Iquitos, siendo las 08:30 horas del día 08 de marzo del 2022, a través de la plataforma ZOOM supervisado en línea por el Secretario Académico del programa Académico de Ingeniería de Sistemas de Información 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: **"PROPUESTA DE UN PLAN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE MAZÁN- 2021"**

Presentado por los sustentantes: **ALBERTO VEINTEMILLA QUINTEROS**

Y

JHORDAN TORRES TANGOA

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

Luego de escuchar la sustentación y formuladas las preguntas las que fueron:
El Jurado después de la deliberación en privado llegó a la siguiente conclusión: **ABSUELTAS**

La sustentación es: **APROBADO POR UNANIMIDAD**

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

Presidente

Miembro

Miembro

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:

"PROPUESTA DE UN PLAN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD DISTRITAL DE MAZÁN- 2021"

De los alumnos: **ALBERTO VEINTEMILLA QUINTEROS Y JHORDAN TORRES TANGOA,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **16% de plagio**.

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

San Juan, 29 de Noviembre del 2021.

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

CJRA/ri-a
496-2021

Curiginal

Document Information

Analyzed document	UCP_SISTEMAS_2021_TESIS_JORDAN_TORRES_V1.pdf (D120353599)
Submitted	2021-11-29T16:30:00.0000000
Submitted by	Comisión Antiplagio
Submitter email	revision.antiplagio@ucp.edu.pe
Similarity	16%
Analysis address	revision.antiplagio.ucp@analysis.urkund.com

Sources included in the report

SA **Universidad Científica del Perú / UCP_INGENIERIAINFORMATICAYDESISTEMAS_2021_TESIS_MANUELSANCHEZ_V1.pdf**
Document UCP_INGENIERIAINFORMATICAYDESISTEMAS_2021_TESIS_MANUELSANCHEZ_V1.pdf (D109849960)
Submitted by: revision.antiplagio@ucp.edu.pe
Receiver: revision.antiplagio.ucp@analysis.urkund.com
12

W URL: https://hdl.handle.net/10669/79269
Fetched: 2021-11-29T16:34:00.0000000
2

DEDICATORIA

A Dios por cuidarme y guiarme en el trayecto de mi vida, a mi esposa Roció del Carmen, mis hijas Fátima Brunella y Zoe Khimberly; por su paciencia y apoyo incondicional; a mis padres Alberto y María Magdalena; por ser siempre el soporte que necesitaba, a mi hermano Ludger, por ser el ejemplo a seguir.

Bach. ALBERTO VEINTEMILLA QUINTEROS

DEDICATORIA

A Dios por iluminar mi camino, prestarme la vida y la salud, a mis padres por su apoyo incondicional en el proceso de formación profesional

Bach. JHORDAN TORRES TANGOA

AGRADECIMIENTO

Expresamos nuestro agradecimiento a todas las personas y profesionales que de una u otra manera impulsaron el inicio y la continuidad de nuestra formación profesional; de manera especial al Señor Coronel EP Don Raziel Eduardo Bamberger Vargas por la oportunidad y confianza dada, a nuestro asesor el Ing. Carlos González Aspajo por acompañarnos en este proceso de elaboración de nuestra tesis.

A la Universidad Científica del Perú, por ser nuestra alma mater.

- **BACH. ALBERTO VEINTEMILLA QUINTEROS**
- **BACH. JHORDAN TORRES TANGOA**

HOJA DE APROBACIÓN

INDICE DEL CONTENIDO

Páginas

INDICE DE TABLAS

Página

INDICE DE GRÁFICOS

Página

INDICE DE FIGURAS

Página

RESUMEN

La presente investigación cuyo título es “Propuesta De Un Plan Para Mejorar La Seguridad Informática De La Municipalidad Distrital De Mazán- 2021, se evaluó los niveles de seguridad informática que debe tener una entidad pública, esto con la finalidad de mantener continuo los servicios administrativos que se brinda a los ciudadanos o pobladores que pertenecen a este distrito, en esta investigación se aplicó la metodología de tipo descriptiva, llegando a la conclusión general que los activos informáticos con que cuenta la municipalidad presentan muchas debilidades y riesgos debido las grandes vulnerabilidades con que cuenta, esa problemática nos sirvió para elaborar el plan de seguridad Informática que tendrá que ser aprobado, publicado e implementado para asegurar la continuidad de los procesos donde se utiliza los sistemas informáticos y aplicaciones con que cuenta la Municipalidad distrital de Mazán.

Palabras Claves: Propuesta, Seguridad, Información.

ABSTRACT

The present investigation whose title is "Proposal of a Plan to Improve Computer Security of the District Municipality of Mazán-2021, was evaluated the levels of computer security that a public entity must have, this in order to maintain continuous administrative services that is provided to citizens or residents who belong to this district, in this research a descriptive methodology was applied, reaching the general conclusion that the computer assets available to the municipality present many weaknesses and risks due to the great vulnerabilities it has. This problem helped us to develop the IT security plan that will have to be approved, published and implemented to ensure the continuity of the processes where the IT systems and applications are used in the district Municipality of Mazán.

Keywords: Proposal, Security, Information.

Capítulo I: Marco teórico

1.1 Antecedentes del estudio

- ✓ **Hernández, Javier (2018)**, en su tesis para optar el grado académico magister en auditoria de tecnologías de la información, titulada: “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”, cuyo objetivo lograr mejoras significativas en la gestión de la seguridad informática en los centros desconcentrados de La Universidad Técnica Nacional, mediante la evaluación de la normativa Institucional, en el mencionado proyecto se identificó, evaluó y analizo los lineamientos y estándares aplicados, este proceso sirvió para emitir un informe del estado situacional de la seguridad informática que se encuentra la entidad, esto con la finalidad de proponer las reglas o directrices para mejorar la seguridad de la información.

- ✓ **Bonilla, Erika (2019)**, en su tesis para optar el título profesional de especialista en Auditoria de Sistemas, titulada: “Propuesta De Mejoramiento Continuo De La Seguridad Informática Y De La Información En Las Instituciones De Educación Superior”, cuyo objetivo general es desarrollar una propuesta para el mejoramiento continuo de seguridad informática y de la información en Instituciones de Educación Superior basado en COBIT, ITILv3 e ISO27001, teniendo como tareas fundamentales identificar los problemas de seguridad de la información en la entidad, así como evaluar los procesos del marco de seguridad de la información, gestión y gobierno de TI, que tienen un impacto en la operación del área de sistemas de la entidad.

- ✓ **Romero, Kevin (2018)**, en su tesis para optar el título profesional de Ingeniero de Telecomunicaciones, titulada: “Propuesta De Seguridad Informática Para Mejorar El Proceso De Acceso Remoto En Una Entidad Financiera”, cuyo objetivo general el presente estudio está asociado a las condiciones en la que se llevan a cabo actualmente las comunicaciones remotas entre esta entidad y sus empleados. En consecuencia, se evaluó la situación actual de su proceso de VPN (Virtual Private Network) o acceso remoto pasando por las políticas,

procedimientos y controles de seguridad en el ámbito informático, donde se identificaron las amenazas hacia este proceso y se determinó que al ser este un proceso de alto riesgo, en caso sea vulnerado, se podría perder grandes cantidades de dinero, además de la potencial pérdida de confianza de sus clientes en el caso de la fuga de información sensible.

- ✓ **Guzmán, Roberto (2015)**, en su tesis para optar el grado académico de magister en ingeniería de sistemas de la Universidad Nacional del centro del Perú, titulada "Metodología para la seguridad de tecnologías de la información y comunicaciones de la clínica Ortega", cuyo objetivo general es medir la importancia que tienen las metodologías de seguridad informática que asegure la continuidad de los servicios que ofrece la clínica que dependen directamente de la tecnología, en la tesis se llegó a la conclusión que para definir y aplicar un modelo de seguridad de TI primero se debe hacer una evaluación del riesgo para detectar las vulnerabilidades y amenazas, luego de esta evaluación y aplicación de la metodología se debe realizar controles periódicos para ir mejorando de manera continua los niveles de seguridad en el área y que uno de los estándares que es más fácil de aplicar es el ISO 19002.

- ✓ **Gavino, Segundo (2018)** En su tesis titulada Auditoria en Seguridad Informática y gestión de riesgo en el hospital regional de huacho, para optar el título profesional de Ingeniero Informático en la Universidad Nacional José Faustino Sánchez Carrión, cuyo objetivo general es evaluar la seguridad informática y su relación con la gestión del riesgo en el hospital regional de huacho, llega a la conclusión que existe una relación positiva entre la seguridad lógica, la seguridad de aplicaciones y la administración de los del centro de procesamiento por lo tanto la implementación de la seguridad en todos los niveles es favorable para la protección de los recursos informáticos.

1.2 Bases teóricas

- Plan de Seguridad Informática:

Para Cano (2017, Pág. 3), es la imagen de un Sistema de Seguridad Informática que se diseña y se plasma en un documento donde se plantea los principios funcionales y organizativos de las actividades a desarrollar respecto a la Seguridad de los recursos informáticos en una organización, por lo tanto y menciona de manera clara y concisa las políticas, responsabilidades, medidas y procedimientos para prevenir, detectar y disminuir las vulnerabilidades y las amenazas que tiene una organización respecto a la seguridad que amerita la información.

Para Merlos (2018, Pág. 18), Un plan de seguridad informática, hace referencia al proceso informático que permite plantear la forma de proteger la infraestructura informática, proporcionando a los lectores, la capacidad de identificar, disminuir y eliminar las amenazas y vulnerabilidades que puede trasgredir o distorsionar la información de una organización, por lo tanto esto permite garantizar la privacidad propiamente de la información y sus derivados, así mismo como la continuidad de los servicios que utilizan esta en la organización.

EcuRed (s.f.): Afirma que en un Plan de Seguridad Informática constituye un documento que sirve para realizar el control y la seguridad en la utilización de la información, donde las medidas que se establecen son de obligatorio cumplimiento para todo el personal que haga uso de las tecnologías informáticas instaladas en la institución.

- Gestión de Información:

Evaluando Software (s.f.) La Gestión de la información es la definición de un conjunto de procesos que se utiliza para designar actividades orientadas a la generación, coordinación, almacenamiento, conservación, búsqueda y recuperación de la información tanto interna como externa contenida en cualquier soporte.

Para (Palmieri y Rivas, 2007, citada por Sánchez, 2006, p. 18), hace referencia a los procesos que se realizan para ingresar, clasificar, preservar, recuperar, compartir y difundir la información que genera, recibe y/o adquiere una organización”

Para García (2010), Es un proceso por el cual se obtienen, despliegan o utilizan recursos básicos para manejar información dentro y para la sociedad a la que sirve”. La misma autora lo vincula con diferentes dimensiones: el entorno, los procesos, las personas, la tecnología, la infraestructura, y los productos y servicios.

1.3 Definición de términos básicos:

- 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 (Aguilera,2010).

- Vulnerabilidades: Es la probabilidad que existen de que las amenazas existentes en el entorno de las TI, se materialice o ejecuten en dé contra un activo. No todos los activos son vulnerables a la misma amenaza. (Aguilera,2010).

- 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. (Aguilera,2010).

- 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. (Aguilera,2010).

- 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 (Laudon,2012).

Capítulo II: Planteamiento del problema

2.1. Descripción del problema

La municipalidad distrital de Mazán, tiene 78 años de fundación e institucionalización, mediante el Decreto Ley Nº 98155, y desde ahí en la municipalidad han pasado por varias gestiones de alcaldes que implementaron modernización tanto administrativa como tecnológica, se ha implementado sistemas informáticos proporcionados por el estado el cual procesa y analiza la gestión de la información tanto económica, administrativa y ciudadana, actualmente la municipalidad distrital ubicada en la ciudad de Mazán, tiene muchas deficiencias a nivel de las tecnológicas de la información y comunicaciones debido a la baja inversión de presupuesto que se designa a la sub gerencia de tecnologías de la información de la municipalidad y al desconocimiento de sus autoridades para la inversión en equipamiento informático, también a la implementación de políticas que permitan asegurar el funcionamiento continuo de los procesos administrativos dentro de las áreas administrativas, este problema persiste a pesar que existe leyes y normativa que obliga a las entidades públicas en especial a las municipales a establecer y presentar dichas políticas ante el ente correspondiente que es la Oficina Nacional de Gobierno Electrónico que pertenece a la presidencia del consejo de ministros, este problema pone en riesgo el manejo de información de la entidad la cual se procesa, almacena y utiliza en todos los procesos administrativos de la municipalidad, es por ello que la Oficina de Tecnología de la Información de la Municipalidad como parte de su trabajo debería proponer e implementar los componentes necesarios para asegurar el manejo de la información cumpliendo los estándares mínimos o normativas establecidas por las entidades del gobiernos encargadas de aprobar y evaluar las medidas a implementar, es por la razón de ser de esta investigación.

2.2. Formulación del problema

2.2.1. Problema general

- ✓ ¿Mediante la elaboración de un Plan se mejorará la Seguridad Informática de la Municipalidad distrital de Mazán - 2021?

2.2.2. Problemas específicos

- ✓ ¿Cuál es el nivel de seguridad lógica informática de la Municipalidad distrital de Mazán?
- ✓ ¿Cuál es el nivel de seguridad de Software de la Municipalidad Distrital de Mazán?
- ✓ ¿Cuál es el nivel de seguridad del Hardware de la Municipalidad Distrital de Mazán?
- ✓ ¿Cuál es el nivel de seguridad del data center de la Municipalidad Distrital de Mazán?

2.3. Objetivos.

2.3.1. Objetivo general:

- ✓ Elaborar de un Plan para mejorar la seguridad informática de la Municipalidad distrital de Mazán 2021.

2.3.2. Objetivos específicos:

- ✓ Evaluar el nivel de Seguridad Lógica Informática existente en la Municipalidad distrital de Mazán.
- ✓ Evaluar el nivel de Seguridad del Software existente en la Municipalidad distrital de Mazán.
- ✓ Evaluar el nivel de seguridad del Hardware existente en la Municipalidad Provincial de Mazán.
- ✓ Evaluar el nivel de seguridad del data center de la Municipalidad distrital de Mazán

2.4. Hipótesis

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

2.5.2. Definición conceptual de la Variable

- ✓ Variable: Elaboración de un plan de seguridad informática es un documento que describe las actividades y procesos a realizar con la finalidad de salvaguardar el equipamiento informático y la información de una entidad pública o privada.

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	Nivel de Seguridad Lógica Informática	Identificación de Usuarios	• Ficha de Observación • Revisión documental • Matriz de Riesgo • Encuesta
		Acceso Mediante Contraseñas	
		Perfiles de Usuarios	
	Nivel de seguridad del Software.	Confiabilidad del Software	
		Seguridad de la Base de datos	
		Control de Instalación de Aplicaciones	
	Nivel de seguridad del hardware	Control de Mantenimiento	
		Seguridad de la red	
	Nivel de Seguridad del Data Center	Backup	
		Accesibilidad	

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 administrativo de la Municipalidad Distrital de Mazán:

Tabla N°02
Distribución del Personal administrativo de la Municipalidad Distrital de Mazán

CANTIDAD	CARGO
03	Gerentes
05	Secretarias
02	Trabajador de la oficina de rentas
03	Trabajadores de la oficina de Registro Civil
Total	13 personas

Fuente: Recursos Humanos MDM

- Muestra:

  Para la investigación se tomará toda la población que consiste en 13 personas que trabajan en la Municipalidad distrital de Mazán.

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: Nivel de Seguridad Lógica

  - Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación al riesgo que existe en el nivel de seguridad lógica:

  Pregunta 01.- ¿En la Municipalidad distrital de Mazán para acceder a un equipo de cómputo los usuarios se identifican?

Tabla N°03

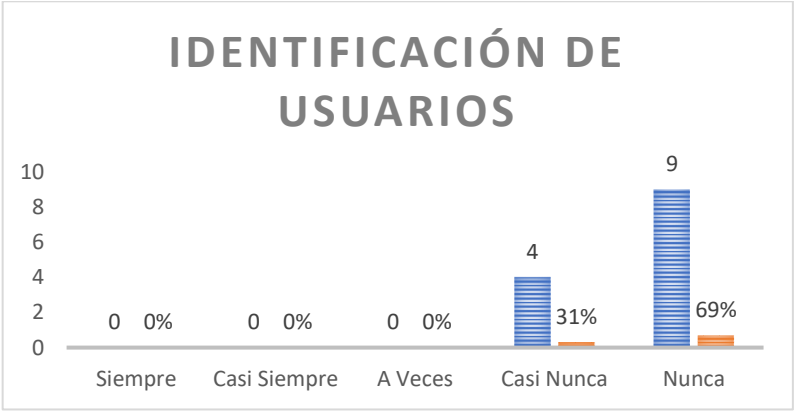
Identificación de Usuarios

Identificación de Usuarios	ni	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
A Veces	0	0%
Casi Nunca	4	31%
Nunca	9	69%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°01

Identificación de Usuarios



Fuente: Elaboración Propia

Interpretación:

De la tabla 03 y gráfico 01, se puede verificar que de 13 Trabajadores de la Municipalidad distrital de Mazán, el 31% señalo que los que tienen a su cargo una computadora casi nunca se identifican, el 69% señalo que nunca se identifican.

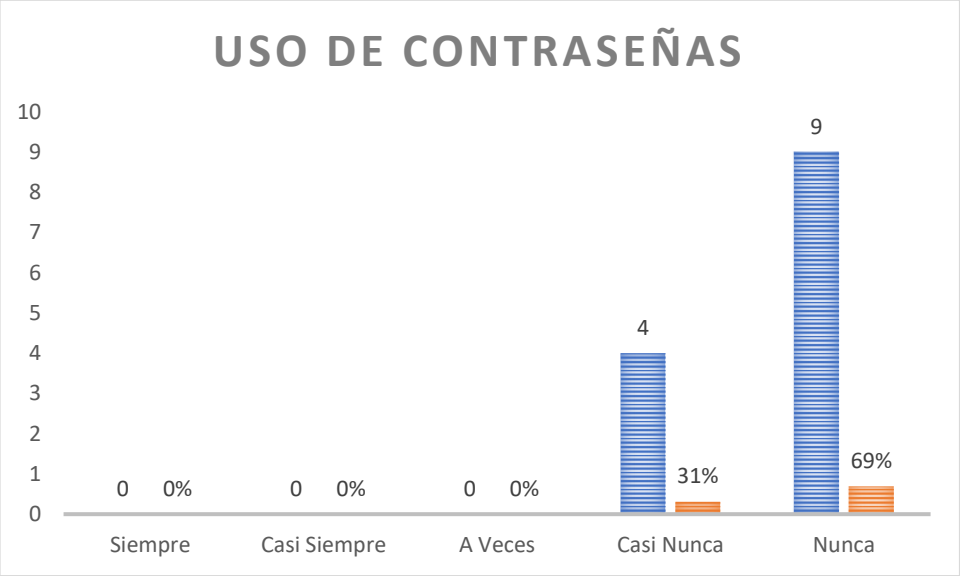
Pregunta 02.- ¿En la Municipalidad distrital de Mazán para acceder a un equipo de cómputo los usuarios hacen uso de una contraseña?

Tabla N°04
Uso de Contraseñas

Uso de Contraseñas	ni	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
A Veces	0	0%
Casi Nunca	4	31%
Nunca	9	69%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°02
Uso de Contraseñas



Fuente: Elaboración Propia

Interpretación:

De la tabla 04 y gráfico 02, se evidencia que de una muestra 13 trabajadores, el 31% señalo que los usuarios que tienen a su cargo una computadora casi nunca usan una contraseña para acceder, el 69% señalo que nunca usan una contraseña para acceder al equipo de cómputo.

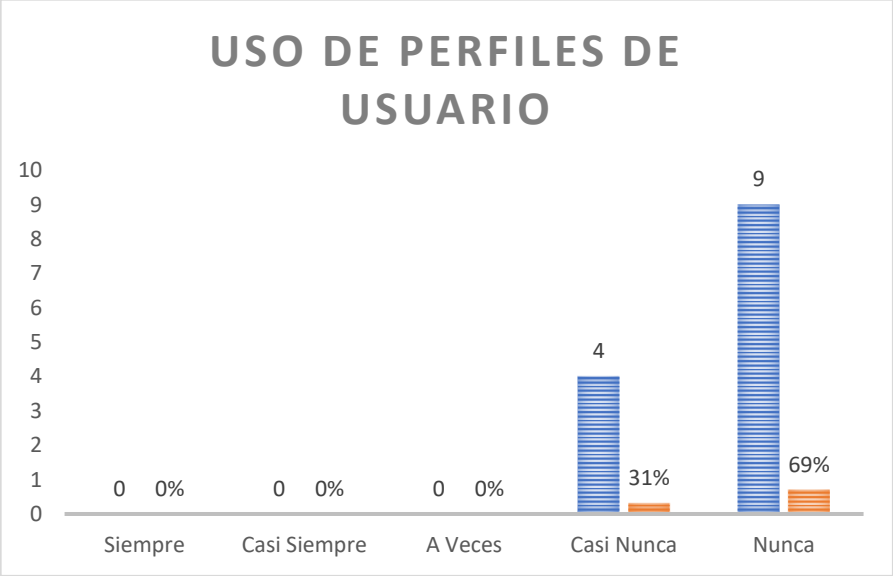
Pregunta 03.- ¿En la Municipalidad distrital de Mazán se ha creado perfiles de usuario para acceder a un equipo de cómputo?

Tabla N°05
Perfiles de Usuarios

Uso de Contraseñas	ni	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
A Veces	0	0%
Casi Nunca	4	31%
Nunca	9	69%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°03
Perfiles de Usuario



Fuente: Elaboración Propia

Interpretación:

De la tabla 05 y gráfico 03, se evidencia que de una muestra 13 Trabajadores, el 31% señalo que los usuarios que tienen a su cargo una computadora casi nunca tienen perfiles de Usuarios, el 69% señalo que nunca tienen perfiles de usuarios para acceder al equipo de cómputo.

Dimensión: Nivel de Seguridad del Software

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación al riesgo que existe en el nivel de seguridad del Software:

  Pregunta 04.- ¿Los sistemas informáticos y aplicaciones con que cuenta la Municipalidad distrital de Mazán son confiables y seguros?

Tabla N°06

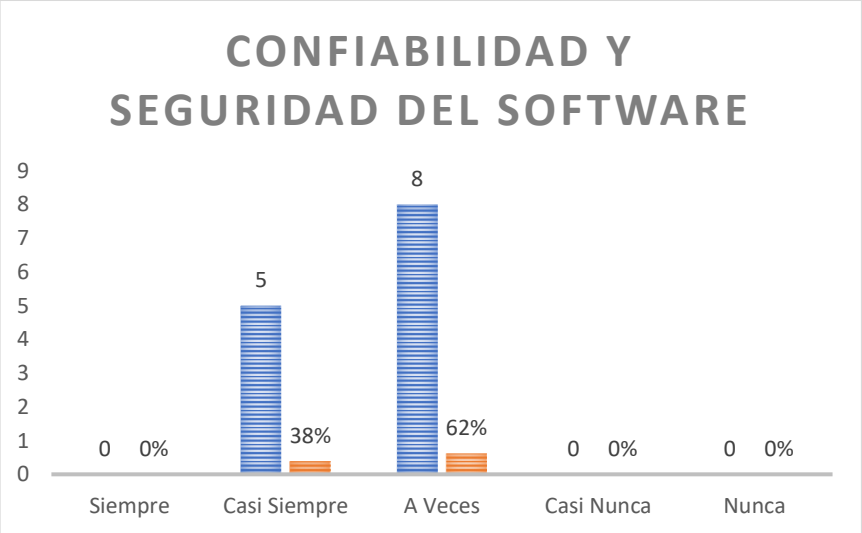
Confiabilidad y Seguridad del Software

Seguridad del Software	ni	Porcentaje
Siempre	0	0%
Casi Siempre	5	38%
A Veces	8	62%
Casi Nunca	0	0%
Nunca	0	0%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°04

Confiabilidad y Seguridad del Software



Fuente: Elaboración Propia

Interpretación:

De la tabla 06 y gráfico 04, se evidencia que de una muestra 13 Trabajadores, el 38% señalo que los usuarios que tienen a su cargo una computadora casi siempre cuentan con sistemas informáticos seguros y confiables, el 62% señalo que a veces cuentan con sistemas informáticos seguros y confiables.

Pregunta 05.- ¿Las bases de datos con que cuentan los sistemas informáticos y aplicaciones con que cuenta la Municipalidad Distrital de Mazán son seguras?

Tabla N°07

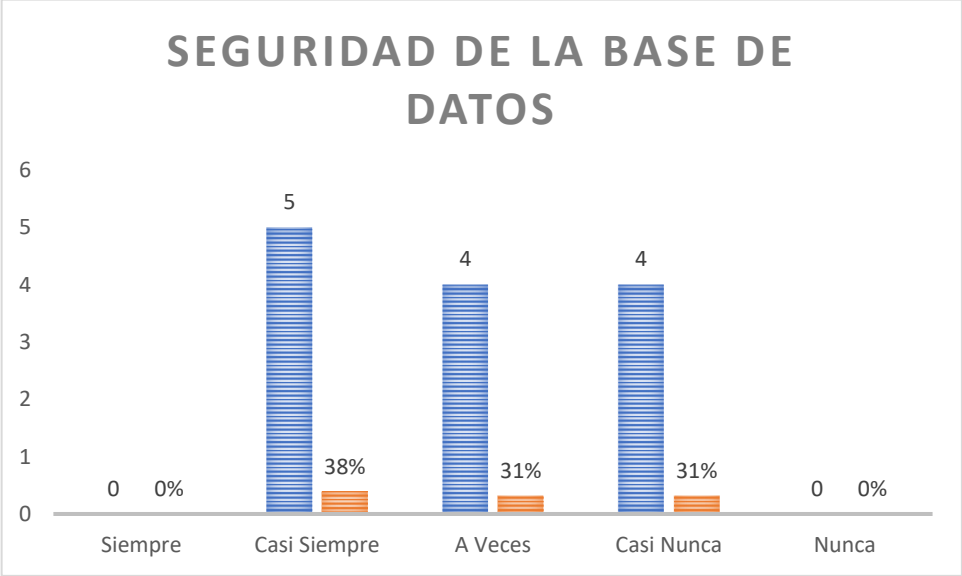
Seguridad de Base de Datos

Seguridad de la Base de Datos	ni	Porcentaje
Siempre	0	0%
Casi Siempre	5	38%
A Veces	4	31%
Casi Nunca	4	31%
Nunca	0	0%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°05

Seguridad de la Base de Datos



Fuente: Elaboración Propia

Interpretación:

De la tabla 07 y gráfico 05, se evidencia que de una muestra 13 Trabajadores, el 38% señalo que la base de datos con que cuenta los sistemas y aplicaciones informáticas son casi siempre seguras, el 31% señalo que a veces son seguras y otro 31% casi nunca son seguras.

Pregunta 06.- ¿Se realiza el control de los sistemas informáticos y aplicaciones instaladas en los equipos de cómputo con que cuenta la Municipalidad Distrital de Mazán?

Tabla N°08

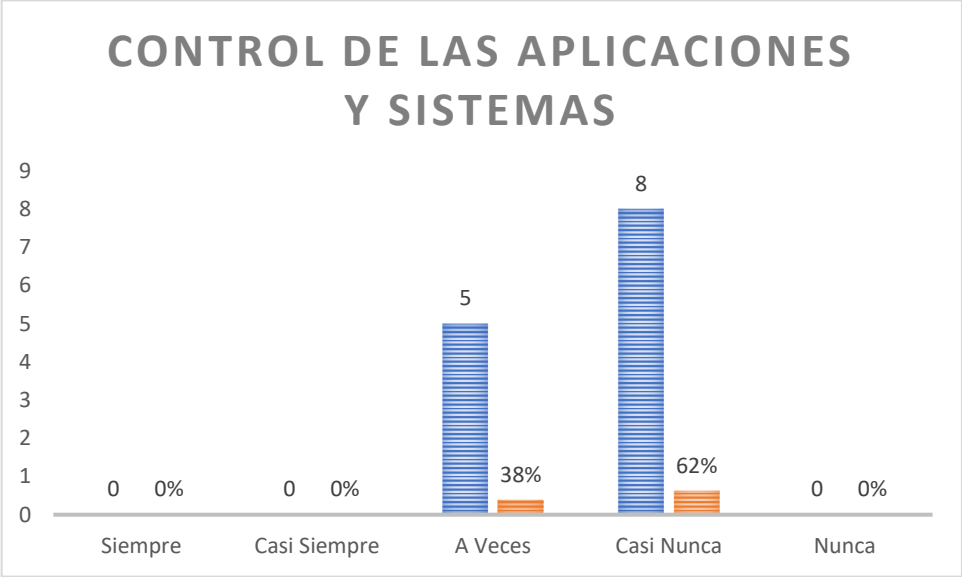
Control de las aplicaciones y sistemas

Control de las aplicaciones y sistemas	ni	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
A Veces	5	38%
Casi Nunca	8	62%
Nunca	0	0%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°06

Control de las aplicaciones y sistemas



Fuente: Elaboración Propia

Interpretación:

De la tabla 08 y gráfico 06, se evidencia que de una muestra 13 Trabajadores, el 38% señalo que a veces se tiene un control de las aplicaciones y sistemas informáticos y el 62% señalo que casi nunca se realiza control de las aplicaciones y sistemas informáticos.

Dimensión: Nivel de Seguridad del Hardware

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación al riesgo que existe en el nivel de seguridad del Hardware:

  Pregunta 07.- ¿Se realiza periódicamente el mantenimiento a los equipos de cómputo con que cuenta la Municipalidad distrital de Mazán?

Tabla N°09

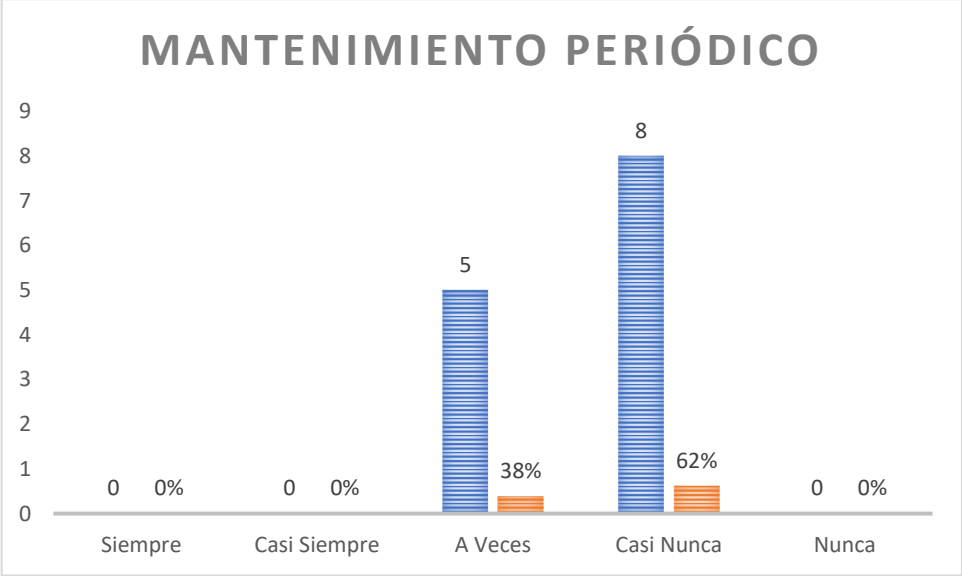
Mantenimiento Periódico

Mantenimiento Periódico	ni	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
A Veces	5	38%
Casi Nunca	8	62%
Nunca	0	0%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°07

Mantenimiento Periódico



Fuente: Elaboración Propia

Interpretación:

De la tabla 09 y gráfico 07, se evidencia que de una muestra 13 Trabajadores, el 38% señalo que a veces se realiza el mantenimiento de los equipos de cómputo con que cuenta la Municipalidad Provincial de Mazan, el 62% señalo que casi nunca se realiza el mantenimiento.

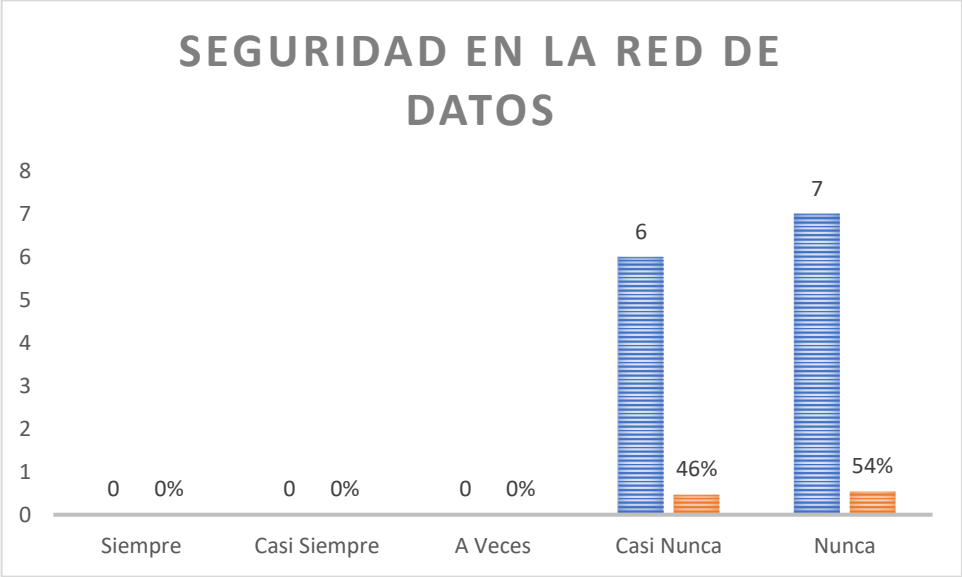
Pregunta 08.- ¿La red de datos de datos de la Municipalidad distrital de Mazán está protegido contra ataques de red?

Tabla N°10
Seguridad en la Red

Seguridad en la Red de Datos	ni	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
A Veces	0	0%
Casi Nunca	6	46%
Nunca	7	54%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°08
Seguridad en la Red



Fuente: Elaboración Propia

Interpretación:

De la tabla 10 y gráfico 08, se evidencia que de una muestra 13 Trabajadores, el 46% señalo que casi nunca está protegido contra ataques de red y el 54% señalo que nunca están protegidos contra ataques de red.

Dimensión: Nivel de Seguridad del Data Center

- Distribución de las frecuencias y porcentajes según nivel de respuestas del cuestionario en relación al riesgo que existe en el nivel de seguridad del data center:

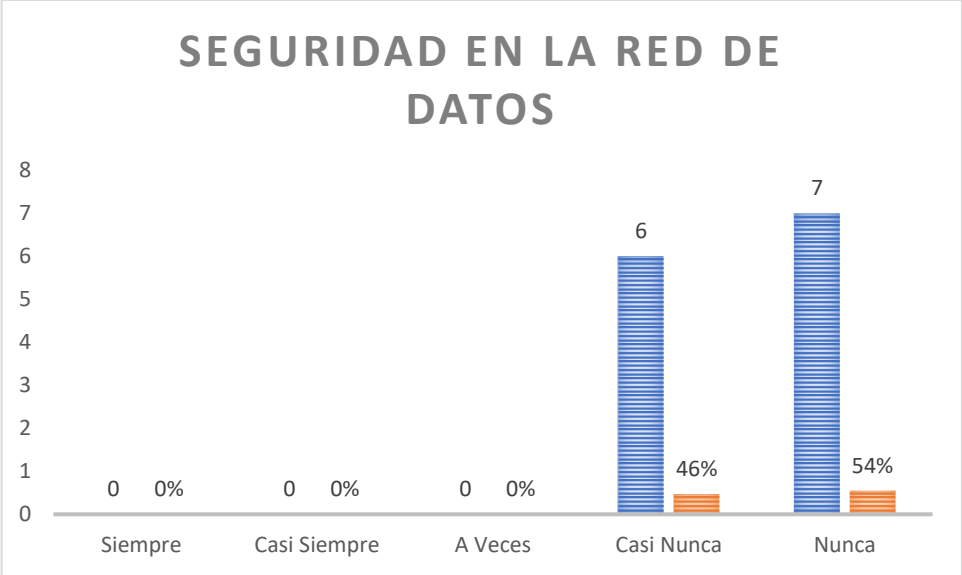
  Pregunta 09.- ¿Se hacen Backup periódicamente los datos de los servidores del data center?

Tabla N°11
Seguridad en la Red

Seguridad en la Red de Datos	ni	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
A Veces	0	0%
Casi Nunca	6	46%
Nunca	7	54%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°09
Seguridad en la Red



Fuente: Elaboración Propia

Interpretación:

De la tabla 11 y gráfico 09, se evidencia que de una muestra 13 Trabajadores, el 46% señalo que casi nunca se hace backup de los datos de los servidores del data center y el 54% señalo que nunca se hacen backup de los datos.

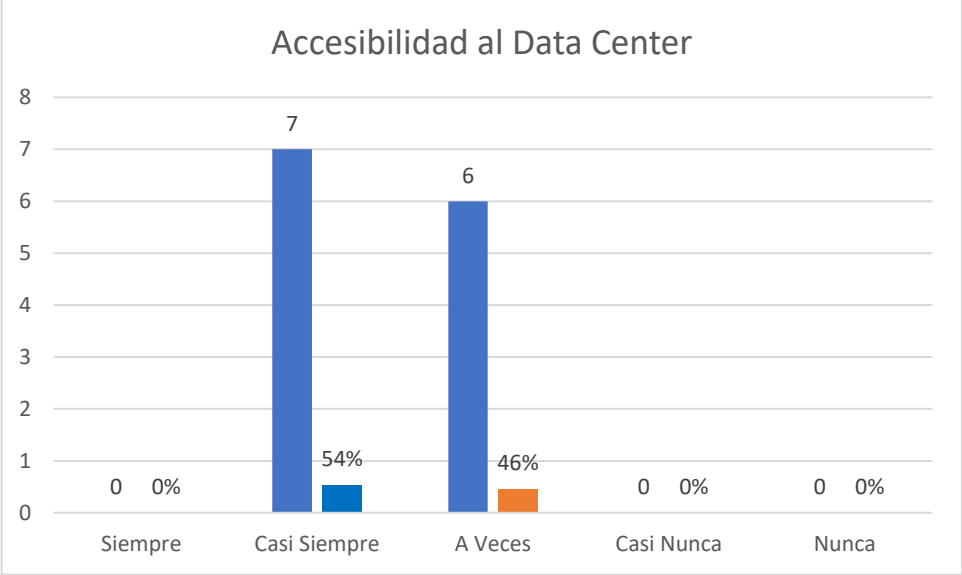
Pregunta 10.- ¿Cualquier personal de la Municipalidad distrital de Mazán puede acceder de manera fácil al ambiente donde se encuentra el data Center?

Tabla N°12
Accesibilidad al Data center

Accesibilidad al Data Center	ni	Porcentaje
Siempre	0	0%
Casi Siempre	7	54%
A Veces	6	46%
Casi Nunca	0	0%
Nunca	0	0%
Total	13	100%

Fuente: Elaboración Propia

Gráfico N°10
Accesibilidad del Data Center



Fuente: Elaboración Propia

Interpretación:

De la tabla 12 y gráfico 10, se evidencia que de una muestra 13 Trabajadores, el 54% señalo que casi siempre cualquier trabajador de la Municipalidad Distrital de Mazan puede acceder al ambiente donde se encuentra el Data Center y el 46% señalo que a veces el personal de la municipalidad puede acceder al ambiente del data center.

Capítulo V. Discusión, conclusiones y recomendaciones

5.1. Discusiones:

- Del mismo modo que Hernández, Javier (2018), en su tesis titulada: “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”, también con nuestra propuesta se logrará mejoras significativas en la gestión de la seguridad informática ya que se aplicara normativa Institucional, identificando y evaluando los lineamientos y estándares, también se podrá emitir un informe del estado situacional de la seguridad informática que se encuentra la entidad, esto con la finalidad de proponer las reglas o directrices para mejorar la seguridad de la información.

- Del mismo modo que Bonilla, Erika (2019), en su tesis titulada: “Propuesta De Mejoramiento Continuo De La Seguridad Informática Y De La Información En Las Instituciones De Educación Superior”, también en nuestro proyecto se desarrolló una propuesta para el mejoramiento continuo de seguridad informática y de la información de la Municipalidad distrital de Mazán basado en la Norma Técnica Peruana ISO/IEC 27001:2014, teniendo como tareas fundamentales identificar los problemas de seguridad de la información en la entidad, así como evaluar los procesos del marco de seguridad de la información, gestión y gobierno de TI, que tienen un impacto en la operación del área de sistemas de la entidad.

- Del mismo modo que Romero, Kevin (2018), en su tesis titulada: “Propuesta De Seguridad Informática Para Mejorar El Proceso De Acceso Remoto En Una Entidad Financiera”, se evaluó, la situación actual de su proceso del acceso remoto proponiendo políticas, procedimientos y controles de seguridad en el ámbito informático, para identificaron las amenazas hacia este proceso y se determinó que al ser este un proceso de alto riesgo, en caso sea vulnerado.

5.2. Conclusiones

- ✓ Se evaluó el nivel de seguridad lógica, donde se determinó que existe un riesgo muy alto de sufrir un daño en los archivos de los equipos de cómputo de la Municipalidad Distrital de Mazán, ya que la seguridad de los accesos y contraseñas no están implementadas como medida de seguridad informática.

- ✓ Se evaluó el nivel de seguridad del software, donde se pudo determinar que existe riesgo muy alto debido a que los sistemas y la base de datos de la Municipalidad Distrital de Mazán, no son muy seguros debido a que no se tienen los controles necesarios para su instalación y funcionamiento.

- ✓ Se evaluó el nivel de seguridad del hardware, donde se determinó que existe un riesgo muy ato debido a que no se realiza los mantenimientos de los equipos de cómputo de la Municipalidad Distrital de Mazán de manera periódica, existiendo el peligro de que se produzcan fallas durante la prestación de los servicios que se dan de manera continua.

- ✓ Se evaluó el Nivel de seguridad del Data center, donde se determinó que existe un riesgo muy alto debido a que cualquier usuario o trabajador común puede acceder a los ambientes donde se encuentra el data center en la Municipalidad distrital de Mazán, y que el ambiente no es el adecuado, también determinó que no se hacen los Backup de la información de los sistemas y base de datos de los servidores que se encuentran en el data center.

5.3. Recomendaciones:

- ✓ Los funcionarios de la Municipalidad Distrital de Mazán deben buscar hacer mas inversión en temas de seguridad informática para de esta manera poder custodiar el activo mas preciado de la organización que es la información

- ✓ La sub gerencia de tecnologías de la información de la Municipalidad distrital de Mazán debe contar con personal capacitado y profesional en informática,

- ✓ Aprobar e implementar el plan de seguridad informática propuesto en esta investigación.

- ✓ Se debe capacitar constantemente al personal del área de informática en la implementación del plan de seguridad informática propuesto en esta investigación.

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

- 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 mejorará la Seguridad Informática de la Municipalidad distrital de Mazán - 2021? **Problemas Específicos** ¿Cuál es el nivel de seguridad lógica informática de la Municipalidad distrital de Mazán? ¿Cuál es el nivel de seguridad de Software de la Municipalidad Distrital de Mazán? ¿Cuál es el nivel de seguridad del Hardware de la Municipalidad Distrital de Mazán? ¿Cuál es el nivel de seguridad del data center de la Municipalidad Distrital de Mazán?	**General** Elaborar de un Plan para mejorar la seguridad informática de la Municipalidad distrital de Mazán 2021 **Específicos** Evaluar el nivel de Seguridad Lógica Informática existente en la Municipalidad distrital de Mazán. Evaluar el nivel de Seguridad del Software existente en la Municipalidad distrital de Mazán. Evaluar el nivel de seguridad del Hardware existente en la Municipalidad Provincial de Mazán. Evaluar el nivel de seguridad del data center de la Municipalidad distrital de Mazán	**General**: Mediante la elaboración de un Plan se logrará mejorar la seguridad informática de la Municipalidad distrital de Mazan en el periodo 2021.	Elaboración de un Plan para mejorar la Seguridad Informática de la Municipalidad distrital de Mazán en el periodo 2021.	Nivel de Seguridad Lógica Informática	Identificación de Usuarios Acceso Mediante Contraseñas Perfiles de Usuarios	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 13 trabajadores administrativos de la municipalidad distrital de Mazán 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.
				Nivel de seguridad del Software.	Confiabilidad del Software Seguridad de la Base de datos Control de Instalación de Aplicaciones	
				Nivel de seguridad del Hardware	Control de Mantenimiento Seguridad de la red	
				Nivel de Seguridad del Data Center	Backup Accesibilidad	

Anexo 2. Instrumento de recolección de información

ENCUESTA N°01

EVALUACION DE VARIABLE: Elaboración de un plan de seguridad informática para mejorar la gestión de la información de la Municipalidad Distrital de Mazán

FEHA: ___/____/____

Las respuestas que usted brinde al siguiente cuestionario será confidencial, es muy importante que responder a las preguntas para que nos ayude a realizar una investigación

Para cada pregunta le presentamos cinco alternativas: Nunca, Casi Nunca, Algunas veces, Casi Siempre, Siempre, marque con una X en la alternativa que crea conveniente.

Gracias por su atención y su ayuda.

N°	PREGUNTAS	NUNCA	CASI NUNCA	ALGUNAS VECES	CASI SIEMPRE	SIEMPRE
NIVEL DE SEGURIDAD LOGICA						
1	¿En la Municipalidad para acceder a un equipo de cómputo los usuarios se identifican?					
2	¿En la Municipalidad para acceder a un equipo de cómputo los usuarios hacen uso de una contraseña?					
3	¿En la Municipalidad se ha creado perfiles de usuario para acceder a un equipo de cómputo?					
NIVEL DE SEGURIDAD DEL SOFTWARE						
4	¿Los sistemas informáticos y aplicaciones con que cuenta la Municipalidad son confiables y seguros?					
5	¿Las bases de datos con que cuentan los sistemas informáticos y aplicaciones con que cuenta la Municipalidad son seguras?					
6	¿Los sistemas informáticos y aplicaciones instaladas en los equipos de cómputo con que cuenta están debidamente controlada?					
NIVEL DE SEGURIDAD DEL HARDWARE						
7	¿Se realiza periódicamente el mantenimiento a los equipos de cómputo con que cuenta la municipalidad?					
8	¿La red de datos de datos de la Municipalidad está protegido contra ataques de red?					
NIVEL DE SEGURIDAD DEL DATA CENTER						
9	¿Se hace Backup periódicamente los datos de los servidores del data center?					
10	¿Cualquier personal de la Municipalidad puede acceder de manera fácil al ambiente donde se encuentra el data Center?					

Anexo 3: De la Redacción

Figura N°01

Foto de Entrada de la Municipalidad Provincial de Mazán

Figura N°02

Oficina de Participación ciudadana de la Municipalidad Distrital de Mazán

Fuente: Propia

Anexo 4:

Plan de Seguridad Informática de la Municipalidad Distrital de Mazán

Se proponen con el objetivo de garantizar la protección de los principales bienes informáticos y la información contenida en ellas. a fin de informar y capacitar a toda la institución en temas de seguridad de la información.

1.3.1 Responsables

Según la "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. En el Artículo 5.- establece la conformación del Comité de Gestión de Seguridad de la Información, que acompañe y haga cumplir el plan de seguridad informática en función de los objetivos planteados.

Los cuales debe de estar presididos por:

Tabla 01: Comité de gestión de la seguridad

CONFORMACIÓN DEL COMITÉ DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
Área	**Encargado**	**Funciones**
Alcaldía	Titular o Burgomaestre de la institución	• Supervisar los incidentes sobre la seguridad. • Cumplir y hacer las políticas propuestas en el plan de seguridad informática. • Aprobar las iniciativas para incrementar la seguridad de la infraestructura informática. • Promover la difusión y apoyo a la seguridad de los activos informáticos de la entidad Municipal.
Gerencia de Administración y Finanzas	Gerente de administración y finanzas.	• Gestionar los recursos financieros para la implementación de la infraestructura informática. • Coordinar continuamente con la Sub Gerencia de Tecnología de Información sobre la implementación y mejoras en aspecto tecnológico de la entidad (Por Jefe Inmediato Superior)
Sub Gerencia de Tecnología de Información	Sub gerente de Tecnologías de la Información.	• Promover la difusión y apoyo a la seguridad informática en la institución. • Monitorear los posibles riesgos que afecten la seguridad de la información • Evaluar y coordinar la implementación de controles específicos de seguridad informática.

Asesoría Jurídica	Jefe de la Oficina de Asesoría Jurídica	• Encargado de dar el visto legal al plan de seguridad informática, si se rige acorde a las normas y leyes de nuestra nación. • Dictaminar las normativas para cumplir y hacer cumplir por todo el personal de la entidad municipal.

Fuente: *Elaboración propia*

Asimismo, se asigna un comité evaluador que realizará los trabajos después de ocurrido un evento y medir cual fue su impacto y qué mejoras se podrían implementar al plan de seguridad, el cual debe estar compuesto por el personal de la SGTI y un representante del comité de gestión de la seguridad de la información.

POLÍTICAS DE SEGURIDAD

1.3.2 Medidas y procedimientos de protección Física

a) A las áreas con tecnologías instaladas

- El control de acceso y cierre de los locales está establecido que todas las áreas con tecnologías de información al terminar la jornada laboral queden cerradas y debidamente selladas. Aquellas donde se maneje información clasificada, los trabajadores de estas áreas deberán extremar las medidas de seguridad.

- Todo visitante debe tener una justificación razonable para tener acceso a la SGTI.

- El personal autorizado tendrá visible o disponible en todo momento su identificación oficial otorgado por la Institución.

- Los visitantes serán escoltados en todo momento por personal designado para esas funciones, quien será responsable de que el visitante tenga una conducta adecuada y aceptable.

- La institución debe contar con extintores en toda la institución o por lo menos de la SGTI, para poder controlarlos en caso llegarán a ocurrir.

- Las practicas o simulacros de desastres naturales serán coordinados y fijados por la Oficina de Defensa Civil.

b) A las tecnologías de información

- Los usuarios que hagan uso de las tecnologías informáticas son responsables de la protección de la información que utilicen o provoquen en el transcurso del desarrollo de sus labores, lo cual incluye:

  - Protección de acceso a las oficinas y a sus computadoras, así como cumplir políticas establecidas por SGTI.

  - Los usuarios de la M.P.R. deben tener acceso sólo a los recursos que necesitan en el cumplimiento de su labor diaria, implementándose mediante la definición del equipamiento, aplicaciones a utilizar mediante los privilegios y derechos de acceso a los activos de información que se le otorgue.

  - Los jefes de áreas de la M.P.R. deben garantizar que la seguridad informática sea tratada como un problema institucional normal al ser afrontado y resuelto, siendo estos los máximos responsables de promover la seguridad informática en su área. Para esto deben utilizar herramientas tecnológicas que estén a su alcance:

    - Uso de Antivirus
    - Uso de Antimalware
    - Uso de Antispyware
    - Uso de Firewall
    - Copias de Seguridad
    - Actualizaciones de sistema

  - Se empleará las tecnologías informáticas y los servicios asociados con fines estrictamente de trabajo.

  - Todo software traído a la entidad se le aplicará un período de cuarentena que permitan asegurar su funcionamiento seguro. El Responsable de Seguridad Informática supervisará todo chequeo que se realice en aras de proteger la integridad de la información del que se dispone.

  - Los jefes de áreas y usuarios que hagan uso de las tecnologías informáticas las protegerán contra posibles hurtos, así como del robo de la información que contengan.

  - El movimiento del equipamiento informático debe ser aprobado por el responsable de la seguridad informática.

- No introducir ni utilizar en las tecnologías ningún producto ni modificar la configuración de las mismas, sin la correspondiente autorización del responsable de seguridad informática.

- Deberán quedar apagados todas las computadoras al concluir la jornada laboral, salvo que por necesidades de explotación continua del sistema o de comunicaciones tengan que seguir funcionando.

- En caso de ocurrencia de tormentas eléctricas severas se apagarán y desconectarán todas las tecnologías informáticas y de comunicaciones, salvo aquellas que por necesidad imperiosa haya que dejar funcionando, en cuyo caso se crearán las condiciones necesarias para su protección.

- Se procederá a desconectar los equipos de la red eléctrica en caso de reparación o instalación eléctrica en la institución.

c) A los soportes de información.

- Es obligatorio la desinfección de los dispositivos externos antes de su uso en las tecnologías informáticas**,** se debe tener en cuenta que el uso de los dispositivos informáticos solo utilizase personas autorizadas y responsables.

- Evitar en la medida de lo posible el uso de memorias USB. En lugar de esto, se utilizará carpetas departamentales con control de acceso lógico basado en perfiles y puestos.
- Una vez que un dispositivo informático haya llegado el final de su vida útil, se debe destruir el soporte de una manera adecuada, para evitar que alguien pueda obtener la información que éste almacena. Para garantizar que nadie acceda a la información, se debe realizar una destrucción física del soporte.

- Se debe cifrar la información de aquellos dispositivos usb que se usa en la institución.

1.3.3 Medidas y procedimientos de protección técnicas o lógicas

a) Identificación de usuarios.

- Crear credenciales de identificación de acceso (usuario y contraseña) en el servicio de directorio para acceder a la red y al correo electrónico institucional.

- Para el trabajo con los servicios de Correo electrónico e Internet, se tendrá en cuenta que no se realice la conexión automática a partir de las aplicaciones empleadas para su gestión.

- Se establecerá identificación de usuarios en las computadoras de cada área en correspondencia al personal que haga uso de las tecnologías informáticas y comunicación.

b) Autentificación de usuarios.

- El identificador y la contraseña corresponde al medio normal de autenticación.
  La contraseña deberá tener al menos 10 caracteres, incluir al menos 2 numéricos y 2 alfabéticos. Se deberá cambiar de contraseña cada mes si así lo corresponde.

c) Control de acceso con huella digital. Todo personal de trabajo de la M.P.R. deberá registrar su entrada y salida del área donde trabaja utilizando su huella dactilar, para evitar el acceso a personas no autorizadas.

d) Control de acceso a los activos y recursos.

- Todo usuario es responsable de proteger y no compartir su contraseña. En caso de que algún usuario piense que su contraseña ha sido descubierta, debe notificar al administrador de seguridad inmediatamente. El administrador de seguridad definirá una contraseña temporal, la cual será cambiada por el usuario.

- Se deberá asegurar el acceso de usuarios autorizados y prevenir el acceso no autorizado a los sistemas de información. Se usará para la asignación de las credenciales de accesos a los diferentes sistemas, un formulario con el nombre del sistema, nombre usuario, contraseña temporal y la asignación de derechos al sistema y/o los servicios.

- La SGTI controlará e identificará los equipos conectados a su red, mediante el uso de controladores de dominio, asignación manual de IP y portal cautivo para la conexión WIFI.

- La SGTI utilizará dispositivos de seguridad “firewalls”, para controlar el acceso de una red a otra.

- Los usuarios tendrán acceso únicamente a los datos/ recursos de acuerdo a su puesto laboral.

e) Integridad de los ficheros y datos.

- Los usuarios notificarán a su jefe de la SGTI sobre cualquier incidente que detecten que afecte o pueda afectar a la seguridad de los datos, o por sospecha de uso indebido del acceso autorizado por otras personas.
- La SGTI debe implementar un Firewall (Protección de los sistemas y redes).
- Las computadoras deben contar con un Antivirus actualizados.
- EI usuario se abstendrá de enviar, vía correo electrónico, archivos que excedan la capacidad de la cuota asignada.
- Los usuarios que utilizan documentos con información “Confidencial” o “Restringida” deben asegurarse de:
  - ✓ Almacenarlos en lugares adecuados.
  - ✓ Evitar que usuarios no autorizados accedan a dichos documentos.
  - ✓ Destruir los documentos si luego de su utilización dejan de ser necesarios.

- Aquellos usuarios que manejen activos de información de carácter confidencial en sus equipos asignados deberán tomar los resguardos necesarios para que dicha información no sea filtrada a terceros en caso de pérdida del equipo.

f) Auditoría y alarma.

- El personal encargado de operar los sistemas de información debe registrar todos los errores y fallas que ocurren en el procesamiento de información o en los sistemas de comunicaciones. Estos registros deben incluir lo siguiente:
  - ✓ Nombre de la persona que reporta la falla
  - ✓ Hora y fecha de ocurrencia de la falla
  - ✓ Descripción del error o problema
  - ✓ Responsable de solucionar el problema
  - ✓ Descripción de la respuesta inicial ante el problema

- ✓ Descripción de la solución al problema
- ✓ Hora y fecha en la que se solucionó el problema

- Adquirir e implementar un sistema de alarmas contra intrusos.

1.3.4 medidas y procedimientos de seguridad de operaciones

Todos los procedimientos de operación de los sistemas deben ser documentados y los cambios realizados a dichos procedimientos deben ser autorizados por la SGTI.

- Todas las tareas programadas en los sistemas para su realización periódica, deben ser documentadas. Este documento debe incluir:

  - Tiempo de inicio.
  - Tiempo de duración de la tarea.
  - Procedimientos en caso de falla.

- Solo el personal encargado del sistema puede realizar o aprobar un cambio de emergencia. Dicho cambio debe ser documentado y aprobado en un periodo máximo de 24 horas luego de haberse producido el cambio.

1.4 PLAN DE RECUPERACIÓN DE DESASTRES

Las medidas que a continuación se plantean deberán ser aprobados por la máxima autoridad dentro de la institución para garantizar su estricta difusión y cumplimiento, las cuales se contemplan de acuerdo a los resultados obtenidos por el análisis de riesgos realizado, frente a posibles eventos naturales o provocados que afecten los equipos informáticos de la Municipalidad Provincial de Requena.

PREVIO AL EVENTO

Se contempla medidas preventivas si ocurriera la amenaza y estar preparados para afrontarlas con una serie de actividades que tienen por objetivo salvaguardar la información, además asegurar bajo cualquier eventualidad un proceso de recuperación con el menor costo posible a nuestra institución.

- **Sistemas de Información.**

  La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por en la SGTI como los hechos por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional, esta información se señala en el **anexo N.º 02.**

- **Equipos de Cómputo** Se deberán considerar las siguientes acciones.

  - inventario actualizado de los equipos de manejo de información, especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional esta información se señala en el **anexo N.º 01**.

  - Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación.

  - Tener siempre actualizado una relación de las computadoras requeridas como mínimo para cada sistema de información permanente de la institución (que por sus funciones constituyen el eje central de los servicios informáticos de la institución), las funciones que llevará a cabo y sus posibles usos en varios turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos sistemas.

- **Obtención y Almacenamiento de los Respaldos de Información (BACKUPS).**

  Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

  - Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

  - Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).

  - Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

- Backups de los Datos (Bases de Datos, Índices, tablas de validación, contraseñas y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).

➢ **Políticas (Normas y Procedimientos de Backups)**

Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente, debiéndose incluir:

- Periodicidad de cada Tipo de Backup.
- Respaldo de Información de movimiento entre los períodos que no se sacan Backups (backups incrementales).
- Uso obligatorio de un formulario estándar para el registro y control de los Backups.
- Correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la empresa, y los backups efectuados.
- Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzó todo el edificio o local estudiado).
- Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

➢ **ENTRENAMIENTO**

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de eventos, de acuerdo a los roles que se le hayan asignado en los planes de evacuación de los equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, robos, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen

todo en comité de gestión de seguridad, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

DURANTE EL EVENTO

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades:

Plan de emergencia

En este plan se establecen las acciones que se deben realizar cuando se presente un evento y es conveniente que se prevean los posibles escenarios de ocurrencia, durante el día, la noche o de madrugada.

Tabla 02: Plan de emergencia - Incendio

1. INCENDIO	**Objetivo:** Proteger del fuego la información de la institución que se encuentra alojada en las estaciones de trabajo. que podrían dañarla de manera parcial o total**.**
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DÍA	1. Utilizar los extintores instalados para sofocar el incendio. 2. Apagar los principales dispositivos de la SGTI, puesto que es el soporte principal de la infraestructura tecnológica. 3. Desconectar las llaves de alimentación eléctrica. 4. Llamar a los bomberos.
RESPONSABLE:	**Sub Gerente de Tecnologías de Información y todo el personal de la institución**
DURANTE LA NOCHE Y MADRUGADA	1. Utilizar extintores del centro de cómputo para sofocar el incendio. 2. Desconectar las llaves de alimentación eléctrica. 3. Traer más extintores ubicados en la institución. 4. Reportar a los bomberos y a seguridad de la institución. 5. Reportar al jefe de informática.
RESPONSABLE:	**Personal de Seguridad**

Fuente: *Elaboración propia*

Tabla 03: Plan de emergencia - Fallas en los Equipos

2. FALLAS EN LOS EQUIPOS, DAÑOS DE ARCHIVOS.	**Objetivo:** Proteger los bienes informáticos, de posibles daños físicos y lógicos, que atenten contra el buen funcionamiento de las mismas.
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DÍA	1. Reportar la falla al Personal de Soporte de la SGTI. 2. El personal de la SGTI, Revisara el equipo, para diagnosticar y proceder a reparar desperfecto. 3. Revisar aplicación y corregir error.
RESPONSABLE:	**Sub Gerente de Tecnología de la Información y personal de la SGTI**
DURANTE LA NOCHE Y MADRUGADA	1. Reportar el incidente a su jefe inmediato del problema presentado. 2. Reportar al Sub Gerente de Informática.
RESPONSABLE:	**Personal de Seguridad**

Fuente: *Elaboración propia*

Tabla 04: Plan de emergencia - Equivocaciones

3. EQUIVOCACIONES, DAÑOS DE RCHIVOS.	**Objetivo:** Proteger de la información de la institución que se encuentra alojada en las estaciones de trabajo de errores humanos que podrían dañarla de manera parcial o total**.**
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	ACTIVIDADES
DURANTE EL DÍA	1. Reportar el problema a la SGTI, para que se proceda a corregir el error. 2. Realizar Copias de Seguridad de los archivos, para salvaguardar la información. 3. Solicitar a la SGTI, la evaluación del equipo y dispositivo donde se alojó el archivo corrupto para descartar fallas a nivel software y hardware que lo hayan provocado.
RESPONSABLE:	**Sub Gerente de Tecnología de la Información y personal de la SGTI**
DURANTE LA NOCHE Y MADRUGADA	1. Reportar al Sub gerente de Tecnología de la Información.
RESPONSABLE:	**Personal de Seguridad**

Fuente: *Elaboración propia*

Tabla 5: Plan de emergencia - Acceso no Autorizado

4. ACCESO NO AUTORIZADO, FILTRACIÓN DE INFORMACIÓN	**Objetivo:** Mejorara el nivel de control de acceso hacia la entidad y las oficinas administrativas, en aras de salvaguardar la información y bienes municipales.
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DÍA	1. Cambiar inmediatamente contraseñas de acceso de administradores y de base de datos. 2. Verificar la información filtrada 3. Realizar el respaldo de la información. 4. Reportar al sub gerente de tecnologías de información.
RESPONSABLE:	**Sub Gerente de Tecnología de la Información y el personal de la SGTI**
DURANTE LA NOCHE Y MADRUGADA	1. informar inmediatamente, al Sub gerente de Tecnología de la Información y a la PNP.
RESPONSABLE:	**Personal de seguridad**

Fuente: *Elaboración propia*

Tabla 6: Plan de emergencia - Robo de datos

5. ROBO DE DATOS	**Objetivo:** Proteger la información relevante y confidencial de la institución.
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DÍA	1. Reportar a la SGTI. 2. Reportar al Sub Gerente de Tecnología de Información 3. Cambiar inmediatamente contraseñas de acceso de administradores, acceso al servidor y del base de datos. 4. Chequear el tráfico de la red para detectar variaciones que pueden ser síntoma de mal uso de la misma.
RESPONSABLE:	**Sub Gerente de Tecnología de la Información y personal de SGTI**
DURANTE LA NOCHE Y MADRUGADA	1. Reportar al jefe Inmediato superior. 2. Reportar al Sub Gerente de Tecnología de Información
RESPONSABLE:	**Personal de Seguridad**

Fuente: *Elaboración propia*

Tabla 7: Plan de emergencia - Robo Común

6. ROBO COMUN	**Objetivo:** Proteger la información y bienes de la institución contra los contases robos, causados por personas externas e internas de la institución.
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DIA	1. Interceptar a los infractores y ponerlos a disposición de las autoridades competentes. 2. Reportar inmediatamente al personal de seguridad de la entidad. 3. Revisar el inventario de bienes informáticos.
RESPONSABLE:	**Sub Gerencia de Tecnología de la Información**
DURANTE LA NOCHE Y MADRUGADA	1. Reportar al jefe inmediato superior para tomar las acciones respectivas. 2. Reportar al Sub gerente de tecnología de la información.
RESPONSABLE:	**Personal de Seguridad**

Fuente: *Elaboración propia*

Tabla 8: Plan de emergencia - Fraude

7. FRAUDE, ALTERACIÓN DE INFORMACIÓN	**Objetivo:** Medidas para la protección contra posibles alteraciones de la información relevante de la institución, dados por software mal intencionado o por el actuar humano dentro y fuera de la entidad.
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DIA	1. Se deberá de realizar un análisis exhaustivo con un software antispyware, para verificar la existencia de programas espías destinados a recopilar información confidencial sobre el usuario. 2. Una selección rigurosa de los colaboradores. 3. Buena administración de los recursos humanos. 4. Buenos controles administrativos. 5. Buena seguridad física en los ambientes donde están los principales componentes informáticos.
RESPONSABLE:	**Sub Gerencia de Tecnología de la Información**
DURANTE LA NOCHE Y MADRUGADA	1. Reportar al Sub Gerente de Tecnología de la Información.
RESPONSABLE:	**Personal de Seguridad.**

Fuente: *Elaboración propia*

Tabla 9: Plan de emergencia - Virus

8. VIRUS Y DAÑO DE ARCHIVOS	**Objetivo:** Proteger los equipos computacionales y la red institucional de posibles infecciones por software malicioso.
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DIA	1. Inmediatamente la Pc infectada deberá ser desconectada de la red institucional, para evitar infectar toda la red. 2. Efectuar la descontaminación de los ordenadores ante la aparición de programas malignos. 3. Se debe de realizar la correcta actualización del Software Antivirus en el Servidor principal. 4. Al detectar en una estación de trabajo indicios de contaminación detener la actividad que se, esté realizando, desconectarla de la red y al personal informático.
RESPONSABLE:	**Sub Gerencia de Tecnología de la Información**
DURANTE LA NOCHE Y MADRUGADA	1. Reportar al Sub gerente de Tecnología de Información.
RESPONSABLE:	**Personal de Seguridad**

Fuente: *Elaboración propia*

Tabla 10: Plan de emergencia - Vandalismo

9. VANDALISMO, DAÑO DE EQUIPOS Y ARCHIVOS	**Objetivo:** Proteger de posibles daños de equipos y perdida de información de la municipalidad
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DIA	1. Cerrar todos los accesos a la municipalidad 2. Llamar al serenazgo 3. Llamar a la policía
RESPONSABLE:	**Sub Gerencia de Tecnología de la Información**
DURANTE LA NOCHE Y MADRUGADA	1. Llamar al serenazgo 2. Llamar a la policía
RESPONSABLE:	**Personal de Seguridad**

Fuente: *Elaboración propia*

Tabla 11: Plan de emergencia - Terremoto

10. TERREMOTO	**Objetivo:** Proteger los bienes informáticos en caso de Suscitar un evento Sísmico
QUE HACER:	**EJECUTAR EL PLAN DE EMERGENCIA**
	Actividades
DURANTE EL DIA	1. Apagar los equipos de forma inmediata 2. Ubicarse en zonas estratégicas (zonas seguras) 3. Poner en conocimiento a la oficina de defensa civil. 4. Realizar junto a defensa civil un reporte de daños de los activos informáticos.
RESPONSABLE:	**Sub Gerencia de Tecnología de la Información**
DURANTE LA NOCHE Y MADRUGADA	1. Reportear al jefe inmediato superior 2. Reportar al Sub gerente de Tecnologías de Información
RESPONSABLE:	**Personal de Seguridad**

Fuente: *Elaboración propia*

1.4.1 DESPUES DEL EVENTO

Después de ocurrido el evento es necesario realizar las actividades como:

- **Evaluación de daños**
  Inmediatamente después que el evento ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.
- **Para situaciones Criticas**
  Se deberán evaluar los daños y priorizar la restauración de acuerdo al orden de ejecución de los planes de acción pre establecidos y a las actividades estratégicas y urgentes de la institución.

  a. La copia de los datos a los nuevos medios de almacenamientos magnéticos y ópticos, así como la habilitación de las comunicaciones, servicios de Internet y correo electrónico.

  b. Incluir el traslado de los medios de almacenamientos magnéticos y ópticos que se encuentren fuera de las instalaciones

  c. El personal mínimo requerido para continuar operando.

  d. Tiempo de restauración de cada uno de los servicios de Red, Comunicaciones, Internet y Correo Electrónico.

e. El tiempo determinado debe ser conocido y aceptado por todos los usuarios principales que operan los sistemas o cuentan con un equipo crítico.

- **Para situaciones de Bajo riesgo**

a. Tiempo de reparación o reposición de una estación de trabajo.

b. Tiempo de configuración de las PC.

c. Tiempo de respuesta del proveedor para la reparación del servidor de antivirus (verificar contratos y garantías).

d. Tiempos de reparación de fallas eléctricas.

e. Tiempo de restauración par el servidor de antivirus y sus aplicaciones.

Toda vez que el Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar. Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignación temporal a las actividades afectadas.

- **Ejecución de actividades**

La ejecución de las actividades de los planes de acción enmarcadas en las políticas establecidas, deberán ser realizadas por los equipos operativos pre establecidos. Cada uno de estos equipos deberán contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación además de cualquier incidente que retrase las actividades de los planes de acción al Sub Gerente de TI.

La restauración deberá intentarse en primer lugar con los recursos afectados y de acuerdo a evaluaciones posteriores, se deberá volver a adquirir los recursos, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de la SGTI.

- **Evaluación e resultados**

Una vez concluida las labores de recuperación de los bienes que fueron afectados por el evento, se realizará una evaluación de los resultados de la restauración: que tan bien se hicieron, que tiempo tomaron, que circunstancias aceleraron o entorpecieron las actividades y como se comportaron los equipos de trabajo, cuál hubiera sido el costo de no haber tenido nuestro el plan de contingencias llevado a cabo.

- **Retroalimentación del plan de acción**

  De la Evaluación de los resultados se deberá obtener dos conclusiones; la retroalimentación del plan de emergencias y las recomendaciones para minimizar los riesgos y pérdida que ocasiono el tipo de contingencia.

  En conclusión, se deberá optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y las que funcionaron adecuadamente.