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 INGENIERÍA INFORMÁTICA Y DE SISTEMAS

PROGRAMA ACADEMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

TESIS

"ELABORACIÓN DE UN PLAN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE RAMÓN CASTILLA - 2021"

PARA OBTAR EL TITÚLO PROFESIONAL DE

AUTORES:

- **BACH. RANDY RENGIFO VASQUEZ**
  INGENIERO INFORMÁTICO Y DE SISTEMAS
- **BACH. GIUSEPPE IVAN NASHNATE MONTALVAN**
  INGENIERO DE SISTEMAS DE INFORMACIÓN

ASESOR:

- **ING. CESAR PALACIOS CHAVEZ**

César A. Palacios Chávez
Ing. Computación y Sistemas
C.I.P. 113736

SAN JUAN BAUTISTA – MAYNAS – LORETO- PERÚ – 2021

DEDICATORIA

A Dios por cuidarme y guiarme en el trayecto de mi vida, a mis padres, a mi esposa por su apoyo incondicional

Bach. RANDY RENGIFO VASQUEZ

DEDICATORIA

A Dios por cuidarme y guiarme en el trayecto de mi vida, a mis padres por su apoyo incondicional

Bach. GIUSEPPE IVAN NASHNATE MONTALVAN

AGRADECIMIENTO

Expresamos nuestro agradecimiento al nuestro asesor el Ing. Cesar Palacios Chávez por acompañarnos en este proceso de elaboración de nuestra tesis.

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

- **BACH. RANDY RENGIFO VASQUEZ**
- **BACH. GIUSEPPE IVAN NASHNATE MONTALVAN**

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 SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE RAMÓN CASTILLA - 2021"

De los alumnos: **RANDY RENGIFO VASQUEZ Y GIUSEPPE IVAN NASHNATE MONTALVAN,** de la Facultad de Ciencias e Ingeniería, pasó satisfactoriamente la revisión por el Software Antiplagio, con un porcentaje de **4% de plagio**.

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

San Juan, 29 de Marzo del 2022.

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

CJRA/ri-a
150-2022

Curiginal

Document Information

Analyzed document	UCP_SISTEMAS_2022_TESIS_RANDY_RENGIFO_V1.pdf (D131408922)
Submitted	2022-03-24T15:09:00.0000000
Submitted by	Comisión Antiplagio
Submitter email	revision.antiplagio@ucp.edu.pe
Similarity	4%
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
2

SA **Universidad Científica del Perú / UCP_SISTEMAS_2021_TESIS_JORDAN_TORRES_V1.pdf**
Document UCP_SISTEMAS_2021_TESIS_JORDAN_TORRES_V1.pdf (D120353599)
Submitted by: revision.antiplagio@ucp.edu.pe
Receiver: revision.antiplagio.ucp@analysis.urkund.com
3

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 002-2022-UCP-FCEI del 05 de enero del 2022, 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 Ramirez Villacorta, Mgr. Presidente
- Ing. Tonny Eduardo Bardales Lozano, Mgr. Miembro
- Lic. Carlos Enrique Marthans Ruiz, Mgr. Miembro

Como Asesor: al **Ing. Cesar Palacios Chavez, Mgr.**

En la ciudad de Iquitos, siendo las 12:00 horas del día 27 de julio 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: **"ELABORACIÓN DE UN PLAN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE RAMÓN CASTILLA - 2021".**

Presentado por el sustentante: **RANDY RENGIFO VASQUEZ**

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: **ABSUELTAS**

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

La sustentación es: APROBADO POR **UNANIMIDAD**

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

Presidente

Miembro

Miembro

"Año del Fortalecimiento de la Soberanía Nacional"

ACTA DE SUSTENTACIÓN DE TESIS

FACULTAD DE CIENCIAS E INGENIERÍA

Con Resolución Decanal N° 002-2022-UCP-FCEI del 05 de enero del 2022, 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 Ramirez Villacorta, Mgr. Presidente
- Ing. Tonny Eduardo Bardales Lozano, Mgr. Miembro
- Lic. Carlos Enrique Marthans Ruiz, Mgr. Miembro

Como Asesor: al **Ing. Cesar Palacios Chavez, Mgr.**

En la ciudad de Iquitos, siendo las 12:00 horas del día 27 de julio 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: **"ELABORACIÓN DE UN PLAN PARA MEJORAR LA SEGURIDAD INFORMÁTICA DE LA MUNICIPALIDAD PROVINCIAL DE RAMÓN CASTILLA - 2021".**

Presentado por el sustentante: **GIUSEPPE IVAN NASHNATE MONTALVAN**

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

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 es aprobada por **UNANIMIDAD**

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

Ing. Jimmy Max Ramirez Villacorta, Mgr
Presidente

Ing. Tonny Eduardo Bardales Lozano, Mgr.
Miembro

Lic. Carlos Enrique Marthans Ruiz, Mgr.
Miembro

INDICE DEL CONTENIDO

Páginas

INDICE DE TABLAS

Página

INDICE DE GRÁFICOS

Página

INDICE DE FIGURAS

Página

RESUMEN

Esta investigación se realizó en la Municipalidad Provincial de Ramón Castilla que se encuentra ubicado en la ciudad de Caballo Cocha, cuyo título es Elaboración de un Plan para Mejorar la Seguridad Informática de la Municipalidad Provincial De Ramón Castilla en el periodo 2021, para el desarrollo de esta investigación se realizó un estudio de los principales riesgos, vulnerabilidades y amenazas existentes respeto al activo informático de la entidad, para luego proponer la solución mediante un Plan de Seguridad Informática aplicando la Norma Internacional ISO 27002:2013, que establece las principales actividades para mantener asegurado los activos informáticos, que son fundamentales para el buen funcionamiento de los procesos desarrollados en la municipalidad.

Palabras Claves: Propuesta, Seguridad, Informática

ABSTRACT

This research was carried out in the Provincial Municipality of Mariscal Ramón Castilla, which is located in the city of Caballo Cocha, whose title is Preparation of a Plan to Improve the Computer Security of the Provincial Municipality of Ramón Castilla in the period 2021, for the development As a result of this research, a study was carried out of the main risks, vulnerabilities and existing threats regarding the entity's computer assets, to then propose the solution through a Computer Security Plan applying the International Standard ISO 27002: 2013, which establishes the main activities for maintain computer assets that are essential for the proper functioning of the processes developed in the municipality.

Keywords: Proposal, Security, Informatics

Capítulo I: Marco teórico

1.1 Antecedentes del estudio

- ✓ **Miranda Cairo, Michel, Valdés Puga, Osmany, Pérez Mallea, Iván, Portelles Cobas, Renier, & Sánchez Zequeira, Raúl. (2016)**, en su artículo científico, establece que la gestión de la seguridad informática debe observarse como un proceso correctamente definido, con la finalidad de mejorar la gestión de forma incremental y continua. En su trabajo de investigación presentan una metodología basada en la combinación de varias normas, modelos, herramientas y buenas prácticas para la implementación de la gestión de controles de seguridad informática de manera automatizada, con un enfoque de automatización en las etapas de operación, monitorización y revisión de un Sistema de Gestión de Seguridad de la Información. Teniendo en cuenta que aproximadamente la aplicación del 30% de los controles contenidos en el estándar internacional ISO/IEC 27002, el resultado de esta investigación acepta que la gestión de la seguridad informática es un proceso simple y más efectivo, validada a través del análisis estadístico donde luego de la aplicación del sistema de gestión de seguridad existe la disminución de la complejidad y el aumento de la eficiencia en cuanto al tiempo y el esfuerzo requerido por el proceso en un factor cercano al 90% para ambos casos.

- ✓ ***Doria, (2015),*** en su investigación titulada "Diseño de un Sistema de Gestión de Seguridad de la Información mediante la Aplicación de la Norma Internacional ISO/IEC 27001:2013 en la Oficina de Sistemas de Información y Telecomunicaciones de la Universidad de Córdoba", cuyo objetivo principal es el estudio y aplicabilidad de los sistemas de gestión de seguridad de información, tomando en consideración los cuatro aspectos fundamentales: organización, personas, tecnología y el aspecto legal, en esta investigación se implementa la Norma ISO/IEC 27001:2013, en la oficina de Sistemas y Telecomunicaciones de la Universidad de Córdoba quien se encarga de velar por los activos informáticos y la seguridad de la información de la entidad. En la fase de planeación se estableció las bases para la implementación de un Sistema de Gestión de la Seguridad de la Información persiguiendo las mejores prácticas del estándar de seguridad internacional ISO/IEC 27001:2013, y mediante una

metodología del análisis de riesgos donde se identifican los activos informáticos que están en estados críticos, que tienen mayor impacto y que requieren de mayores controles de seguridad y así establecer un plan para la continuidad de los servicios.

- ✓ **Abalco, David & Ruilova, Romel (2015)**, en su tesis para optar el título profesional de Ingeniero en Sistemas Informáticos y de Computación, titulada: "Elaboración del Plan de Seguridad de la Información para el Fondo de Cesantía y Jubilación del MDMQ", en cuyo objetivo es dar a conocer que es muy importante que se implemente una Norma Técnica que considera la ISO/IEC 27001:2011, con esto se garantiza la protección de los activos informáticos que posee una organización, en este trabajo de investigación se identifica, evalúa y se trata los riesgos que comprometen la integridad y seguridad de los activos Informáticos, concluyendo con su implantación correspondiente.

- ✓ **Cortez, Amelia & Santiago, Wilfredo (2018),** En su tesis para optar el título profesional de Ingeniero de Sistemas, titulada "Plan De Seguridad Informática Basado En La Norma ISO 27002 Para Mejorar La Gestión Tecnológica Del Colegio Carmelitas – Trujillo", en cuyo objetivo general es gestionar de forma segura todos los activos informáticos de la institución así mismo definir políticas que permitan el cifrado de la información, también instaurar la seguridad física y ambiental, establecer la seguridad en las operaciones del negocio, establecer la seguridad en las telecomunicaciones y definir medidas adecuadas para la adquisición, desarrollo y mantenimiento de los sistemas de información , todo ello aplicando la norma internacional ISO 27001:2013 que hacen referencia a un plan de seguridad informática.

1.2 Bases teóricas

- Seguridad

  Para Porto (2018), es el aseguramiento de conservación del hardware en un buen estado. También hace mención que la seguridad permite que los recursos del sistema informático se utilicen de la forma en la que se espera y que quienes puedan acceder a la información que en él se encuentran, sean las personas acreditadas para hacerlo.

- Seguridad de los Activos Informáticos

  SGSI (2015), el activo más valioso en una organización es la información y necesita un aseguramiento o protección adecuada a posibles daños que puedan suscitarse durante su ingreso, procesamiento y almacenamiento, donde participan tanto el hardware como el software, estos activos debe protegerse de las amenazas para lograr que los procesos del negocio se mantengan continuos, también minimizar los daños de la organización, maximizar el retorno de las inversiones y las oportunidades de negocio.

- Seguridad de la Información

  Según el IRAM (2010), La información, que es un recurso cuyo valor para una organización es de suma importancia, por lo tanto, debe ser asegurada de la forma más extrema. La seguridad que se debe dar a la información es para proteger de una amplia gama de amenazas y al mismo tiempo minimizar el daño que dichas amenazas puedan ocasionar.

  Según la ISO Tools (2010), la seguridad de la información contempla los aspectos expuestos a continuación, según La Seguridad de la Información tiene como finalidad proteger la información, de los sistemas y su control de acceso, uso, divulgación, interrupción o destrucción no autorizada.

  La seguridad de la información contempla que se debe conservar las siguientes características:

  - Confidencialidad: Es la propiedad de prevenir que se divulgue la información a personas o sistemas no autorizados.

- Integridad: Es la propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.
- Disponibilidad: Es una característica, cualidad o condición de la información que se encuentra a disposición, de quien tiene que acceder a ésta, bien sean personas, procesos o aplicaciones.

- Seguridad Informática

  Según la ISO Tools (2010), La Seguridad de la Informática consiste en asegurar los recursos que se utiliza en el funcionamiento de los Sistema de Información de una organización, así mismo se utilicen de la forma que ha sido decidido y el acceso de información se encuentra contenida, 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 de la autorización.

- Normas Internacionales de Seguridad Informática ISO

  Según la ISO Tools (2017), son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organizaciones internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

- Norma ISO/IEC 27002

  Esta norma es muy referente dentro del sector ya que, considera como base a todos los posibles riesgos a los que se enfrenta la entidad en sus procesos diarios, y su objetivo principal es establecer, instituir, mantener y mejorar de manera continua la seguridad de la información de la organización.

  La norma ISO 27002 está estructurada en 14 capítulos donde se describen las áreas que se deben considerar para garantizar la seguridad de la información de las que se dispone. El documento recomienda un total de 114 controles, si bien no hace falta cumplirlos todos, sí que hay que tenerlos en cuenta y considerar su posible aplicación, además del grado de la misma.

A continuación, se describen las siguientes áreas de control:

Área de Control 1: Gestión de Activos
1.1 Responsabilidad sobre los Activos
1.1.1 Inventario de activos
1.1.2 Propiedad de los activos
1.1.3 Uso aceptable de los activos
1.1.4 Devolución de activos
1.2 Clasificación de la Información
1.2.1 Directrices de clasificación
1.2.2 Etiquetado y manipulado de la información
1.2.3 Manipulación de activos
1.3 Manejo de los Soportes de Almacenamiento
1.3.1 Gestión de soportes extraíbles
1.3.2 Eliminación de soportes
1.3.3 Soportes físicos en tránsito

Área de Control 2: Control de Accesos
2.1 Requisitos de negocio para el Control de Accesos
2.1.1 Política de control de accesos
2.1.2 Control de acceso a las redes y servicios asociados
2.2 Gestión de Acceso de Usuario
2.2.1 Gestión de altas/bajas en el registro de usuarios
2.2.2 Gestión de los derechos de acceso asignados a usuarios
2.2.3 Gestión de los derechos de acceso con privilegios especiales
2.2.4 Gestión de información confidencial de autenticación de usuarios
2.2.5 Revisión de los derechos de acceso de los usuarios
2.2.6 Retirada o adaptación de los derechos de acceso
2.3 Responsabilidades del Usuario
2.3.1 Uso de información confidencial para la autenticación
2.4 Control de Acceso a Sistemas y Aplicaciones
2.4.1 Restricción del acceso a la información
2.4.2 Procedimientos seguros de inicio de sesión
2.4.3 Gestión de contraseñas de usuario

2.4.4 Uso de herramientas de administración de sistemas

2.4.5 Control de acceso al código fuente de los programas

Área de Control 3: Cifrado

3.1 Controles Criptográficos

3.1.1 Política de uso de los controles criptográficos

3.1.2 Gestión de claves

Área de Control 4: Seguridad Física y Ambiental

4.1 Áreas Seguras

4.1.1 Perímetro de seguridad física

4.1.2 Controles físicos de entrada

4.1.3 Seguridad de oficinas, despachos y recursos

4.1.4 Protección contra las amenazas externas y ambientales

4.1.5 El trabajo en áreas seguras

4.1.6 Áreas de acceso público, carga y descarga

4.2 Seguridad de los Equipos

4.2.1 Emplazamiento y protección de equipos

4.2.2 Instalaciones de suministro

4.2.3 Seguridad del cableado

4.2.4 Mantenimiento de los equipos

4.2.5 Salida de activos fuera de las dependencias de la empresa

4.2.6 Seguridad de los equipos y activos fuera de las instalaciones

4.2.7 Reutilización o retirada segura de dispositivos de almacenamiento

4.2.8 Equipo informático de usuario desatendido

4.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla

Área de Control 5: Seguridad en las Operaciones

5.1 Responsabilidades y Procedimientos de Operación

5.1.1 Documentación de procedimientos de operación

5.1.2 Gestión de cambios

5.1.3 Gestión de capacidades

5.1.4 Separación de entornos de desarrollo, prueba y producción

5.2 Protección contra Código Malicioso

5.2.1 Controles contra el código malicioso
5.3 Copias de Seguridad
5.3.1 Copias de seguridad de la información
5.4 Registro de Actividad y Supervisión
5.4.1 Registro y gestión de eventos de actividad
5.4.2 Protección de los registros de información
5.4.3 Registros de actividad del administrador y operador del sistema
5.4.4 Sincronización de relojes
5.5 Control del Software en Explotación
5.5.1 Instalación del software en sistemas en producción
5.6 Gestión de la Vulnerabilidad Técnica
5.6.1 Gestión de las vulnerabilidades técnicas
5.6.2 Restricciones en la instalación de software
5.7 Consideraciones de las Auditorías de los Sistemas de Información
5.7.1 Controles de auditoría de los sistemas de información

Área de Control 6: Seguridad en las Telecomunicaciones
6.1 Gestión de la Seguridad en las Redes
6.1.1 Controles de red
6.1.2 Mecanismos de seguridad asociados a servicios en red
6.1.3 Segregación de redes
6.2 Intercambio de Información con Partes Externas
6.2.1 Políticas y procedimientos de intercambio de información
6.2.2 Acuerdos de intercambio
6.2.3 Mensajería electrónica
6.2.4 Acuerdos de confidencialidad y secreto

Área de Control 7: 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
7.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas
7.1.3 Protección de las transacciones por redes telemáticas

- Plan de Seguridad Informática:

  Para Cano (2017, Pág. 3), es el retrato 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.

1.3 Definición de términos básicos:

- Vulnerabilidades: Es la probabilidad que existen de que las amenazas existentes en el entorno de las TI, se materialice o ejecuten en contra de un activo. 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.

Capítulo II: Planteamiento del problema

2.1. Descripción del problema

En la actualidad las instituciones públicas de acuerdo al Decreto Supremo N° 050-2018, que aprueban la definición de seguridad digital tomando en consideración donde señala que en el ámbito nacional es el estado de confianza en el entorno digital, que resulta de la gestión y aplicación de un conjunto de medidas proactivas y reactivas frente a los riesgos que afectan la seguridad de las personas, la prosperidad económica y social, la seguridad nacional y los objetivos nacionales en dicho entorno. Se sustenta en la articulación con actores del sector público, sector privado y otros quienes apoyan en la implementación de controles, acciones y medidas, por lo tanto, la Municipalidad Provincial de Ramón Castilla, que se encuentra ubicado en la ciudad de Caballo Cocha, al no contar con este documento de gestión está obligada a poseer e implementar su plan de seguridad informática.

La Municipalidad Provincial de Ramón Castilla presenta una serie de inconvenientes de amenazas y vulnerabilidades que a continuación se nombran:

Gestión poco segura de los activos, no cuenta con controles de los accesos a los recursos informáticos, no cuenta con políticas de cifrado de la información, existe mínima seguridad física y ambiental, existe poca seguridad en las operaciones y procesos, existe poca seguridad en las redes, además de ellos se carece de la adquisición, desarrollo y mantenimiento de los sistemas de información.

De acuerdo a lo indicado en esta realidad problemática de la Municipalidad Provincial de Ramón Castilla se necesita contar con un plan de seguridad informática que le permita implementar adecuadamente un conjunto de controles de seguridad.

2.2. Formulación del problema

2.2.1. Problema general

- ✓ ¿Mediante la elaboración de un Plan se mejorará la Seguridad Informática de la Municipalidad Provincial de Ramón Castilla - 2021?

2.2.2. Problemas específicos

- ✓ ¿Cuál es el nivel de seguridad lógica informática de la Municipalidad Provincial de Ramón Castilla?
- ✓ ¿Cuál es el nivel de seguridad de Software de la Municipalidad Provincial de Ramón Castilla?
- ✓ ¿Cuál es el nivel de seguridad del Hardware de la Municipalidad Provincial de Ramón Castilla?
- ✓ ¿Cuál es el nivel de seguridad del Centro de Datos de la Municipalidad Provincial de Ramón Castilla?

2.3. Objetivos.

2.3.1. Objetivo general:

- ✓ Elaborar un Plan para mejorar la seguridad informática de la Municipalidad Provincial de Ramón Castilla 2021.

2.3.2. Objetivos específicos:

- ✓ Evaluar el nivel de Seguridad Lógica Informática existente en la Municipalidad Provincial de Ramón Castilla.
- ✓ Evaluar el nivel de Seguridad del Software existente en la Municipalidad Provincial de Ramón Castilla.
- ✓ Evaluar el nivel de seguridad del Hardware existente en la Municipalidad Provincial de Ramón Castilla.
- ✓ Evaluar el nivel de seguridad del Centro de datos de la Municipalidad Provincial de Ramón Castilla.

2.4. Hipótesis

- ✓ Hipótesis General: Mediante la elaboración de un Plan se logrará mejorar la seguridad informática de la Municipalidad Provincial de Ramón Castilla 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 Provincial de Ramón Castilla 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 • 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 Centro de datos	Respaldo	
		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 Provincial de Ramon Castilla:

Tabla N°02
Distribución del Personal administrativo de la Municipalidad Provincial de Ramon Castilla

CANTIDAD	CARGO
02	Gerentes
02	Secretarias
07	Trabajadores Administrativos
02	Trabajadores de la oficina de Informática
Total	13 personas

Fuente: Recursos Humanos MPDRC

- Muestra:

  Para la investigación se tomará toda la población que consiste en 13 personas que trabajan en la Municipalidad Provincial de Ramón Castilla.

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 para acceder a un equipo de cómputo los usuarios se identifican?

Tabla N°03

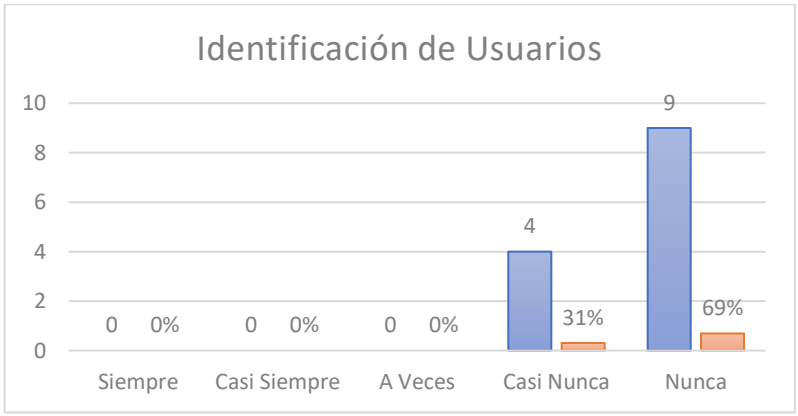
Identificación de Usuarios

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 evidenciar que, de 13 trabajadores encuestados de la Municipalidad Provincial de Ramón Castilla, el 31% señalo que los que tienen a

su cargo una computadora casi nunca se identifican, el 69% señalo que nunca se identifican.

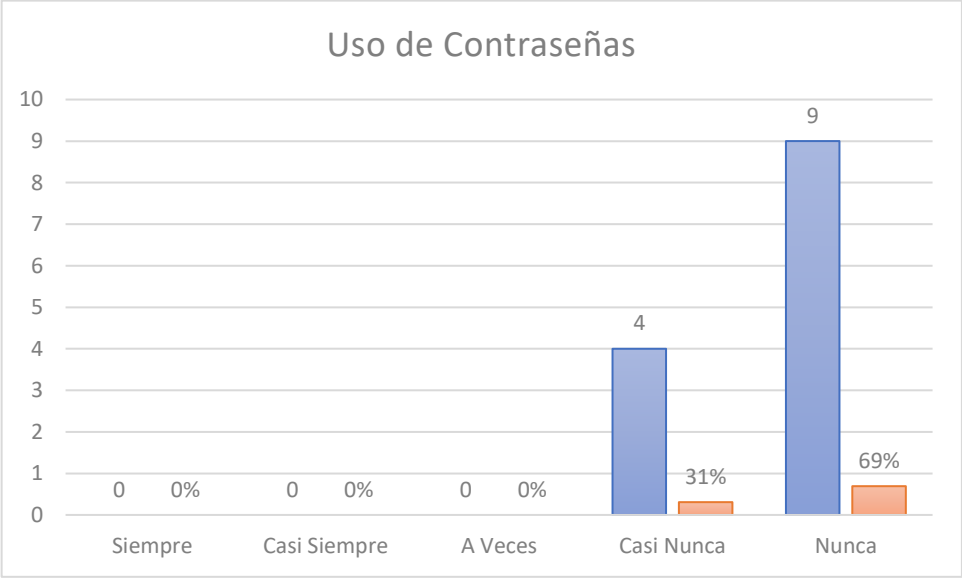
Pregunta 02.- ¿En la Municipalidad para acceder a un equipo de cómputo los usuarios hacen uso de una contraseña?

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 los 13 trabajadores encuestados de la municipalidad provincial de Ramón Castilla, el 31% señalo que los usuarios de los trabajadores 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.

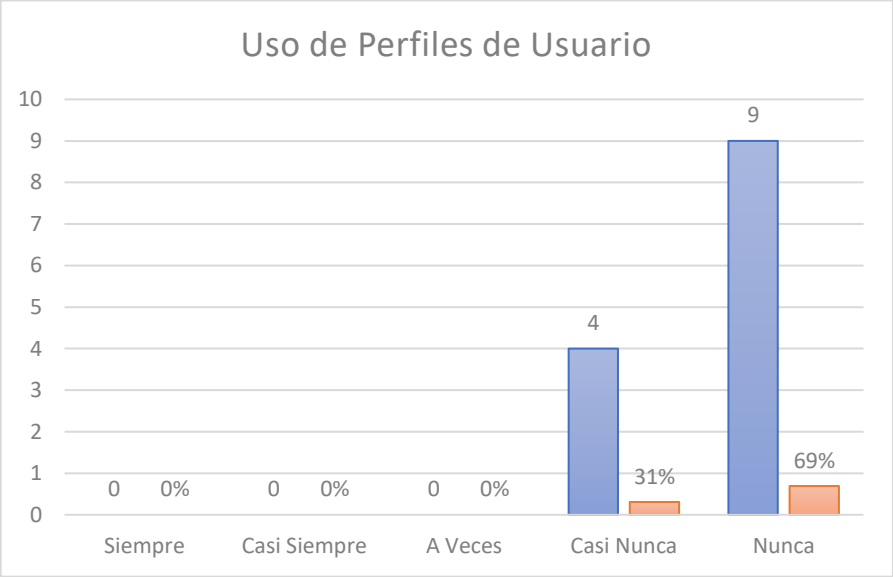
Pregunta 03.- ¿En la Municipalidad se ha creado perfiles de usuario para acceder a un equipo de cómputo?

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 de la municipalidad provincial de Ramón Castilla encuestados, 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 son confiables y seguros?

Tabla N°06

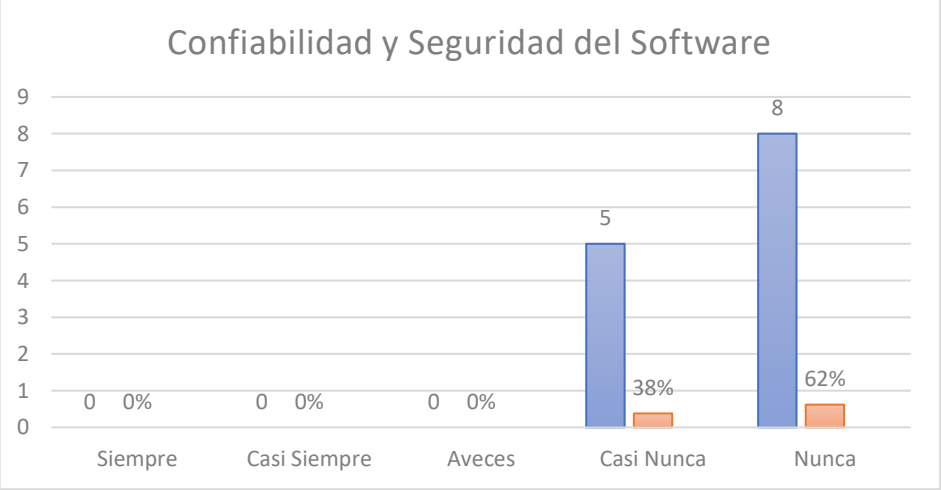
Confiabilidad y Seguridad del Software

Seguridad del Software	ni	Porcentaje
Siempre	0	0%
Casi Siempre	0	0%
A Veces	0	0%
Casi Nunca	5	38%
Nunca	8	62%
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 encuestados de la municipalidad provincial de Ramón Castilla, el 38% señalo que los

usuarios que tienen a su cargo una computadora casi nunca tienen seguridad y confiabilidad de los sistemas, el 62% señalo que nunca tienen.

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

Tabla N°07

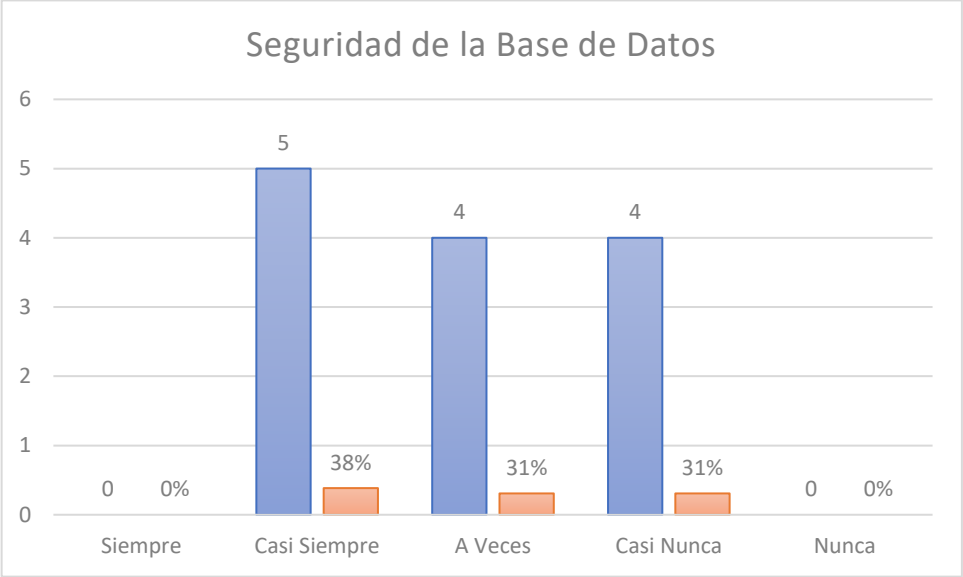
Seguridad de la Base de Datos

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 administrativos de la municipalidad provincial de Ramón Castilla, 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.- ¿Los sistemas informáticos y aplicaciones instaladas en los equipos de cómputo con que cuenta la Municipalidad tiene un Control?

Tabla N°08

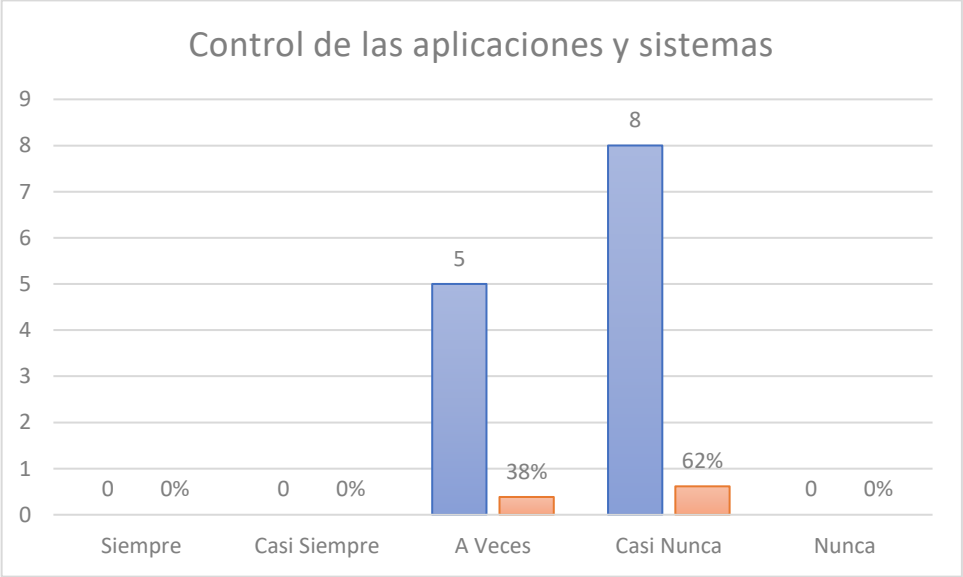
Control de las Aplicaciones y Sistemas

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 encuestados de la municipalidad de Ramon Castila, 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:

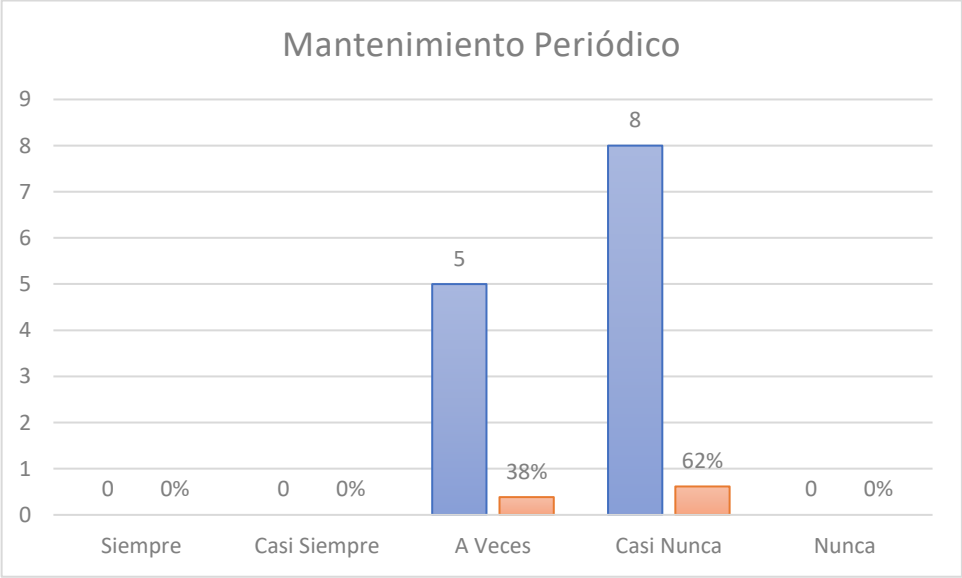
Pregunta 07.- ¿Se realiza periódicamente el mantenimiento a los equipos de cómputo con que cuenta la Municipalidad?

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 administrativos encuestados de la Municipalidad, el 38% señalo que a veces se realiza

el mantenimiento de los equipos de cómputo con que cuenta la Municipalidad Provincial de Ramon Castila, el 62% señalo que casi nunca se realiza el mantenimiento.

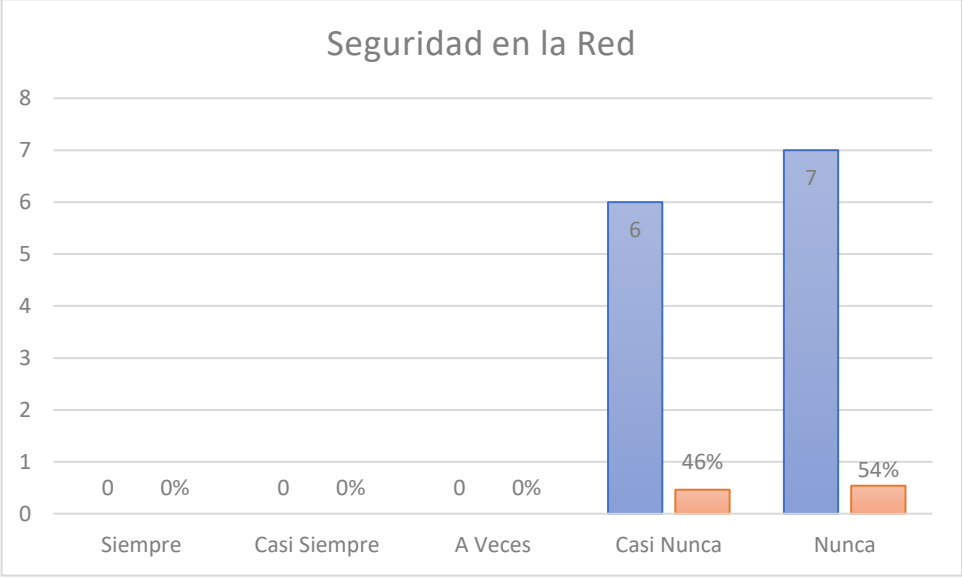
Pregunta 08.- ¿La red de datos de datos de la Municipalidad está protegido contra ataques de red?

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 de la Municipalidad Provincial de Ramón Castilla, 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 Centro de Datos

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

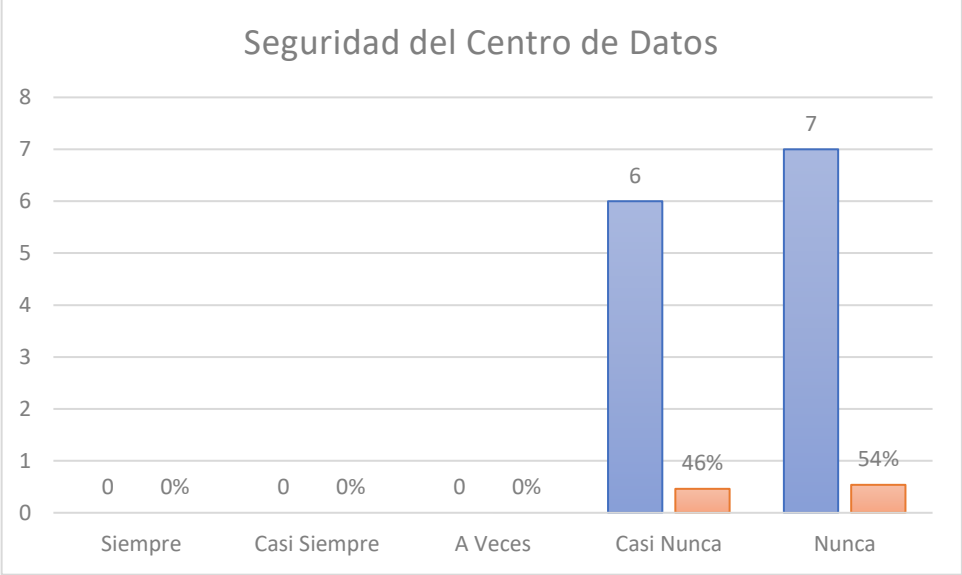
  Pregunta 09.- ¿Se hacen Copias de Respaldo periódicamente los datos de los servidores del Centro de datos de la Municipalidad?

Tabla N°11
Seguridad del Centro de Datos

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 del Centro de Datos



Fuente: Elaboración Propia

Interpretación:

De la tabla 11 y gráfico 09, se evidencia que de una muestra 13 trabajadores de la Municipalidad Provincial de Ramón Castilla, 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.

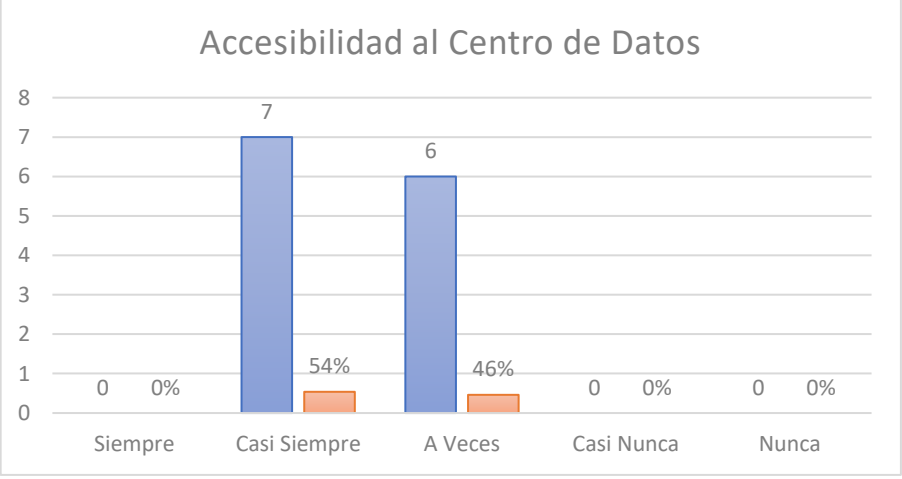
Pregunta 10.- ¿Cualquier personal de la Municipalidad puede acceder de manera fácil al ambiente donde se encuentra el Centro de datos?

Tabla N°12
Accesibilidad al Centro de datos

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 al Centro de Datos



Fuente: Elaboración Propia

Interpretación:

De la tabla 12 y gráfico 10, se evidencia que de una muestra 13 trabajadores de la municipalidad provincial de Ramón Castilla, el 54% señalo que casi siempre cualquier

trabajador de la Municipalidad Provincial de Ramon Castilla puede acceder al ambiente donde se encuentra el Centro de datos y el 46% señalo que a veces el personal de la municipalidad puede acceder al ambiente del centro de datos.

Capítulo V. Discusión, conclusiones y recomendaciones

5.1. Discusiones:

- Nuestra investigación coincide con la de Miranda Cairo, Michel, Valdés Puga, Osmany, Pérez Mallea, Iván, Portelles Cobas, Renier, & Sánchez Zequeira, Raúl. (2016), a través de la aplicación de la norma internacional de seguridad informática ISO/IEC 27002, teniendo como resultado en nuestra investigación, se acepta que la gestión de la seguridad informática es un proceso simple y más efectivo, también ha sido validada a través del análisis estadístico donde luego de la aplicación del sistema de gestión de seguridad existe la disminución de la complejidad y el aumento de la eficiencia en cuanto al tiempo y el esfuerzo requerido por el proceso en un factor cercano al 95% para ambos casos.

- Nuestra investigación coincide con la de Doria, (2015), donde realiza el Diseño de un Sistema de Gestión de Seguridad de la Información mediante la Aplicación de la Norma Internacional ISO/IEC 27001:2013 del mismo modo que en nuestra investigación se desarrolla mediante una metodología del análisis de riesgos en las cueles se identifican los activos informáticos que están en estado críticos, que tienen mayor impacto y que requieren de mayores controles de seguridad, y así establecer un plan para la continuidad de los servicios.

- Nuestra investigación coincide con la de Abalco, David & Ruilova, Romel (2015), donde se ha elaborado un Plan de Seguridad de la Información usando la Norma Técnica que considera la ISO/IEC 27001:2011, del mismo modo que nuestra investigación garantizamos la protección de los activos informáticos que posee nuestra entidad, identificando, avaluando y tratando los riesgos que comprometen la integridad y seguridad de los activos Informáticos, concluyendo con su implantación correspondiente.

- Nuestra Investigación Coincide con la de Cortez, Amelia & Santiago, Wilfredo (2018), donde se Elabora un Plan De Seguridad Informática Basado En La Norma ISO 27002 y se logra Mejorar La Gestión Tecnológica Del Colegio Carmelitas – Trujillo", en esta investigación también se aplica la norma internacional ISO 27001:2013 que hacen referencia a un plan de seguridad informática

5.2. Conclusiones

- ✓ Se realizó una evaluación del nivel de seguridad lógica, donde se logró determinar que existe un riesgo muy alto de sufrir un daño en los archivos de los equipos de cómputo de la Municipalidad Provincial de Ramón Castilla, ya que la seguridad de los accesos y contraseñas no están implementadas como medida de un plan de seguridad informática.

- ✓ Se realizó una evaluación del nivel de seguridad del software, donde se logró determinar que existe riesgo muy alto de sufrir daños en los sistemas y base de datos de la Municipalidad Provincial de Ramón Castilla, no están seguros debido a que no se tienen y aplican los controles necesarios para su instalación y funcionamiento.

- ✓ Se realizó una evaluación del nivel de seguridad del hardware, donde se logró determinar que existe un riesgo muy alto de que los equipos informáticos se malogren, debido a que no se están realizando los mantenimientos preventivos y correctivos de los equipos informáticos de la Municipalidad Provincial de Ramón Castilla de manera periódica y permanente, existiendo el peligro de que estos equipos fallen constantemente.

- ✓ Se realizó una evaluación del Nivel de seguridad del Centro de Datos, donde se logró determinar que existe un riesgo muy alto de robo o perdida de información o equipos, debido a que cualquier persona común puede acceder a los ambientes donde se encuentra el centro de datos de la Municipalidad Provincial de Ramón Castilla, también se pudo evidenciar que el ambiente donde están los servidores no cumple con los requisitos establecidos para ser

un centro de datos, no se están haciendo las copias de seguridad periódica, todo esto pone en riesgo la información.

5.3. Recomendaciones:

- ✓ La Oficina de Tecnologías de la Información de la Municipalidad debería solicitar la aprobación del Plan de Seguridad Informática de manera urgente puesto que su información se encuentra en riesgo alto.

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

- ✓ La Municipalidad Provincial de Ramón Castilla 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 temas, elaborar una nueva metodología tomando como modelos las normas ISO 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 mejorará la Seguridad Informática de la Municipalidad Provincial de Ramón Castilla - 2021? **Problemas Específicos** ¿Cuál es el nivel de seguridad lógica informática de la Municipalidad Provincial de Ramón Castilla? ¿Cuál es el nivel de seguridad de Software de la Municipalidad Provincial de Ramón Castilla? ¿Cuál es el nivel de seguridad del Hardware de la Municipalidad Provincial de Ramón Castilla? ¿Cuál es el nivel de seguridad del centro de datos de la Municipalidad Provincial de Ramón Castilla?	**General** Elaborar de un Plan para mejorar la seguridad informática de la Municipalidad Provincial de Ramón Castilla - 2021 **Específicos** Evaluar el nivel de Seguridad Lógica Informática existente en la Municipalidad Provincial de Ramón Castilla Evaluar el nivel de Seguridad del Software existente en la Municipalidad Provincial de Ramón Castilla Evaluar el nivel de seguridad del Hardware existente en la Municipalidad Provincial de Ramón Castilla Evaluar el nivel de seguridad del Centro de Datos de la Municipalidad Provincial de Ramón Castilla	**General**: Mediante la elaboración de un Plan se logrará mejorar la seguridad informática de la Municipalidad Provincial de Ramón Castilla en el periodo 2021	Elaboración de un Plan para mejorar la Seguridad Informática de la Municipalidad Provincial de Ramón Castilla 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 provincial de Ramón Castilla 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 Centro de datos	Copias de Seguridad Accesibilidad	

Anexo 2. Instrumento de recolección de información

CUESTIONARIO

EVALUACION DE VARIABLE: ELABORACIÓN DE UN PLAN DE SEGURIDAD INFORMÁTICA PARA MEJORAR LA GESTIÓN DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE RAMÓN CASTILLA

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 centro de datos?					
10	¿Cualquier personal de la Municipalidad puede acceder de manera fácil al ambiente donde se encuentra el centro de datos?					

Anexo 3: De la Redacción

Figura N°01

Foto de Entrada de la Municipalidad Provincial de Ramón Castilla

Anexo 4:

Plan de Seguridad Informática de la Municipalidad Provincial de Ramón Castilla

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 Municipalidad.

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 Municipalidad; 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 Municipalidad.

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.
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 Municipalidad.

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 Municipalidad (que solución es utilizada para cada proceso de la Municipalidad); - 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 Municipalidad (en cuyo caso las claves también se archivan).

Recuperar claves que se han perdido o corrompido como parte de la gestión de continuidad de la municipalidad, 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 Municipalidad."

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 Municipalidad 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 Municipalidad 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 Municipalidad 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 Municipalidad

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 Municipalidad no sea mayor de tres (3) días.
c) El usuario deberá reportar cualquier inconveniente que suceda con los activos que estén fuera de la Municipalidad.
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 Municipalidad 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 Municipalidad, ¿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 Municipalidad 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 la Municipalidad 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 Municipalidad 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 del colegio 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 Municipalidad.

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 Municipalidad 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 Municipalidad.

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 Municipalidad.

Los controles que deberían incluir en todas las aplicaciones de la Municipalidad 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 Municipalidad.

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 Municipalidad.