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 ACADÉMICO DE INGENIERÍA DE SISTEMAS DE INFORMACIÓN

TÍTULO PROFESIONAL

TRABAJO DE SUFICIENCIA PROFESIONAL

(Sustentación de Caso)

"PROPUESTA DE PLAN DE SEGURIDAD INFORMÁTICA PARA LA SUB GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE REQUENA, EN EL AÑO 2019"

PARA OPTAR AL TÍTULO PROFESIONAL DE:

INGENIERO DE SISTEMAS DE INFORMACIÓN

AUTOR (es): BACH. DENNIS ALBERTO VASQUEZ GUTIERREZ
BACH. PAULO MANUEL RENGIFO SAQUIRAY

ASESOR (es): ING. JIMMY RAMIREZ VILLACORTA Mg.

San Juan Bautista – Loreto – Maynas –Perú

2019

Dedicatoria

Dedicado a Dios y a mi madre por darme la vida, formarme con valores y enseñarme que todo se logra con trabajo y dedicación.

A mi padre por su apoyo incondicional, por haberme inculcado en mi principios sólidos y el deseo de superación y por creer en mí.

A mis hermanos por su apoyo moral y afectivo infinito en esta etapa de mi vida.

A mis amigos y demás familiares que has estado conmigo animándome y acompañándome en estos años decisivos de mi vida.

Dennis

Dedicatoria

A mí querida mamá y abuelo, quienes con su amor, paciencia y esfuerzo me han permitido llegar a cumplir hoy un sueño más, gracias por inculcar en mí el ejemplo de esfuerzo y valentía.

A mis hermanos, tías, primos y amigos que de alguna u otra manera estuvieron siempre apoyándome y alentadme durante mis estudios, para poder así ver cristalizado mis objetivos.

Paulo

Agradecimientos

A Dios todo poderoso por la vida y la salud, porque siempre está con nosotros.

A la Universidad Científica del Perú, por habernos permitido formarnos como profesionales y por sembrar en nosotros el deseo de aprender y construir una sociedad mejor.

Al programa Nacional de Becas (Pronabec), a través de Beca 18, que nos dio la oportunidad de seguir una carrera profesional en una universidad que no hubiéramos podido costear.

A la Municipalidad Provincial de Requena, en especial a la Sub Gerencia de Tecnologías de la Información por darnos todas las facilidades para poder realizar el presente trabajo.

A nuestras queridas familias, amigos y a todas las personas que fueron partícipes de este proceso, ya sea de manera directa o indirecta, gracias a todos ustedes, que fueron los responsables de motivarnos a seguir adelante, y que el resultado de todo nuestro esfuerzo se ve reflejado en la culminación exitosa de nuestro paso por la universidad el día de hoy.

Los Autores

ACTA DE SUSTENTACIÓN DE TRABAJO DE SUFICIENCIA PROFESIONAL

Con Resolución Decanal N°449 -2019- UCP - FCEI del 17 de junio de 2019, la **FACULTAD DE CIENCIAS E INGENIERÍA DE LA UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP** designa como Jurado Evaluador y Dictaminador de la Sustentación de Tesis a los Señores:

- Ing. Paul David Telio Gatica, Mg. — Presidente
- Ing. Cesar Palacios Chávez — Miembro
- Ing. Tonny Eduardo Bardales Lozano, Mg. — Miembro

En la ciudad de Iquitos, siendo las 06:30 pm, del día viernes 05 de julio de 2019, en las instalaciones de la UNIVERSIDAD CIENTÍFICA DEL PERÚ - UCP, se constituyó el Jurado para escuchar la sustentación y defensa del Trabajo de Suficiencia Profesional:

"PROPUESTA DE PLAN DE SEGURIDAD INFORMÁTICA PARA LA SUB GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN DE LA MUNICIPALIDAD PROVINCIAL DE REQUENA, EN EL AÑO 2019"

Presentado por los sustentantes:

VASQUEZ GUTIERREZ DENNIS ALBERTO
Y
RENGIFO SAQUIRAY PAULO MANUEL

Asesor (es): **Ing. Jimmy Max Ramírez Villacorta.**

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:

Por lo que la Sustentación es: Aprobado por unanimidad

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

Presidente

Miembro

Miembro

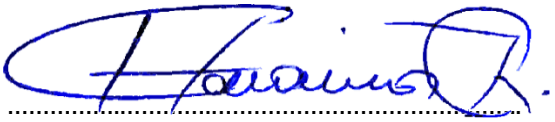
CALIFICACIÓN:

Aprobado (a) Excelencia	: 19 – 20
Aprobado (a) Unanimidad	: 16 - 18
Aprobado (a) Mayoría	: 13 – 15
Desaprobado (a)	: 00 – 12

.....

Ing. Paul David Tello Gatica Mg.

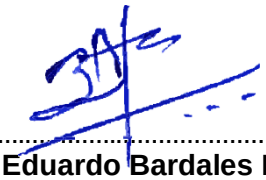
Presidente



.....

Ing. Cesar Palacios Chávez

Miembro



.....

Ing. Tonny Eduardo Bardales Lozano Mg.

Miembro

.....

Ing. Jimmy Max Ramírez Villacorta, Mg.

Asesor

ÍNDICE GENERAL

INDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Hoy en día vivimos en un mundo de constantes cambios, donde la era digital ha obligado a instituciones y empresas, a implementar sistemas informáticos que contribuyan en mejorar los procesos o actividades en la que estas operan, convirtiéndose así en la parte fundamental del desarrollo de la organización, pero vale hacer hincapié y recordar que no solo se trata de poseer activos informáticos y ya se solucionó el problema, sino que también se deben de establecer normas que regulen el uso de las mismas, y minimicen el riesgo de seguridad tanto por ataques internos y externos a la que está expuesta toda organización.

Es así que un Plan de Seguridad Informática constituye un documento fundamental para establecer políticas de seguridad informática y debe ser de obligatorio cumplimiento para todo el personal que labora en una institución.

Siguiendo estos principios, en el presente trabajo se realizó un diagnóstico situacional, que constituyó en una evaluación total de los bienes informáticos: software, hardware, unidades de red, y niveles de accesibilidad a la sub gerencia de tecnología de la información, que es el área encargada del adecuado desarrollo, adquisición, soporte, implementación y supervisión de los recursos informáticos de la Municipalidad Provincial de Requena.

Asimismo, fue posible constatar los riesgos y del precario estado en la que se encuentra la infraestructura tecnológica, desde un cableado estructurado que sucumbe frente a la falta de mantenimiento, hasta la falta de un resguardo de la información relevante e histórica de la Municipalidad, cosa que es de mucha preocupación, porque está muy propenso a la pérdida de toda ella, ya que se encuentra alojada de forma física en las computadoras personales, y no en un servidor de archivos.

Identificando todas estas problemáticas, se elaboró el presente plan de seguridad, donde se estableció algunas propuestas de seguridad, buenas prácticas y se dió recomendaciones para corregir algunos problemas que podrían ocurrir.

Palabras Claves: Sub Gerencia de Tecnología de información, Comité de Gestión de la Seguridad de la Información, Política de Seguridad, seguridad de la Información, Estación de Trabajo.

ABSTRACT

Today we live in a world of constant change, where the digital era has forced institutions and companies to implement computer systems that contribute to improving the processes or activities in which they operate, thus becoming the fundamental part of the development of the organization, but it is worth emphasizing and remembering that not only is it a question of having computer assets and the problem has already been solved, but that rules must also be established to regulate their use, and minimize the security risk both from internal and external attacks to which every organization is exposed.

It is so a computer security Plan constitutes a fundamental document to establish computer security policies and must be enforced for all personnel working in an institution.

Following these principles, the present work was carried out a situational analysis, which constituted a total assessment of computer assets: software, hardware, network drives, and accessibility to the technology management sub levels of the information, which is the area responsible for the development, acquisition, support, implementation and supervision of the computing resources of the Provincial Municipality of Requena.

It was also possible to verify the risks and the precarious state of the technological infrastructure, from structured cabling that succumbs to the lack of maintenance, to the lack of a backup of the relevant and historical information of the Municipality, which is of great concern, because it is very prone to the loss of all of it, since it is physically housed in personal computers, and not in a file server.

Identifying all these problems, was the present security plan, which was established some proposals for security, good practices and gave recommendations to correct some problems that could occur.

Keys words: Information Technology Sub-Manager, Information Security Management Committee, Information Security Policy, Information Security, Workstation.

CAPÍTULO I

Introducción

La Municipalidad Provincial De Requena, es una entidad del estado peruano, que se encuentra ubicado en la región Loreto, con jurisdicción sobre la provincia de requena, tiene una extensión de 49 477.8 km² y se divide en 11 distritos, con sede Municipal en la Ciudad del mismo nombre. El palacio Municipal, por ser el ente principal de los procesos administrativos, se encuentra implementado con una gran infraestructura informática; pero que por el pasar de los años y la falta de un correcto mantenimiento, éste viene siendo grandemente afectado y presentando problemas constantes en el hardware y software de los equipos, e infraestructura de red, sumándose a ellos la falta de normas o políticas que regulen el funcionamiento de estos.

La municipalidad provincial de Requena actualmente no cuenta con un plan de seguridad informática la cual constituye un gran riesgo a la seguridad de los bienes informáticos, viéndose expuesta y comprometida a perderse la información y el daño de los equipos.

Dado que es la primera vez que se realiza un plan de seguridad informática para la municipalidad provincial de Requena, no existen registros de antecedente alguno, pero debido a que la norma técnica peruana (NTP) exige que las instituciones públicas cuenten con un plan de seguridad es que realizamos este trabajo.

La información es la sangre de todas las organizaciones y sin ella la empresa dejaría de funcionar, principalmente si hablamos de empresas altamente automatizadas por lo que su seguridad sigue siendo un punto pendiente y por tanto el factor más determinante por el cual fracasan.

Es muy importante ser conscientes de que por más que nuestra empresa a nuestro criterio sea la más segura, con el incremento del uso de nueva tecnología para manejar la información nos hemos abierto a un mayor número y tipos de amenazas. Es por eso que, en el ambiente competitivo de hoy, es necesario que las entidades aseguren la confidencialidad, integridad y disponibilidad de la información vital corporativa.

Por lo tanto; la seguridad informática debe ser dada por una colaboración entre los encargados de la seguridad de la información, que deben disponer de las medidas al

alcance de su mano y los usuarios que deben ser conscientes de los riesgos que implican determinados usos de los sistemas y de los recursos que consumen cada vez que les pasa algún problema, ya que esto les hace que pierdan tiempo de producción y el consumo de recursos en horas de la recuperación de la actividad normal que en muchos casos es irrecuperable.

Sin embargo, gran parte de esa concientización está en manos de los responsables de la seguridad de la información, apoyados en todo momento por la gerencia de forma explícita y activa, por ello es importante indicarles no sólo cuales son las principales amenazas en cada momento, sino qué deben hacer para evitarlas, impartiendo así procedimientos de actuación que permitan que las medidas técnicas que se disponen desde el comité de gestión de la seguridad de la información sean efectivas.

Por lo tanto, en este nuevo entorno, es imprescindible que las empresas se preparen no sólo para prevenir el peligro de comprometer sus operaciones de negocio por una falla de seguridad, sino también que se preparen en establecer medidas que permitan reducir los problemas de seguridad que pueden surgir.

Entonces el objetivo de este trabajo es realizar una propuesta de plan de seguridad informática para la sub gerencia de la municipalidad provincial de Requena y así proteger los bienes tecnológicos (Hardware y software) con los que cuenta la institución. Para lograrlo se plantearon los siguientes objetivos específicos:

- Realizar el estudio actual del estado situacional de los bienes informáticos y de la información de la sub gerencia de tecnologías de la información de la municipalidad provincial de Requena.
- Realizar el análisis de riesgo de la seguridad informática de la sub gerencia de tecnologías de la información de la municipalidad provincial de requena.
- Proponer políticas y medidas de seguridad informática para la sub gerencia de tecnologías de la información de la municipalidad provincial de Requena.
- Proponer un plan de contingencia, para proteger temporalmente los bienes informáticos de la municipalidad provincial de Requena.

Las mismas que puedan garantizar la protección y/o reducción del impacto que puedan causar alguna amenaza.

CAPÍTULO II

Marco Referencial

Antecedente Internacional

La referencia internacional es un “diseño del plan de seguridad informática del sistema de información misional de la procuraduría general de la nación” llevado a cabo en Bogotá – Colombia el año 2016.

La Procuraduría General de la Nación (PGN), es la Entidad que representa a los ciudadanos ante el estado el cual cuenta con un sistema de información misional -SIM- que es la herramienta tecnológica que apoya integralmente las funciones misionales de intervención, disciplinaria y preventiva. “Es un software moderno, integral y robusto que cumple las necesidades de información misional de la PGN en las diferentes dependencias de todo el territorio nacional.

El presente trabajo tuvo como finalidad diseñar un plan de seguridad informática para el sistema de información misional de la PGN mediante la aplicación de buenas prácticas de seguridad, que permita desarrollar políticas y estándares claros para la preservación de la confidencialidad, integridad y disponibilidad de la información, con este proyecto se buscó plasmar estrategias para proteger el sistema de información misional mediante el uso de metodologías conocidas que permiten evaluar la seguridad en activos de información (Alfaro Iván, Vargas Edwin,2016).

Antecedente Nacional

Tomamos como referencia nacional el Plan de contingencia y seguridad de la información de la municipalidad provincial de Canchis v1.01. Elaborado en la municipalidad Provincial de Canchis – Sicuani – Cusco.

La Sub gerencia de Tecnologías de la información y sistemas (SGTIS) Elaboró un plan de contingencia y seguridad de la información en la municipalidad Provincial de Canchis; cuyo objetivo fue asegurar la información mediante políticas que conllevan a un nivel de protección aceptable para así garantizar la continuidad de las actividades de la institución que podrían alterar el normal funcionamiento de las TICs, a fin de minimizar el riesgo no previsible, críticos o de emergencia, y responder de forma inmediata hacia la recuperación de las actividades normales; fundamentado con la resolución ministerial N.º 04-2016-PCM que aprueba el uso obligatorio de la norma técnica peruana “NTP-ISO/IEC 27001:2014 Sistema de Gestión de la Seguridad de la Información. Requisitos. 2da edición” en todas las entidades integradas al sistema nacional de informática. (SGTIS,2016).

DEFINICIONES TEÓRICAS

Plan de seguridad

Conjunto de decisiones que definen cursos de acción futuros, así como los medios que se van a utilizar para conseguirlos. (Gómez, 2011).

Políticas de seguridad

Una política de seguridad consiste de enunciados que clasifican los riesgos de información, identifican los objetivos de seguridad aceptables y también los mecanismos para lograr estos objetivos. (Laudon,2012).

Seguridad Informática

"Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información segura y confiable." (Aguilera,2010).

Declaración de intenciones de alto nivel que cubre la seguridad de los sistemas informáticos y que proporciona las bases para definir y delimitar responsabilidades para las diversas actuaciones técnicas y organizativas que se requieran. (Gómez, 2011)

Seguridad Informática

"cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema" (Gómez,2011)

La seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta. (Baca, 2016).

Sistema de información (SI)

Podemos plantear la definición técnica de un sistema de información como un conjunto de componentes interrelacionados que recolectan (o recuperan), procesan, almacenan y distribuyen información para apoyar los procesos de toma de decisiones y de control en una organización. Además de apoyar la toma de decisiones, la coordinación y el

control, los sistemas de información también pueden ayudar a los gerentes y trabajadores del conocimiento a analizar problemas, visualizar temas complejos y crear nuevos productos. (laudon kenneth y Laudon Jane, 2012).

Un sistema de información, no obstante, las medidas de seguridad que se le apliquen, no dejan de tener siempre un margen de riesgo.

Para afrontar el establecimiento de un sistema de seguridad es necesario conocer:

- Cuáles son los **elementos** que componen el sistema. Esta información se obtiene mediante entrevistas con los responsables directivos de la organización para la que se hace el estudio de riesgos y mediante la apreciación directa.
- Cuáles son los **peligros** que afectan al sistema, accidentales o provocados. Se deducen tanto de los datos aprobados por la organización como por el estudio directo del sistema mediante la realización de pruebas y muestreo sobre el mismo
- Cuáles son las **medidas** que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos potenciales. Se trata de decir cuáles serán los servicios y mecanismos de seguridad que reducirían los riesgos al máximo posible. (Aguilera,2010).

Tipos de Seguridad

- **Activa**

  Comprende el conjunto de defensas o medidas cuyo objetivo es evitar o reducir los riesgos que amenazan al sistema.

  Ejemplos: impedir el acceso a la información a los usuarios no autorizados mediante introducción de usuarios y contraseñas; evitar la entrada de virus instalando un antivirus; impedir mediante encriptación, la lectura no autorizada de mensajes. (Aguilera,2010).

- **Pasiva**

  Está formada por las medidas que se implantan para, una vez producido el incidente de seguridad, minimizar su repercusión y facilitar la recuperación del sistema; por ejemplo, teniendo siempre al día copias de seguridad de los datos. (Aguilera,2010).

Propiedades de un sistema de información seguro

Se considera seguro a un sistema que cumple con las siguientes propiedades:

- **Integridad**

  Este principio garantiza la autenticidad y recisión de la información sin importar el momento en que se solicita, o, dicho de otra manera, una garantía de que los datos no han sido alterados ni destruidos de modo no autorizado. (Aguilera,2010).

- **Confidencialidad**

  La OCDE (Organización para la Cooperación y el Desarrollo Económico), en sus directrices para la seguridad de los sistemas de información define la confidencialidad como "el hecho de que los datos o informaciones estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en los momentos autorizados y de una manera autorizada".

  Para prevenir errores de confidencialidad debe diseñarse un control de acceso al sistema: quién puede acceder, a que parte del sistema, en qué momento y para realizar qué tipo de operaciones. (Aguilera,2010).

- **Disponibilidad**

  La información ha de estar disponible para los usuarios autorizados cuando la necesiten.

  Se deben aplicar medidas que protejan la información, así como crear copias de seguridad y mecanismos para restaurar los datos que accidental o intencionalmente se hubieses dañado o destruido. (Aguilera,2010).

DEFINICIONES CONCEPTUALES

Amenaza: Se entiende por amenaza a la presencia de uno más factores de diversos indoles (Personas, maquinas o sucesos) que de tener oportunidad atacan al sistema produciéndole daños Aprovechando de su nivel de vulnerabilidad. (Aguilera,2010).

Activo: Son los activos 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).

Control: son métodos, políticas y procedimientos organizacionales que refuerzan la seguridad de los activos de la organización; la precisión y confiabilidad de sus registros, y la adherencia operacional a los estándares gerenciales. (Laudon,2012).

Hacker: Es un individuo que intenta obtener acceso sin autorización a un sistema computacional (Laudon,2012).

Información: Datos que se han modelado en una forma significativa y útil para los seres humanos. (Laudon,2012).

Impacto: Son las consecuencias de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema, dicho de otra manera, el daño causado. (Aguilera,2010).

Informática: Es la ciencia que estudia la transmisión (Recepción y envío), el almacenamiento y el análisis de datos, que al ser procesados se convierten en información, realizando estos procesos con la ayuda de un dispositivo automático. (Baca, 2016)

Riesgo: Se denomina riesgo a 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).

Servidor: un servidor es un tipo de software que realiza ciertas tareas en nombre de los usuarios. El término servidor ahora también se utiliza para referirse al ordenador físico en el cual funciona ese software, una máquina cuyo propósito es proveer datos de modo que otras máquinas puedan utilizar esos datos. (masadelante.com)

Seguridad: se refiere a las políticas, procedimientos y medidas técnicas que se utilizan para evitar el acceso sin autorización, la alteración, el robo o el daño físico a los sistemas de información. (Laudon,2012).

Virus: Es un programa de software malintencionado que se une a otros programas de software o archivos de datos para poder ejecutarse, por lo general sin el conocimiento o permiso del usuario. (Laudon,2012).

Vulnerabilidad: Probabilidades que existen de que una amenaza se materialice contra un activo. No todos los activos son vulnerables a la misma amenaza. (Aguilera,2010).

CAPÍTULO III

Metodología

Para desarrollar el presente trabajo, se tuvo como referencia la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición".

Base legal

- Ley Orgánica de Municipalidades LEY N.º 27972
- Resolución Ministerial N. º 004-2016-PCM, que Aprueba el uso obligatorio de la Norma Técnica Peruana "NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición", en todas las entidades integrantes del Sistema Nacional de Informática.

Alcance del Plan de Seguridad Informática

El presente plan de seguridad informática tiene un alcance total de las áreas de la Municipalidad Provincial de Requena, ubicada en la calle San Francisco de Asís Nro. 138 - 140 y pretende dar a conocer una serie de medidas de seguridad con las cuales se llegarán a plantear los procedimientos y restricciones de seguridad en la SGTI y en toda la institución; los usuarios de las estaciones de trabajo de la municipalidad tendrán la obligación de seguir al pie de la letra las presentes políticas emitidas por el comité de seguridad de la información a través de la Sub Gerencia de Tecnología de la Información y aprobadas por Alcaldía y Gerencia Municipal, comprendiendo la revisión de las siguientes funciones al interior de la SGTI y demás áreas administrativas:

- Políticas y medidas de seguridad para la protección de los bienes informáticos.
- Evaluación y retroalimentación continua del plan de seguridad.

La Sub Gerencia de Tecnología de la Información es la encargada de administrar estas políticas de seguridad.

SITUACIÓN ACTUAL

Recolección de datos

Para conocer las funciones y estructura de la Municipalidad, se quería los principales documentos de gestión, que rigen toda entidad, tales como: POI (Plan Operativo Informático - 2018) MOF (Manual de Organización y Funciones - 2017) ROF (Reglamento de Organización y funciones - 2017) PEI (Plan estratégico Institucional - 2019) y se solicitó el inventario de la infraestructura Tecnológica a la SGTI, así como otros documentos que nos sirvieron para conocer, analizar y sustentar la propuesta del plan de seguridad.

Además, se realizó una entrevista al Sub gerente de Tecnologías de Información y una ficha de observación para los funcionarios de la SGTI, así como de las demás áreas administrativas.

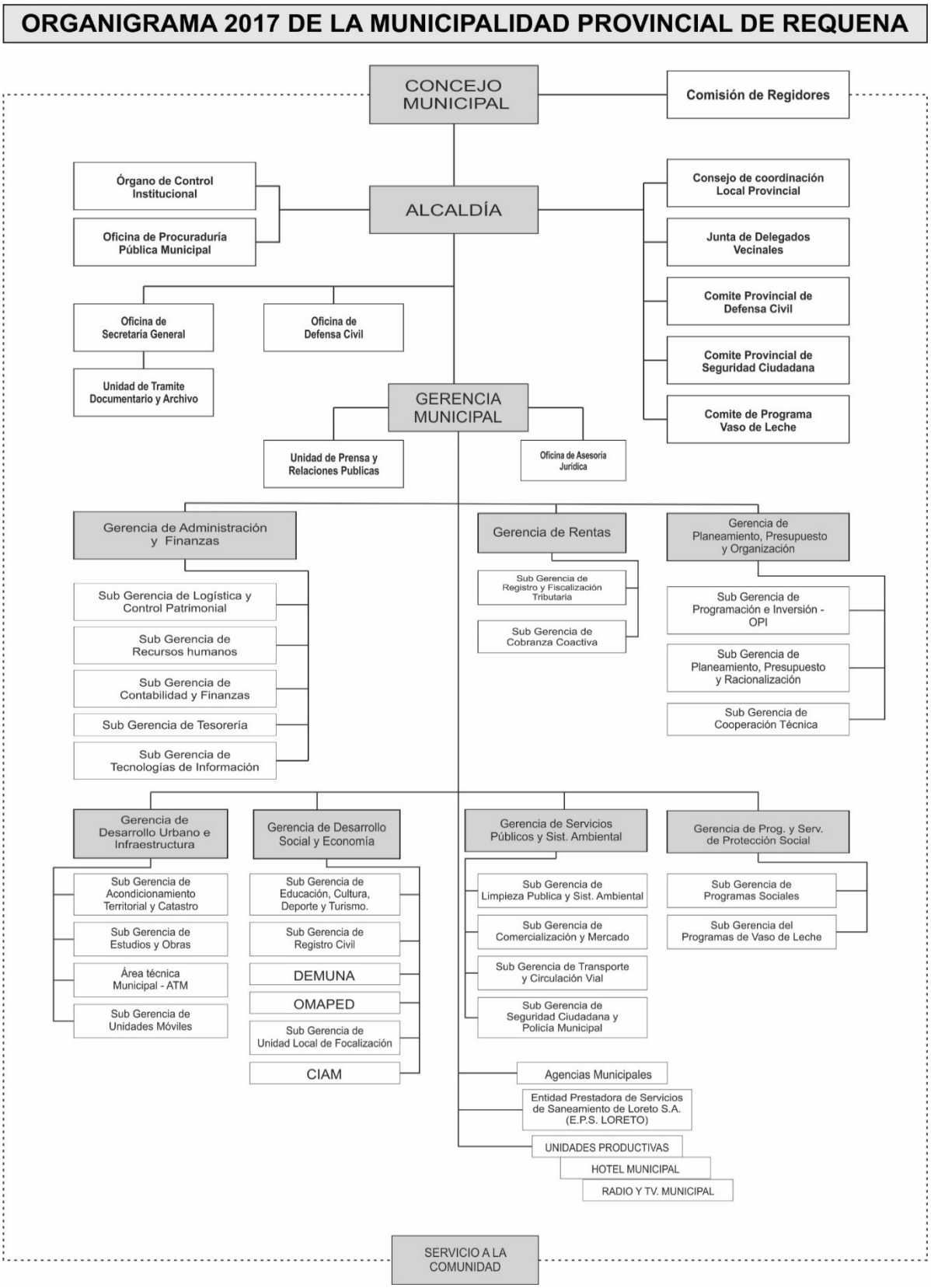
Diagnostico

Los ambientes y los recursos tecnológicos de la municipalidad se encuentran en un estado de vulnerabilidad, a distintas amenazas que podrían dañar la disponibilidad, integridad y confiabilidad de la información, que supondría un impacto económico y operativo a la institución.

Para ello se realizaron las evaluaciones de los posibles riesgos y sus probabilidades de ocurrencia en el entorno informático, identificando allí la necesidad de la elaboración del plan de seguridad informática, que contemple medidas de seguridad que permitan evitar en la medida de lo posible una contingencia que afecten los bienes tecnológicos de la institución.

Organización

Ilustración 01: Organigrama Institucional



Fuente: *MOF - MPR*

ESTRUCTURA Y FUNCIONES

a) Concejo Municipal.

Ejerce funciones normativas y de fiscalización que la ley orgánica de municipalidades lo Faculta, conforme a la ley N.º 27972- Ley Orgánica de Municipalidades.

b) Alcalde.

Ejerce la representación legal de la institución y las funciones ejecutivas que la ley encomienda. Además, que canaliza y dirige las necesidades de la comunidad. Así mismo busca optimizar el manejo de los fondos públicos y recursos materiales de la entidad.

c) Oficina de Defensa Civil.

Tiene como función general, programar, controlar, dirigir, y evaluar las acciones relacionadas con el almacenamiento, distribución de los materiales logísticos en el ámbito de la jurisdicción de Requena.

d) Gerencia Municipal.

Tiene como función principal, planear, organizar, integrar, dirigir, coordinar y supervisar las actividades de las unidades orgánicas de la municipalidad, para el cumplimiento de los objetivos institucionales.

e) Prensa y Relaciones Públicas.

Mantener informado a los vecinos de las actividades que realiza la institución a través de los diferentes medios de comunicación, local y regional.

f) Oficina de Secretaria General.

Es el órgano encargado de dirigir, supervisar, evaluar, coordinar y difundir las gestiones del alcalde y del concejo municipal.

g) Unidad de Trámite y archivos.

Registrar, clasificar, controlar, distribuir los diferentes, trámites administrativos, de acuerdo al texto único de procedimientos de la municipalidad.

h) Órgano de control institucional y defensa Judicial.

Programar, dirigir y ejecutar acciones de control posterior interno a las unidades orgánicas de la Municipalidad, así como realizar exámenes especiales, de conformidad con los dispositivos y normas legales que rigen al sistema nacional de control.

i) Procuraduría Pública.

Programar, dirigir y ejercer la representación judicial de la entidad y asumir su defensa en los procesos civil o penal de conformidad con los dispositivos y normas legales vigentes.

j) Oficina de Asesoría Jurídica.

Programar, ejecutar, coordinar y supervisar los asuntos de carácter jurídico en los ámbitos, administrativos, así como otra índole jurídica.

k) Gerencia de Planeamiento, presupuesto, y Organización. Asesora a los órganos de gobierno en la formulación de proyectos de inversión, de procedimientos. Mejoramiento de métodos y sistemas de trabajo, levantamiento de datos estadísticos para la formulación de diagnóstico de socio-económico en entidades públicas y privadas.

l) Gerencia de Administración y Finanzas.

Administrar los recursos financieros o áreas de fondos cumpliendo lo señalado en el sistema Nacional de Tesorería

m) Gerencia de Recursos Humanos.

Organizar, ejecutar, controlar, supervisar y evaluar los procesos del sistema administrativos de Personal, velando por la correcta aplicación de las normas y dispositivos legales vigentes sobre la materia.

n)Sub gerencia de tecnología de la Información.

Organizar, ejecutar, controlar, supervisar y evaluar los procesos del sistema e infraestructura tecnológica de la Municipalidad.

CARACTERÍSTICAS DEL SISTEMA INFORMÁTICO

Actualmente la Sub Gerencia de Tecnología de la Información **(SGTI)** de la Municipalidad Provincial de Requena, dentro de su infraestructura tecnológica esta soportado por bienes informáticos que se describen en el **Anexo Nro. 01, y Anexo Nro. 02**, el cual comprenden del inventario de: Software, Hardware, Conectividad, Sistemas de Información y del personal informático.

A continuación, se describe brevemente el funcionamiento de la infraestructura tecnológica:

a) Condiciones del ambiente físico

La SGTI se encuentra ubicado en el tercer piso del palacio municipal, específicamente al lado izquierdo del auditorio municipal, cuenta con un área, de $60m^2$ (5m ancho, 12m largo), cabe mencionar que la estructura física es de concreto armado, puertas y ventanas de madera. Actualmente la estructura de la sub gerencia y del palacio municipal se encuentra en regular estado de conservación.

En la SGTI, se alojan el servidor de Actualización de Antivirus y los equipos de comunicación, tales como el Switch central de la red municipal, el cual se distribuye a todas las estaciones, así como los dispositivos del proveedor de Servicio de internet-IPS (IQ series, Servidor CentOs OS 6.9), que son muy necesarios para la operación de todas las actividades informáticas que se realizan dentro de las distintas áreas de la Municipalidad Provincial de Requena.
Mediante observación directa se pudo apreciar y comprobar que las áreas más vulnerables, o críticas tanto por su importancia o por el flujo de trabajo que realiza, son las siguientes:

- Gerencia de Rentas.
- Sub gerencia de Logística y control patrimonial.
- Gerencia de Desarrollo Urbano e Infraestructura.
- Sub gerencia de Tecnología de la Información.
- Sub gerencia de Contabilidad.

b) De la Infraestructura de Red

- La SGTI cuenta con una red local (privado), que se distribuye en todas las áreas de la planta 1,2 y 3 del Palacio Municipal (sede Central) y en la sede del Hotel Municipal.

- Para la gestión de la red y el servicio de internet Satelital, se cuenta con un servidor que aloja el sistema Operativo CentOs 6.9(Linux), de propiedad del proveedor del servicio de internet, quien a su vez administra un dominio local, proxy cache y realiza el filtro de contenidos (squid), Los servicios implementados en la red son navegación Internet(con restricciones de contenido), correo electrónico corporativo y los sistemas de información con la que opera cada área, descrito en el **Anexo Nro. 2**

- El cableado de la red está soportado por cable UTP categoría 5 y 6, con topología hibrida (topología estrella-bus y estrella-anillo) las cuales se conectan al Router IQ series del proveedor de servicio de internet. Las estaciones de trabajo se agrupan por áreas y pisos a partir de conmutadores (switches) cabe resaltar que dicha infraestructura se encuentra en malas condiciones por falta de mantenimiento.

- El intercambio de información tanto interna como externa se realiza básicamente a través del correo electrónico.

c) Del Personal

- El personal de la SGTI. Posee los conocimientos y la preparación necesaria para su empleo y en la mayor parte de los casos tiene nivel medio o superior.

- El personal de la SGTI. está comprometido con su trabajo, dando soluciones eficaces a los problemas informáticos de la entidad.

d) De los Servicios

- Se cuenta con un portal web institucional y un servicio de Hosting donde se administra los correos corporativos.

- Para la gestión del Antivirus se cuenta con un servidor Virtualizado que utiliza el sistema Operativo Windows server R2 2008, el antivirus que utiliza la SGTI es ESET ENDPOINT v6 que distribuye por todas las estaciones de trabajo (Windows XP, 7,8.1, 10).

- Para la elaboración de documentos se cuenta con el paquete de Microsoft Office 2010, 2013 (No Licenciado).

ANÁLISIS DE RIESGO

Contempla una evaluación integral para identificar riesgos potenciales que puedan ocurrir y las consecuencias que puede traer a la institución en caso se materialicen.

Se tendrá en cuenta ítems referentes a los distintos aspectos de seguridad.

Tabla 01: Cuestionario Para el Análisis de Riesgo

RIESGO	PREGUNTAS
1. Fuego, que puede destruir los equipos y los archivos.	- ¿La Municipalidad cuenta con protección contra incendios? - ¿Cuenta con diversos extintores? ¿Detectores de humo? - ¿Los empleados están preparados para enfrentar un posible incendio?
2. Robo común, llevándose los equipos y archivos	- ¿En qué tipo de vecindario se encuentra la Institución? - ¿Hay venta de drogas? - ¿Los equipos de cómputo se ven desde la calle? - ¿Hay personal de seguridad en la Institución? ¿Cuántos vigilantes hay? - ¿Los vigilantes, están ubicados en zonas estratégicas? - ¿Existe un sistema de seguridad para prevenir el ingreso de personas no autorizadas
3. Vandalismo, que dañen los equipos y archivos	- ¿Existe la posibilidad que un ladrón cause daños? - ¿Hay la probabilidad que causen algún otro tipo de daño intencionado?
4. Fallas en los equipos, que dañen los archivos	- ¿Cuánto saben los empleados de computadoras o redes? - Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda? - Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?
5. Equivocaciones que dañen los archivos	- ¿Cuánto saben los empleados de computadoras o redes? - Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?
6. Acción de virus, que dañen los archivos	- ¿Se prueba software en la oficina sin hacerle un examen previo? - ¿Está permitido el uso de disquetes en la oficina? - ¿Todas las máquinas tienen unidades de disquetes? - ¿Se cuentan con procedimientos contra los virus?
7. Terremotos, que destruyen los equipos y archivos	- ¿La Institución se encuentra en una zona sísmica? - ¿El edificio cumple con las normas antisísmicas? - Un terremoto, ¿cuánto daño podría causar?
8. Accesos no autorizados, filtrándose datos importantes	- ¿Existe registro de personal autorizado en la Municipalidad? - ¿Qué probabilidad hay que un colaborador intente hacer un acceso no autorizado? - ¿Existe comunicación remota de la red? ¿Qué tipo de servicio se utiliza? - ¿Contamos con Sistemas de Seguridad en el Correo Electrónico o Internet?
9. Robo de datos; y la posible difusión de estos.	- ¿Cuánto valor tienen actualmente las Bases de Datos? - ¿Cuánta pérdida podría causar en caso de que se hicieran públicas? - ¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?
10. Fraude, vía computadora.	- ¿Cuántas personas se ocupan de la contabilidad de la Institución? - ¿Los sistemas son confiables? ¿Pueden copiar datos en archivos? - Las personas que trabajan en las diferentes áreas, ¿qué tipo de antecedentes laborales tienen? - ¿Existe acceso a los sistemas desde otros sistemas externos o por personas no autorizadas?

Fuente: *Elaboración propia*

Para poder establecer los riesgos a los cuales está propensa la Municipalidad Provincial de Requena, se clasificó por niveles los factores de riesgos más comunes:

Factor de Riesgo:

Tabla 02: Factor de Riesgo

Muy alto
Alto
Medio
Bajo
Muy Bajo

Fuente: *Elaboración Propia*

Ellos determinan nuestra tabla de riesgos y nivel de factores que a continuación detallamos.

Resultado del análisis de riesgo

Tabla 03: Resumen del Análisis de Riesgo

RESUMEN DE ANALISIS DE RIESGOS					
RIESGO	**FACTOR DE RIESGO**				
	MUY BAJO	**BAJO**	**MEDIO**	**ALTO**	MUY ALTO
Incendio				✖	
Inundación		✖			
Robo Común			✖		
Vandalismo, daño de equipos y archivos.		✖			
Fallas en los equipos.				✖	
Equivocaciones, daño de archivos.			✖		
Virus, daño de equipos y archivo.			✖		
Terremotos.		✖			
Acceso no autorizado, filtración de información.				✖	
Robo de datos				✖	
Fraude, alteración de información.			✖		

Fuente*: Elaboración propia*

En base a la tabla anteriormente presentada, concluimos que nuestro análisis de riesgo de manera general, nos hace ver que los posibles riesgos que pudieran presentarse en su mayoría van de acuerdo a un factor de ocurrencia.

A continuación, se describe las puntuaciones de acuerdo a nivel de riesgos a la que está expuesta La Municipalidad Provincial De Requena:

Tabla 04: Tabla de Valoración de Riesgo

TABLA VALORACIÓN DE RIESGOS			
VALOR	**TIPO DE RIESGO**	**RIESGO**	**PROTECCCIÓN ACTUAL**
ALTO:	Incendio	Pérdida de equipos e información	Ninguna
	Fallas en los equipos	Pérdida de equipos e información	Ninguna
	Equivocaciones y daños de archivos	Daño de archivos por Procesos inadecuados.	Ninguna
	Acceso no autorizado, filtración de información	Filtrado de datos por terceros o personal interno.	Ninguna
	Robo de datos	Filtrado de datos por terceros o personal interno.	Ninguna
MEDIO:	Robo Común	Pérdida de equipos e información	- Se cierran las puertas y ventanas después fuera del horario de trabajo. - Se encuentra al costado de la comisaria de la ciudad. - Cuenta con cámaras de video vigilancia.
	Fraude, alteración de información.	Uso de sistemas para intereses propios.	Ninguna
	Virus y daño de archivos	Pérdida o deterioro de la información.	- Eset ENDPOINT v6
BAJO:	Inundación	Deterioro de equipos y pérdida de información	Ubicación en el tercer piso
	Vandalismo, daño de equipos y archivos.	Daño de equipos y pérdida de información	- Cuenta con vigilancia. - Patrullaje de la policía.
	Terremotos	Daño de equipos y pérdida de información	-Simulacros

Fuente: *Elaboración propia*

ANÁLISIS DE RESULTADOS DEL DIAGNÓSTICO DE RIESGOS

Riesgos altos

- **Incendio.**

  Podrían ser ocasionados por cortos circuitos o condiciones climáticas adversas que podrían dañar de manera parcial o total los equipos y la información de la institución, además de que no se cuenta con medidas preventivas, lo que genera un gran problema al suscitarse un evento de esta naturaleza.

- **Fallas en los equipos que dañan los archivos.**

  Puede suceder debido a defectos de fábrica o porque no recibe el mantenimiento adecuado, generando problemas constantes en el hardware y software de los equipos, a su vez estos tienden a desconfigurarse, crear errores de lectura de archivos, hasta quemarse. es importante mencionar que la Municipalidad No cuenta con un servidor de archivos, lo que genera que la información solo se aloje de forma local en las estaciones de trabajo, aumentando la posibilidad de pérdida de dicha información, se suma a todo esto la falta de herramientas *y* materiales en la SGTI para que el personal pueda hacer el mantenimiento adecuado.

- **Equivocaciones y daño de archivos.**

  Pueden ser ocasionados por la inexperiencia o por la falta de cuidado de los trabajadores al manipular los equipos y los sistemas de información, que conlleva a la pérdida involuntaria de la información dentro de la institución.

- **Acceso no autorizado, filtración de información.**

  Existe la posibilidad de que internamente un personal con conocimientos informáticos pueda acceder a la Pc de otro usuario y sustraer información, ya que aún no existe una política de actualización y mantenimiento de contraseñas, que regule el acceso a las estaciones de trabajo.

- **Robo de datos**

  Pueden ser ocasionado por que no existe un firewall adecuado, que impida el acceso remoto o por la red interna hacia las estaciones de trabajo de los usuarios, además de que cualquier persona puede insertar una memoria USB, en una PC de Usuario y sustraer la información.

No existe un documento de listado de asignación de usuarios. Exponiéndose a no saber que personal tiene asignado algún equipo y a que servicios tiene acceso.

Riesgos medios

- **Robo Común.**
  Pueden ser ocasionados por personas inescrupulosas que ocasionarían la pérdida completa de los equipos y la información alojada en ellas.

- **Fraude, alteración de información.**
  Pueden ser ocasionado por personas con acceso no controlado que tienden a lucrar con la información que obtienen en los sistemas.

- **Virus y daño de archivos**
  Es muy probable que ocurra debido a que no existe un dominio con usuario administrador que controle la instalación de aplicaciones potencialmente peligrosas y por falta de previsión de un antivirus actualizado y licenciado.

Riesgos bajos

- **Inundación**
  No se descarta, debido a que la zona donde se ubica específicamente el palacio municipal, está rodeada por el Rio Tapiche (comprende las calles: malecón Bolognesi/mártires del petróleo) y la quebrada Camaná (calle Unión y Mártires del petróleo) además esto podría suscitarse por lluvias torrenciales y por falta de un adecuado sistema de desagüe en la ciudad.

- **Vandalismo, daño de equipos y archivos.**
  No se descarta frente a grupos multitudinarios generalmente paros regionales o nacionales.

- **Terremotos.**
  Casi no existen posibilidades de que ocurra, aun así, se podrían dar y causar daño a la institución por falta de prevención.

De acuerdo a la tabla de análisis de riesgo, hicimos una lista de los bienes más importantes de la institución que nos permitirá saber cuáles son más vulnerables frente a las distintas amenazas y poder priorizar su protección.

Tabla 05: Vulnerabilidad de los bienes más importantes de la MPR

BIENES MÁS IMPORTANTES A PROTEGER	AMENAZAS
La red de trabajo interno de la MPR	- Espionaje - Denegación de Servicio - El secuestro de sesiones - Intercepción de comunicaciones - Intrusiones - Ingeniería social - Puertas traseras
Bases de datos del todos los Sistemas de Información **(SIAF, SIAF-RENTAS, SIMI, SOFT_REGISTRO CIVIL)**	- Perdida de información indispensable y confidencial de la institución. - Alteración de los datos almacenados. - Inyección por SQL - Malware
Base de datos del Portal web Institucional	- Acceso a la base de datos y el robo de información de la institución. - La alteración de código del portal web con el fin de cambiar lo que ven los usuarios. - Inyección por SQL
Servicio de correo Corporativo	- Eliminación de correos enviados y recibidos. - Acceso a las claves de los distintos sistemas estatales con las que cuentan los funcionarios.

Fuente: *Elaboración propia*

POLÍTICAS DE SEGURIDAD INFORMÁTICA

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.

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 06: 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. • 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.

1. 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 correctamente cerradas. Aquellas donde se maneje información clasificada, los trabajadores de estas áreas deberán extremar las medidas de seguridad.
- Se deberá tener un control adecuado de los mobiliarios con las que cuentan las distintas oficinas donde se encuentran alojadas las tecnologías instaladas, previniendo que estas se encuentren deterioradas o sin medidas de protección adecuadas (puertas sin candado, estantes en mal estado, etc.)
- Todo visitante debe tener una justificación razonable para tener acceso a la SGTI y a las distintas áreas administrativas de la municipalidad.
- 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 medidas de protección en caso de ocurrencia de algún siniestro tales como incendios, terremotos, tormentas eléctricas, entre otras, para poder controlarlas en caso llegarán a ocurrir.
- Se deberán llevar a cabo simulacros periódicos que permitan a todo el personal de la institución estar capacitado frente a la ocurrencia de algún evento natural o provocado, el cual debe ser coordinado y dirigido por el comité de seguridad de la información.
- Cuando suscite algún incidente (robo, extravío, daño físico, etc.) que afecte de manera directa a un equipo tecnológico da la Municipalidad Provincial de Requena se deberá reportar de forma inmediata a la Sub gerencia de Tecnología de la Información.

- El personal de la SGTI deberá mantener un comportamiento ético y moral adecuado, orientado al cuidado de los bienes tecnológicos y la información de la institución.
- El personal deberá tener especial cuidado con la infraestructura red instalada en las diferentes oficinas de la municipalidad (switches, cableado estructurado, conectores, supresores, etc.).
- Las áreas con tecnologías instaladas deben contar con las señaléticas de seguridad correspondientes según 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 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 en coordinación con el personal de la SGTI. 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.

- Para el personal que haga uso de los sistemas de información estará prohibido alterar o modificar la configuración de las mismas, sin la correspondiente autorización del responsable de la SGTI.

- Deberán quedar correctamente apagados todas las computadoras al concluir la jornada laboral, salvo que por necesidades de trabajo continuo 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.

- La SGTI, es la encargada de validar y realizar las configuraciones a los equipos informáticos; para su posterior distribución a las distintas áreas de la municipalidad.

- El personal de la SGTI, es la única encargada de dar soporte y mantenimiento a los equipos informáticos de las distintas áreas administrativas.

c) A los soportes de información.

- 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 como memorias flash que se usa en la institución.
- Queda prohibido el uso de memorias flash, discos duros externos, y otros dispositivos de almacenamiento en las áreas donde se cuente con información confidencial, quedando a disposición del área de recursos humanos la transgresión de la medidas administrativas o judiciales.

2. 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.
- Las cuentas y claves de acceso de los servicios de internet y correo institucional son personales y confidenciales y se rigen por las políticas de contraseñas definidas en esta propuesta, para evitar el acceso a personas no autorizadas.
- Para el trabajo con los servicios de Correo institucional 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.
- En caso de que el usuario crea que su contraseña ha sido descubierta o no lo recuerda deberá informar lo más pronto posible a la SGTI, para la asignación de una contraseña temporal y hasta que se resuelva su caso.
- El personal tiene la obligación de usar los servicios informáticos exclusivamente con fines institucionales.

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.

- 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.

c) 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.
- Solo el personal que forman parte del comité de seguridad de tecnologías de la información a través de la SGTI puede realizar o aprobar un cambio de emergencia de los activos informáticos. Dicho cambio debe ser documentado y aprobado en un periodo máximo de 24 horas luego de haberse producido el cambio.

d) Integridad de los ficheros y datos.

- Los usuarios notificarán a 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.
- El acceso a todo tipo de datos en todas las computadoras está restringido en dependencia de los permisos que tiene asignado cada usuario.

- Las contraseñas de los usuarios son almacenadas de forma encriptada y deben cambiarse con periodicidad (al menos cada 6 meses).

- La SGTI debe implementar un Firewall (Protección de los sistemas y redes).
- Las computadoras deben contar con un Antivirus actualizados.

- El 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.

e) programas malignos

- El servicio de protección de antivirus debe estar siempre actualizado y controlado por la SGTI al igual que en todas las estaciones de trabajo de trabajo de las áreas administrativas.

- Es obligatorio la desinfección de los dispositivos externos antes de su uso en las estaciones de trabajo**,** se debe tener en cuenta que el uso de los dispositivos informáticos solo debe ser utilizadas por 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.

- Se prohíbe el acceso, descarga o transmisión de material cuyo origen no sea constatado como seguro o de aquél que se desconozca su confiabilidad.

- El personal de SGTI es responsable de comprobar la correcta actualización del Software Antivirus instalado en el ordenador a su cargo.

- El personal de la SGTI, será la encargada de efectuar la descontaminación de los ordenadores ante la aparición de programas malignos.

f) Respaldo de información

- El comité de seguridad de la información debe establecer una periodicidad de cada tipo de backup.
- La SGTI debe respaldar la Información de movimiento entre los períodos que no se sacan Backups (backups incrementales).
- La SGTI debe contar de manera obligatoria con un formulario estándar para el registro y control de los Backups.
- Debe existir correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la institución, y los backups efectuados.
- El almacenamiento de los Backups debe ser en condiciones ambientales óptimas, dependiendo del medio magnético empleado.
- Se debe reemplazar los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).
- El almacenamiento de los Backups debe ser en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzó todo el edificio o local estudiado).
- Se debe realizar pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

g) 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.
- Ante cualquier anomalía que se detecte, investigar las causas y determinar si se está ante algún incidente de seguridad.

Plan de Contingencia

Es de vital importancia ya que se establece con el fin de garantizar la continuidad de los servicios ante cualquier desastre que pueda ocurrir previo a la implementación del plan de seguridad. Por tal Motivo se plantean estas medidas, de acuerdo al resultado del análisis de riesgos realizado anteriormente:

Tabla 07: Plan de Contingencia – 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 CONTINGENCIA**
	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 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 08: Plan de Contingencia - 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 CONTINGENCIA**
	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 09: Plan de Contingencia - 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 CONTINGENCIA**
	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 10: Plan de Contingencia - 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 CONTINGENCIA**
	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 11: Plan de Contingencia - Robo de datos

5. ROBO DE DATOS	**Objetivo:** Proteger la información relevante y confidencial de la institución.
QUE HACER:	**EJECUTAR EL PLAN DE CONTINGENCIA**
	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 12: Plan de Contingencia - 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 CONTINGENCIA**
	Actividades
DURANTE EL DÍA	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 13: Plan de Contingencia - 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 CONTINGENCIA**
	Actividades
DURANTE EL DÍA	1. Se deberá de realizar un análisis exhaustivo con el antivirus ENDPOINT para verificar la existencia de programas espías. 2. Identificación de los responsables. 3. Tomar medidas correctivas contra el personal involucrados (Administrativas y/o judiciales)
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 14: Plan de Contingencia - 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 CONTINGENCIA**
	Actividades
DURANTE EL DÍA	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 15: Plan de Contingencia - 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 CONTINGENCIA**
	Actividades
DURANTE EL DÍA	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 16: Plan de Contingencia - Terremoto

10. TERREMOTO	**Objetivo:** Proteger los bienes informáticos en caso de Suscitar un evento Sísmico
QUE HACER:	**EJECUTAR EL PLAN DE CONTINGENCIA**
	Actividades
DURANTE EL DÍA	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*

Después de ocurrido la contingencia es necesario realizar las actividades como:

Evaluación de daños

Después de la contingencia, 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.
La evaluación de daños, 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 enmarcadas en las políticas establecidas, deberán ser realizadas por los equipos operativos pre establecidos por el comité de gestión de la seguridad de la información. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar el avance de los trabajos de recuperación además de cualquier incidente que retrase las actividades de los planes posteriores a la emergencia.
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 que brinda la SGTI y las oficinas administrativas de la municipalidad provincial de Requena.

Evaluación y resultados

Una vez concluida las labores de recuperación posteriores a la contingencia, se realizará una evaluación de los resultados del plan de contingencia las mismas que nos servirán para aplicar mejoras al plan de seguridad informática y fortalecer las políticas de seguridad hasta dejar de lado el plan de contingencia.

Retroalimentación del plan de seguridad informática

De la evaluación de los resultados se deberá obtener dos conclusiones:

- La retroalimentación del plan de seguridad informática y
- La implementación de nuevas políticas de seguridad que nos ayuden a prevenir que vuelva a ocurrir alguna emergencia.

En conclusión, se deberá optimizar el plan de seguridad original, mejorando constantemente las políticas de seguridad propuestas.

CAPÍTULO IV

Resultados

- ✓ Se logro realizar una evaluación a la SGTI donde se pudo determinar que no existe un plan de seguridad informática.

- ✓ Se logró realizar la propuesta del plan de seguridad informática para la Sub Gerencia de Tecnologías de Información (SGTI), de la municipalidad de Provincial de Requena.

- ✓ Se logró establecer políticas y procedimientos de acuerdo al análisis de riesgo realizado y a las normas peruanas, esperando que sea revisado por la institución para que en un futuro con algunas mejoras que se pueda hacer al plan de seguridad implementarla en la municipalidad provincial de Requena, en beneficio del resguardo de la información.

- ✓ Se logro hacer la propuesta del plan de seguridad Informática.

CAPÍTULO V

Discusión

El propósito del presente trabajo fue elaborar un plan de seguridad informática que tenga como propósito prevenir y salvaguardar la información de la municipalidad provincial de Requena, empleando nuevas formas de análisis de riesgo y teniendo en cuenta las propiedades de protección de seguridad de la información establecidos en la norma internacional del ISO 27001 para las organizaciones, que son la disponibilidad, confiabilidad e integridad de la información.

Todo el presente trabajo se llevó a cabo empezando por un análisis de los riesgos al que está expuesto actualmente los ambientes, la infraestructura tecnológica y por ende la información de la municipalidad, los cuales fueron tomados como prioridad para el establecimiento de las políticas de seguridad de acuerdo a lo que establece las normas técnicas peruanas “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, la ley Orgánica de Municipalidades LEY N.º 27972 y la Resolución Ministerial N. º 004-2016-PCM, que Aprueba el uso obligatorio de la Norma Técnica Peruana “NTP ISO/IEC 27001:2014 Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de Seguridad de la Información. Requisitos. 2a. Edición”, en todas las entidades integrantes del Sistema Nacional de Informática.

Tomando en cuenta las investigaciones anteriores y el análisis exhaustivos de las referencias teóricas y conceptuales que nos sirvió como un esquema general para llevar a cabo el presente plan de seguridad, el mismo que recomendamos someter a evaluación de su efectividad y por qué no implementar como parte de su protección de la institución por factores tales como seguridad lógica, seguridad en las comunicaciones, seguridad en las aplicaciones, seguridad física, administración del centro de procesamiento de datos, auditorías y revisiones y plan de contingencia.

El presente plan de seguridad, está estrictamente acogido la realidad actual de la entidad municipal, comprende detalles exhaustivos y análisis crítico de la situación, así como plantea soluciones más adaptadas a su realidad teniendo en cuenta la disponibilidad presupuestal que esta posee y el nivel de entrenamiento de los funcionarios.

CAPÍTULO VI

Conclusiones

Las áreas más vulnerables dentro de la institución son aquellas donde se genera el flujo económico y/ presupuestal de la entidad, teniendo en cuenta que en ellas están instaladas los principales sistemas informáticos con las que se gestiona la entidad Municipal (Gerencia de Rentas, Gerencia de Presupuesto, Gerencia de Administración), es así que partiendo de estos indicadores se procedió a realizar el diagnóstico situacional de la infraestructura informática, encontrando deficiencias en nivel de software y hardware, graves vulnerabilidades que atentan contra el correcto funcionamiento de los dispositivos y de las áreas como tal.

Se llego a plantear medidas de seguridad a través de un análisis de riesgo determinando las prioridades de la protección a equipos, según sus vulnerabilidades para poder garantizar la protección y manejo de información dentro de la entidad, manteniendo la confidencialidad, integridad, y disponibilidad de la información en la entidad Municipal.

Se formuló un plan de acción y emergencia, que engloba procedimientos y responsables para el accionar en caso de suscitarse un hecho que atente en contra de la seguridad de la infraestructura tecnología de la entidad.

Se planteó recomendaciones para la adquisición de bienes (servidor de archivos, software Protección perimetral) que nos ayudaran a salvaguardar la información y la protección de los activos informáticos.

Finalmente podemos concluir que el presente trabajo de investigación fue satisfactorio, puesto que nos permitió conocer las deficiencias que posee la municipalidad provincial de Requena y frente a ello poder presentar propuestas de mejora para contrarrestar dicha problemática.

Recomendaciones:

- Es de carácter primordial capacitar al personal de la SGTI para que, puedan mantener el correcto funcionamiento de la infraestructura y los servicios que brinda la oficina y no existan inconvenientes en el uso de las aplicaciones de trabajo cotidiano.

- Capacitar al personal que labora en la institución, sobre el adecuado uso de los recursos informáticos, promoviendo talleres de Alfabetización digital y la utilización de las nuevas tecnologías.

- Proponer que estas políticas formen parte del Reglamento de Organización y funciones (ROF) de la Municipalidad provincial de Requena.

- Recomendamos además la implementación en una primera etapa, de nuevas infraestructuras necesarias y consideradas de inmediata atención, que son los de alojamiento de información y de seguridad, debidamente licenciados. Para garantizar su correcto funcionamiento, por lo que recomendamos:

  a) **Adquisición de un servidor de archivos.**
  Un servidor de archivos que será de mucha urgencia puesto que actualmente no se cuenta con uno, razón de la constante pérdida de información relevante en la institución, se propone la adquisición de un servidor de archivos que incluye un sistema operativo y antivirus descrito en el anexo **N.º 05**.

  b) **Adquisición de licencias de un sistema de seguridad antimalware que incluya contención, veredicto de malware en la nube, herramientas de administración de ti y mesa de ayuda.**
  Contar con un sistema de seguridad antimalware que incluya contención, veredicto de malware en la nube, herramientas de administración de TI y mesa de ayuda, que asegure la protección de los equipos de cómputo, servidores y dispositivos móviles para que disminuya el riesgo de vulnerabilidades que pueda tener la infraestructura de la red causada por malware. De esta manera, evitar que los servicios y funciones que se presta a todos los usuarios no se vea afectados. Asimismo, el sistema debe contar con una plataforma de veredicto en la nube que permita recibir muestras del malware enviadas por el sistema de

contención para la actualización de las mejoras heurísticas y se eliminen malware del día cero.

También, el sistema debe incluir herramientas de administración de TI que permita tener el control de aplicaciones, control de dispositivos, control de acceso remoto, inventario de hardware, inventario de software, instalación de aplicaciones de forma masiva, control de recursos de hardware, sistemas de alertas y eventos, control de cuentas de usuarios, entre otras funciones y permita realizar el mantenimiento de pc y servidores de forma remota y centralizada. Por último, debe incluir un sistema de mesa de ayuda (generación de tickets atención e incidencias) que permita tener documentado el servicio del soporte técnico brindado por la oficina de informática y el personal de soporte técnico con la finalidad de mejorar los servicios que la oficina de informática presta a los usuarios de la organización.
Se detalla su cotización en el **anexo N.º 05**

Se describe a continuación el costo total de la implementación primordial de estos servicios en el **Anexo N.º 06.**

Recalcando nuevamente que son soluciones primordiales para la institución.

- Se recomienda, realizar la reestructuración de toda la infraestructura de red.
- Realizar periódicamente simulacros de Desastres Naturales, Inundación, incendio y sismos, para que se sepa cómo actuar en caso de suscitar alguno de estos eventos.
- Se recomienda licenciar las aplicaciones que son de usos administrativos.
- Se recomienda la instalación de un sistema de pozo a tierra, para contrarrestar las descargas eléctricas que puedan quemar los equipos de la Institución.
- Se recomienda la implementación del certificado digital de seguridad del portal web institucional (Protocolo SSL).

Referencias Bibliográficas:

Bibliografía

- Aguilera Lopez, P. (2010). *Seguridad Informatica.* Editorial Editex.
- GÓMEZ VIEITES, A. (2011). *ENCICLOPEDIA DE LA SEGURIDAD INFORMATICA. 2ª EDICION ACTUALIZADA.* Madrid: RA-MA EDITORIAL.
- Laudon , K. C., & Laudon , J. P. (2012). *SIstemas de Información Gerencial* . Mexico: Pearson Educación.
- Alfaro Viana, I. A., & Vargas León, E. (2016). *DISEÑO DEL PLAN DE SEGURIDAD INFORMÁTICA DEL SISTEMA DE INFORMACIÓN MISIONAL DE LA PROCURADURÍA DE LA NACIÓN.* Bogotá: Universidad Piloto de Colombia.
- Baca Urbina, G. (2016). *Introducción a la Seguridad Informatica.* Grupo Editorial Patria.
- Coqueña, E. W. (2018). *Plan de Seguridad Informática en la Municipalidad provincial de San Roman (Sistema Web).* juliaca - Perú: Universidad Andina Nestor Caceres Velasquez.
- PCM. (2016). *Norma Tecnica Peruana "NTP ISO/IEC 27001: 2014 Tecnologia de la Información. Tecnicas de Seguridad. Sistema de Gestión de Seguridad de la Información. Requisitos.2aEdición ".* Lima.
- SISTEMAS, S. G. (2016). *Plan de Contingencia y Seguridad de la Información* . Sicuani - Perú: Municipalidad Provincial de Chanchis.
- Rodríguez Ruiz, S. (24 de junio de 2019). Obtenido de mas adelante: https://www.masadelante.com

ANEXOS

ANEXO N.º 01

Tabla 17: Características del sistema informático

SUB – GERENCIA DE TECNOLOGÍA DE LA INFORMACIÓN		
RECURSOS HUMANOS		
N.°	**CARGOS**	**CANTIDAD**
01	Director de Sistemas Administrativos I	01
02	Operador PAD II	01
N.°	SOFTWARE	CANTIDAD
SISTEMAS OPERATIVOS		
01	Linux Centos 6.x	02
02	Windows XP	02
03	Windows 7	60
04	Windows 8	10
05	Windows 10	04
MOTORES DE BASE DE DATOS		
08	MySQL 5.0	01
HERRAMIENTAS DE DESARROLLO		
10	Visual Fox Pro	03
11	Visual Studio 6	01
DE OFICINA		
12	MS Office 2000	0
13	MS Office 2010	60
14	MS Office 2010 STR	0
15	MS Office 2013	12
17	Open Office 3.x	0
ANTIVIRUS		
18	ESET NOD 32 VERSION 6	35
HARDWARE		**CANTIDAD**
SERVIDORES		
01	System x3400 M3	01
COMPUTADORAS PERSONALES		
02	Core 2 duo	01
03	Core i3	10
04	Core i5	60
05	Core i7	01
06	Intel Atom	0
07	Pentium D	0
08	PIV/Celeron/CeleronD/Quad Core/ Dual Core	01
IMPRESORAS		
10	Impresora de Tinta	02
11	Impresora Láser de Red	24
12	Impresora Láser Personal	14
13	Impresora Matricial	02
SCANNER		
15	Scanner alimentador Automático de Hojas	1
16	Scanner Cama Plana	0
N.°	**CONECTIVIDAD**	**CANTIDAD**
SWITCHES		
01	Switch 08 Puertos	03
02	Switch 16 Puertos	0
03	Switch 24 Puertos	05
04	Switch 48 Puertos	0
WIRELES		
07	Acces Point	02

Fuente: *POI 2018-MPR-SGTI*

ANEXO N.º 02

Sistemas de Información

Tabla 18: Características de los sistemas de información

NOMBRE DEL SISTEMA	CARACTERISTICAS	UBICACIÓN DEL SISTEMA	UNIDADES QUE USAN EL SISTEMA
SIAF	El sistema de Integración de Administración Financiera, realiza el registro de las operaciones de gastos, ingresos y otras complementarias, estos son procesados, permitiendo la obtención de los estados financieros y presupuestales.	Sub Gerencia de Contabilidad y Finanzas (Segundo Piso) En equipo portátil LAPTOP, que a su vez hace de servidor.	- Sub Gerencia de Contabilidad y Finanzas - Gerencia de Planeamiento Presupuesto y Racionalización - Sub Gerencia de Logística y Control Patrimonial - Sub Gerencia de Tesorería - Jefatura de Almacén
SAT-RENTAS	Es un sistema de administración de pagos de los tributos Municipales, que posee módulos como: Impuesto predial, cuentas corrientes, limpieza pública, cobranza coactiva.	Gerencia de Rentas (Primer Piso) CPU, que a su vez hace de servidor	- Gerencia de Rentas - Sub Gerencia de Recaudación y Fiscalización Tributaria.
SIMI v1 SISTEMA DE CONTROL PATRIMONIAL	Permite registrar operaciones de la oficina de control, patrimonial: inventarios de todos los bienes de la institución.	Sub Gerencia de Logística y Control Patrimonial (Segundo Piso) CPU, que a su vez hace de servidor	- Jefatura de Control Patrimonial
SISTEMA DE PLANILLAS	Permite definir y procesar diferentes tipos de planillas de los empleados en la sub gerencia de RR. HH por mes, permite la transferencia de información a PDT SUNAT y permite realizar reportes	Sub Gerencia de Recursos Humanos (Primer Piso) CPU, que a su vez hace de servidor	- Sub Gerencia de Recursos Humanos
SISTEMA DE CONTROL DE ASISTENCIA (BIOMETRICO)	Sistema de control de personal, que permite registrar los ingresos y salidas de Personal mediante control biométrico.	Sub Gerencia de Recursos Humanos (Primer Piso) CPU, que a su vez hace de servidor	- Sub Gerencia de Recursos Humanos
R-SOFT SISTEMA DE REGISTRO CIVIL	Permite escanear, procesar e imprimir actas de nacimiento, matrimonio y defunción. Es un sistema automatizado para procesos informáticos de la Subgerencia de Registro Civil. Este sistema fue instalado por terceros, y es la misma quien brinda el soporte técnico.	Sub Gerencia de Registro Civil (Primer piso) CPU, que a su vez hace de servidor.	- Sub gerencia de Registro Civil.
RUBEN	Permite registrar, procesar, consolidar, importar, exportar y consultar información de los BENEFICIARIOS(AS) de los programas sociales, validando los datos a diferentes niveles.	Sub Gerencia de Programas Sociales (Sede alterna) CPU, que a su vez hace de servidor	- Sub Gerencia de Programas Sociales - Gerencia de Programa y Servicio de Protección Social

Fuente: *Elaboración propia*

ANEXO N.º 03

Ilustración 02: Ficha de Observación

FICHA DE OBSERVACIÓN

DATOS DE LA APLICACION

Nombre de Institución	:	Municipalidad Provincial de Requena
Oficina	:	Sub Gerencia de Tecnologías de Información
Fecha	:	23/04/2019
Funcionario a Cargo	:	Janan Cesar Candamo García **Sub Gerente de Tecnología de la Información**
Encargados de la Aplicación	:	Paulo Manuel Rengifo Saquiray Dennis Alberto Vasquez Gutierrez

Documentos de Gestión Revisados:

DOCUMENTOS	Tiene		Se reviso	
	Si	No	Si	No
Plan estratégico Institucional (PEI)	X		X	
Manual de Organización y Funciones (MOF)	X		X	
Plan Operativo Informático (POI)	X		X	
Reglamento de Organización y funciones (ROF)	X		X	
Inventario de Equipos Informáticos	X		X	
Inventario de Usuarios con acceso a red		X		X

MUNICIPALIDAD PROVINCIAL REQUENA V°B° Sub Gerencia de Tecnología de la Información

Infraestructuras físicas Observadas:

Infraestructura Física	Estado		
	Bueno	Malo	Regular
Cableado estructurado y equipos de comunicaciones			X
Ambientes de la Municipalidad Provincial de Requena			X
Herramientas de la SGTI		X	
Estado de los equipos computacionales			X

Fuente: *Elaboración propia*

Anexo N.º 04

Adquisición De Servidor De Archivos, Incluye Sistema Operativo Y Antivirus Server

Tabla 19: Presupuesto del servidor

CANT	DESCRIPCIÓN	P. UNIT. S/.	P. TOTAL S/.
01	Servidor Lenovo ThinkSystem TS150, Intel Xeon E3-1245 v6 3.7 GHz, 8GB DDR4, 2TB SATA.	3870.00	3870.00
01	Sistema operativo solución Microsoft Windows server 2016 standard	3150.00	3150.00
01	Antivirus Eset File Server, 1 Server, Seguridad completa para servidor de archivos Windows	220.00	220.00
	TOTAL	**7240.00**	**7240.00**
DATOS DE LA EMPRESA:			
INGENIERIA DE LA INFORMATICA S.A - INFORDATA S.A.			
RUC: 20102188293			
CCI: Banco Continental S/. N.º 011-147-000100005794-61			

fuente: *Elaboración propia*

ANEXO N.º 05

Tabla 20: Cotización Sistema de Seguridad Antimalware

<table>
<tr><th colspan="5">COTIZACIÓN</th></tr>
<tr><td colspan="5">SISTEMA DE SEGURIDAD ANTIMALWARE</td></tr>
<tr><th>Periodo de licenciamiento</th><th>Calidad de licencias</th><th>Producto</th><th>Precio Unitario</th><th>Total 1 año</th></tr>
<tr><td rowspan="2">1 año</td><td rowspan="2">50</td><td rowspan="3">COMODO ONE Seguridad más Gestión de TI y Mesa de Ayuda (2019)</td><td>S/ 75.00</td><td>S/ 3,750.00</td></tr>
<tr><td>SUBTOTAL</td><td>S/ 3,750.00</td></tr>
<tr><td colspan="2">Cotización valida por 30 días</td><td>I.G.V. 18%</td><td>S/ 675.00</td></tr>
<tr><td colspan="2">Forma de Pago 7 días</td><td></td><td>TOTAL</td><td>S/ 4,425.00</td></tr>
<tr><td colspan="5">DATOS DE LA EMPRESA</td></tr>
<tr><td colspan="5">Empresa: INFORLAND PERU SAC
RUC: 20604676488
Dirección: Calle San Martin de Porres Nro. 150 dpto. 1503 (Módulo 3, Torre 2) Urb. Miramar-San Miguel
Correo: ventas@inforlandperu.com
Teléfonos: 511-763-7007 / 51-988888594</td></tr>
</table>

Fuente: *Inforland Perú SAC.*

ANEXO N.º 06

Tabla 21: Presupuesto de adquisición de equipos recomendados

Descripción de Solución	Costo
Adquisición de servidor de archivos, incluye sistema operativo y antivirus server	**4,425.00**
Adquisición de licencias de un sistema de seguridad antimalware que incluya contención, veredicto de malware en la nube, herramientas de administración de ti y mesa de ayuda.	**7,240.00**
Costo total de la propuesta	**11,665.00**

Fuente: *Elaboración propia*

ANEXO N.º 07

Evidencia Fotográfica

Ilustración 03: Palacio Municipal

Fuente: *Elaboración propia*

Ilustración 04: Sub Gerencia de TI

Fuente: *Elaboración propia*