UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Propuesta de guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC en la seguridad de la información de la Municipalidad Provincial de Recuay - 2015

Tesis para obtener el título profesional de ingeniero en informática y de sistemas

Autores

Javier Macedo Elizabeth Haydee

Luna Castillo Henry Wiley

Asesor

Ascón Valdivia Oscar Arquímedes

Huaraz – Perú

2019

PALABRAS CLAVE

Tema	Seguridad de la información
Especialidad	Informática

KEYWORDS

Theme	Information Security
Specialty	Informatics

LÍNEA DE INVESTIGACIÓN

Área	Ingeniería y Tecnología
Sub Área	Ingeniería eléctrica, electrónica e informática
Disciplina	Ingeniería de Sistemas y Comunicación

TÍTULO

Propuesta de guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC en la seguridad de la información de la Municipalidad Provincial de Recuay - 2015

RESUMEN

La presente investigación tuvo como objetivo general proponer una Guía Metodológica basada en ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014 para la seguridad de la información en la Municipalidad Provincial de Recuay.

La investigación fue del tipo no experimental descriptivo porque se describieron los aportes de las normas estudiadas a la seguridad de la información de la municipalidad. La población de estudio estuvo conformada por 48 servidores públicos que utilizan el sistema de información y a la vez procesan información en Municipalidad Provincial de Recuay, y la muestra por 20 servidores públicos, para el desarrollo del presente informe se utilizó la Norma ISO/IEC 27001:2013 Y NTP ISO/IEC 27001:2014

La investigación concluyó que el estado en que se encontró la seguridad de la información además de los riesgos, vulnerabilidades y formas de prevención en la Municipalidad Provincial de Recuay fue porcentualmente bueno y que las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración de la información fue mayormente buena

ABSTRACT

The present research had as general objective to propose a Methodological Guide based on ISO / IEC 27001: 2013, NTP ISO / IEC 27001: 2014 for the security of the information in the Municipality of Recuay.

The research was of the non - experimental descriptive type because the contributions of the norms studied to the information security of the municipality were described. The study population consisted of 48 employees who use the information system and at the same time process information in Municipality of Recuay, and the sample by 20 employees, for the development of this report, was used the standard ISO/IEC 27001:2013 Y NTP ISO/IEC 27001:2014

The investigation concluded that the state in which the security of information, information, risks, vulnerabilities and forms of prevention has, been seen in the Provincial Municipality of Recuay, as well as those of the norm, NTP ISO / IEC 27001: 2014 in structuring the information was mostly good

INDICE

PALABRA CLAVE	i
TITULO	ii
RESUMEN	iii
ABSTRACT	iv
1. INTRODUCCION	1
2. METODOLOGÍA DE TRABAJO	29
3. RESULTADOS	60
4. ANALISIS Y DISCUSION	81
5. CONCLUSIONES Y RECOMENDACIONES	85
6. AGRADECIMIENTO	86
7. REFERENCIAS BIBLIOGRAFICAS	87
8. ANEXOS	90

1. INTRODUCCIÓN

De los antecedentes más significativos de la presente investigación.

Rayme (2007), realizó una investigación en tres Universidades de Lima Metropolitana: la Universidad Nacional Mayor de San Marcos (UNMSM), la Universidad Nacional Federico Villarreal (UNFV) y la Universidad Privada San Juan Bautista (UPSJB), teniendo como objetivo proponer estrategias de Gestión de Seguridad de la Información y sus implicancias en la calidad y eficacia en los servicios críticos de las universidades. El estudio reveló que las estrategias que se deben utilizar en la gestión de seguridad de la información son: primero, la importancia de desarrollar políticas de seguridad: UNMSM 37 %, UNFV 19% y UPSJB 24%; segundo, los programas de capacitación al personal, donde los expertos consultados informaron el interés por asistir: UNMSM 60%, UNFV 70% y UPSJB 70% y tercero, la protección a los recursos de información.

El Ministerio de la Protección Social COLCIENCIAS (2010). Elaboró una Guía Metodológica para la elaboración de Guías de Atención Integral en el Sistema General de Seguridad Social en Salud colombiano. ISBN: 978-958-8361-81-9. Bogotá, Colombia. Concluyó que la Guía Metodológica para la elaboración de Guía de Atención Integral en el Sistema General de Seguridad Social en Salud colombiano, sintetiza, analiza y estructura en pasos organizados, las metodologías internacionales para el desarrollo, adaptación y evaluación de GPC y para la realización de estudios de evaluación económica en salud aplicables para Colombia. También estableció pautas metodológicas precisas para adelantar estudios del impacto en el presupuesto, en este caso, en la Unidad de Pago por Capitación UPC, para las tecnologías en salud que se consideraron ser incluidas el Plan Obligatorio de Salud POS.

Flores & Arellano (2012), en su tesis “Guía metodológica para la implementación de un Sistema Integrado de Gestión en la empresa Cortiplast S. A.” realizada en la Universidad Politécnica Salesiana de Guayaquil. Ecuador; el objetivo general fue proponer una Guía metodológica para la implementación de un Sistema Integrado de

Gestión de la Calidad, Ambiente y Seguridad para la empresa Cortiplast S. A. basado en la integración de las normas ISO 9001, ISO 14001 y OHSAS 18001. Concluyó que la elaboración de la guía permitió crear sinergias en los procesos de formación con la mayoría del personal, conocer las herramientas que se utilizan para las mediciones de los procesos. El personal y la organización sienten un vínculo del SGI con la estrategia de la empresa. La gerencia reconoce que la mejora de la calidad de sus productos debe ir de la mano con la gestión en seguridad laboral y ambiental. Los colaboradores, hacen conciencia que su aporte en seguridad laboral y ambiental es importante para el desarrollo de la organización en la que trabajan. Realizar una evaluación inicial de la situación de algunos procesos dentro de la empresa, en base a las normas ISO 9001, ISO 14001 y OHSAS 18001. Crear un equipo de trabajo y que la organización se plantee objetivos. Que la gerencia reconozca su involucramiento y compromiso en los procesos de la organización.

Merizalde & Alvarado (2013), en su tesis "Propuesta de Guía Metodológica de un Sistema Integrado de Gestión - basado en ISO 9001, ISO 14001 y OHSAS 18001- para Airful International S.A.", realizada en la Universidad Politécnica Salesiana Sede Guayaquil. Ecuador; tuvo como objetivo general desarrollar una Guía Metodológica para la implementación del Sistema Integrado de Gestión, basado en ISO 9001, ISO 14001 y OHSAS 18001 para la compañía Airfuel International S.A. que permita proveer servicios de mejor calidad, ser responsable con el ambiente, optimizar recursos, proteger la salud de los trabajadores, cumplir aspectos legales y reglamentarios. Concluyó que los resultados de las evaluaciones a todo el personal presentaron total desconocimiento de las normas ISO 9001, ISO 14001 y OHSAS 18001 de todo el personal, que el Manual Integrado de Calidad que nos ayudará como propuesta a direccionar a la empresa al cumplimiento total de todos los requisitos y a su vez a la implementación de los Sistemas Integrados de Gestión.

La presente investigación se fundamenta en las teorías de la seguridad de la Información, teoría de redes, teoría de las telecomunicaciones, principios de la ingeniería de software. La propuesta de la Guía Metodológica se fundamenta en el uso de las normas internacionales ISO/IEC 27001:2013 y en la norma peruana NTP ISO/IEC 27001:2014.

La Investigación es relevante socialmente porque**,** desde la perspectiva de que la información es un activo, que al igual que los demás, tiene valor para la institución y por lo tanto necesita ser protegida adecuadamente, y contribuye decididamente en la economía de la municipalidad, los servidores públicos, Los vecinos, los trabajadores, la Municipalidad Provincial de Recuay, sus autoridades y la sociedad en su conjunto se verán beneficiados con la implementación de una Guía Metodológica de evaluación de la seguridad de la información, debido a que la seguridad es un bien muy preciado porque brinda a las autoridades y a los vecinos la seguridad física, psicológica, económica y social que toda sociedad exige para convivir. La implementación de una Guía Metodología va a asegurar la continuidad adecuada evaluación de la seguridad de la información.

Así mismo, aporta Científicamente porque las normas constituyentes de la presente Guía Metodológica van a permitir que se evalúe la seguridad de la información de acuerdo a las normas y leyes internacionales, nacionales, regionales y locales, se asigne a los trabajadores y autoridades de la municipalidad la responsabilidad legal ante el uso y manejo de la información, así como de mecanismo de cómo hacer frente a los riesgos, amenazas y vulnerabilidades de la información. Las normativas asignan responsabilidades, deberes y derechos frente al tratamiento de la seguridad de la información. Se alcanza una Guía Metodológica de evaluación de seguridad de la información basada en ISO/IEC 27001:2013, NTP ISO/IEC 17799:2014, la cual guía los procesos de evaluación de la seguridad de la información y las formas de enfrentar los riesgos, vulnerabilidades y amenazas que pueden afectar a toda información generada en sistemas informáticos.

El problema presentado en la Municipalidad Provincial de Recuay es que Los sistemas de información se han convertido en partes cruciales de las actividades empresariales, gubernamentales, académicas y cotidianas, en estos espacios en donde la información adquiere mayor importancia y requiere del tratamiento adecuado para su aprovechamiento. De allí surge la necesidad de protegerla y asegurarse que sea precisa y confiable. La información es algo intangible, que se concentra dentro de los sistemas de información, la cual puede: almacenarse dentro de archivos de computadoras, transmitirse a través de redes computacionales, registrarse en papel o en cualquier soporte de datos digital para su movilización.

Según Laudon (2004), los datos automatizados (digitales) requieren de seguridad, son más propensos a destrucción, fraude, error o abuso por parte de personas no autorizadas quienes pueden estar fuera o dentro de la institución. Señala que las fallas en la seguridad de un sistema de información o un funcionamiento indebido del mismo, produce en las organizaciones que dependen de ellos, grandes y graves pérdidas de su capacidad de operación. La seguridad informática se refiere, al establecimiento de evaluaciones continuas o periódicas para administrar y controlar que la información se genere, se procese, se registre y utilice en un nivel de seguridad estandarizado de aceptabilidad, que permita asegurar que la información está protegida del acceso de personas no autorizadas, alteración de datos o daños físicos a su plataforma tecnológica.

En la actualidad ninguna organización puede darse el lujo de carecer de mecanismos de seguridad, protección y de evaluación para los sistemas de información, en la actualidad las empresas invierten más dinero que otras en seguridad informática, pero todas necesitan del aseguramiento de sus datos, para garantizar su funcionamiento operacional (Hernando, 2005).

A nivel nacional, las municipalidades provinciales disponen de sistemas de seguridad y personal calificado para contrarrestar las vulnerabilidades y riesgos a los que están expuestos, sin embargo, ellos han sabido afrontar los riesgos y ataques aplicando diversas metodologías de seguridad informática con resultados muy aceptables.

La Municipalidad Provincial de Recuay es una institución gubernamental cuya función es gobernar y administrar las necesidades de los habitantes de su jurisdicción territorial, en ese proceso de atención, genera información muy valiosa tanto de la institución como para los vecinos. Para ello dispone de un sistema informático que presenta los siguientes problemas: Estar propenso a diversos tipos de ataques informáticos externos e internos. Se han encontrado sistemas de cómputo o computadoras infectadas de virus que generan lentitud en el desarrollo de los procesos informáticos para la generación de documentos. Robos de archivos valiosos para la municipalidad y los usuarios de servicios de la municipalidad que han causado pérdidas económicas para ambos. Demora en la atención a los usuarios causando pérdidas de imagen a la municipalidad. Problemas legales y de conflicto social tanto para la municipalidad como para los vecinos. Pérdida de información con la cual la municipalidad distrital podría perder recursos económicos y financieros, así como propiciar la ingobernabilidad dentro de la municipalidad.

Dada esta realidad problemática que pudiera ocurrir si no se toman decisiones respectivas a una adecuada seguridad de la información, la Municipalidad Provincial de Recuay podría vulnerase importantes archivos, robarse información confidencial de la municipalidad, etc., como consecuencia de ellos, la municipalidad podría deteriorar su imagen ante la colectividad que gobierna y ante las autoridades gubernamentales superiores a quien tiene que informar sobre el desarrollo de sus funciones. Ante esta realidad problemática, se propone una guía metodológica de evaluación de la seguridad de la información basada en ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014.

Ante esta realidad problemática, se propone una guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 aplicada a la seguridad de la información en la Municipalidad Provincial de Recuay. La investigación, formula la siguiente interrogante problemática. ¿Cómo proponer una Guía Metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 en la seguridad de la información en la Municipalidad Provincial de Recuay?

Guía Metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014

La Guía Metodológica. Es un instrumento que ha sido diseñado para promover metodologías participativas de trabajo que animen y fomenten que a nivel organizacional las personas se apropien del tema y contribuyan con sus experiencias al proceso de diagnóstico y planificación local (Valdez, 2005).

La guía busca lograr que sean los propios trabajadores o empleados, incluyendo las autoridades que como participantes relevantes contribuyen de forma activa al proceso en vez de sólo recibir pasivamente la información que se va a obtener.
Con esta metodología se fomenta (Valdez, 2005):

- ✓ Que la gente comparta información
- ✓ Que aprendan unos de otros y,
- ✓ Que trabajen juntos para encontrar soluciones comunes.

Los participantes en el proceso de diagnóstico organizacional con perspectiva de derechos, género y ciclo de vida aprenderán a realizarlo como herramienta de apoyo para el desarrollo de las actividades de sus propias organizaciones y comunidades.

Es un proceso de aprendizaje participativo que también proporciona a la gente un marco de habilidades y conocimientos que podrán usar en cualquier situación en la que se encuentren y actuar sobre ella. A medida que cada uno/a vaya adquiriendo más experiencia con las herramientas del diagnóstico participativo, irá tomando más responsabilidades para realizar su propio proceso en función de sus necesidades y posibilidades (Ministerio de la Protección Social – COLCIENCIAS, 2010).

Los **Objetivos de la guía Metodológica**

- ✓ Fomentar las prácticas de buena administración, tales como: transparencia, equidad, democracia y gobernabilidad.
- ✓ Desarrollar las capacidades locales para elaborar diagnósticos con la participación de los diferentes actores y sectores con perspectiva de derechos, género y ciclo de vida.

Es un instrumento que puede servir tanto para realizar un proceso de diagnóstico participativo a nivel municipal como para la capacitación de los diferentes actores para que puedan realizar su propio.

Tal como lo definiremos más adelante se utilizará la **Norma ISO/IEC 27001:2013**

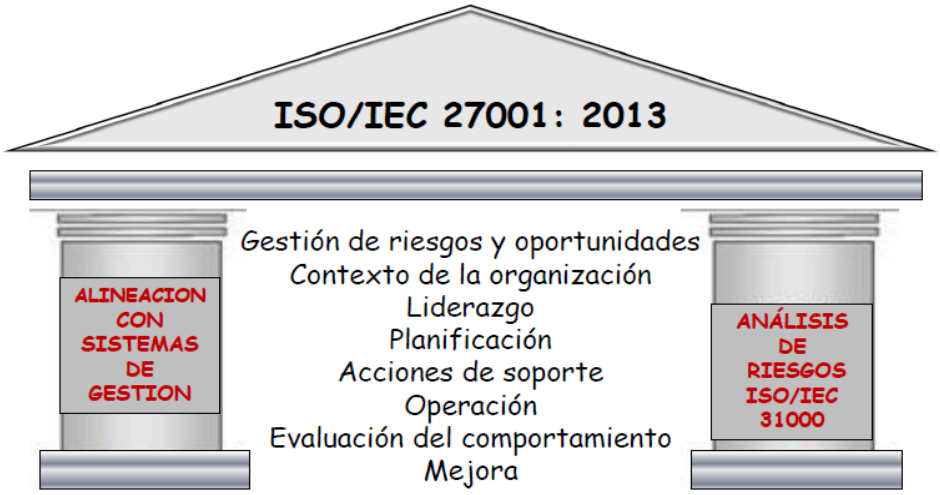


Figura 1. ISO/IEC27001:2013
Fuente: ISO/IEC27001:2013

Ventajas de ISO/IEC 27001:2013

Los beneficios que genera la implementación de la norma ISO/IEC 27001:2013 se pueden resumir en los siguientes puntos:

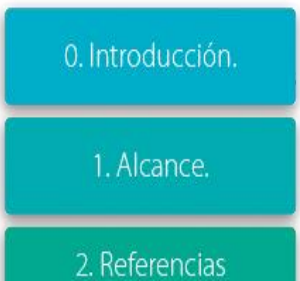
- ✓ En el ámbito de la propia organización, ya que se establece un importante compromiso con la seguridad de la información. Existen diferentes registros y medidas de control que facilitan que la seguridad de la información se encuentre garantizada en la empresa y que todos los esfuerzos realizados puedan demostrarse.
- ✓ En el cumplimiento legal de las exigencias, se manifiesta la conformidad de la organización en el cumplimiento de los requisitos legales que se le aplique la legislación de la región en la que se encuentra ubicada la organización y la actividad que realice.
- ✓ Se desarrolla una adecuada gestión de riesgos. La empresa conoce a la perfección su organización y los Sistemas de Información que aplican, los problemas que se encuentran y las medias de protección que le son aplicados, además deben terminar garantizando la mejor disponibilidad de los materiales y los datos, y asegurando la continuidad sin alteraciones que no han sido controladas.
- ✓ En el aspecto comercial, se genera credibilidad y confianza entre todos los clientes de la organización. Se debe tener presente que nos encontramos en una sociedad

en la que falta confianza de los clientes afecta a nuestras ventas de la misma forma que la calidad y la funcionalidad de los productos, por lo que se debe cuidar los dos aspectos.

- ✓ En el mundo financiero, las empresas tienen que conseguir una disminución de los costes vinculados a los diferentes incidentes y se consigue minimizar las primas de los seguros que tienen contratados.
- ✓ En cuanto a los humanos, se genera una sensibilización del personal en relación con la importancia de la correcta manipulación de la información, a la aplicación adecuada de todas las medidas de seguridad que se tiene que adoptar por parte de la organización y la responsabilidad del personal y de la organización con relación a la información que la que disponen y por supuesto, no nos podemos olvidar de los dueños de la información.

En la implementación de un Sistema de Gestión de Seguridad de la Información basado en la ISO/IEC 27001:2013 se puede beneficiarla organización en todas las ventajas indicadas, se deben adaptar de forma adecuada a todas las necesidades que tenga su organización y que se le deben aportar todas las ventajas que se deriven de una correcta implementación de la norma ISO/IEC 27001:2013.

Estructura de ISO/IEC 27001:2013, ha sido desarrollado con base en el anexo SL de ISO/IEC del "Suplemento Consolidado de las Directivas ISO/IEC", en el cual se proporciona un formato y un conjunto de lineamientos a seguir para el desarrollo documental de un sistema de gestión sin importar su enfoque empresarial, alineando bajo una misma estructura todos los documentos relacionados con los sistemas de gestión y evitando así problemas de integración con otros marcos de referencia. Así pues, la nueva estructura queda como sigue:



Information Security Management System

Figura 2. Estructura del estándar ISO/IEC 27001:2013
Fuente: ISO/IEC 27001:2013

Las principales secciones se describen a continuación:

Alcance: Esta sección establece la obligatoriedad de cumplir con los requisitos especificados en los capítulos 4 a 10 del documento, para poder obtener la conformidad de cumplimiento y certificarse.

Referencias normativas: El estándar ISO-27002 ya no es una referencia normativa para ISO-27001:2013, aunque continúa considerándose necesario en el desarrollo de la

declaración de aplicabilidad (SOA, por sus siglas en inglés). El estándar ISO 27000:2013 se convierte en una referencia normativa obligatoria y única, ya que contiene todos los nuevos términos y definiciones.

Términos y definiciones: Los términos y definiciones que se manejaban en 27001:2005 los trasladaron y agruparon en la sección 3 de ISO 27000:2013 "Fundamentos y vocabulario" (lo cual se llevará a cabo en todos los documentos que forman parte de esta familia), con el objetivo de contar con una sola guía de términos y definiciones que sea consistente.

Contexto de la organización: Esta cláusula hace hincapié en identificar los problemas externos e internos que rodean a la organización.

- ✓ Instituye los requerimientos para definir el contexto del SGSI sin importar el tipo de organización y su alcance.
- ✓ Introduce una nueva figura (las partes interesadas) como un elemento primordial para la definición del alcance del SGSI.
- ✓ Establece la prioridad de identificar y definir formalmente las necesidades de las partes interesadas con relación a la seguridad de la información y sus expectativas con relación al SGSI, pues esto determinará las políticas de seguridad de la información y los objetivos a seguir para el proceso de gestión de riesgos.

Liderazgo: Ajusta la relación y responsabilidades de la Alta Dirección respecto al SGSI, destacando de manera puntual cómo debe demostrar su compromiso, por ejemplo:

- ✓ Garantizando que los objetivos del SGSI y "La política de seguridad de la información", anteriormente definida como "Política del SGSI", estén alineados con los objetivos del negocio.
- ✓ Garantizando la disponibilidad de los recursos para la implementación del SGSI (económicos, tecnológicos, etcétera).
- ✓ Garantizando que los roles y responsabilidades claves para la seguridad de la información se asignen y se comuniquen adecuadamente.

Planeación: Esta es una nueva sección enfocada en la definición de los objetivos de seguridad como un todo, los cuales deben ser claros y se debe contar con planes específicos para alcanzarlos. Se presentan grandes cambios en el proceso de evaluación de riesgos:

- ✓ El proceso para la evaluación de riesgos ya no está enfocado en los activos, las vulnerabilidades y las amenazas.
- ✓ Esta metodología se enfoca en el objetivo de identificar los riesgos asociados con la pérdida de la confidencialidad, integridad y disponibilidad de la información.
- ✓ El nivel de riesgo se determina con base en la probabilidad de ocurrencia del riesgo y las consecuencias generadas (impacto), si el riesgo se materializa.
- ✓ Se ha eliminado el término "Propietario del activo" y se adopta el término "Propietario del riesgo".
- ✓ Los requerimientos del SOA no sufrieron transformaciones significativas.

Soporte: Marca los requerimientos de soporte para el establecimiento, implementación y mejora del SGSI, que incluye:

- ✓ Recursos
- ✓ Personal competente
- ✓ Conciencia y comunicación de las partes interesadas

Se incluye una nueva definición "información documentada" que sustituye a los términos "documentos" y "registros"; abarca el proceso de documentar, controlar, mantener y conservar la documentación correspondiente al SGSI.

El proceso de revisión se enfoca en el contenido de los documentos y no en la existencia de un determinado conjunto de estos.

Operación: Establece los requerimientos para medir el funcionamiento del SGSI, las expectativas de la Alta Dirección y su realimentación sobre estas, así como el cumplimiento con el del estándar. Además, plantea que la organización debe planear y controlar las operaciones y requerimientos de seguridad, erigiendo como el pilar de este proceso la ejecución de evaluaciones de riesgos de seguridad de la información de manera periódica por medio de un programa previamente elegido.

Los activos, vulnerabilidades y amenazas ya no son la base de la evaluación de riesgos. Solo se requiere para identificar los riesgos asociados con la confidencialidad, integridad y disponibilidad.

Evaluación del desempeño: La base para identificar y medir la efectividad y desempeño del SGSI continúan siendo las auditorías internas y las revisiones del SGSI. Se debe considerar para estas revisiones el estado de los planes de acción para atender no conformidades anteriores y se establece la necesidad de definir quién y cuándo se deben realizar estas evaluaciones, así como quién debe analizar la información recolectada.

Mejora: El principal elemento del proceso de mejora son las no-conformidades identificadas, las cuales tienen que contabilizarse y compararse con las acciones correctivas para asegurar que no se repitan y que las acciones correctivas sean efectivas.

Aquí se observa uno de los cambios más importantes porque las medidas preventivas se fusionarán con la evaluación y tratamiento del riesgo, algo más natural e intuitivo que permite enfrentar los riesgos y las oportunidades con base en cuándo estos se identifican y cómo se tratan. Además, se distingue entre las correcciones que se ejecutan como una respuesta directa a una “no conformidad”, en oposición a las acciones correctoras que se realizan para eliminar la causa de la no conformidad.

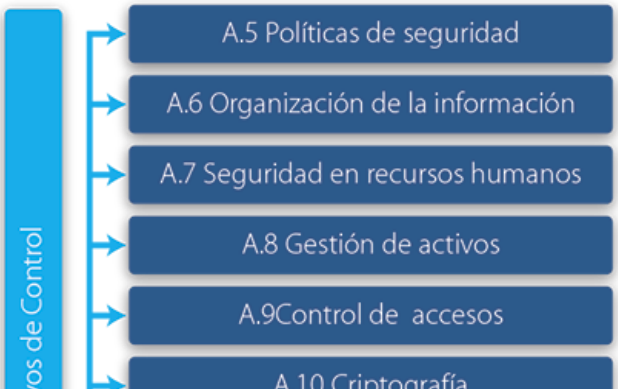


Figura 3. Dominios Anexo “A” de ISO 27001:2013
Fuente: ISO 27001:2013

La Seguridad de la información. La Seguridad viene a ser la protección de los activos frente a acciones o situaciones no deseadas, mediante la implantación de los controles, lo que suele suponer una inversión y un esfuerzo. Y todo ello en las entidades para proteger los intereses de los accionistas, de los empleados, de los clientes, de los proveedores y de los ciudadanos afectados según el sector (Peso, 2004).

La seguridad total no existe, que varían las medidas, de unos a otros, sobre elementos, sistemas, equipos o servicios que se deben de tomar en cuenta, ello de acuerdo a una serie de factores a estudiar, si tomamos las medidas preventivas correctas, se reduce el riesgo de (amenazas, vulnerabilidades e impacto) y las medidas adoptadas para disminuirlo.

En el mundo de la informática y la computación, se entiende como seguridad a la capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos

almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles (Montes, 2010).

El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales), Control y Autenticidad de la información manejada por computadora (Aldegani, 1997).

La información es el recurso clave para quien trabaja con el conocimiento en general, y especialmente para el ejecutivo. Cada vez más, la información crea el eslabón entre trabajadores de una empresa, con su organización y con su red. La información es el elemento que permite que aquéllos que trabajan con el conocimiento lleven a cabo su labor. Por otra parte, solamente los que trabajan con el conocimiento y especialmente los ejecutivos, pueden decidir cómo organizar su información para convertirla en un recurso clave para una acción eficaz, pues mientras no está organizada la información sigue siendo datos (Drucker, 1999).

Es un conjunto de datos procesado y con un significado, reduce la incertidumbre o aumenta el conocimiento de algo. La información es un mensaje con significado en un determinado contexto, disponible para uso inmediato y que proporciona orientación a las acciones por el hecho de reducir el margen de incertidumbre con respecto a las tomas de decisiones (Chiavenato, 2006). En se mismo sentido, también se entiende como conjunto de datos seleccionados y ordenados con un propósito específico (Czinkota & Masaaki, 2001).

Un riesgo constituye “un evento (o condición con cierta incertidumbre y si este ocurre tiene un efecto positivo o negativo en los objetivos del proyecto. Un riego tiene una causa y, en caso de ocurrencia, también implica una consecuencia” (PMBOK, 2004). Potencial de que una amenaza (interna o externa) explote una vulnerabilidad de uno o varios activos ocasionando daño a la organización. Su naturaleza puede depender de aspectos operativos, financieros, regulatorios (legales) y administrativos (ISO, 2008).

La RAE (2001) define el riesgo como contingencia o proximidad de un daño, o como cada una de las contingencias que pueden ser objeto de un contrato de seguro. El riesgo se presenta como una incertidumbre en el resultado de la aplicación de un servicio o

proceso, el cual está relacionado a la probabilidad de que un evento se materialice alterando su normal ejecución (Tupia, 2013b)

Es la probabilidad de que una amenaza se materialice explotando una vulnerabilidad sobre un activo, provocando un impacto negativo sobre él. El proceso de identificación y evaluación de riesgos permite determinar qué tan expuestos se encuentran los activos de información a ataques por la presencia de vulnerabilidades propias o inherentes a la actividad de la organización.

El termino de seguridad de información (SI) surge por la necesidad de proteger la información y a los sistemas que administran, bien sean físicos o informáticos. La seguridad de la información, es un conjunto de reglas, planes y acciones que permiten asegurar la información manteniendo las propiedades de Confidencialidad, Integridad y Disponibilidad.

Se entiende por seguridad de la información a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información buscando mantener la confidencialidad, la autenticidad e Integridad de la misma. Diferenciando el concepto de seguridad de la información con el de seguridad informática, en que este último sólo se encarga de la seguridad en el medio informático (Fitzgerald, 2007).

La seguridad de información se caracteriza por la preservación de la confidencialidad, asegurando que la información sea accesible sólo por aquellos que están autorizados; la integridad, salvaguardando la exactitud de la información en su procesamiento; y finalmente su disponibilidad, asegurando que los usuarios tengan acceso a la información y a los activos asociados cuando sean requeridos (Villena, 2006).

La seguridad de la información protege a la información, propiamente dicha, de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios. (INDECOPI, 2004).

La mayoría de usuarios particulares y de empresas poseen la percepción de que la seguridad de la información es una tarea difícil de aplicar, que exige gran cantidad de dinero y tiempo. En realidad, con muy poco esfuerzo se puede alcanzar un nivel de seguridad razonable, capaz de satisfacer las expectativas de seguridad de particulares, pequeñas y medianas empresas.” (CSIC, 1997).

Las Características de seguridades son:

Los usuarios: Son las personas que utilizan la estructura tecnológica, zona de comunicaciones y que gestionan la información. La seguridad informática debe establecer normas que minimicen los riesgos a la información o infraestructura informática.

- Horarios de funcionamiento
- Restricciones a ciertos lugares
- Autorizaciones
- Denegaciones
- Perfiles de usuario
- Planes de emergencia

Tipos de seguridad

La seguridad lógica: Consiste en restringir al acceso a programas y archivos mediante claves y/o encriptación. Asignar las limitaciones correspondientes a cada usuario del sistema informático. Esto significa, no darle más privilegios extras a un usuario, sino sólo los que necesita para realizar su trabajo.

La seguridad lógica aplica mecanismos y barreras que mantengan a salvo la información de la organización desde su propio medio. Algunos de los controles utilizados en la seguridad lógica son:

- Se limita el acceso a determinados aplicaciones, programas o archivos mediante claves o a través de la criptografía.
- Se otorgan los privilegios mínimos a los usuarios del sistema informático. Es decir, sólo se conceden los privilegios que el personal necesita para desempeñar su actividad.

- Cerciorarse de los archivos, las aplicaciones y programas que se utilizan en la compañía se adaptan a las necesidades y se usan de manera adecuada por los servidores públicos.
- Controlar que la información que entra o sale de la empresa es íntegra y sólo está disponible para los usuarios autorizados.

Subestados de la seguridad de la información o atributos de la seguridad de la información, también conocidos como requisitos ACID (autenticación, confidencialidad, integridad y disponibilidad), son los siguientes:

- **Autenticación:** Garantiza que el usuario es quien dice ser.
- **Confidencialidad:** Se garantiza que la información es accesible sólo a aquellas personas autorizadas a tener acceso a la misma.
- **Integridad:** La información debe ser siempre exacta y completa, y sólo puede ser modificada por personal autorizado.
- **Disponibilidad:** La información sólo ha de estar disponible cuando se necesite y de la forma que la requieran los usuarios autorizados.

Además, se pueden considerar otros aspectos adicionales a de seguridad:

- **No repudio:** Es una manera de asegurar que ninguna de las partes involucradas pueda negar su participación. Característica importante en el comercio electrónico y banca.
- **Trazabilidad:** permite asociar acciones realizadas en un sistema con el individuo o sistema que las llevó a cabo y en qué momento.

Figura 4. Riesgos
Fuente: Brinkley & SChell (1995)

Característica de la información que se logra mediante la adecuada combinación de políticas, procedimientos, estructura organizacional y herramientas informáticas especializadas a efectos que dicha información cumpla criterios de:

- Confidencialidad, garantía de que la información sea accedida por las personas convenientemente autorizadas.
- Integridad, la información debe mantenerse permanentemente correcta, compleja y protegida.
- Disponibilidad, la información debe estar disponible para su uso, cuando se lo requiera. También se considera como parte de la disponibilidad, la rapidez con que se puede ofrecer servicios o realizar operaciones. (Tupia, 2013ª)

De quien se debe proteger un sistema informático

De los intrusos o atacantes que atacan a usuarios de computadora sin la debida autorización a un sistema ajeno, ya sea en forma intencional o no.

Los tipos de intrusos existentes actualmente, según Ardita, son:

Clase A: El 80% en la base son los nuevos intrusos que bajan programas de Internet y prueban, están jugando son pequeños grupitos que se juntan y prueban.

Clase B: Es el 12% son más peligroso, saben compilar programas, aunque no saben programar. Prueban programas, conocen como detectar que sistema operativo que está usando la víctima, testean las vulnerabilidades del mismo e ingresan por ellas.

Clase C: Es el 5%. Es gente que sabe, que conoce y define sus objetivos. A partir de aquí buscan todos los accesos remotos e intentan ingresar.

Clase D: el 3% restante. Cuando entran a determinados sistemas buscan la información que necesitan.

Para llegar desde la base hasta el último nivel se tarda desde 4 a 6 años, por el nivel de conocimiento que se requiere asimilar. Es práctica, conocer, programar, mucha tarea y mucho trabajo".

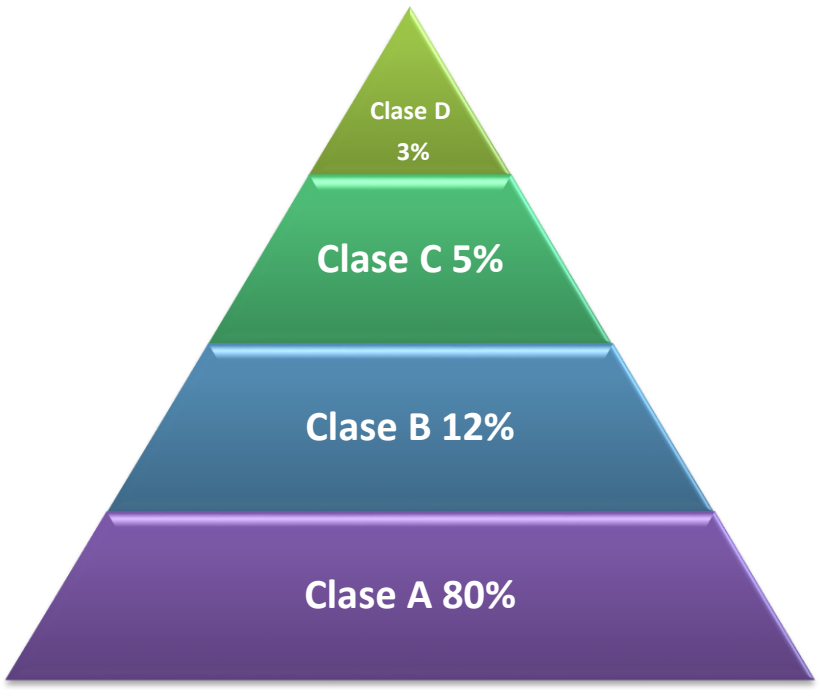


Figura 5. Tipos de Intrusos. Fuente: CybSec S.A. http://www.cybsec.com
Fuente: CybSec S.A. http://www.cybsec.com

¿Qué se debe proteger?

En cualquier sistema informático existen tres elementos básicos a proteger: el hardware, el software y los datos. Además, generalmente se habla de un cuarto elemento llamado fungible; que son los aquellos que se gastan o desgastan con el uso continuo: papel, tóner, tinta, cintas magnéticas, disquetes. De los cuatro, los datos que maneja el sistema serán los más importantes ya que son el resultado del trabajo realizado. Si existiera daño del hardware, software o de los elementos fungibles, estos pueden adquirirse nuevamente desde su medio original; pero los datos obtenidos en el transcurso del tiempo por el sistema son imposibles de recuperar: Se ha de pasar obligatoriamente por un sistema de copias de seguridad, y aun así es difícil de devolver los datos a su forma anterior al daño.

Para cualquiera de los elementos descriptos existen multitud de amenazas y ataques que se los puede clasificar en:

Ataques Pasivos: El atacante no altera la comunicación, sino que únicamente la "escucha" o monitoriza, para obtener información que está siendo transmitida. Sus objetivos son la intercepción de datos y el análisis de tráfico. Generalmente se emplean para: Obtención del origen y destinatario de la comunicación, a través de la lectura de las cabeceras de los paquetes monitorizados, control del volumen de tráfico intercambiado entre las entidades monitorizadas, obteniendo así información acerca de actividad o inactividad inusuales, y control de las horas habituales de intercambio de datos entre las entidades de la comunicación, para extraer información acerca de los períodos de actividad.

Ataques Activos: Estos ataques implican algún tipo de modificación del flujo de datos transmitido o la creación de un falso flujo de datos. Generalmente son realizados por hackers, piratas informáticos o intrusos remunerados y se los puede subdividir en cuatro categorías:

- ✓ **Interrupción:** Si hace que un objeto del sistema se pierda, quede inutilizable o no disponible.
- ✓ **Intercepción:** Si un elemento no autorizado consigue el acceso a un determinado objeto del sistema.

- ✓ **Modificación:** Si además de conseguir el acceso consigue modificar el objeto.
- ✓ **Fabricación:** Se consigue un objeto similar al original atacado de forma que es difícil distinguirlos entre sí.
- ✓ **Destrucción:** Es una modificación que inutiliza el objeto.

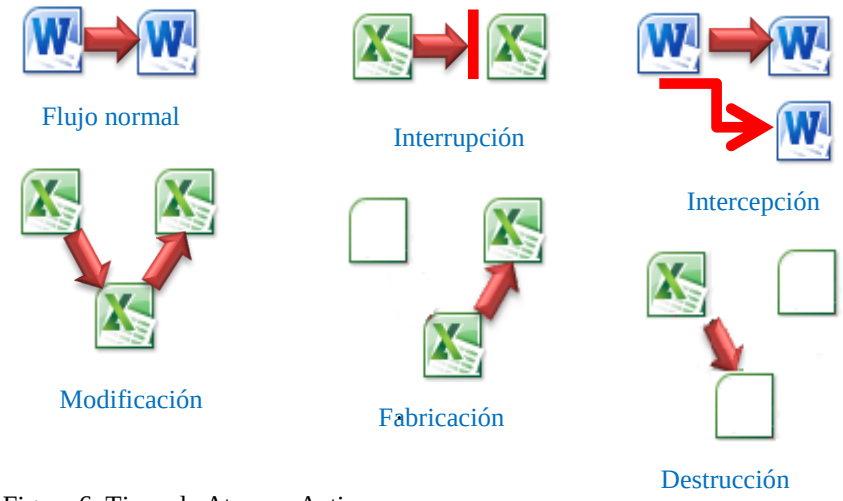


Figura 6. Tipos de Ataques Activos.
Fuente: Howard 1989–1995.

Relación operatividad y seguridad

Seleccionar las medidas de seguridad a implantar requiere considerar el equilibrio entre los intereses referidos a la seguridad, los requerimientos operacionales y la "amigabilidad" para el usuario. La Seguridad y la Utilidad de una computadora son inversamente proporcionales; es decir que incrementar la seguridad en un sistema informático, su operatividad desciende y viceversa.

$$\text{Operatividad} = \frac{1}{\text{Seguridad}}$$

Como se observa en el gráfico esta función se vuelve exponencial al acercarse al 100% de seguridad. Los costos se disparan (tendientes al infinito) por los complejos estudios que se deberán realizar para mantener este grado de seguridad.

seguridad	costo $ x mil
10%	2
20%	5
30%	9
40%	11
50%	16
60%	19
70%	22
80%	42
90%	80
100%	150

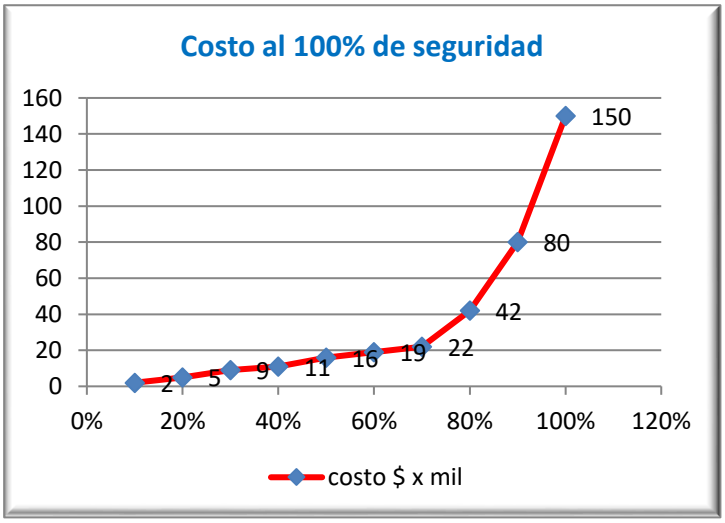


Figura 7. Relación Operatividad–Seguridad
Fuente: Aldegani (1997: 26)

Implementación de ISO 27001

Para implementar la norma ISO 27001 en una empresa u organización, usted tiene que seguir estos 16 pasos:

- ✓ Obtener el apoyo de la dirección
- ✓ Utilizar una metodología para gestión de proyectos
- ✓ Definir el alcance del SGSI
- ✓ Redactar una política de alto nivel sobre seguridad de la información
- ✓ Definir la metodología de evaluación de riesgos
- ✓ Realizar la evaluación y el tratamiento de riesgos
- ✓ Redactar la Declaración de aplicabilidad
- ✓ Redactar el Plan de tratamiento de riesgos
- ✓ Definir la forma de medir la efectividad de sus controles y de su SGSI
- ✓ Implementar todos los controles y procedimientos necesarios
- ✓ Implementar programas de capacitación y concienciación
- ✓ Realizar todas las operaciones diarias establecidas en la documentación de su SGSI
- ✓ Monitorear y medir su SGSI

- ✓ Realizar la auditoría interna
- ✓ Realizar la revisión por parte de la dirección
- ✓ Implementar medidas correctivas

Sistema de Gestión de Seguridad de Información (SGSI) Este sistema se fundamenta en la norma UNE-ISO/IEC 27001:2007, es parte del sistema gerencial general, está basado en un enfoque de riesgo comercial para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de información; sigue un enfoque basado en procesos que utilizan el ciclo de mejora continua o ciclo Deming, o más conocido como PDCA (Plan-Do- Check-Act), asimismo se tiene su fundamento en la norma UNE-ISO/IEC 27002:2009 que recoge una lista de controles necesarios para lograr los objetivos de seguridad de información. El SGSI está diseñado para asegurar una selección de controles de seguridad que protejan los activos de información y den confianza a las partes interesadas (AEC, 2012).

Figura 8. Ciclo de Deming
Fuente 3. MAGERIT (2012)

El diseño e implementación del SGSI de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización. Se espera que éstos y sus sistemas de soporte cambien a lo largo del tiempo, así como las situaciones simples requieran soluciones SGSI simples.

Figura 9. Esquema del Sistema de Gestión de Seguridad de Información ISO 27001
Fuente: Normas.ISO.com

Gestión de Riesgos, Es un enfoque integral de manejo de riesgos o amenazas, que tiene como fin evaluar, administrar y comunicar estos riesgos, basados en los objetivos estratégicos de la organización. A continuación, se describe algunas de las metodologías y/o métodos de Gestión de Riesgos.

Amenazas lógicas

Para evitar posibles amenazas lógicas en una organización, es importante que todos los servidores públicos, especialmente los administradores de los equipos, tomen conciencia del cuidado que deben poner para que no se materialicen posibles daños en la compañía. Además, es fundamental implementar mecanismos de prevención, detección y recuperación ante posibles amenazas lógicas como virus, gusanos, bombas lógicas y otros códigos maliciosos.

Seguridad Física: Deben resguardar de amenazas producidas tanto por el hombre como por la naturaleza. Básicamente, las amenazas físicas que pueden poner en riesgo un sistema informático son: Desastres naturales, amenazas ocasionadas involuntariamente por personas, fraude o sabotajes.

Principios de la seguridad de la información

La Seguridad de la información se basa en la preservación de unos principios básicos, los cuales son enumerados y definidos por diferentes autores, con algunas variantes. Cada uno de dichos principios tiene un propósito específico dentro del marco del objetivo de la seguridad informática (Harris, 2004). Los cuales son:

Confidencialidad: Es la necesidad de que la misma sólo sea conocida por personas autorizadas. En casos de falta de confidencialidad, la Información puede provocar severos daños a su dueño (por ejemplo, conocer antecedentes médicos de una persona) o volverse obsoleta (por ejemplo: los planes de desarrollo de un producto que se "filtran" a una empresa competidora, facilitarán a esta última desarrollar un producto de características semejantes).

Este principio tiene como propósito asegurar que una sola persona o un grupo de personas autorizadas tengan acceso a cierta información dentro de la organización. La información no siempre puede ser conocida por todos o cualquier empelado, si no por el contrario, está destinada para cierto grupo de personas, y en muchas ocasiones, a una sola persona. Este principio demanda que se debe asegurar que las personas no autorizadas, no tengan acceso a la información restringida para ellos. La confidencialidad de la información debe prevalecer y permanecer, por espacios de tiempo determinados, tanto en su lugar de almacenamiento, es decir en los sistemas y dispositivos en los que reside dentro la red, como durante su procesamiento y tránsito, hasta llegar a su destino final (Stoneburner, 2001).

Integridad: La integridad tiene como propósito principal, garantizar que la información no sea modificada o alterada en su contenido por sujetos no autorizados o de forma indebida. Asimismo, la integridad se aplica a los sistemas, teniendo como propósito garantizar la exactitud y confiabilidad de los mismos. Debido a esto, la integridad como principio de la Seguridad Informática, se ha definido en dos partes: integridad de los datos e integridad de los sistemas.

La integridad de los datos, se refiere a que la información y los programas solo deben ser modificados de manera autorizada por las personas indicadas para ello. Estas alteraciones pueden darse por inserciones, sustituciones o eliminaciones de contenido de la información. Por su parte, la integridad de los sistemas, hace referencia a que todo sistema debe poder cumplir su función a cabalidad, sin ninguna violación o

modificación del mismo, en su estructura física y/o lógica, sin perder necesariamente su disponibilidad (NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, 1995).

La Integridad de la Información es la característica que hace que su contenido permanezca inalterado a menos que sea modificado por personal autorizado, y esta modificación sea registrada para posteriores controles o auditorias. Una falla de integridad puede estar dada por anomalías en el hardware, software, virus informáticos y/o modificación por personas que se infiltran en el sistema.

Disponibilidad: Es su capacidad de estar siempre disponible para ser procesada por las personas autorizadas. Esto requiere que la misma se mantenga correctamente almacenada con el hardware y el software funcionando perfectamente y que se respeten los formatos para su recuperación en forma satisfactoria

Este principio tiene como propósito, asegurar que la información y los sistemas que la soportan, estén disponibles en el momento en que se necesiten, para los usuarios autorizados a utilizarlos. Al referirse a los sistemas que soportan la información, se trata de toda la estructura física y tecnológica que permite el acceso, tránsito y almacenamiento de la información (Academia Latinoamericana de la Seguridad Informática, 2011).

La Municipalidad Provincial de Recuay, es una Institución de nivel del Gobierno Local del Estado Peruano, cuya función es la atención de los habitantes de su jurisdicción territorial, en ese proceso de atención, genera información muy valiosa tanto de la Institución como para los vecinos de la comuna recuayina.

Orgánicamente está estructurada de las siguientes áreas o gerencias:

✓ **Alcaldía:** Es el órgano ejecutivo del gobierno local, liderado por el alcalde, quien es el representante legal de la municipalidad y su máxima autoridad administrativa. Entre las atribuciones más importantes señaladas por la ley Orgánica de Municipalidades respecto a auditorias son: emitir ordenanzas para el desarrollo de las auditorías internas o externas.

✓ **Comisión de Regidores:** Legislan que las auditorias se lleven a cabo con la frecuencia que la ley del gobierno central o municipal indica.

✓ **Secretaria General:** En acuerdo con Alcaldía, Regidores y gerencias, apoya con planificación, organización, dirección y control del proceso de auditoría.

✓ **Unidad de Tesorería y Rentas:** Área a ser auditada en la recepción, generación y transmisión de la información.

✓ **Unidad de Abastecimiento:** Área a ser auditada en la recepción, generación y transmisión de la información.

✓ **Unidad de Planificación, Presupuesto y de Inversiones:** Área de interés ser auditada en la recepción, generación y transmisión de la información, por la importancia de los archivos digitales que administra.

✓ **Unidad Social y Capacidades Humanas:** Es importante que la información que administra esta área sea evaluada con la finalidad de tomar decisiones respecto a las funciones que desarrolla.

✓ **Unidad de Desarrollo Urbano:** En esta unidad, los archivos de catastro, planificación urbana, etc., serán auditadas de conformidad a las normas técnicas internacionales, nacionales y locales.

✓ **Unidad de Estudios, Obras y Medio Ambiente:** Esta unidad representa, conjuntamente con Planificación, la columna vertebral de una buena parte de las funciones de la municipalidad, por lo tanto, su participación en la auditoria es de vital importancia.

✓ **Informática**: Es el órgano de apoyo en los aspectos del manejo de información tecnológica. Conjuntamente con Alcaldía, y las gerencias planifican, organizan, dirigen y controlan el proceso del desarrollo de las auditorias informáticas a todas las unidades de la municipalidad.

La investigación no formula hipótesis por ser una propuesta de una Guía Metodológica que se enmarca dentro una investigación no experimental descriptiva.

Se plantea como Objetivo General: Proponer una Guía Metodológica basada en ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014 para la seguridad de la información en la Municipalidad Provincial de Recuay.

Y como objetivos específicos: 1) Determinar el estado actual en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay. 2) Identificar las características que presenta la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades y sus formas de prevención.

3) Determinar las contribuciones de la norma ISO/IEC 27001:2013 en la estructuración en la información en la Municipalidad Provincial de Recuay. 4) Establecer cuáles son las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay.

2. METODOLOGÍA DE TRABAJO

El presente trabajo se basa en el tipo de investigación descriptivo no experimental y consiste en una propuesta de guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 en la seguridad de la información en la municipalidad Provincial de Recuay.

Población: Para el presente estudio, está conformada por 48 servidores públicos que utilizan el sistema de información y a la vez procesan información en la Municipalidad Provincial de Recuay. Dado el tamaño de la población, la muestra estará conformada por 20 servidores públicos de la Municipalidad Provincial de Recuay.

Muestreo

El muestreo es tipo probabilístico aleatorio; porque cualquiera de los elementos de la población forma parte de la muestra, con la aplicación de formula estadística.

Criterios de selección

- Son funcionarios y servidores públicos nombrados y contratados de la Municipalidad Provincial de Recuay, de los siguientes órganos: La Unidad de Tesorería y Rentas, la Unidad de Abastecimiento, la Unidad de Planificación, Presupuesto y de Inversiones, la Unidad de Estudios, Obras y Medio Ambiente y la oficina de Informática
- Funcionarios y Servidores Públicos con edades de 25 a 60 años.
- Funcionarios y Servidores Públicos que desean participar voluntariamente en la investigación.

Técnicas e Instrumentos de Investigación

Observación: Se observarán el sistema de información de la Municipalidad Provincial de Recuay, así como los recursos de internet y software de gestión utilizados.

Análisis: Se analizará el estado actual de los procesos de información, así como los fundamentos de los modelos de administración de sistemas informáticos.

Síntesis: Las variables a estudiar serán sintetizadas para proponer una guía metodológica basada en la normativa internacional ISO/IEC 27001:2013 y la norma técnica peruana NTP ISO/IEC 270012014.

Técnica e Instrumento de Recolección de Datos: Se utilizó la encuesta.

La encuesta: Se denomina encuesta al método o técnica de relevar datos mediante un instrumento como el cuestionario, y se denomina encuesta al procedimiento general de investigar cuantitativamente empleando un cuestionario. Es una técnica que utiliza interrogantes en la formulación del instrumento, con base a las variables e indicadores de estudio, de acuerdo al objetivo de investigación para la solución del problema y la demostración de las hipótesis (Gomero, 1999, p. 39).

Instrumentos:

Son dos cuestionarios estructurados. Uno por cada variable analizada

El cuestionario: Se define como una forma de encuesta caracterizada por la ausencia del investigador, lo que obliga a éste a manifestar explicaciones que orienta la forma de encuestar. Es una técnica de recogida de información que supone un interrogatorio en el que las preguntas establecidas de antemano se plantean siempre en el mismo orden y se formulan con los mismos términos, con el objetivo de que un segundo investigador pueda repetirlo siguiendo los mismo pasos, es decir tiene un carácter sistemático. Fue un instrumento elaborado por el investigador, es decir un formato que comprendió las siguientes partes: Título del instrumento (cuestionario estructurado), el objetivo (objetivo general de la investigación); instrucción, con el fin de orientar al encuestado de acuerdo al principio ético de la investigación (conocimiento informado), preguntas y alternativas de respuesta de la variable 1, preguntas y alternativas de respuesta de la variable 2, responsable (Guerra, 2010, p. 86).

Norma ISO/IEC 27001:2013, es un conjunto de lineamientos que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Estos requisitos describen el comportamiento esperado del Sistema de Gestión una vez que esté en pleno funcionamiento.
ISO/IEC 27001:2013 especifica los requerimientos para establecer, implementar, mantener y mejorar continuamente un SGSI. Estos requerimientos describen el comportamiento previsto de un SGSI una vez que es completamente operacional. El estándar no es una guía paso a paso sobre cómo construir o crear un SGSI.

Norma NTP ISO/IEC 27001:2014, La Norma Técnica Peruana (NTP) ISO/IEC 27001:2014 tiene una correspondencia con la norma internacional ISO/IEC 27001:2013

e incluye las correcciones publicadas por ISO posteriormente a su publicación. NTP ISO/IEC 27001:2014 es un Estándar Peruano basado en la ISO 27001:2013.

Es una Norma Técnica Peruana que abarca a todos los tipos de organizaciones (empresas comerciales, agencias de gobierno y organizaciones sin fines de lucro). Promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, mantener y mejorar la efectividad de un ISMS (Information Security Management System) en la organización. La adopción de un ISMS debe ser una decisión estratégica para una organización. El diseño e implementación del ISMS de una organización está influenciado por las necesidades y objetivos del negocio, requisitos de seguridad, procesos, tamaño y estructura de la organización. Se espera que éstos y sus sistemas de soporte cambien a lo largo del tiempo, así como que las situaciones simples requieran soluciones ISMS simples.

Especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI) documentado dentro del contexto de los riesgos de negocio de la organización, Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información 2da Edición, Resolución Ministerial N.º 197-2007-PCM, Sobre la fecha límite para diversas entidades de la Administración Pública implementen el Plan de Seguridad del a Información Dispuesto en la NTP 17799:2007 EDI, Resolución de Contraloría General N.º 320-2006 CG Normas de control Interno y Resolución Ministerial N.º 129-2012-PCM.

Esta Norma Técnica Peruana cubre todos los tipos de organizaciones (como, por ejemplo: empresas comerciales, agencias de gobierno y organizaciones sin fines de lucro). Esta NTP especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un ISMS documentado dentro del contexto de los riesgos de negocio de la organización. Especifica los requisitos para implementar los controles de seguridad adaptada a las necesidades individuales de las organizaciones o partes de las mismas. El ISMS ha sido diseñado para garantizar y proporcionar controles de seguridad adecuados que protejan los activos de información, brindando confianza a las partes interesadas.

Siguiendo los lineamientos establecidos se asegurará mejorar la seguridad de la información al dar tratamiento a los riesgos más críticos. Asegurar la mejora continua a través de las revisiones gerenciales y auditorias.

PLAN DE PROCESAMIENTO Y ANÁLISIS ESTADÍSTICO DE LA INFORMACIÓN

El procesamiento consiste de tres etapas bien diferenciadas:

ETAPA I: Diagnóstico

- ✓ Diagnosticar la situación de la seguridad de la información de la municipalidad, poniendo énfasis en la adecuada identificación de los activos de información vinculados a los procesos de provisión, considerando información, personas e infraestructura y sus características, además del respectivo análisis de criticidad de cada uno de ellos (en función de los niveles de confidencialidad, integridad y disponibilidad), para llegar a conformar un inventario de activos de información debidamente priorizado en términos de criticidad.
- ✓ Para los activos con criticidad media y alta, especificar los riesgos más relevantes considerando los aspectos que conforman la criticidad del activo (Reserva, Integridad media o alta, y disponibilidad media o alta) y los correspondientes controles que permiten su mitigación de aquellos que propone NTP ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014.
- ✓ Establecer el nivel en que la municipalidad se encuentra con respecto a los controles, declarando si están o no cumplidos.

ETAPA II: Planificación

En esta etapa se planifican la organización de las actividades, uso de recursos y productos a generar en las etapas siguientes. Los productos y sus actividades asociadas incluidas en esta etapa adquieren la calidad de compromisos, a los cuales se les realizará un seguimiento que continúa en la etapa de Evaluación.

Las acciones concretas son:

- ✓ Formular o actualizar la guía metodológica de seguridad de la información.
- ✓ Nombrar al Encargado de Seguridad de la Información, a través de una Resolución.
- ✓ Conformar el Comité Municipal de Seguridad de la Información.
- ✓ Definir el Plan General de Seguridad de la Información de la municipalidad en base a los tratamientos de controles no cumplidos.
- ✓ Elaborar plan de trabajo para elaborar la guía de seguridad de la información definido.

ETAPA III: Implementación

- ✓ Implementar el programa de trabajo.
- ✓ Registrar y controlar los resultados de la implementación del programa de trabajo verificando el avance en el nivel de cumplimiento de los controles que requiere el servicio.
- ✓ Comenzar a medir, sobre todo los indicadores de desempeño definidos.

Documentos a entregar

Reportar el diagnóstico y la planificación con las actualizaciones correspondientes. Los documentos propios de la etapa se agregan los de las etapas anteriores.

MARCO NORMATIVOS/REFERENCIAS APLICABLE

- ✓ Constitución Política del Perú 1993.
- ✓ Ley Marco de la Administración Financiera del Sector Público, Ley Nº 28112, Título III: Sistema Nacional de Presupuesto (Normas Pertinentes).
- ✓ Ley Nº 27658, Ley Marco de la Modernización del Estado.
- ✓ Ley Nº 27783, Ley de Bases de la Descentralización.
- ✓ Ley Orgánica de Municipalidades, Ley Nº 27972.
- ✓ Ley Nº 28056, Ley Marco de Presupuesto Participativo.
- ✓ Ley Nº 27815, del Código de Ética de la Función Pública.

- ✓ Resolución Directoral N° 003-2003-EF/68.01 Directiva para la reformulación de los Planes Estratégicos Sectoriales Multianuales para el período 2004 –2006.
- ✓ Resolución Directoral N° 010-2004-EF/76.01, Instructivo para el proceso de Planeamiento del desarrollo concertado y presupuesto participativo.
- ✓ Guía para la Reformulación de los Planes Estratégicos Sectoriales.
- ✓ Otros dispositivos complementarios y/o conexos aplicables.
- ✓ Ley N° 27783, Ley de Bases de la Descentralización.
- ✓ Ley N° 28411, Ley General del Sistema Nacional de Presupuesto
- ✓ Ordenanza Municipal Nº 592-2010-MPR/A que aprueba el Plan de Desarrollo Concertado 2011 al 2021 de la provincia de Recuay.
- ✓ Ordenanza Municipal Nº 038-2010-MPR que aprueba el Reglamento de Organización y Funciones (ROF).
- ✓ COBIT
- ✓ Normativa/referencial Nacional
- ✓ 500 normas de control interno para auditoria de sistemas computarizados.
- ✓ Norma técnica peruana NTP-ISO/IEC 27001 2013.
- ✓ Resolución Ministerial N° 197-2007-PCM: sobre la fecha límite para que diversas entidades de la Administración Pública implementen el plan de seguridad de la información
- ✓ Resolución de Contraloría General N°320-2006 Cg Normas de Control Interno
- ✓ Resolución Ministerial 129-2012-PCM

GUÍA METODOLÓGICA BASADA EN ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014, PARA LA MUNICIPALIDAD DISTRITAL DE RECUAY

1.1.1. Generalidades

La seguridad informática para la Municipalidad Distrital de Recuay es de vital importancia debido a la cantidad de población que gobierna, así como a la cantidad de información que recepciona, procesa y transmite. La aparición de nuevas plataformas tecnológicas informáticas disponibles ha configurado el procesamiento rápido de atención de grandes volúmenes de información, pero a la vez también ha configurado una realidad insegura que en este caso la Municipalidad debe atender. Las vulnerabilidades y riesgos a las que se tiene que enfrentar la Municipalidad implica que la administración de la misma desarrolle un conjunto de políticas de seguridad informática con la finalidad de salvaguardar la información valiosa que siempre van a estar al acecho de los piratas informáticos de cualquier parte del entorno de la Municipalidad.

En este sentido, las políticas de seguridad informática definidas partiendo desde el análisis de los riesgos a los que se encuentra amenazado los archivos de las diferentes unidades de la municipalidad, surgen como una herramienta organizacional para coordinar a los empleados y trabajadores de la institución edilicia sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la institución crecer y mantenerse competitiva y eficiente. Ante esta situación, se proponer una guía metodológica de seguridad de la información, la cual requiere un alto compromiso de todos quienes trabajan en la municipalidad.

Alcance de la Guía Metodológica

La guía metodológica para garantizar la seguridad de la información en el sistema informático de la Municipalidad Provincial de Recuay tiene como alcance a todas las áreas de esta instrucción quienes trabajan o hacen uso del sistema informático.

Definición

La Guía Metodológica consiste en un conjunto de políticas de seguridad de información, es un conjunto de reglas aplicadas a todas las actividades relacionadas con la generación, registro y manejo de la información de la Municipalidad, y de esta manera se pueda evitar cualquier tipo de riesgos, vulnerabilidades, así como minimizar

el robo de información, garantizar un nivel de seguridad en la generación y uso de la información.

Objetivos

Proponer un conjunto de guías y políticas referentes a la seguridad informática, específicamente para hacer frente a los ataques informáticos en diversas modalidades, controlar las actividades para mantener y garantizar la integridad física y lógica de los recursos informáticos que se utilizan en la municipalidad.

Los objetivos que se desean alcanzar luego de implementar la Guía Metodológica son los siguientes:

- ✓ Establecer normas que contribuyan a la seguridad con meridiana claridad y transparencia bajo la responsabilidad del responsable de área.
- ✓ Comprometer a todo el personal de la Municipalidad, específicamente a quienes trabajan en las unidades más sensibles y de generación de información privilegiada con el proceso de seguridad, agilizando la aplicación de los controles con dinamismo y armonía.
- ✓ Que la prestación del servicio de seguridad gane en calidad.
- ✓ Lograr que todos los empleados de la Municipalidad se conviertan en interventores del sistema de seguridad.

El propósito de la Guía Metodológica es alcanzar un conjunto de orientaciones y políticas de seguridad de la información para proteger la información y los activos de datos de la Municipalidad. Las políticas son guías para asegurar la protección y la integridad de los datos dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales.

Obligaciones y derechos

Obligaciones-. El cumplimiento de la presente Guía Metodológica sobre seguridad de la información es obligatorio y debe ser considerado como una condición en los contratos del personal, para todo el personal, use o no use el sistema de información.

Es obligación de cada trabajador o empleado de la Municipalidad estudiar, analizar y aplicar la presente política de seguridad de la información. Toda excepción a la política debe ser documentada y aprobada por el área de seguridad informática, detallando el motivo que justifica el no cumplimiento de la política.

Derechos: Los empleados y trabajadores de la municipalidad tienen el derecho a que se les implemente con un sistema informático adecuado en sus dimensiones de hardware y software, es decir, los sistemas informáticos deben estar en condiciones óptimas de uso, el software debe ser actualizado periódicamente de acuerdo con las realidades exigidas por el avance tecnológico de los ataques informáticos. El incumplimiento en los derechos del empelado o trabajador no puede generar responsabilidades o penalidades, aunque ello podría suponer previamente una investigación minuciosa de las responsabilidades.

Organización de la Seguridad: Los servidores públicos y autoridades de la Municipalidad deben trabajar organizadamente frente a los ataques externos e internos informáticos en general. Todos los servidores públicos son responsables de mantener un ambiente seguro, en tanto que el área de seguridad informática debe monitorear el cumplimiento de la política de seguridad definida y realizar las actualizaciones que sean necesarias, producto de los cambios en el entorno informático y las necesidades del negocio.

Estructura Organizacional: En la administración de la seguridad de la información participan todos los servidores públicos siguiendo uno o más de los siguientes roles:

- Alcaldía
- Informática
- Secretaria General
- Unidad de Tesorería y Rentas
- Unidad de Abastecimiento
- Unidad de Planificación, Presupuesto y de Inversiones
- Unidad Social y Capacidades Humanas
- Unidad de Desarrollo Urbano
- Unidad de Estudios, Obras y Medio Ambiente

Determinación de Riesgos en el sistema informático

Los riesgos del sistema informático deben ser determinados usando una tabla por separado para cada unidad de la Municipalidad y ordenados en niveles de riesgo de menor a mayor riesgo. Los riesgos deben ser clasificados en riesgos internos, externos, de persona, de instalación de sistema eléctrico, de hardware y de software.

Evaluación de la seguridad de la información

La evaluación tiene por objeto reunir evidencia suficiente, pertinente y válida para sustentar los juicios a emitir respecto al área examinada. Deben establecerse los objetivos de la evaluación en consonancia con los criterios, los procedimientos y técnicas de evaluación a desarrollar.

Los procedimientos y técnicas de auditoría deben describirse en forma minuciosa y orientada a la verificación de los problemas reales o potenciales detectados en el examen preliminar. Todo programa de auditoría informática deberá comprender al menos el análisis y la evaluación de la estructura organizativa, misión, objetivos y políticas; controles financieros y operativos; formas de operar y aprovechamiento de los recursos en cualquier unidad de la municipalidad. La elaboración es responsabilidad del encargado de la auditoría y la revisión y aprobación del jefe de la unidad de auditoría interna de la municipalidad.

Ejecución

Realización de pruebas y obtención de evidencia

En esta etapa se debe evaluar las normas de auditoría generalmente aceptadas manteniendo la independencia y aplicando el debido cuidado profesional y la supervisión constante, agotando todos los recursos a su alcance para documentar y sustentar la evidencia en papeles de trabajo cuidadosamente preparados durante el curso de la auditoría, a fin de que sea suficiente competente, relevante y útil, es decir que deben contener toda la información obtenida y los análisis efectuados, ya que servirán de base para las conclusiones y recomendaciones que se efectúen; deben ser preparados por el auditor y revisados por la dirección de la unidad de auditoría interna.

GUÍA METODOLÓGICA DE SEGURIDAD INFORMÁTICA

Artículo 1°. El presente conjunto de políticas tiene por objetivo asegurar la información de manera general y específicamente en la seguridad de datos e información de la municipalidad.

Artículo 2°. Para los efectos de este documento, se entiende por Guía Metodológica de seguridad informática, al conjunto de reglas obligatorias, orientaciones, que deben observar todos los servidores públicos de la municipalidad, es responsabilidad de la administración de la Municipalidad, de Informática y de todos los usuarios, vigilar su estricta observancia en el ámbito de su competencia, tomando las medidas preventivas y correctivas para que se cumplan.

Artículo 3°. La instancia rectora de la seguridad de la información recae sobre la administración de la municipalidad, es Alcaldía e Informática.

Artículo 4°. Las gerencias responsables de la información contenida en las unidades a su cargo, delimitarán las responsabilidades de sus subordinados y determinarán quien está autorizado a efectuar operaciones emergentes con dicha información tomando las medidas de seguridad pertinentes.

Artículo 5°. Se establecen tres tipos de prioridad para la información:

- ✓ Información vital para el funcionamiento de la unidad;
- ✓ Información necesaria, pero no indispensable en la unidad.
- ✓ Información ocasional o eventual.

Artículo 6°. En caso de información vital para el funcionamiento del área, se deberán tener procesos colaborativos, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos históricos semanalmente.

Artículo 7°. La información necesaria pero no indispensable, deberá ser respaldada con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.

GUÍA METODOLÓGICA DE CLASIFICACIÓN DEL ACCESO DE LA INFORMACIÓN

Artículo 8°. Toda la información debe de ser clasificada como: Confidencial, Integridad y Disponibilidad.

Artículo 9°. Las definiciones de la clasificación de la información son las siguientes:

Confidencial: La Información debe ser accesible solo a aquellas que están autorizados para el cumplimiento de sus funciones. Tiene acceso el personal que lo genera y la gerencia de la municipalidad.

Integridad: Resguardar la veracidad e integridad de la información deben de ser manejados solo por personal autorizado por la municipalidad.

Disponibilidad: La Información que es generada específicamente para su divulgación a la población general de usuarios. Tiene acceso todo el personal implicado y la gerencia de la municipalidad.

Artículo 10°. Información confidencial son los documentos de proyectos que implican grandes montos de inversión, licitaciones, liquidaciones, informes de avance, contraloría, rendición de cuentas, etc.

Artículo 11°. Toda información debe ser controlada por cada gerencia, así como por Informática, las medidas de seguridad a ser aplicadas a los activos de información confidencial e integridad que deben ser controladas por el personal asignado.

GUÍA METODOLÓGICA DE CAPACITACIÓN DE USUARIOS

Artículo 12°. Es responsabilidad de Informática promover constantemente la importancia de la seguridad a todos los usuarios de los sistemas de información. Se recomienda capacitar a los empleados y trabajadores de la municipalidad en los aspectos de la seguridad de la información, específicamente en el robo de información. El programa de concientización en seguridad debe de contener continuas capacitaciones y charlas, adicionalmente se puede emplear diversos métodos como afiches, llaveros, etc., los cuales recuerden permanentemente al usuario el papel importante que cumplen en el mantenimiento de la seguridad de la información.

Artículo 13°. Para contratar a un empleado nuevo y/o el servicio de algún tercero, se debe de entregar la política de seguridad, así como las normas y procedimientos para el uso de las aplicaciones y los sistemas de información de la municipalidad. Asimismo, se debe entregar un resumen escrito de las medidas básicas de seguridad de la información. Considerar:

- El personal debe de ser comunicado de las implicancias de seguridad en relación a las responsabilidades de su trabajo

- Una copia firmada de la política de seguridad de información debe de ser guardada en el archivo del empleado

Artículo 14°. Los usuarios deben de ser informados anualmente sobre la importancia de la seguridad de la información. Un resumen escrito de la información básica debe de ser entregada nuevamente a cada empleado y una copia firmada debe de ser guardada en sus archivos.

Artículo 15°. La capacitación en seguridad de la información debe de incluir, entre otros aspectos:

- Requerimientos de identificador de usuario y contraseña
- Seguridad de PC, incluyendo protección de virus
- Responsabilidades de la organización de seguridad de información
- Concientización de las técnicas utilizadas por "hackers"
- Uso de correo electrónicos para evitar robos de información
- Guías de acceso a Internet
- Procesos de monitoreo de seguridad de la información utilizados
- Persona de contacto para información adicional

GUÍA METODOLÓGICA DE RESPUESTA ANTE INCIDENTES DE SEGURIDAD

Artículo 16°. El jefe de Informática debe ser plenamente identificado por todos los empleados de la Municipalidad. Si un empleado de la municipalidad detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al jefe de dicha área. Si se sospecha la presencia de un ataque de robo de información, el usuario debe desconectar el equipo de la red de datos, notificar al área de informática quien trabajará en coordinación con el área de soporte técnico, para la eliminación del virus antes de restablecer la conexión a la red de datos. Es responsabilidad del usuario (con la apropiada asistencia técnica) asegurarse que el virus haya sido eliminado por completo del sistema antes de conectar nuevamente el equipo a la red de datos.

Artículo 17°. Si un empleado detecta una vulnerabilidad en la seguridad de la información debe notificarlo al personal encargado de la administración de la seguridad, asimismo, está prohibido para el empleado realizar pruebas de dicha vulnerabilidad o aprovechar ésta para propósito alguno.

Artículo 18°. Informática con el área de Alcaldía debe documentar todos los reportes de incidentes de seguridad. Cualquier error o falla en los sistemas debe ser notificado a soporte técnico, quién determinará si el error es indicativo de una vulnerabilidad en la seguridad.

Artículo 19°. 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

Artículo 20°. Los registros de fallas deben ser revisados semanalmente. Los registros de errores no solucionados deben permanecer abiertos hasta que se encuentre una solución al problema. Además, estos registros deben ser almacenados para una posterior verificación independiente.

GUÍA METODOLÓGICA DE CONTROL DE INFORMACIÓN

Artículo 21°. Todo medio de almacenamiento secundario (Disco duro, USB, DVD, CD´s, copias de backup, etc.), deben presentar una etiqueta con la clasificación correspondiente.

Artículo 22°. La información en formato digital clasificada como de acceso "Disponibilidad", puede ser almacenada en cualquier sistema de la Municipalidad. Sin embargo, se deben tomar las medidas necesarias para no mezclar información "General" con información correspondiente a otra clasificación.

Artículo 23°. Todo usuario, antes de transmitir información clasificada como "Confidencial o "Integridad", debe asegurarse que el destinatario de la información esté autorizado a recibir dicha información.

Artículo 24°. Todo usuario que requiere acceso a información clasificada como "Confidencial o "Integridad", debe ser autorizado por el personal que lo genero o

propietario de la misma. Las autorizaciones de acceso a este tipo de información deben ser documentadas.

Artículo 25°. La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

Artículo 26°. Se recomienda el uso de técnicas de encriptación para la información clasificada como "Confidencial o "Integridad", transmitida a través de la red de datos de la municipalidad.

Artículo 27°. Toda transmisión de Información clasificada como "Confidencial o "Integridad", o de "Uso Interno" realizada hacia o a través de redes externas a la municipalidad debe realizarse utilizando un medio de transmisión seguro o utilizando técnicas de encriptación aprobadas.

Artículo 28°. Todo documento en formato digital, debe presentar la clasificación correspondiente en la parte superior (cabecera) e inferior (pie de página) de cada página del documento.

Artículo 29°. Todo documento o contenedor de información debe ser etiquetado como "Confidencial o "Integridad", de "Uso interno" o de Acceso "Disponibilidad", dependiendo de la clasificación asignada.

Artículo 30°. Todo documento que presente información clasificada como "Confidencial o "Integridad", debe ser etiquetado en la parte superior e inferior de cada página con la clasificación correspondiente.

Artículo 31°. Todo documento clasificado como "Confidencial o "Integridad", debe contar con una carátula en la cual se muestre la clasificación de la información que contiene.

Artículo 32°. Los activos de información correspondiente a distintos niveles de clasificación, deben ser almacenados en distintos contenedores, de no ser posible dicha distinción, se asignará el nivel más crítico de la información identificada a todo el contenedor de información.

Artículo 33°. El ambiente donde se almacena la información clasificada como "Confidencialidad", debe contar con adecuados controles de acceso y asegurado cuando se encuentre sin vigilancia. El acceso debe ser permitido solo al personal

formalmente autorizado. Personal de limpieza debe ingresar al ambiente acompañado por personal autorizado.

Artículo 34°. Solo el personal formalmente autorizado debe tener acceso a información clasificada como “Confidencial o “Integridad”.

Artículo 35°. Los usuarios que utilizan documentos con información “Confidencial o “Integridad”, deben asegurarse de: Almacenarlos en lugares adecuados, evitar que usuarios no autorizados accedan a dichos documentos y destruir los documentos si luego de su utilización dejan de ser necesarios.

GUÍA METODOLÓGICA DE INTERCAMBIOS DE INFORMACIÓN Y CORREO ELECTRÓNICO

Artículo 36°. Los mensajes de correo electrónico deben ser considerados de igual manera que un memorándum formal, son considerados como parte de los registros de la municipalidad y están sujetos a monitoreo y auditoria.

Artículo 37°. Los sistemas de correo electrónico no deben ser utilizados para lo siguiente:

- Enviar cadenas de mensajes
- Enviar mensajes relacionados a seguridad, exceptuando al personal encargado de la administración de la seguridad de la información
- Enviar propaganda de candidatos políticos
- Actividades ilegales, no éticas o impropias
- Actividades no relacionadas con el negocio de la municipalidad
- Diseminar direcciones de correo electrónico a listas públicas

Artículo 38°. No utilizar reglas de reenvío automático a direcciones que no pertenecen a la organización. No existe control sobre los mensajes de correo electrónico una vez que estos se encuentran fuera de la red de la municipalidad.

Artículo 39°. Establecer controles sobre el intercambio de información de la municipalidad con terceros para asegurar la confidencialidad e integridad de la información, y que se respete la propiedad intelectual de la misma. Debe tomarse en consideración:

- Acuerdos para el intercambio de software
- Seguridad de medida en tránsito
- Controles sobre la transmisión mediante redes

Artículo 40°. Debe establecerse controles sobre equipos de oficina como teléfonos, faxes e impresoras que procesan información sensible de la municipalidad.

Artículo 41°. La información restringida o confidencial solo debe imprimirse en equipos específicamente designados para esta tarea.

GUÍA METODOLÓGICA DE SEGURIDAD DE INSTALACIONES DE PROCESAMIENTO DE DATOS

Artículo 42°. Implementar medidas de seguridad física para asegurar la integridad de los datos y documentos. Las medidas de protección deben ser consistentes con el nivel de clasificación de los activos y el valor de la información procesada y almacenada en las computadoras.

Artículo 43°. El acceso a cualquier instalación de cómputo debe estar restringido únicamente al personal autorizado.

Artículo 44°. Todas las visitas deben ser identificadas y se debe mantener un registro escrito de las mismas. Estas visitas deben ser en compañía de un empleado durante la permanencia en las instalaciones de cómputo. La visita de los proveedores de mantenimiento, a quienes se les otorga acceso continuo a las áreas sensibles, estén siempre acompañados por un empleado autorizado de la municipalidad, puede resultar poco práctico en algunos casos.

Artículo 45°. Todo el personal en las instalaciones de cómputo debe de portar un carné, placa o ficha de identificación. Sistemas automatizados de seguridad para acceso físico deben de ser instalados en centros de cómputo principales. Centros pequeños pueden controlar el acceso físico mediante el uso de candados de combinación o llaves.

Artículo 46°. El retiro de cualquier equipo o medio electrónico de las instalaciones de cómputo debe de ser aprobado por escrito por personal autorizado.

GUÍA METODOLÓGICA PARA LA ADMINISTRACIÓN DE COMUNICACIONES Y OPERACIONES

Artículo 47°. La administración de las comunicaciones y operaciones de la Municipalidad, son esenciales para mantener un adecuado nivel de servicio a los clientes. Los requerimientos de seguridad deben ser desarrollados e implementados para mantener el control sobre las comunicaciones y las operaciones. Los procedimientos operacionales y las responsabilidades para mantener accesos adecuados a los sistemas, así como el control y la disponibilidad de los mismos, deben ser incluidos en las funciones operativas de la municipalidad.

Artículo 48°. Todas las comunicaciones e intercambios de información, tanto dentro de las instalaciones y sistemas de la Municipalidad como externas a ella, deben ser aseguradas, de acuerdo al valor de la información protegida.

Artículo 49°. Todos los procedimientos de operación de los sistemas deben ser documentados y los cambios realizados a dichos procedimientos deben ser autorizados por la autoridad respectiva.

Artículo 50°. Todos los procedimientos de encendido y apagado de los equipos deben ser documentados; dichos procedimientos deben incluir el detalle de personal clave a ser contactado en caso de fallas no contempladas en el procedimiento regular documentado.

Artículo 51°. Todas las tareas programadas en los sistemas para su realización periódica, deben ser documentadas. Este documento debe incluir tiempo de inicio, tiempo de duración de la tarea, procedimientos en caso de falla, entre otros.

Artículo 52°. Todos los cambios operacionales realizados en los sistemas de la municipalidad, a excepción de los cambios de emergencia, deben seguir los procedimientos de cambios establecidos.

GUÍA METODOLÓGICA DE PROTECCIÓN CONTRA VIRUS

Artículo 53°. Es responsabilidad de Informática de realizar esfuerzos para determinar el origen de la infección por virus informático, para evitar la reinfección de los equipos de la municipalidad.

Artículo 54°. El programa antivirus debidamente actualizado debe encontrarse habilitado en todas las computadoras de la municipalidad y debe ser actualizado

periódicamente. En caso de detectar fallas en el funcionamiento de dichos programas éstas deben ser comunicadas al área de soporte técnico.

Artículo 55°. El programa antivirus debe ser configurado para realizar revisiones periódicas para la detección de virus en los medios de almacenamiento de las computadoras de la municipalidad.

Artículo 56°. Debe contarse con un procedimiento para la actualización periódica de los programas antivirus y el monitoreo de los virus detectados.

Artículo 57°. Es obligación del personal de la municipalidad, emplear sólo los programas cuyas licencias han sido obtenidas por la Municipalidad y forman parte de su plataforma estándar. Asimismo, se debe evitar compartir directorios o archivos con otros usuarios; en caso de ser absolutamente necesario, coordinar con la administración de la municipalidad.

GUÍA METODOLÓGICA DE CONTROL DE ACCESO DE DATOS

Artículo 58°. La información manejada por los sistemas de información y las redes asociadas debe estar adecuadamente protegida contra modificaciones no autorizadas, divulgación o destrucción. El uso inteligente de controles de acceso previene errores o negligencias del personal, así como reduce la posibilidad del acceso no autorizado.

Artículo 59°. Cada usuario de una computadora en la municipalidad debe de ser identificado de manera única, y el acceso del usuario, así como su actividad en los sistemas debe de ser controlado, monitoreado y revisado.

Artículo 60°. Cada usuario de un sistema debe tener un código de identificación que no sea compartido con otro usuario. Para lograr el acceso a los sistemas automatizados, se requiere que el usuario provea una clave que solo sea conocida por él.

Artículo 61°. Debe establecerse un procedimiento para asegurar que el código de identificación de un usuario sea retirado de todos los sistemas cuando un empleado es despedido o transferido.

Artículo 62°. Los terminales y computadoras personales deben bloquearse luego de quince (15) minutos de inactividad. El usuario tendrá que autenticarse antes de reanudar su actividad.

Artículo 63°. El usuario debe ser instruido en el uso correcto de las características de seguridad del terminal y funciones de todas las plataformas, estaciones de trabajo,

terminales, computadoras personales, etc., y debe cerrar la sesión o bloquear la estación de trabajo cuando se encuentre desatendida.

Artículo 64°. Todas las computadoras de la municipalidad deben proveer pistas de auditoria del ingreso a los sistemas y violaciones de los mismos. A partir de estos datos, los custodios de los sistemas deben elaborar reportes periódicos los cuales deben ser revisados por el área de seguridad informática. Estos reportes también deben incluir la identidad del usuario, y la fecha y hora del evento. Si es apropiado, las violaciones deben ser reportadas al gerente del individuo. Violaciones repetitivas o significantes o atentados de accesos deben ser reportados al gerente a cargo de la persona y al área de seguridad de la información.

GUÍA METODOLÓGICA DE SEGURIDAD DE CONTRASEÑAS

Artículo 66°. Todas las contraseñas deben tener una longitud mínima de ocho (8) caracteres y no deben contener espacios en blanco.

Artículo 67°. Las contraseñas deben ser difíciles de adivinar. Palabras de diccionario, identificadores de usuario y secuencias comunes de caracteres, tales como “12345678” o “QWERTY”, no deben ser empleadas. Así mismo, detalles personales como los nombres de familiares, número de documento de identidad, número de teléfono o fechas de cumpleaños no deben ser usadas salvo acompañados con otros caracteres adicionales que no tengan relación directa. Las contraseñas deben incluir al menos un carácter no alfanumérico. Las contraseñas deben contener al menos un carácter alfabético en mayúscula y uno en minúscula.

Artículo 68°. Todas las contraseñas deben expirar dentro de un periodo que no exceda los noventa (90) días. Cada gerente debe determinar un máximo periodo de vigencia de las contraseñas, el cual es recomendable no sea menos de (30) días.

Artículo 69°. No debe permitirse la reutilización de ninguna de las 5 últimas contraseñas. Esto asegura que los usuarios no utilicen las mismas contraseñas en intervalos regulares. Los usuarios no deben poder cambiar sus contraseñas más de una vez al día.

Artículo 70°. A los usuarios con privilegios administrativos, no se les debe permitir la reutilización de las últimas 13 contraseñas.

Artículo 71°. Todos los servidores públicos están obligados a proteger sus contraseñas, debiéndose seguir las siguientes regulaciones:

- ✓ Bajo ninguna circunstancia, se debe escribir las contraseñas en papel, o almacenarlas en medios digitales no encriptados.
- ✓ Las contraseñas no deben ser divulgadas a ningún otro usuario salvo bajo el pedido de un gerente, con autorización del área de seguridad informática y auditoria interna. Si se divulga la contraseña, esta debe ser cambiada durante el próximo ingreso.
- ✓ El usuario autorizado es responsable de todas las acciones realizadas por alguna persona a quién se le ha comunicado la contraseña o identificador de usuario.
- ✓ Los sistemas no deben mostrar la contraseña en pantalla o en impresiones, para prevenir que éstas sean observadas o recuperadas.
- ✓ Las contraseñas deben estar siempre encriptados cuando se encuentren almacenadas o cuando sean transmitidas a través de redes.
- ✓ El control de acceso a archivos, bases de datos, computadoras y otros sistemas de recursos mediante contraseñas compartidas está prohibido.

Artículo 72°. Los servidores públicos deben tener acceso únicamente al conjunto de transacciones en línea requeridas para ejecutar sus tareas asignadas. Este conjunto de transacciones debe estar claramente definido para prevenir alguna ocurrencia de fraude y malversación.

Artículo 73°. El acceso para la ejecución de transacciones sensibles debe ser controlado mediante una adecuada segregación de tareas. Por ejemplo, los usuarios que tengan permiso para registrar instrucciones de pago no deben poder verificar o aprobar su propio trabajo.

Artículo 74°. Toda operación realizada en los sistemas que afecten información sensible como saldos operativos contables, deben contar con controles duales de aprobación, dichos controles de aprobación deben ser asignada con una adecuada segregación de funciones.

Artículo 75°. Reportes de auditoria de transacciones sensibles o de alto valor deben ser revisados por la gerencia usuaria responsable en intervalos regulares apropiados. Los reportes deben incluir la identidad del usuario, la fecha y la hora del evento.

Artículo 76°. Los controles de acceso de programas deben asegurar que los usuarios no puedan acceder a la información sin autorización Los programas deben poder generar una pista de auditoria de todos los accesos y violaciones.

Artículo 77°. Las violaciones de los controles de acceso se registran y revisan por el usuario y por el personal de Informática. Las violaciones de seguridad deben ser reportadas al gerente del empleado y al área responsable de la administración de la seguridad de la información.

Artículo 78°. Se debe tener especial cuidado particular en todos los ambientes para asegurar que ninguna persona tenga control absoluto. Los operadores de sistemas no deben tener acceso ilimitado a los identificadores de súper usuario. Dichos identificadores de usuario, son solo necesarios durante una emergencia y deben ser cuidadosamente controlados por la gerencia usuaria, quien debe realizar un monitoreo periódico de su utilización.

Artículo 79°. Es responsabilidad del propietario de la información y de los administradores de sistemas ver que los privilegios de acceso estén alineados con las necesidades del negocio, sean asignados basándose en requerimientos y que se comunique la lista correcta de accesos al Área de Informática.

Artículo 80°. En las situaciones donde los usuarios con accesos a información altamente sensible sean despedidos, los supervisores deben coordinar directamente con el área de seguridad informática para eliminar el acceso de ese usuario.

Artículo 81°. Se debe buscar el desarrollo de soluciones técnicas para evitar el uso de accesos privilegiados innecesarios. Luego del despido o renuncia de algún empleado, es responsabilidad del jefe del empleado revisar cualquier archivo físico o digital elaborado o modificado por el usuario. El gerente debe también asignar la propiedad de dicha información a la persona relevante, así como determinar la destrucción de los archivos innecesarios.

Artículo 82°. Todos los usuarios que tienen acceso a las cuentas privilegiadas deben tener sus propias cuentas personales para uso del negocio. Por ende, los administradores de sistemas y servidores públicos con acceso a cuentas privilegiadas deben usar sus cuentas personales para realizar actividades de tipo no privilegiadas.

Artículo 83°. Las cuentas de usuario que no son utilizadas por noventa (90) días deben ser automáticamente deshabilitadas. Las cuentas que no han sido utilizadas por un

periodo largo demuestran que el acceso de información de ese sistema no es necesario. Los custodios de la información deben informar al propietario de la información la existencia de las cuentas inactivas.

Artículo 84°. Todos los accesos a los sistemas de información deben estar controlados mediante un método de autenticación incluyendo una combinación mínima de identificador de usuario/contraseña. Dicha combinación debe proveer la verificación de la identidad del usuario.

Artículo 85°. Para los usuarios con tareas similares, se debe utilizar grupos o controles de acceso relacionados a roles para asignar permisos y accesos a las cuentas del individuo.

Artículo 86°. Todos los usuarios de los sistemas de información deben de tener un identificador de usuario único que sea válido durante el período laboral del usuario. Los identificadores de usuarios no deben de ser utilizados por otros individuos incluso luego de que el usuario original haya renunciado o haya sido despedido.

Artículo 87°. Los sistemas no deben permitir que los usuarios puedan tener sesiones múltiples para un mismo sistema, salvo bajo autorización específica del propietario de la información.

Artículo 89°. Todo equipo de cómputo, alquilado o de propiedad de la municipalidad, así como los servicios compartidos facturados a cada unidad de negocio será usado solo para actividades relacionadas a las funciones de la municipalidad.

Artículo 90°. Los sistemas de la Municipalidad no pueden ser usados para desarrollar software para negocios personales o externos a la municipalidad.

Artículo 91°. Los equipos no deben ser usados para preparar documentos para uso externo, salvo bajo la aprobación escrita de la autoridad competente.

Artículo 92°. Ningún empelado o trabajador usuario recibirá un identificador de acceso a la Red de Comunicaciones, Recursos Informáticos o Aplicaciones hasta que no acepte formalmente la Guía Metodológica de Seguridad propuesta.

Artículo 93°. Los usuarios tendrán acceso autorizado únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones, conforme a los criterios establecidos por el responsable de la información.

Artículo 94°. La longitud mínima de las contraseñas será igual o superior a ocho caracteres, y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.

Artículo 96°. Los identificadores para usuarios temporales se configurarán para un corto período de tiempo. Una vez expirado dicho período, se desactivarán de los sistemas.

GUÍA METODOLÓGICA DE CONTROL DE ACCESO A REDES

Artículo 97°. Los sistemas de red son vulnerables y presentan riesgos inherentes a su naturaleza y complejidad. Los accesos remotos y conexiones con redes externas, exponen a los sistemas de la Municipalidad a niveles mayores de riesgo. Asegurando que todos los enlaces de una red cuenten con adecuados niveles de seguridad, se logra que los activos más valiosos de las unidades de negocio estén protegidos de un ataque directo o indirecto.

Artículo 98°. Todas las conexiones realizadas entre la red interna de la municipalidad e Internet, deben ser controladas por un firewall para prevenir accesos no autorizados. El área de seguridad de información debe aprobar todas las conexiones con redes o dispositivos externos.

El acceso desde Internet hacia la red interna de la municipalidad no debe ser permitido sin un dispositivo de fuerte autenticación o certificado basado en utilización de contraseñas dinámicas.

Artículo 99°. El esquema de direccionamiento interno de la red no debe ser visible desde redes o equipos externos. Esto evita que “hackers” u otras personas pueden obtener fácilmente información sobre la estructura de red de la municipalidad y computadoras internas.

Artículo 100°. Los accesos a los recursos de información deben solicitar como mínimo uno de los tres factores de autenticación:

- ✓ Factor de conocimiento: algo que solo el usuario conoce. Contraseña o PIN.
- ✓ Factor biométrico: algo propio de las características biológicas del usuario. Lectores de retina o identificadores de voz.

Artículo 101°. La posibilidad de efectuar encaminamiento y re-direccionamiento de paquetes, debe ser configurada estrictamente en los equipos que necesiten realizar dicha función.

Artículo 102°. Todos los componentes de la red deben mostrar el siguiente mensaje de alerta en el acceso inicial. "Aviso de alerta: Estos sistemas son de uso exclusivo del personal y agentes autorizados de la municipalidad. El uso no autorizado está prohibido y sujeto a penalidades legales".

Artículo 103°. Todos los componentes de la red de datos deben ser identificados de manera única y su uso restringido. Esto incluye la protección física de todos los puntos vulnerables de una red.

Artículo 104°. Las estaciones de trabajo y computadoras personales deben ser bloqueadas mediante la facilidad del sistema operativo, mientras se encuentren desatendidas.

Artículo 105°. Todas las conexiones de red internas y externas deben cumplir con las políticas de la Municipalidad sobre servicios de red y control de acceso. Es responsabilidad del área de sistemas de información y seguridad de información determinar lo siguiente:

- ✓ Elementos de la red que pueden ser accedidos
- ✓ El procedimiento de autorización para la obtención de acceso
- ✓ Controles para la protección de la red.

Artículo 106°. Todos los servicios habilitados en los sistemas deben contar con una justificación coherente con las necesidades del negocio. Los riesgos asociados a los servicios de red deben determinarse y ser resueltos antes de la implementación del servicio. Algunos servicios estrictamente prohibidos incluyen TFTP e IRC/Chat.

Artículo 107°. Está prohibido conectar a ninguno de los Recursos, ningún tipo de equipo de comunicaciones (Ej. módem) que posibilite la conexión a la red municipal.

Artículo 108°. Está prohibido conectarse a la red municipal a través de otros medios que no sean los definidos.

Artículo 109°. Está prohibido intentar obtener otros derechos o accesos distintos a aquellos que les hayan sido asignados.

Artículo 110°. Está prohibido intentar acceder a áreas restringidas de los Sistemas de Información o de la Red municipal.

Artículo 111°. Está prohibido intentar descifrar las claves, sistemas o algoritmos de cifrado y cualquier otro elemento de seguridad que intervenga en los procesos telemáticos.

Artículo 112°. Está prohibido ingresar a las redes sociales sin previa autorización de la autoridad correspondiente.

Artículo 113°. La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo.

Artículo 114°. El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con cortafuegos incorporado en la misma. No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

Artículo 115°. Internet es una herramienta de trabajo. Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

Artículo 116°. Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

Artículo 117°. En caso de tener que producirse una transmisión de datos importante, confidencial o relevante, sólo se podrán transmitir en forma encriptado.

GUÍA METODOLÓGICA DE CONTROL DE ACCESO AL SISTEMA OPERATIVO

Artículo 118°. Los usuarios que posean privilegios de súper usuario, deben utilizar el mismo identificador con el que se autentican normalmente en los sistemas. Los administradores deben otorgarle los privilegios especiales a los identificadores de los usuarios que lo necesiten.

Artículo 119°. Todos los usuarios deben poseer un único identificador. El uso de identificadores de usuario compartidos debe estar sujeto a autorización. Cada cuenta de usuario debe poseer una contraseña asociada, la cual solo debe ser conocida por el dueño del identificador de usuario.

Artículo 120°. Seguridad adicional puede ser añadida al proceso, como identificadores biométricos o generadores de contraseñas dinámicas.

Artículo 121°. Las aplicaciones críticas deben estar sujetas a periodos de acceso restringidos, el acceso a los sistemas en un horario distinto debe ser deshabilitado o suspendido.

Artículo 122°. Los sistemas, durante el proceso de autenticación, deben mostrar avisos preventivos sobre los accesos no autorizados a los sistemas.

Artículo 123°. Los identificadores de los usuarios deben ser bloqueados luego de 3 intentos fallidos de autenticación en los sistemas, el desbloqueo de la cuenta debe ser realizado manualmente por el administrador del sistema.

Artículo 124°. Los sistemas deben ser configurados para no mostrar ninguna información que pueda facilitar el acceso a los mismos, luego de intentos fallidos de autenticación.

GUÍA METODOLÓGICA DE CONTROL DE ACCESO DE APLICACIÓN

Artículo 125°. Para la generación de cuentas de usuario en los sistemas, así como para la asignación de perfiles, el gerente del área usuaria es el responsable de presentar la 'Solicitud de Usuarios y/o Perfiles de Acceso a los Sistemas de Cómputo', al área de Seguridad Informática, quien generará los Usuarios y Contraseñas correspondientes, para luego remitirlas a Unidad de Capacidades Humanas, para que éste a su vez los entregue al Usuario Final, con la confidencialidad requerida.

Artículo 126°. Se debe otorgar a los usuarios acceso solamente a la información mínima necesaria para la realización de sus labores. Esta tarea puede ser realizada utilizando una combinación de:

- Seguridad lógica de la aplicación.
- Ocultar opciones no autorizadas en los sistemas
- Restringir el acceso a línea de comando
- Limitar los permisos a los archivos de los sistemas (solo lectura)
- Controles sobre la información de salida de los sistemas (reportes, consultas en línea, etc.)

Artículo 127°. Los sistemas que procesan información muy crítica deben ser aislados físicamente de sistemas que procesan información menos crítica.

Artículo 128°. Los relojes de todos los sistemas deben ser sincronizados para asegurar la consistencia de todos los registros de auditoria.

Artículo 129°. Los administradores de los sistemas deben realizar monitoreo periódico de los sistemas como parte de su rutina diaria de trabajo, este monitoreo no debe estar limitado solamente a la utilización y performance del sistema sino debe incluir el monitoreo del acceso de los usuarios a los sistemas.

Artículo 130°. La actividad de los usuarios vinculada al acceso a información clasificada como "Confidencial o "Integridad", debe ser registrada para su posterior inspección. El propietario de la información debe revisar dicho registro mensualmente.

GUÍA METODOLÓGICA SOBRE COMPUTACIÓN MÓVIL Y TELETRABAJO

Artículo 131°. Los usuarios que realizan trabajo en casa con información de la municipalidad, pueden tener el concepto errado de que la seguridad de información solo es aplicable en el trabajo en oficina, sin tomar en cuenta que algunas amenazas de seguridad son comunes en ambos entornos de trabajo y que incluso existen algunas nuevas amenazas en el trabajo en casa.

Artículo 132°. La utilización de programas para el control remoto de equipos está prohibida a menos que se cuente con el consentimiento formal del administrador de seguridad. La utilización inapropiada de este tipo de programas puede facilitar el acceso de un intruso a los sistemas de información de la municipalidad.

Artículo 133°. Medidas de seguridad adicionales deben ser implementadas para proteger la información almacenada en dispositivos móviles. Entre las medidas a tomarse se deben incluir:

- ✓ Encriptación de los datos
- ✓ Contraseñas de encendido
- ✓ Concientización de usuarios
- ✓ Protección de la data transmitida hacia y desde dispositivos móviles.
- ✓ Medidas de autenticación adicionales para obtener acceso a la red de datos.

Artículo 134°. Con el propósito de evitar los problemas relacionados a virus informáticos y propiedad de los datos existentes en computadoras externas, solamente equipos de la municipalidad deben ser utilizados para ser conectados a su red de datos. La única excepción a este punto es la conexión hacia el servidor de correo electrónico para recepción y envío del correo electrónico.

GUÍA METODOLÓGICA DE RESPONSABILIDADES PERSONALES

Artículo 135°. Los usuarios son responsables de toda actividad relacionada con el uso de su acceso autorizado.

Artículo 136°. Los usuarios no deben revelar bajo ningún concepto su identificador y/o contraseña a otra persona ni mantenerla por escrito a la vista, ni al alcance de terceros.

Artículo 137°. Los usuarios no deben utilizar ningún acceso autorizado de otro usuario, aunque dispongan de la autorización del propietario.

Artículo 138°. Si un usuario tiene sospechas de que su acceso autorizado (identificador de usuario y contraseña) está siendo utilizado por otra persona, debe proceder al cambio de su contraseña e informar a su jefe inmediato y éste reportar al responsable de la administración de la red.

Artículo 139°. En el caso que el sistema no lo solicite automáticamente, el usuario debe cambiar su contraseña como mínimo una vez cada 30 días. En caso contrario, se le podrá denegar el acceso y se deberá contactar con el jefe inmediato para solicitar al administrador de la red una nueva clave.

Artículo 140°. El usuario debe proteger, en la medida de sus posibilidades, los datos de carácter personal a los que tienen acceso, contra revelaciones no autorizadas o accidentales, modificación, destrucción o mal uso, cualquiera que sea el soporte en que se encuentren contenidos los datos.

Artículo 141°. Los usuarios sólo podrán crear ficheros que contengan datos de carácter personal para un uso temporal y siempre necesario para el desempeño de su trabajo. Estos ficheros temporales nunca serán ubicados en unidades locales de disco de la computadora de trabajo y deben ser destruidos cuando hayan dejado de ser útiles para la finalidad para la que se crearon.

Artículo 142°. Los usuarios deben notificar a su jefe inmediato cualquier incidencia que detecten que afecte o pueda afectar a la seguridad de los datos de carácter personal: pérdida de listados y/o disquetes, sospechas de uso indebido del acceso autorizado por otras personas, recuperación de datos.

Artículo 143°. Los usuarios únicamente introducirán datos identificativos y direcciones o teléfonos de personas en las agendas de contactos de las herramientas ofimáticas (por ejemplo, en Outlook)

GUÍA METODOLÓGICA DE USO APROPIADO DE LOS RECURSOS

Artículo 144°. Los Recursos Informáticos, Datos, Software, sistema de red están disponibles exclusivamente para cumplimentar las obligaciones y propósito de los procesos operativos. Todo el personal usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

Artículo 145°. Está prohibido el uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.

Artículo 146°. Están prohibidos las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de la municipalidad.

Artículo 147°. Está prohibido introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.

Artículo 148°. Está prohibido introducir voluntariamente programas, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos. El personal contratado por la municipalidad tendrá la obligación de utilizar los programas antivirus y sus actualizaciones para prevenir la entrada en los Sistemas de cualquier elemento destinado a destruir o corromper los datos informáticos.

Artículo 149°. Está prohibido intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.

Artículo 150°. Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.

Artículo 151°. Cualquier fichero introducido en la red corporativa o en el puesto de trabajo del usuario a través de soportes automatizados, Internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas normas y, en especial, las referidas a propiedad intelectual y control de virus.

Artículo 152°. Todo el personal tiene prohibido instalar copias ilegales de cualquier programa, incluidos los estandarizados.

Artículo 153°. Está prohibido poseer, desarrollar o ejecutar programas que pudieran interferir sobre el trabajo de otros usuarios, ni dañar o alterar los Recursos Informáticos.

DISPOSICIONES TRANSITORIAS

Artículo primero. Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día siguiente de su difusión.

Artículo segundo. Las políticas de seguridad de la información para la municipalidad podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo con todas las unidades o por decisión de las autoridades correspondientes.

Artículo tercero. La falta de conocimiento de las normas aquí descritas por parte de los trabajadores y empleados de la municipalidad no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

3. RESULTADOS

Con fines de implementar la Guía Metodológica de seguridad de la información se debe crear el Comité Municipal de Seguridad de la Información (CMSI), la misma que dependerá del área de Informática y Alcaldía.

El CMSI tiene como finalidad la Seguridad de la Información de la Municipalidad Distrital de Recuay. Tiene las siguientes funciones:

- ✓ Velar por el cumplimiento de la normativa de aplicación legal, regulatoria y sectorial referente a la seguridad de la información y a la protección de datos de carácter personal.
- ✓ Recabar de los responsables de las áreas de la municipalidad informes regulares, al menos una vez al semestre, del estado de seguridad de la información de la organización municipal y de los posibles incidentes referentes a Tecnologías de Información y Comunicación (TIC); trasladando sus conclusiones a la jefatura de informática de la municipalidad.
- ✓ Coordinar las actuaciones de seguridad y dar respuesta a las inquietudes de seguridad transmitidas a través de los responsables de las distintas áreas de la municipalidad.
- ✓ Promover la difusión y apoyo a la seguridad de la información dentro de la estructura orgánica de la municipalidad.
- ✓ Llevar a cabo acciones de concienciación, formación y motivación del personal municipal, sobre la importancia de lo establecido en el marco de gestión de seguridad de la información y sobre su implicación en el cumplimiento de las expectativas de los departamentos municipales, usuarios y ciudadanos y la protección de su información.

El CMSI tiene las siguientes funciones:

- ✓ Elaborar y evaluar la Política de Seguridad de la Información de la Municipalidad Distrital de Recuay.

- ✓ Proponer criterios de seguridad: redactar, revisar y evaluar las normas y pautas de seguridad basadas en las normas técnicas peruanas, así como los procedimientos de notificación de incidentes de seguridad.
- ✓ Evaluar e informar sobre los riesgos de seguridad en los activos TIC.
- ✓ Velar por el alineamiento de las actividades de seguridad de la información y los objetivos de la organización municipal, llevando a cabo acciones orientadas a la mejora continua de los procesos de seguridad de la información.
- ✓ Velar por que la seguridad de la información sea parte del proceso de planificación de la organización municipal.

Está conformado por jefe de informática, un representante de las gerencias de la municipalidad y un representante del alcalde.

ROLES: FUNCIONES Y RESPONSABILIDADES

Responsable de Seguridad de la Información

Todas las unidades, así como alcaldía son responsables de la seguridad de la información. Todos están en la obligación bajo responsabilidad de cumplir funciones relativas a la seguridad de los sistemas de información de la Municipalidad Distrital de Recuay, lo cual incluye determinar las decisiones para satisfacer los requisitos de seguridad de la información y de los servicios prestados por la municipalidad.

Por otra parte, tendrá la función de incluir medidas de seguridad en todas las fases de los procesos de seguridad de la información siguiendo una metodología de ciclo de vida apropiada.

Responsable del área de Unidad Social y Capacidades Humanas

Pertenece a la estructura orgánica de la municipalidad, cumple funciones de implicar a todo el personal de la organización municipal en el conocimiento y cumplimiento de la Política de Seguridad de la Información y de todas las normas, procedimientos y prácticas que de ella surjan, así como de los cambios que en aquellas se produzcan. Igualmente, se responsabilizará de la implementación de los compromisos de confidencialidad que deban suscribir los servidores públicos municipales y de la

capacitación continua de los mismos en materia de seguridad. Este rol es desempeñado por el titular de la Dirección General de Personal, Organización y Calidad.

Responsable del Asesoría Legal

Pertenece al Comité de Seguridad Municipal de la Información y asesorará en material legal en lo que se refiere al diseño e implementación de las políticas y medidas que se establezcan en relación a la seguridad de la información. Específicamente en cuanto se refiere al cumplimiento de la legislación sobre seguridad de la información de cuantos contratos, convenios, acuerdos, ordenanzas y similares sea parte la municipalidad. Este rol recae sobre el titular de la Asesoría Jurídica de la organización municipal.

Una vez aprobada la Política de Seguridad de la Información, la municipalidad creará el Comité Municipal de Seguridad de la Información y designará a sus componentes, para el ejercicio de las competencias definidas en la presente política.

ANÁLISIS Y GESTIÓN DE RIESGOS

La red y la información deberán ser sometidas a análisis y gestión de riesgos, evaluando los activos, amenazas y vulnerabilidades a los que están expuestos y proponiendo las contramedidas adecuadas para mitigar los riesgos. Aunque se precisa un control continuo de los cambios realizados en los sistemas, este análisis se repetirá:

- ✓ Al menos una vez al año (mediante revisión y aprobación formal).
- ✓ Cuando ocurra un incidente grave de seguridad.

Para la armonización de los análisis de riesgos, se establecerá una valoración de referencia, mediante rangos, para los diferentes tipos de información manejados y los diferentes servicios prestados.

Para el análisis y gestión de riesgos se usará la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información).

ANÁLISIS DE FODA

Análisis Interno: Permite identificar los puntos fuertes y débiles del interior de la municipalidad. Está constituido por las capacidades y limitaciones de la municipalidad, en los cuales se puede intervenir por encontrarse al interior del objeto

de planificación. Aquí se identifican las fortalezas y debilidades. Las fortalezas son las capacidades (competitivas, tecnológicas, culturales, organizacionales, etc.).

Análisis Externo: Permite identificar los puntos fuertes y débiles del exterior o entorno de la municipalidad. Está constituido por todo aquello que se encuentra fuera de la municipalidad, pero que tiene influencia en ella. Aquí se identifican las oportunidades y amenazas. Las oportunidades son los actores positivos externos a la municipalidad que pueden ser utilizados a favor de su desarrollo; se identifican para ser aprovechadas. Las amenazas son los factores negativos externos a la municipalidad que pueden incidir en contra de su desarrollo; se identifican para ser evitadas, mediatizadas o neutralizadas.

Tabla 1
Análisis Interno y externo

Análisis Interno	
Fortalezas	**Debilidades**
✓ Voluntad política de trabajadores y autoridades ✓ La gestión actual cuenta con un mayor conocimiento sobre las necesidades de la población en la provincia de Recuay. ✓ Coordinación permanente entre el alcalde y los trabajadores municipales. ✓ Trabajos rotativos que brindan oportunidad laboral a la población. ✓ Posee ingresos propios ✓ Existencia de cuadros técnicos que manejan temas relacionados a la gestión municipal, inversión pública (SNIP) y desarrollo local. ✓ Cuenta con equipos de computo ✓ Cuenta con unidades móviles de limpieza ✓ Cuenta con maquinaria pesada ✓ Infraestructura municipal propia ✓ Buena atención y equipamiento del centro médico municipal ✓ Existencia de proyectos que contribuirán con el desarrollo de la provincia de Recuay.	✓ Escasa capacitación del personal ✓ Carencia de sistema de recaudación ✓ Excesiva población laboral ✓ Se desaprovecha la capacidad laboral instalada. ✓ Inadecuada distribución de presupuesto. ✓ Insuficientes unidades móviles para limpieza y obras (Volquete, cortadora) ✓ Demora para cumplir con los requerimientos hechos por el personal (papel, pasajes, etc.) ✓ Infraestructura deficiente, ambientes no aptos para el desenvolvimiento de las funciones. ✓ Débil institucional.

✓ Buen trato al contribuyente y público en general.	

Análisis Externo	
Oportunidades	**Amenazas**
✓ Presencia del programa de modernización municipal (PMM) y plan de Incentivos Municipales (PI). ✓ Presencia de ONGs que realizan acciones de capacitación para trabajadores y funcionarios municipales. ✓ Presencia de colegios particulares ✓ Se encuentra una respuesta favorable por parte del vecino, a las políticas de puertas abierta y el dialogo directo establecido por la actual gestión. ✓ El avance de la tecnología, permite ofrecer una mejor atención al usuario. Por ejemplo, el desarrollo de la web de la municipalidad. ✓ Emisión de dispositivos legales de parte del estado: Ministerio de Economía y Finanzas, Contraloría General de la Republica, entre otros, proporcionan las orientaciones necesarias para el desarrollo de un buen trabajo. ✓ Crecimiento económico del Perú, quien seguirá siendo el país de mayor crecimiento económico de Latinoamérica al menos hasta el 2015.	✓ La crisis económica y recesiva que atraviesa el mundo, afecta las inversiones en el país por ende en los Ingresos municipales, entre otros. ✓ La falta de conciencia tributaria por parte de la población e instituciones que operan en la provincia, que viene ocasionando un alto índice de morosidad en el pago de los tributos. ✓ Fenómenos naturales y cambios climáticos ✓ Inseguridad ciudadana. ✓ Débil conciencia cívica y de valores de los vecinos. ✓ Incremento del índice de violencia en la sociedad, genera que se haga un mayor esfuerzo a fin de poder brindar la seguridad del caso a los vecinos de la provincia. ✓ Crecimiento poblacional. ✓ Existen grupos de reducidos de personas que distorsionan la información sobre la gestión, con el fin de confundir y alarmar a los vecinos.

Fuente: Elaboración Propia

DESARROLLO DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Instrumentos de desarrollo

La Política de Seguridad de la Información de la Municipalidad Distrital de Recuay se desarrollará por medio de normativa de seguridad que afronte aspectos específicos.

Se usarán los siguientes instrumentos:

- Normas de seguridad: Uniformizan el uso de aspectos concretos del sistema.
- Indican el uso correcto y las responsabilidades de los usuarios. Son de carácter obligatorio. También suelen denominarse políticas de seguridad.
- Guías de seguridad: Tienen un carácter informativo y buscan ayudar a los usuarios a aplicar correctamente las medidas de seguridad proporcionando razonamientos en los casos en los que no existan procedimientos precisos.
- Ayudan a prevenir que se pasen por alto aspectos importantes de seguridad que pueden materializarse de varias formas.
- Procedimientos operativos de seguridad (POS): Afrontan tareas concretas, indicando lo que hay que hacer, paso a paso, sin entrar en detalles de proveedores, marcas comerciales o comandos técnicos. Son útiles en tareas repetitivas.
- Instrucciones técnicas (IT): Desarrollan los POS llegando al máximo nivel de detalle, indicando proveedores, marcas comerciales y comandos técnicos servidores públicos para la realización de las tareas.

Estructura general

El desarrollo de esta guía metodológica incluirá, basándose en el análisis de riesgos, aspectos específicos de la Seguridad de la Información tales como las medidas de seguridad.

Marco organizativo: orientado a administrar la seguridad de la información dentro de la organización municipal y establecer un marco gerencial para controlar su implementación. Partiendo de la presente guía metodológica de seguridad se desarrollará el resto del marco normativo de seguridad.

Marco operacional: constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

Planificación: mediante análisis de riesgos, controlando la arquitectura de seguridad y la adquisición de nuevos componentes entre otros aspectos.

Control de Acceso: orientado a controlar el acceso lógico a la información.

Explotación: medidas para la gestión de la seguridad en explotación; partiendo del inventario de activos y controlando la gestión de incidencias, cambios, gestión de la configuración, registros de actividad, entre otros.

Servicios externos: medidas de seguridad orientadas a garantizar que empresas y personas terceras que realicen servicios de cualquier clase contratados por la municipalidad o que de alguna manera se presten bajo el control y/o la dirección de la municipalidad cumplan las políticas y normas de seguridad de la información establecidas.

Continuidad del servicio: acciones a ejecutar en caso de interrupción de los servicios prestados con los medios habituales.

Monitorización del sistema: orientado a garantizar la disponibilidad de las actividades diarias y proteger los procesos críticos de los efectos de fallas significativas o desastres.

Medidas de Protección: para la protección de activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

Gestión del personal: orientado a reducir los riesgos de error humano o uso inadecuado de las instalaciones y equipamientos.

Protección de los equipos: medidas para la protección de los equipos.

Protección de las comunicaciones: dirigido a garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información y elementos y sistemas de comunicación.

Protección de los soportes de información: para garantizar la información que contienen.

Protección de las aplicaciones informáticas: orientado a garantizar la incorporación de medidas de seguridad en los sistemas de información desde su desarrollo y/o implementación y durante su mantenimiento.

Protección de la información: cumpliendo lo dispuesto en la Ley Orgánica de protección de datos de carácter personal y gestionando la información en base a su clasificación.

Protección de los servicios: definiendo las medidas necesarias para mantener la seguridad de los servicios TI.

La normativa de seguridad estará a disposición de todos los miembros de la organización municipal que necesiten conocerla, en particular para aquellos que utilicen, operen o administren los sistemas de información y comunicaciones. La normativa de seguridad estará disponible en la intranet municipal.

Sanciones previstas por incumplimiento

El incumplimiento de la Política de Seguridad de la Información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y características de los preceptos incumplidos. El procedimiento y las sanciones a aplicar serán las establecidas en la legislación sobre régimen disciplinario de la municipalidad.

SEGURIDAD DE LA INFORMACIÓN

Aunque la seguridad de la información no es lo mismo que la seguridad de las TIC, la relación entre ambas es fuerte y crítica. La clasificación de la información de carácter personal (nivel alto, medio o bajo) no se decide por criterios TIC o STIC. Pero una vez determinado su nivel, este implica una serie de requisitos sobre su manipulación en entornos TIC.

Clasificación de la Información

Se debe establecer niveles de información en función de sus exigencias de seguridad.

Estos nivelen son: Confidencial, difusión limitada, sin clasificar y público.

Toda la documentación, digital o impresa, debe indicar la clasificación de la información que contiene, salvo la información catalogada como Pública.

Para dicha clasificación se definirán procedimientos de control tales como:

- ✓ Procedimiento para clasificar información: quién determina a qué clase pertenece y en base a qué criterios.
- ✓ Procedimiento para cambiar la clasificación: quién puede alterar la etiqueta de una información, en base a qué criterios y dejando qué registro.
- ✓ Procedimientos para tratar la información en base a su nivel.

La clasificación de la información debe tener en cuenta las consecuencias que se derivarían de su conocimiento por personas que no deben tener acceso a ella.

Datos de carácter personal

La Municipalidad Distrital de Recuay está formada por la Alcaldía y sus Gerencias Generales, y demás entes que de acuerdo a ley estructuran el Gobierno Local.

Todos los sistemas de información de la municipalidad se ajustarán a los niveles de seguridad requeridos por la normativa.

Obligaciones del personal

Todos los miembros de la municipalidad y las empresas y personas terceras que realicen servicios de cualquier clase contratados por la municipalidad que de alguna manera se presten bajo el control y/o la dirección de la municipalidad tienen la obligación de conocer y cumplir esta Política de Seguridad de la Información y la Normativa de Seguridad.

ANALISIS DE RIESGO
Tabla 2
Valoración de Activos

Ámbito	Ref	Activo	Valor	S/	Aspectos Críticos				
					A	C	I	D	T
Instalaciones	I01	Centro de procesamiento de datos	MA	S/. 100,000.00	8	7	6	7	5
	I02	Computadoras clientes	A	S/. 60,000.00	7	6	6	6	5
Hardware	H01	Controlador de servidor principal	A	S/. 200,000.00	8	5	5	6	5
	H02	Antivirus	M	S/. 3,000.00	4	3	4	4	3
Aplicaciones	A01	SIAF GL	A	S/. 100,000.00	8	6	6	6	6
	A02	SIGA	M	S/. 800,000.00	5	4	4	5	5
	A03	OFIMATICA	M	S/. 100,000.00	5	5	5	5	5
	A04	SISTEMA DE REGISTRO CIVIL		S/. 100,000.00	5	5	5	5	5
	A05	SISTEMA DE CATASTRO	M	S/. 150,000.00	4	4	4	4	5
Datos	D01	BASE DE DATOS	A	S/. 100,000.00	7	7	6	6	6
	D02	BD Sistemas de control	M	S/. 50,000.00	5	4	5	5	6
	D03	BD Gestión Documental	M	S/. 40,000.00	6	6	5	5	6
Red	R01	Cable UTP cat5							
	R02	Switch core x3	M	S/. 40,000.00	5	3	3	4	5
	R03	Access Point	M	S/. 20,000.00	5	3	3	4	5
Servicios	S01	Internet	M	S/. 60,000.00	5	3	3	4	5
	S02	Instalaciones eléctricas	M	S/. 60,000.00	5	3	3	4	5
	S03	Red LAN	M	S/. 60,000.00	4	4	4	4	4
Personal	P01	Soporte técnico	M	S/. 80,000.00	4	4	4	4	4
	P02	Seguridad Informática	M	S/. 100,000.00	6	6	5	4	4
	P03	Planificación y presupuesto		S/. 100,000.00	6	6	5	4	4
	P04	Infraestructura y Comunicaciones	M	S/. 150,000.00	4	5	4	5	5
	P05	Personal administrativo	M	S/. 80,000.00	4	4	4	5	5

Leyenda: A = Autenticidad; C=Confidencialidad; I=Integridad; D=Disponibilidad; T = Trazabilidad

Fuente: MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Tabla 3

Amenazas

Grupo	Ref	Amenaza	Dimensión Afectada					Activos Afectados						
			A	C	I	D	T	I	H	A	D	R	S	P
Desastres naturales	N1	Incendios (rayos)				x		x	x					
	N2	Daños por lluvia/inundaciones				x		x	x					
	N3	Otros desastres Naturales				x		x	x					
De Origen Institucional	I1	Incendios				x		x	x					
	I2	Computadoras clientes				x		x	x					
	I3	Avería de origen físico o lógico				x			x	x				
	I4	Corte del suministro eléctrico				x			x					
	I5	Condiciones inadecuadas de temperatura o humedad				x			x					
	I6	Fallo de serv. de comunicaciones				x						x		
Errores y fallos no intencionados	E1	Difusión de software dañino		x	x	x				x				
	E2	Escapes de información		x							x			
	E3	Alteración accidental de la inform			x					x	x	x	x	
	E4	Destrucción de información				x				x	x	x	x	
	E5	Fugas de información		x						x	x		x	x
	E6	Vulnerabilidades de los programas (software)		x	x	x				x				
	E7	Errores de mant./ actualización de programas (software)			x	x				x				
	E8	Errores de mant/actualización de equipos (hardware)				x			x					
	E9	Pérdida de equipos		x		x			x					
	E10	Indisponibilidad del personal				x								x
Ataques intencionados	A1	Manipulación de los registros documentarios			x		x				x			
	A2	Manipulación de la configuración	x	x	x						x			
	A3	Suplantación de la identidad del usuario	x	x	x					x	x	x	x	
	A4	Uso no previsto		x	x	x			x	x	x	x	x	
	A5	Difusión de software dañino		x	x	x				x				

Grupo	Ref	Amenaza	Dimensión Afectada					Activos Afectados						
			A	C	I	D	T	I	H	A	D	R	S	P
	A6	Alteración de secuencia			x					x		x	x	
	A7	Acceso no autorizado		x	x			x	x	x	x	x	x	
	A8	Destrucción de información				x				x	x	x	x	
	A9	Divulgación de información		x						x	x	x	x	
	A10	Manipulación de programas		x	x	x				x				
	A11	Manipulación de los equipos		x		x			x					
	A12	Robo		x		x			x		x			
	A13	Extorsión		x	x	x								x
	A14	Ingeniería social		x	x	x								x

Fuente: MAGERIT – Versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

DECLARACION DE APLICABILIDAD

Leyenda: (Razón de controles seleccionados)

LR: Requerimientos Legales, CO: Obligaciones Contractuales, BR/BP: Requerimientos del negocio/Mejores Prácticas,

RRA: Resultado de Análisis de Riesgos

Tabla 4
Controles ISO 27001:2013

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
Política de Seguridad	5.1	Política de seguridad de la información								
	5.1.1	Documento de política de seguridad de la información	▪	Ya se encuentra documentado.						Se pueden incluir mejoras
	5.1.2	Revisión de la política de seguridad de la información					▪		SI	Se revisará por lo menos una vez al año.
Aspectos Organizativos de la seguridad	6.1	Organización Interna								
	6.1.1	Compromiso de la Dirección con la	▪	Políticas y presupuesto aprobado.		▪	▪			

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
de la información		seguridad de la información.								
	6.1.2	Coordinación de la seguridad de la información.	▪							
	6.1.3	Asignación de responsabilidades relativas a la seguridad de la información.	▪				▪		SI	Diseño de matriz RACI.
	6.1.4	Proceso de autorización de recursos para el tratamiento de la información.	▪	Aprueba		▪	▪		SI	Por documentar y formalizar.
	6.1.5	Acuerdos de confidencialidad.	▪	Control ya implementado.						
	6.1.6	Contacto con las autoridades.	▪	Control ya implementado.						
	6.1.7	Contacto con grupos de especial interés.	▪	Control ya implementado.						
	6.1.8	Revisión independiente de la seguridad de la información	▪	Auditoria Externa Anual			▪	▪	SI	Por documentar y formalizar
	6.2	Terceros								
	6.2.1	Identificación de los riesgos derivados del acceso de terceros.	▪	Se evalúan los riesgos y firman acuerdos			▪		SI	Se realizaran mejoras para establecer métricas
	6.2.2	Tratamiento de la seguridad en la relación con los clientes.	▪	Solo son 5 grandes clientes ya regulados						
	6.2.3	Tratamiento de la seguridad en contratos con terceros.					▪		SI	Diseñar procedimientos
Gestión de Activos	7.1	Responsabilidad sobre los activos.								
	7.1.1	Inventario de activos.	▪	Control ya implementado.						
	7.1.2	Propiedad de los activos.	▪	Control ya implementado.						
	7.1.3	Uso aceptable de los activos.	▪	Control ya implementado.			▪		SI	Reforzar (sanciones y registros)
	7.2	Clasificación de la información.								
	7.2.1	Directrices de clasificación.					▪		SI	Diseñar e implementar controles
	7.2.2	Etiquetado y manipulado de la información.					▪		SI	Diseñar e implementar controles
Seguridad asociada a Recursos Humanos	8.1	Antes del empleo.								
	8.1.1	Funciones y responsabilidades.	▪	Descripciones de cargos y aceptación de contratos.						Diseño de Matriz RACI
	8.1.2	Investigación de antecedentes.	▪	Control implementado por RRHH	▪					

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
	8.1.3	Términos y condiciones de contratación.	▪	Implementado por Legal y RRHH	▪					
	8.2	Durante el empleo.								
	8.2.1	Responsabilidades de la Dirección.	▪	Control implementado por RRHH						
	8.2.2	Concienciación, formación y capacitación en seguridad de la información.					▪		SI	Diseñar programas de capacitación.
	8.2.3	Proceso disciplinario.	▪	Descargos y suspensiones						
	8.3	Cese del empleo o cambio de puesto de trabajo.								
	8.3.1	Responsabilidad del cese o cambio.								
	8.3.2	Devolución de activos.	▪	Control implementado						
	8.3.3	Retirada de los derechos de acceso.	▪	Control implementado						
Seguridad Física y del Entorno	9.1	Áreas seguras.								
	9.1.1	Perímetro de seguridad física.	▪			▪	▪		SI	Se puedes hacer mejoras
	9.1.2	Controles físicos de entrada.	▪				▪		SI	Habilitar log de visitantes y revisión de los mismos.
	9.1.3	Seguridad de oficinas, despachos e instalaciones.	▪	Controles implementados						
	9.1.4	Protección contra las amenazas externas y de origen ambiental.	▪	Algunos controles implementados		▪	▪		SI	Continuar desarrollo de BCP
	9.1.5	Trabajo en áreas seguras.	▪	Controles Señaléticas	▪				SI	Por defensa civil
	9.1.6	Áreas de acceso público y de carga y descarga.	▪	Regulaciones ambientales (carga y descarga de carbón)			▪		SI	Almacén re recepción
	9.2	Seguridad de los equipos.								
	9.2.1	Emplazamiento y protección de equipos.								
	9.2.2	Instalaciones de suministro.	▪	Algunos controles implementados			▪		SI	Formalizar procedimientos.
	9.2.3	Seguridad del cableado.	▪	Controles implementados			▪		SI	Formalizados
	9.2.4	Mantenimiento de los equipos.					▪		SI	Formalizar procedimientos.
	9.2.5	Seguridad de los equipos fuera de las instalaciones.								
	9.2.6	Reutilización o retirada segura de equipos.								

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
	9.2.7	Retirada de materiales propiedad de la empresa.								
	10.1	Responsabilidades y procedimientos de operación.								
	10.1.1	Documentación de los procedimientos de operación.	▪	Algunos documentos formalizados.			▪		SI	Formalizar y publicar documentos.
	10.1.2	Gestión de cambios.	▪	Controles Implementados.						
	10.1.3	Segregación de tareas.								
	10.1.4	Separación de los recursos de desarrollo, prueba y operación.	▪	Controles Implementados.						
	10.2	Gestión de la provisión de servicios.								
	10.2.1	Provisión de servicios.					▪		SI	Documentar procedimientos.
	10.2.2	Supervisión y revisión de los servicios prestados por terceros.	▪	Controles Implementados.						
	10.2.3	Gestión del cambio en los servicios prestados por terceros.								
	10.3	Planificación y aceptación del sistema.								
Gestión de Comunicaciones y operaciones	10.3.1	Gestión de capacidades.	▪	Algunos documentos formalizados.			▪		SI	Documentar procedimientos.
	10.3.2	Aceptación del sistema.	▪	Controles Implementados.			▪		SI	Sistema interactivo
	10.4	Protección contra el código malicioso y descargable.								
	10.4.1	Controles contra el código malicioso.	▪	Controles Implementados.			▪		SI	Implementados
	10.4.2	Controles contra el código descargado en el cliente.	▪	Controles Implementados.			▪		SI	Implementados
	10.5	Copias de seguridad.								
	10.5.1	Copias de seguridad de la información.	▪	Controles Implementados.			▪		SI	Implementados
	10.6	Gestión de la seguridad de las redes.								
	10.6.1	Controles de red.	▪	Controles Implementados.			▪		SI	Implementados
	10.6.2	Seguridad de los servicios de red.	▪	Controles Implementados.						
	10.7	Manipulación de los soportes.								
	10.7.1	Gestión de soportes extraíbles.	▪	Controles Implementados.			▪		SI	Formalizar procesos de monitoreo.

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
	10.7.2	Retirada de soportes.	▪	Controles Implementados.						
	10.7.3	Procedimientos de manipulación de la información.					▪		SI	Diseñar controles y procedimientos.
	10.7.4	Seguridad de la documentación del sistema.					▪		SI	Formalizar documentación.
	10.8	Intercambio de información.								
	10.8.1	Políticas y procedimientos de intercambio de información.	▪	Política definida.	▪				SI	Mensajería corporativa
	10.8.2	Acuerdos de intercambio.								
	10.8.3	Soportes físicos en tránsito.								
	10.8.4	Mensajería electrónica.	▪	Política definida.					SI	Mensajería corporativa
	10.8.5	Sistemas de información empresariales.	▪	Algunos documentos formalizados.			▪		SI	Formalizar documentación.
	10.9	Servicios de comercio electrónico.								
	10.9.1	Comercio electrónico.		No aplica actualmente.						
	10.9.2	Transacciones en línea.		No aplica actualmente.						
	10.9.3	Información públicamente disponible.	▪	Sitio web corporativo			▪		SI	Transparencia
	10.10	Supervisión.								
	10.10.1	Registros de auditoría.	▪	Logs de sistemas y aplicativos.						
	10.10.2	Supervisión del uso del sistema.								
	10.10.3	Protección de la información de los registros.	▪	Copias de respaldo a logs			▪		SI	Por contingencia
	10.10.4	Registros de administración y operación.								
	10.10.5	Registro de fallos.	▪	Logs y alertas			▪		SI	Cuaderno de bitácora
	10.10.6	Sincronización del reloj.	▪	Servidores NTP						
Control de Acceso	11.1	Requisitos de negocio para el control de acceso.								
	11.1.1	Política de control de acceso.	▪	Política definida.	▪					Formalizar documentos
	11.2	Gestión de acceso de usuario.								
	11.2.1	Registro de usuario.	▪	Procedimiento establecido.			▪			Por formalizar
	11.2.2	Gestión de privilegios.	▪	Gestión centralizada.			▪			Por formalizar

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
	11.2.3	Gestión de contraseñas de usuario.	▪	Gestión centralizada.			▪			Por formalizar
	11.2.4	Revisión de los derechos de acceso de usuario.	▪	Gestión centralizada.			▪			Por formalizar
	11.3	Responsabilidades de usuario.								
	11.3.1	Uso de contraseñas.	▪	Norma definida y publicada.			▪			Obligatorio
	11.3.2	Equipo de usuario desatendido.	▪	Política definida.			▪			Por Formalizar
	11.3.3	Política de puesto de trabajo despejado y pantalla limpia.					▪		SI	Definir Política.
	11.4	Control de acceso a la red.								
	11.4.1	Política de uso de los servicios en red.	▪	Política definida.	▪				SI	Por formalizar
	11.4.2	Autenticación de usuario para conexiones externas.	▪	Política definida.	▪				SI	Por formalizar
	11.4.3	Identificación de los equipos en las redes.	▪	Sistemas de monitoreo y detección.	▪				SI	Por formalizar
	11.4.4	Protección de los puertos de diagnóstico y configuración remotos.	▪	Algunos controles establecidos.			▪		SI	Establecer Línea Base
	11.4.5	Segregación de las redes.								
	11.4.6	Control de la conexión a la red.	▪	Controles implementados.						
	11.4.7	Control de encaminamiento (routing) de red.	▪	Controles implementados.						
	11.5	Control de acceso al sistema operativo.								
	11.5.1	Procedimientos seguros de inicio de sesión.	▪	Algunos controles establecidos.			▪		SI	Formalizar procedimientos.
	11.5.2	Identificación y autenticación de usuario.	▪	Controles implementados.						
	11.5.3	Sistema de gestión de contraseñas.	▪	Controles implementados.						
	11.5.4	Uso de los recursos del sistema.	▪	Controles implementados.						
	11.5.5	Desconexión automática de sesión.	▪	Controles implementados.						
	11.5.6	Limitación del tiempo de conexión.	▪	Controles implementados.						
	11.6	Control de acceso a las aplicaciones y a la información.								
	11.6.1	Restricción del acceso a la información.	▪	Controles implementados.	▪				SI	Formalizar procedimientos

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
	11.6.2	Aislamiento de sistemas sensibles.	▪	Controles implementados.	▪				SI	Formalizar procedimientos
	11.7	Ordenadores portátiles y teletrabajo.								
	11.7.1	Ordenadores portátiles y comunicaciones móviles.	▪	Algunos controles establecidos.			▪		SI	Formalizar procedimientos
	11.7.2	Teletrabajo.								
Adquisición, desarrollo y mantenimiento de Sistemas de Información	12.1	Requisitos de seguridad de los sistemas de información.								
	12.1.1	Análisis y especificación de los requisitos de seguridad.	▪	Procedimientos establecidos			▪			Revisar y fortalecer controles.
	12.2	Tratamiento correcto de las aplicaciones.								
	12.2.1	Validación de los datos de entrada.	▪	Controles establecidos.						
	12.2.2	Control del procesamiento interno.	▪	Controles establecidos.						
	12.2.3	Integridad de los mensajes.	▪	Controles establecidos.						
	12.2.4	Validación de los datos de salida.	▪	Controles establecidos.						
	12.3	Controles criptográficos.								
	12.3.1	Política de uso de los controles criptográficos.					▪		SI	Definir e implementar controles.
	12.3.2	Gestión de claves.					▪		SI	
	12.4	Seguridad de los archivos de sistema.								
	12.4.1	Control del software en explotación.	▪	Controles establecidos.						
	12.4.2	Protección de los datos de prueba del sistema.	▪	Controles establecidos.						
	12.4.3	Control de acceso al código fuente de los programas.	▪	Controles establecidos.						
	12.5	Seguridad en los procesos de desarrollo y soporte.								
	12.5.1	Procedimientos de control de cambios.	▪	Controles establecidos.						
	12.5.2	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	▪	Controles establecidos.						
	12.5.3	Restricciones a los cambios en los paquetes de software.								
	12.5.4	Fugas de información.	▪	Algunos controles establecidos			▪		SI	Fortalecer a nivel de endpoints
	12.5.5	Externalización del desarrollo de software.								
	12.6	Gestión de la vulnerabilidad técnica.								
	12.6.1	Control de las vulnerabilidades técnicas	▪	Algunas actividades definidas			▪		SI	Formalizar procedimientos.

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
Gestión de incidentes de la seguridad de la Informaci ón	13.1	Notificación de eventos y puntos débiles de seguridad de la información.								
	13.1.1	Notificación de los eventos de seguridad de la información.	▪	Controles Implementados .						
	13.1.2	Notificación de puntos débiles de seguridad.	▪	Análisis de vulnerabilidad es			▪		SI	Establecer frecuencia y formalizar.
	13.2	Gestión de incidentes y mejoras de seguridad de la información.								
	13.2.1	Responsabilidades y procedimientos.					▪		SI	Formalizar comité de seguridad.
	13.2.2	Aprendizaje de los incidentes de seguridad de la información.	▪	Algunos controles implementados .			▪		SI	Formalizar procedimientos.
	13.2.3	Recopilación de evidencias.	▪	Controles Implementados .			▪		SI	Estandarizar métodos.
Gestión de la continuida d del negocio	14.1	Aspectos de seguridad de la información en la gestión de la continuidad del negocio.								
	14.1.1	Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	▪	En etapa inicial			▪		SI	Continuar desarrollo
	14.1.2	Continuidad del negocio y evaluación de riesgos.	▪	En etapa inicial			▪		SI	Continuar desarrollo
	14.1.3	Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.					▪		SI	Formalizar documentos.
	14.1.4	Marco de referencia para la planificación de la cont. del negocio.					▪		SI	Definir directrices
	14.1.5	Pruebas, mantenimiento y reevaluación de planes de continuidad.					▪		SI	Diseñar plan de pruebas y mejoramiento.
Cumplimi ento	15.1	Cumplimiento de los requisitos legales.								
	15.1.1	Identificación de la legislación aplicable.		No existen regulaciones aplicables					NO	
	15.1.2	Derechos de propiedad intelectual (DPI).								
	15.1.3	Protección de los documentos de la organización.	▪	Controles establecidos.	▪					Formalizar procedimientos

CONTROLES ISO 27001:2013			Control Actual	Comentarios (o Justificación de exclusión)	Controles seleccionados y razones de selección				¿Aplica?	Comentarios de implementación
					LR	CO	BR/BP	RRA		
Clausula	**Sec.**	**Control/Objetivo de Control**								
	15.1.4	Protección de datos y privacidad de la información de carácter personal.	▪	Algunos controles aplicados.			▪		SI	Fortalecer controles y formalizar documentación.
	15.1.5	Prevención del uso indebido de recursos de tratamiento de la información.				▪	▪		SI	Diseñar e implementar controles.
	15.1.6	Regulación de los controles criptográficos.					▪			Diseñar e implementar controles.
	15.2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.								
	15.2.1	Cumplimiento de las políticas y normas de seguridad.	▪	Controles establecidos.	▪					Formalizar procedimientos
	15.2.2	Comprobación del cumplimiento técnico.	▪	Controles establecidos.						Formalizar procedimientos
	15.3	Consideraciones sobre las auditorías del sistema de información.								
	15.3.1	Controles de auditoría de los sistemas de información.	▪	Controles establecidos.			▪			Formalizar procedimientos
	15.3.2	Protección de las herramientas de auditoría de los sistemas de información.	▪	Controles establecidos.			▪			Formalizar procedimientos

Fuente: ISO 27001-2013 Elaboración: Propia

4. ANÁLISIS Y DISCUSIÓN

Respecto al estado actual en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay, el 30.0% señalaron que se encuentra entre malo y regular, el 50.0% calificaron que se encuentra entre normal y bueno, y el 20.0% dijeron que se encuentra en estado excelente. Sobre la disponibilidad de la Guía Metodológica en el tratamiento de la seguridad de la información, 35.0% señalaron como malo y regular, el 45% como normal y bueno, y el 20.0% como excelente. Con referencia a las características que presenta la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades y sus formas de prevención, el 25.0% señaló como malo y como regular, el 5% como normal y bueno, y el 20.0% como excelente.

Sobre si la Guía metodológica concientiza a los servidores públicos sobre la seguridad física del sistema informático, el 20% valoraron como malo y regular, el 55.0% como normal y bueno, y el 25.0% como excelente. Respecto a concientización de la Guía metodología a los servidores públicos sobre la seguridad lógica del sistema informático, el 20.0% valoró como malo y regular, el 55.0% como normal y bueno, y el 25.0% como excelente. Con referencia a cómo califican la participación de los trabajadores en función de la Guía metodológica propuesta, el 25.0% valoraron como malo y regular, el 50.0% como normal y bueno, y el 20.0% como excelente.

Con referencia a cómo consideran el nivel de seguridad generado por la Guía metodológica en la generación de documentos en el sistema informático, el 20.0% valoraron como malo y regular, el 55.0% como normal y bueno, y el 25.0% como excelente. Sobre cómo es el nivel de seguridad en la generación de documentos aportado por la Guía Metodológica en el sistema informático, el 20.0% valoró como malo y regular, el 60.0% como normal y bueno, y el 20.0% como excelente. Sobre cómo califican el nivel de seguridad del sistema informático, el 35.0% calificaron como malo y regular, el 45.0% como normal y bueno, y el 20.0% como excelente.

Respecto a cómo consideran el aporte de mejora del nivel de seguridad en el procesamiento de documentos generado por la guía metodológica en el sistema

informático, el 15.0% valoró como malo y regular, el 60.0% normal y bueno, y el 25.0% calificaron como excelente. Sobre cómo califican el nivel de seguridad del sistema informático, el 20.0% valoraron como malo y regular, el 55.0% como normal y bueno, y el 25.0% calificaron como excelente. Con referencia a cuáles son las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay, el 15.0% valoraron como malo y regular, el 60.0% como normal y bueno, y el 20.0% como excelente.

Con respecto a las investigaciones antecedentes, las conclusiones a las que arriba Merizalde & Alvarado (2013), en el sentido de que los resultados de las evaluaciones a todo el personal que el Manual Integrado de Calidad ayuda a direccionar a la empresa al cumplimiento total de todos los requisitos y a su vez a la implementación de los Sistemas Integrados de Gestión concuerdan ligeramente ya que en el caso de la presente investigación ayuda ligeramente entre un 25% al 30%.

Flores & Arellano (2012), concluyó que la elaboración de la guía permitió crear sinergias en los procesos de formación con la mayoría del personal, conocer las herramientas que se utilizan para las mediciones de los procesos. En ese sentido, los resultados obtenidos sobre la Guía Metodológica mejora ligeramente la seguridad de la información están d acuerdo con los resultados de la investigación antecedente.

Los resultados obtenidos concuerdan con los de la investigación antecedente del Ministerio de la Protección Social COLCIENCIAS (2010) en el sentido de que la Guía Metodológica para la elaboración de Guía de Atención Integral en el Sistema General de Seguridad Social en Salud colombiano, sintetiza, analiza y estructura en pasos organizados, las metodologías internacionales para el desarrollo, adaptación y evaluación de los procesos.

Los resultados obtenidos en la presente investigación concuerdan ligeramente en las porcentualidades obtenidas Rayme (2007) respecto a que las estrategias que se deben utilizar en la gestión de seguridad de la información son: primero, la importancia de desarrollar políticas de seguridad: UNMSM 37 %, UNFV 19% y UPSJB 24%.

5. CONCLUSIONES Y RECOMENDACIONES

El estado actual, según la encuesta, en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay, el 30.0% señalaron que se encuentra entre malo y regular, el 50.0% calificaron que se encuentra entre normal y bueno, y el 20.0% dijeron que se encuentra en estado excelente.

Las características que presenta la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades y sus formas de prevención, el 25.0% señalaron como malo y como regular, el 55.0% como normal y bueno, y el 20.0% como excelente.

Las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay, para el 15.0% de los encuestados valoraron como malo y regular, el 60.0% como normal y bueno, y el 20.0% como excelente.

Respecto a las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay se estableció que es en la seguridad de la información, la cual fue calificado por el 15.0% como malo y regular, el 60.0% normal y bueno, y el 25.0% calificaron como excelente.

Recomendaciones

La Alcaldía, Regidores y el área de Informática deben tener en cuenta el estado actual de la seguridad de la información en la Municipalidad Provincial de Recuay, ya que el 30.0% señalaron que se encuentra entre malo y regular, para ello se recomienda realizar evaluaciones periódicas de la seguridad de la información con la participación conjunta de todos los trabajadores de la municipalidad involucrados con el sistema de la información.

Evaluar periódicamente la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades y sus formas de prevención, aplicar la Guía Metodológica en cada período.

Continuar con capacitaciones internas y externas en el conocimiento y aplicación de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay.

Valorar y evaluar periódicamente las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay.

6. AGRADECIMIENTOS

A los docentes de la Universidad San Pedro, quienes supieron formarnos en el ámbito profesional, social y humano.

Al Ing. Oscar Ascón Valdivia, por la asesoría y el apoyo académico profesional que nos brindó en el desarrollo de la presente investigación.

A la Municipalidad Provincial de Recuay por el apoyo y permiso de realizar en sus instalaciones el presente trabajo de investigación.

Elizabeth y Henry

7. REFERENCIAS BIBLIOGRÁFICAS

Academia Latinoamericana de la Seguridad Informática. (2011 de 01 de 14). Unidad 1: *Introducción a la Seguridad de Información.*

Aldegani, Gustavo. Miguel. (1997). *Seguridad Informática*. MP Ediciones. Argentina. Página 22.

Brinkley, D. L., & SChell, R. R. (1995). *Information Security: An Integrated Collection of Essays: Essay 1 What is there to worry about?* An Introduction to the Computer Security Problem. California USA: ACSAC.

Chiavenato I. (2006). *Introducción a la teoría general de la administración*, McGraw-Hill Interamericana.

Czinkota Michael y Kotabe Masaaki. (2001). *Administración de Mercadotecnia.* International Thomson Editores. Segunda Edición. Pág. 115.

Drucker, P. F. (1999). *Management Challenges for the 21st Century*. New York: Prenticel Hall.

Flores Cornejo, Gary & Arellano Yungazaca, Luis (2012). *Guía metodológica para la implementación de un Sistema Integrado de Gestión en la empresa Cortiplast S. A.* Universidad Politécnica Salesiana. Guayaquil. Ecuador.

Harris, S. (2004). CISSP Certification: *All in One Exam Guide*. Emerville California USA: Mc Graw Hill.

Hernando, S. (2005). *El coste de los problemas de seguridad*. Hispasec Sistemas.

INDECOPI. (2004). *Norma Técnica Peruana "NTP-ISO/ IEC 17799:2004 EDI. Tecnología de la Información.* Primera versión. Lima.

INDECOPI. (2009). *NTP -ISO/IEC 27005,2009 EDI Tecnologías de Información. Técnicas de Seguridad. Gestión de Riesgo en Seguridad de Información.* Lima.

Laudon, Kenneth C. & Laudon, Jane P. (2004). *Sistemas de Información Gerencial,* Pearson Educación S.A. de C.V.

MAGERIT (2012). *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información"* Libro I - Método MAGERIT 3.0.

Merizalde Guerra, Federico & Alvarado San Andrés, Luis (2013). *Propuesta de Guía Metodológica de un Sistema Integrado de Gestión - basado en ISO 9001, ISO 14001 y OHSAS 18001- para Airful International S.A. prestadora de servicios en el Aeropuerto Internacional José Joaquín de Olmedo, Guayaquil.* Universidad Politécnica Salesiana Sede Guayaquil. Ecuador.

Ministerio de la Protección Social – COLCIENCIAS (2010). *Guía Metodológica para la elaboración de Guías de Atención Integral en el Sistema General de Seguridad Social en Salud colombiano.* ISBN: 978-958-8361-81-9. Bogotá, Colombia.

Montes De Paz, Marta (2010). *Seguridad Lógica y de accesos y su auditoría*. Universidad Carlos III de Madrid. España.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. (1995). *An Introduction to Computer Security: The NIST Handbook. Special Publication 800-12 Washington USA:* National Institute of Standards and Technology (NIST).

Rayme Serrano, Rubén Alejandro (2007). *Gestión de seguridad de la información y los servicios críticos de las universidades: un estudio de tres casos en Lima Metropolitana.* Lima Perú. http://cybertesis.unmsm .edu.pe/xmlui/handle/cybertesis/428

REAL ACADEMIA DE LA LENGUA ESPAÑOLA RAE (2001). *Diccionario de la Real Academia de la Lengua Española.* 22ª edición. España: French & European Publications.

Stoneburner, G. (2001). *NIST Special Publication 800-33: Underlying Technical*. Gaithersburg USA: National Institute of Standards and Technology (NIST).

Tupia, Manuel (2013) *Gestión de Servicios de tecnologías de información bajo la óptica de ITIL* V3. Primera edición. Lima: Tupia Consultores y Auditores S.A.C.

Tupia, Manuel (2013ª) *Administración de la Seguridad de Información*. Segunda edición. Lima: Tupia Consultores y Auditores S.A.C.

Valdez, Guadalupe (2005). *Guía Metodológica para el Diagnóstico Municipal Participativo y Planificación Local con Perspectiva de Derechos, Género y Ciclo de Vida*.

Villena Aguilar, Moiss Antonio. (2006). *Sistema de gestión de seguridad de información para una institución financiera*. Pontificia Universidad Catolica del Perú.

8. ANEXOS

ANEXO N° 01: RESULTADOS ESTADISTICOS

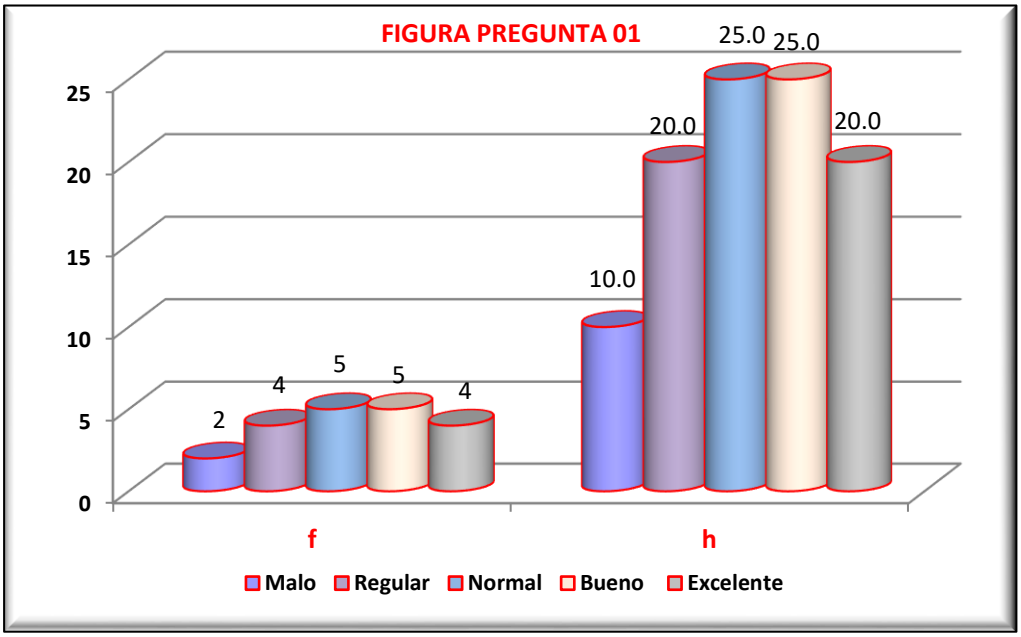
Tabla 5. Pregunta 1

P1. ¿Cuál es el estado actual en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	2	10.0
Regular	4	20.0
Normal	5	25.0
Bueno	5	25.0
Excelente	4	20.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 1 de la encuesta planteada sobre cuál es el estado actual en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay, 02 personas encuestadas (10.0%) valoraron como malo, 04 de ellos (20.0%) valoraron como regular, 05 personas encuestadas (25.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 04 personas encuestadas (20.0%) calificaron como excelente.

Figura 10. Pregunta 1



Fuente: Encuesta

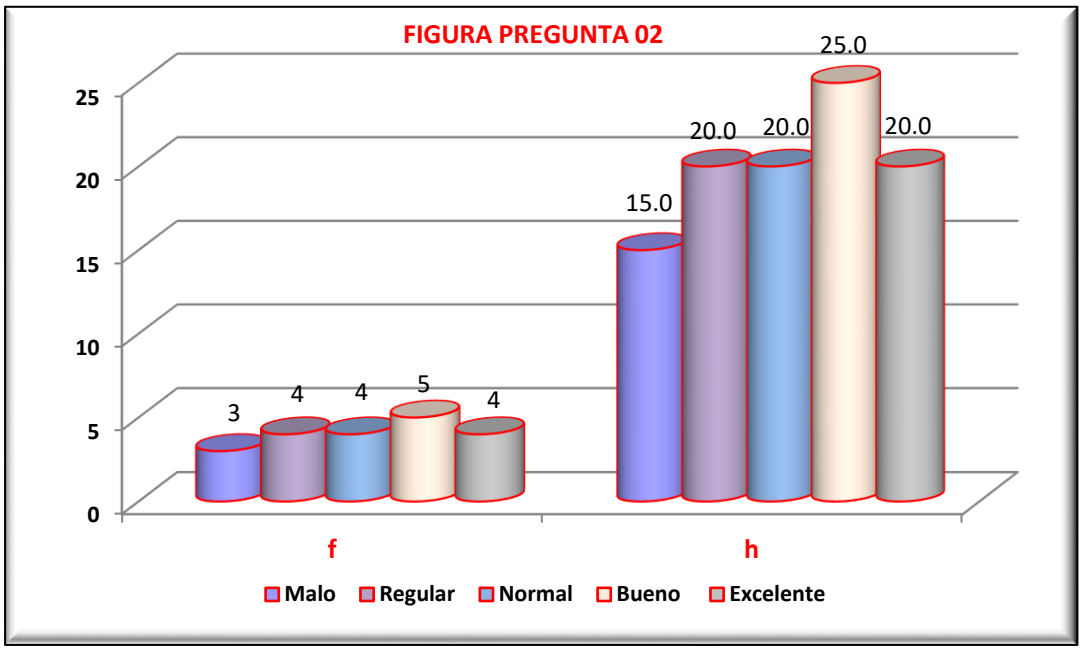
Tabla 6. Pregunta 2

P2. ¿Está disponible la Guía Metodológica en el tratamiento de la seguridad de la información en la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	3	15.0
Regular	4	20.0
Normal	4	20.0
Bueno	5	25.0
Excelente	4	20.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 2 de la encuesta planteada sobre si está disponible la Guía Metodológica en el tratamiento de la seguridad de la información en la Municipalidad Provincial de Recuay, 03 personas encuestadas (15.0%) valoraron como malo, 04 de ellos (20.0%) valoraron como regular, 04 personas encuestadas (20.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 04 personas encuestadas (20.0%) calificaron como excelente.

Figura 11. Pregunta 2



Fuente: Encuesta

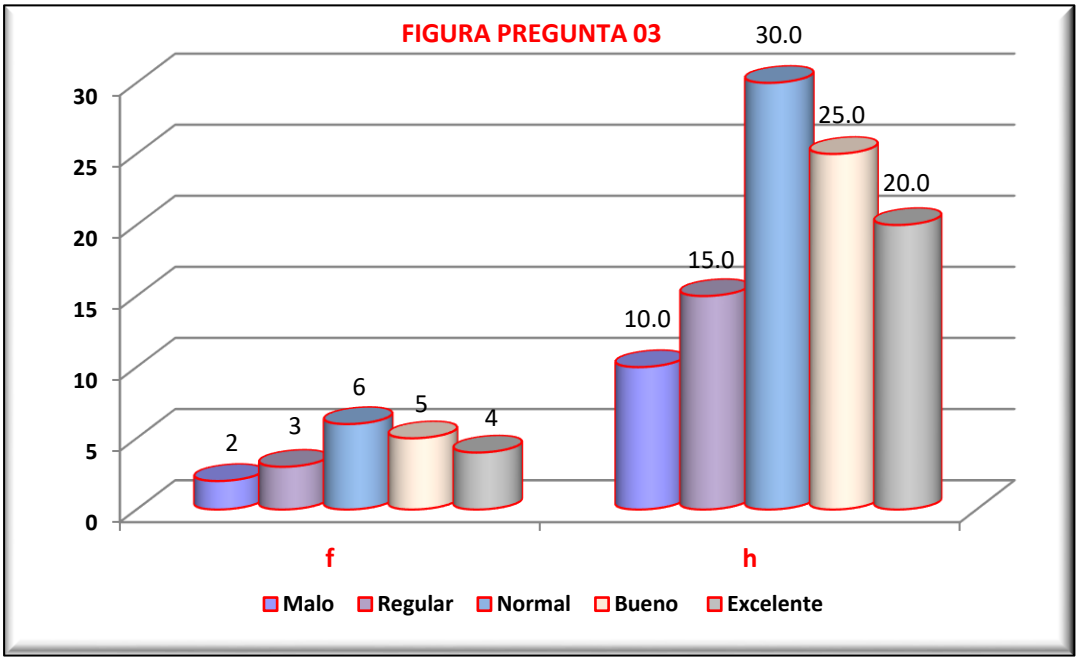
Tabla 7.
Pregunta 3

P3. ¿Qué características presenta la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades y sus formas de prevención?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	2	10.0
Regular	3	15.0
Normal	6	30.0
Bueno	5	25.0
Excelente	4	20.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 3 de la encuesta planteada sobre qué características presenta la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades y sus formas de prevención, 02 personas encuestadas (10.0%) valoraron como malo, 03 de ellos (15.0%) valoraron como regular, 06 personas encuestadas (30.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 04 personas encuestadas (20.0%) calificaron como excelente.

Figura 12. Pregunta 3



Fuente: Encuesta

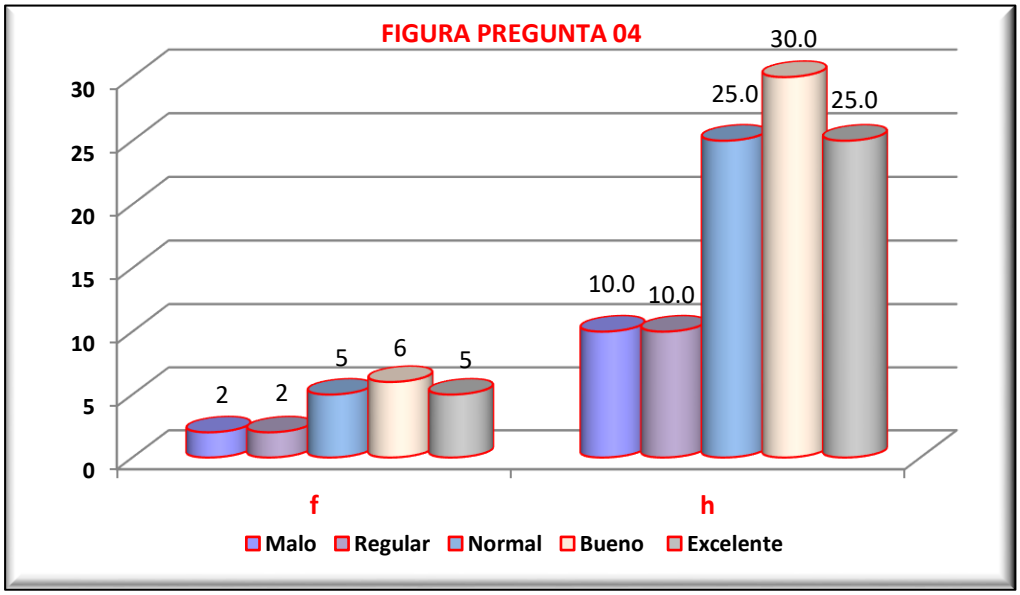
Tabla 8. Pregunta 4

P4. ¿La Guía metodología concientiza a los servidores públicos sobre la seguridad física del sistema informático en la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	2	10.0
Regular	2	10.0
Normal	5	25.0
Bueno	6	30.0
Excelente	5	25.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 4 de la encuesta planteada sobre si la Guía metodológica concientiza a los servidores públicos sobre la seguridad física del sistema informático en la Municipalidad Provincial de Recuay qué características presenta la seguridad de la información de la Municipalidad Provincial de Recuay, 02 personas encuestadas (10.0%) valoraron como malo, 02 de ellos (10.0%) valoraron como regular, 05 personas encuestadas (25.0%) calificaron como normal, 06 de ellos (30.0%) valoraron como bueno y 05 personas encuestadas (25.0%) calificaron como excelente.

Figura 13. Pregunta 4



Fuente: Encuesta

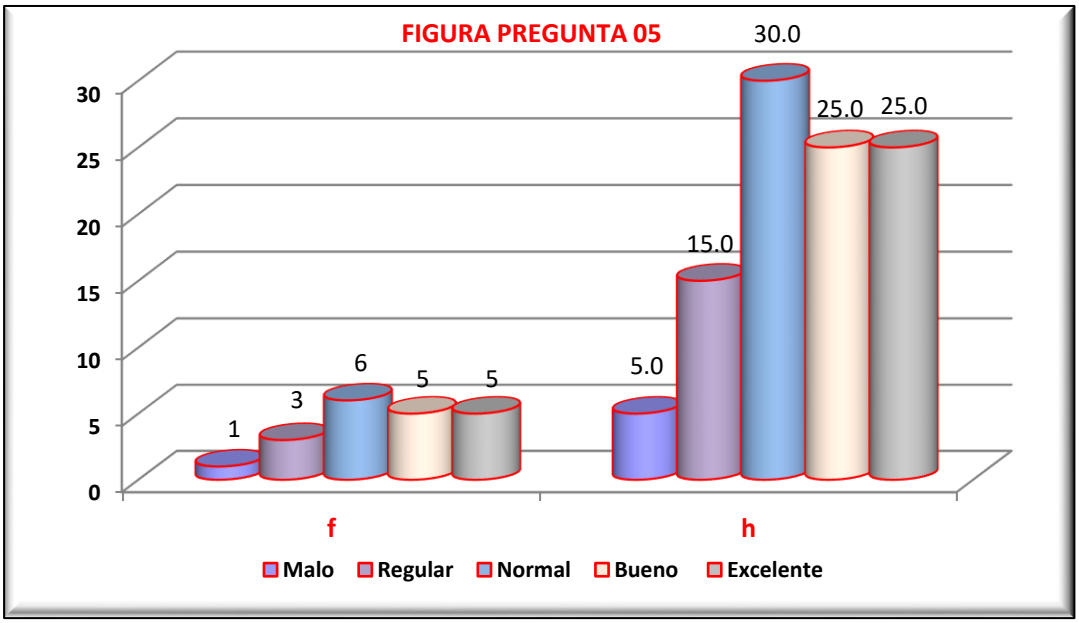
Tabla 9. Pregunta 5

P5. ¿Cómo valora la concientización de la Guía metodología a los servidores públicos sobre la seguridad lógica del sistema informático en la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	1	5.0
Regular	3	15.0
Normal	6	30.0
Bueno	5	25.0
Excelente	5	25.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 5 de la encuesta planteada sobre cómo valora la concientización de la Guía metodología a los servidores públicos sobre la seguridad lógica del sistema informático en la Municipalidad Provincial de Recuay, 01 persona encuestada (5.0%) valoró como malo, 03 de ellos (15.0%) valoraron como regular, 06 personas encuestadas (30.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 05 personas encuestadas (25.0%) calificaron como excelente.

Figura 14. Pregunta 5



Fuente: Encuesta

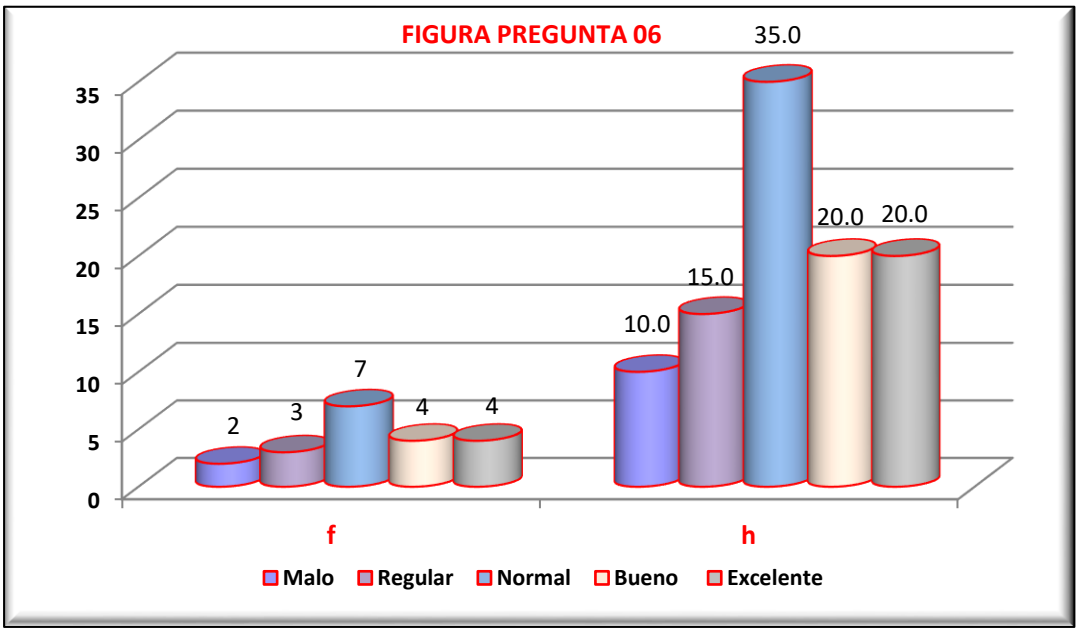
Tabla 10. Pregunta 6

P6. ¿Cómo calificas la participación de los trabajadores participan en función de la Guía metodológica propuesta en la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	2	10.0
Regular	3	15.0
Normal	7	35.0
Bueno	4	20.0
Excelente	4	20.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 6 de la encuesta planteada sobre cómo califican la participación de los trabajadores participan en función de la Guía metodológica propuesta en la Municipalidad Provincial de Recuay, 02 personas encuestadas (10.0%) valoraron como malo, 03 de ellos (15.0%) valoraron como regular, 07 personas encuestadas (35.0%) calificaron como normal, 04 de ellos (20.0%) valoraron como bueno y 04 personas encuestadas (20.0%) calificaron como excelente.

Figura 15. Pregunta 6



Fuente: Encuesta

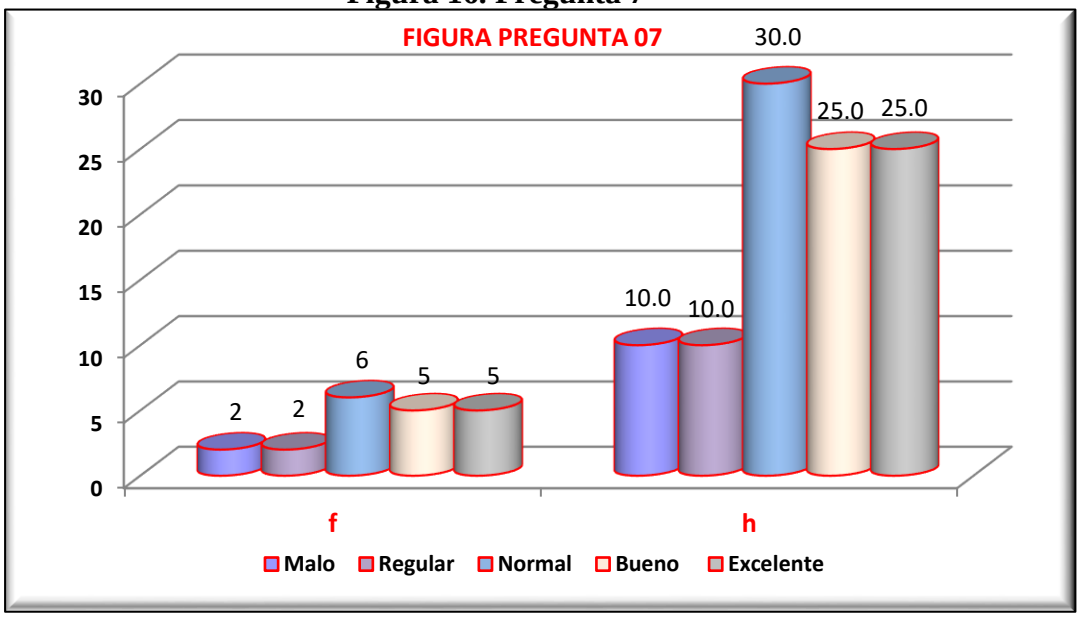
Tabla 11. Pregunta 7

P7. ¿Cómo consideras el nivel de seguridad generado por la Guía metodológica en la generación de documentos en el sistema informático de la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	2	10.0
Regular	2	10.0
Normal	6	30.0
Bueno	5	25.0
Excelente	5	25.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 7 de la encuesta planteada sobre cómo consideran el nivel de seguridad generado por la Guía metodológica en la generación de documentos en el sistema informático de la Municipalidad Provincial de Recuay, 02 personas encuestadas (10.0%) valoraron como malo, 02 de ellos (10.0%) valoraron como regular, 06 personas encuestadas (30.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 05 personas encuestadas (25.0%) calificaron como excelente.

Figura 16. Pregunta 7



Fuente: Encuesta

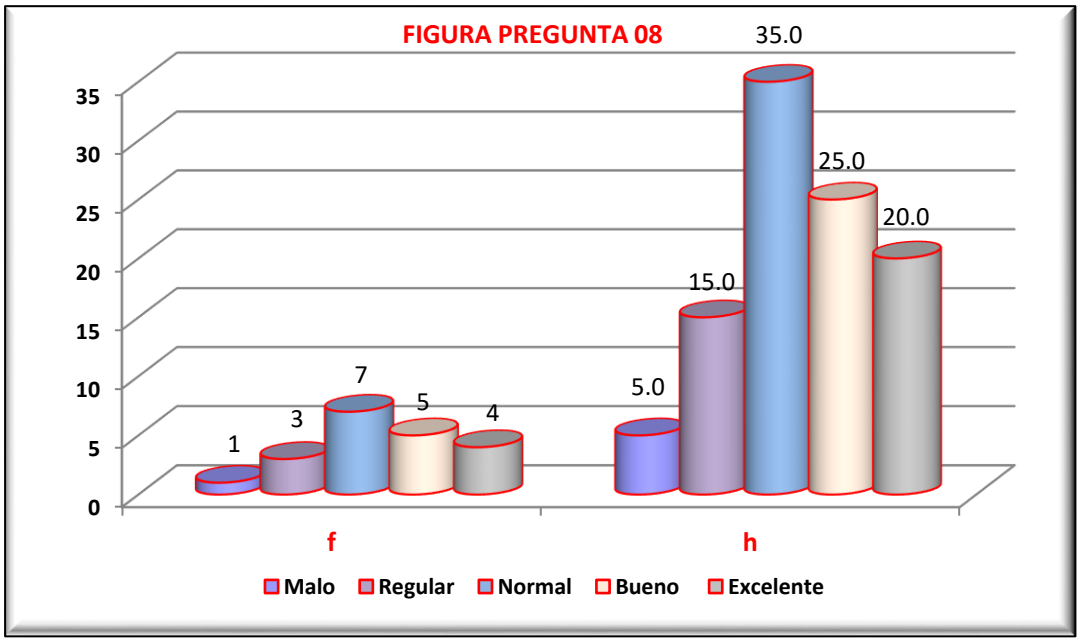
Tabla 12. Pregunta 8

P8. ¿Cómo es el nivel de seguridad en la generación de documentos aportado por la Guía Metodológica en el sistema informático de la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	1	5.0
Regular	3	15.0
Normal	7	35.0
Bueno	5	25.0
Excelente	4	20.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 8 de la encuesta planteada sobre cómo es el nivel de seguridad en la generación de documentos aportado por la Guía Metodológica en el sistema informático de la Municipalidad Provincial de Recuay, 01 persona encuestada (5.0%) valoró como malo, 03 de ellos (15.0%) valoraron como regular, 07 personas encuestadas (35.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 04 personas encuestadas (20.0%) calificaron como excelente.

Figura 17. Pregunta 8



Fuente: Encuesta

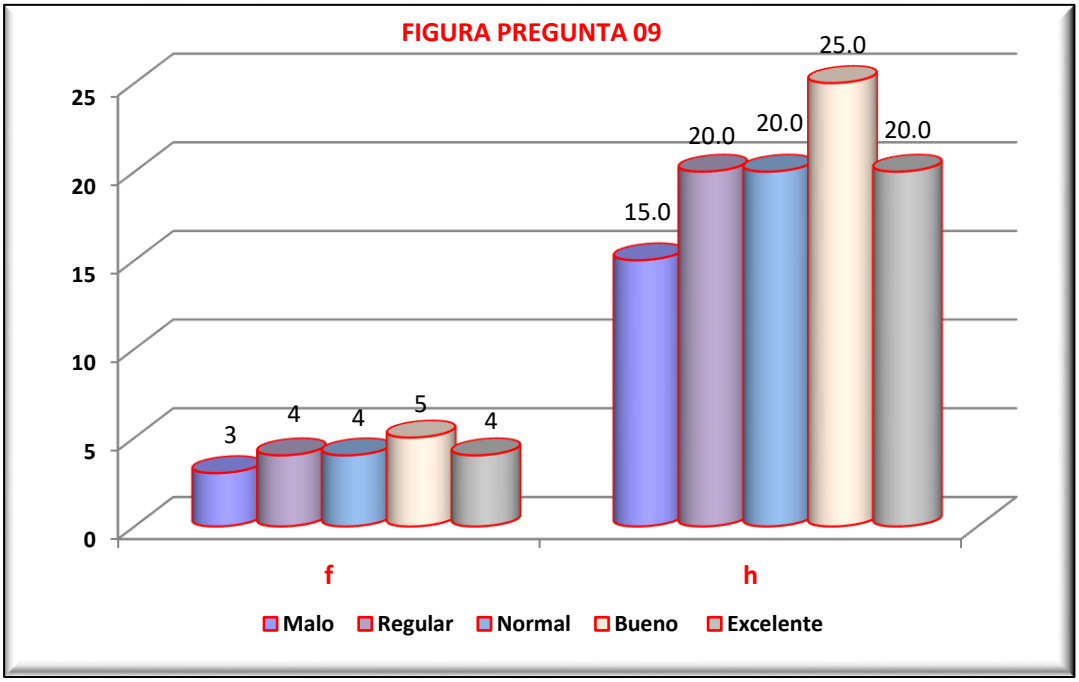
Tabla 13. Pregunta 9

P9. ¿Cómo calificas el nivel de seguridad del sistema informático de la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	3	15.0
Regular	4	20.0
Normal	4	20.0
Bueno	5	25.0
Excelente	4	20.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 9 de la encuesta planteada sobre cómo califican el nivel de seguridad del sistema informático de la Municipalidad Provincial de Recuay, 03 personas encuestadas (15.0%) calificaron como malo, 04 de ellos (20.0%) valoraron como regular, 04 personas encuestadas (20.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 04 personas encuestadas (20.0%) calificaron como excelente.

Figura 18. Pregunta 9



Fuente: Encuesta

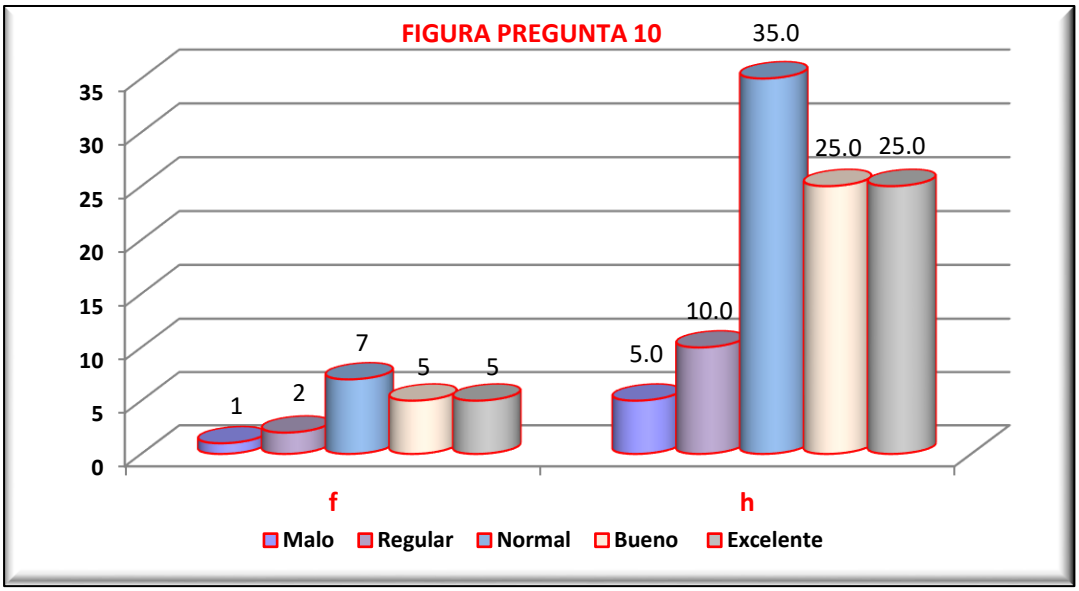
Tabla 14. Pregunta 10

P10. ¿Cómo consideras el aporte de mejora del nivel de seguridad en el procesamiento de documentos generado por la guía metodológica en el sistema informático de la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	1	5.0
Regular	2	10.0
Normal	7	35.0
Bueno	5	25.0
Excelente	5	25.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 10 de la encuesta planteada sobre cómo consideran el aporte de mejora del nivel de seguridad en el procesamiento de documentos generado por la guía metodológica en el sistema informático de la Municipalidad Provincial de Recuay, 01 persona encuestada (5.0%) valoró como malo, 02 de ellos (10.0%) valoraron como regular, 07 personas encuestadas (35.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 05 personas encuestadas (25.0%) calificaron como excelente.

Figura 19. Pregunta 10



Fuente: Encuesta

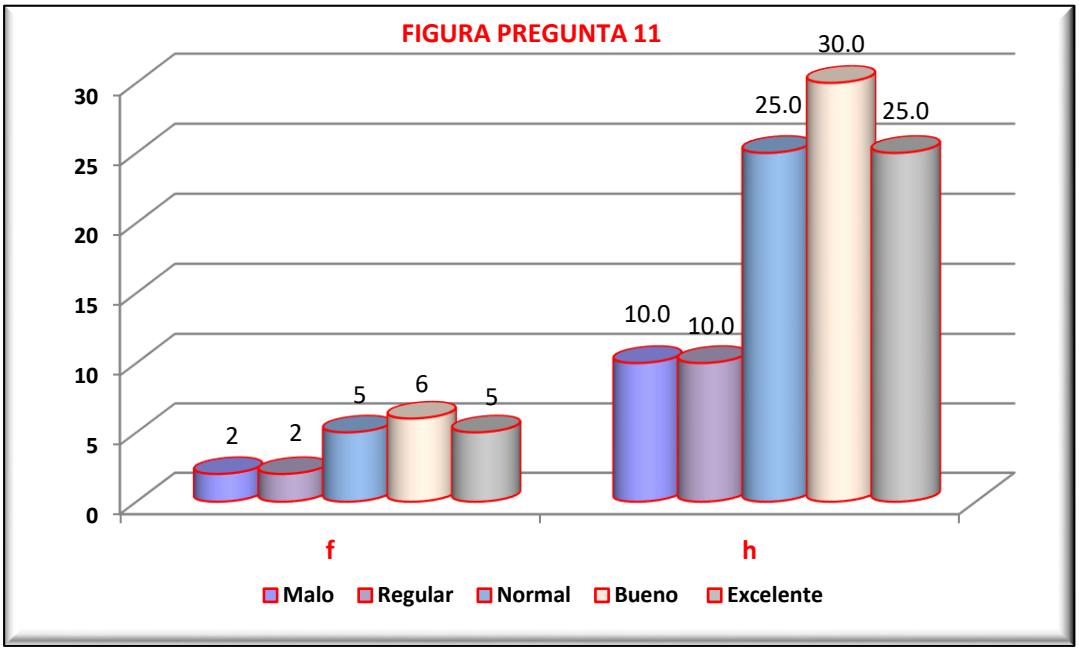
Tabla 15. Pregunta 11

P11. ¿Cómo califica las contribuciones de la norma ISO/IEC 27001:2013 en la estructuración de la información en la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	2	10.0
Regular	2	10.0
Normal	5	25.0
Bueno	6	30.0
Excelente	5	25.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 11 de la encuesta planteada sobre cómo califican el nivel de seguridad del sistema informático de la Municipalidad Provincial de Recuay, 02 personas encuestadas (10.0%) calificaron como malo, 02 de ellos (10.0%) valoraron como regular, 05 personas encuestadas (25.0%) calificaron como normal, 06 de ellos (30.0%) valoraron como bueno y 05 personas encuestadas (25.0%) calificaron como excelente.

Figura 20. Pregunta 11



Fuente: Encuesta

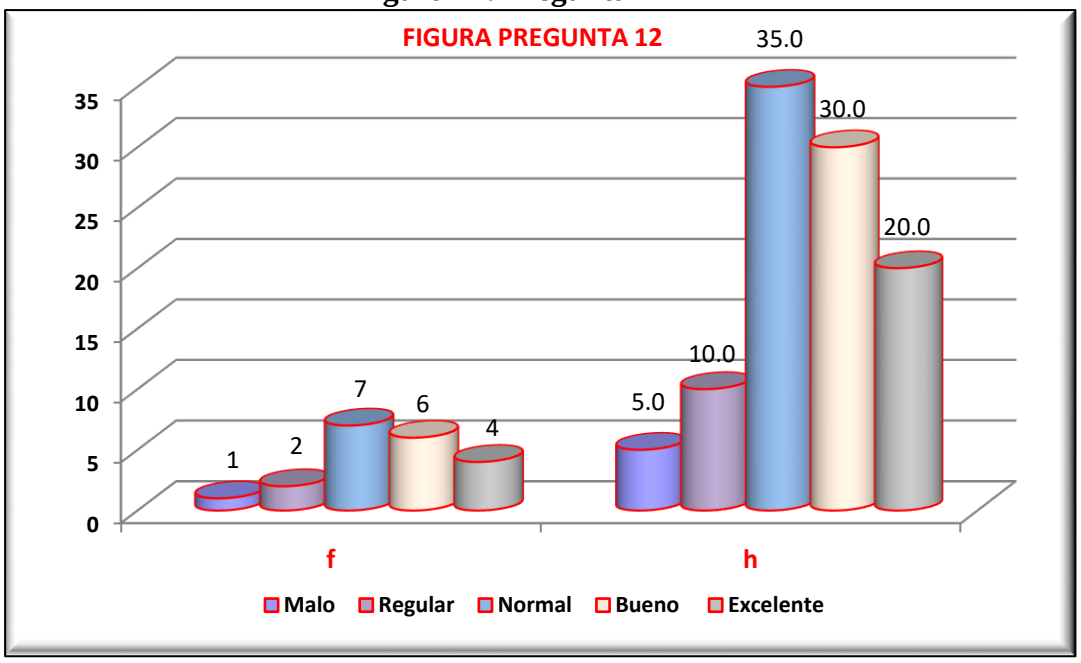
Tabla 16. Pregunta 12

P12. ¿Cuáles son las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay?		
ESCALA	**FRECUENCIAS**	
	f	**h**
Malo	1	5.0
Regular	2	10.0
Normal	7	35.0
Bueno	6	30.0
Excelente	4	20.0
TOTAL	**20**	**100.0**

Fuente: Encuesta

En la pregunta 12 de la encuesta planteada sobre cuáles son las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay, 01 persona encuestada (5.0%) valoró como malo, 02 de ellos (10.0%) valoraron como regular, 07 personas encuestadas (35.0%) calificaron como normal, 05 de ellos (25.0%) valoraron como bueno y 04 personas encuestadas (20.0%) calificaron como excelente.

Figura 21. Pregunta 12



Fuente: Encuesta

ANEXO 02: MATRIZ DE OPERACIONALIZACION DE VARIABLES

VARIABLES	DEFINICION CONCEPTUAL	DEFINICION OPERACIONAL	DIMENSIONES	INDICADORES	ESCALA
Variable 1 Propuesta de Guía Metodológica basada en ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014	Es un conjunto de lineamientos que especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (S GSI). Estos requisitos describen el comportamient o esperado del Sistema de Gestión una vez que esté en pleno funcionamiento	Es una construcción mental documentada cuya aplicación se dimensiona generalmente en: Sencillez, concientización y direccionalidad.	Sencillez	Grado de disponibilidad del modelo de administración	
				Grado de sencillez del modelo de administración	
				Porcentaje de trabajadores que comprenden el plan de comunicación	
			Compromiso	Nivel de concientización sobre la seguridad física	
				Nivel de concientización sobre la seguridad lógica.	
				Nivel de concientización sobre los ataques informáticos externos	
			Direccionalidad	Grado en que los trabajadores participan en el modelo de administración	
				Nivel en que el modelo de administración logra los objetivos generales	
				Nivel en que el modelo de administración logra los objetivos de área	
Variable 2 Seguridad de la información en la Municipalidad Provincial de Recuay	Es un conjunto de actividades que conforman parte de la administración de la Institución municipal	Es un conjunto de actividades que se encargan del Estado actual, características y de la seguridad de información.	Estado actual de la seguridad de información	Estado actual de seguridad de las computadoras	[0 – 20]
				Estado actual de seguridad de la red	
				Nivel de estado actual de seguridad de archivos	
			Características de la seguridad de información	Nivel de procesamiento de documentos	
				Nivel de seguridad de los procesamientos de documentos	
				Nivel de procesamiento del sistema informático	
			Seguridad	Nivel de seguridad física	
				Nivel de seguridad lógica	
				Nivel de seguridad de la distribución de documentos	

Fuente: Elaboración Propia

ANEXO 03: MATRIZ DE CONSISTENCIA

TITULO	FORMULACIÓN DEL PROBLEMA	OBJETIVOS	HIPÓTESIS	DISEÑO DE LA INVESTIGACION	VARIABLES
Propuesta de guía metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 para mejorar la seguridad de la información en la Municipalidad Provincial de Recuay-2015	**GENERAL:** ¿En qué medida la propuesta de una Guía Metodológica basada en ISO/IEC 27001:2013 y NTP ISO/IEC 27001:2014 mejora la seguridad de la información en la Municipalidad Provincial de Recuay?	**GENERAL:** Proponer una Guía Metodológica basada en ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014 para mejorar la seguridad de la información en la Municipalidad Provincial de Recuay.	**GENERAL:** La propuesta de una Guía Metodológica basada en ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014 mejora significativamente la seguridad de la información en la Municipalidad Provincial de Recuay.	**TIPO DE INVESTIGACIÓN:** Descriptivo correlacional	**V. I.** Propuesta de Guía metodológica
	ESPECIFICO: ¿Cuál es el estado actual en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay? ¿Qué características presentan los riesgos, vulnerabilidades y sus formas de prevención a los que se encuentra expuesta la seguridad de la información de la Municipalidad Provincial de Recuay? ¿Cuáles son las contribuciones de la norma ISO/IEC 27001:2013 en la estructuración en la información en la Municipalidad Provincial de Recuay? ¿Cuáles son las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay?	**ESPECIFICO:** Determinar el estado actual en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay. Identificar las características que presenta la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades y sus formas de prevención. Determinar las contribuciones de la norma ISO/IEC 27001:2013 en la estructuración en la información en la Municipalidad Provincial de Recuay. Establecer cuáles son las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay.	**ESPECIFICAS** El estado actual en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay es deficiente y sujeto a riesgos y vulnerabilidades. Las características que presenta la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades son débiles con carencia de formas de prevención. Las contribuciones de la norma ISO/IEC 27001:2013 en la estructuración en la información en la Municipalidad Provincial de Recuay es significativamente positiva. Las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay es significativamente positiva.	**DISEÑO DE INVESTIGACIÓN** Diseño descriptivo correlacional	**V. D.** Seguridad de información en la municipalidad Provincial de Recuay

Fuente: Elaboración Propia

ANEXO 4: ENCUESTA

UNIVERSIDAD SAN PEDRO
ESCUELA DE INGENIERIA INFORMATICA Y DE SISTEMAS

ENCUESTA

Estimado empleado: Sírvase responder con absoluta sinceridad la siguiente encuesta, que corresponde a la propuesta de una Guía Metodológica basada en ISO/IEC 27001:2013, NTP ISO/IEC 27001:2014 para mejorar la seguridad de la información en la Municipalidad Provincial de Recuay. Sírvase responder la encuesta con responsabilidad y honestidad. Este proceso es totalmente anónimo, se reitera el pedido de absoluta honestidad en sus respuestas. Muchas Gracias por su participación.

I. DATOS GENERALES

1. Edad ☐
2. Sexo: Masculino ☐ Femenino ☐

II. CUESTIONARIO

1. ¿Cuál es el estado actual en que se encuentra la seguridad de la información en la Municipalidad Provincial de Recuay?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

2. ¿Está disponible la Guía Metodológica en el tratamiento de la seguridad de la información en la Municipalidad Provincial de Recuay?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

3. ¿Qué características presenta la seguridad de la información de la Municipalidad Provincial de Recuay respecto a riesgos, vulnerabilidades y sus formas de prevención?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

4. ¿La Guía metodología concientiza a los servidores públicos sobre la seguridad física del sistema informático en la Municipalidad Provincial de Recuay?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

5. ¿Cómo valora la concientización de la Guía metodología a los servidores públicos sobre la seguridad lógica del sistema informático en la Municipalidad Provincial de Recuay?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

6. ¿Cómo califica la participación de los trabajadores participan en función de la Guía metodológica propuesta en la Municipalidad Provincial de Recuay?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

7. ¿Cómo consideras el nivel de seguridad generado por la Guía metodológica en la generación de documentos en el sistema informático de la Municipalidad Provincial de Recuay?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

8. ¿Cómo es el nivel de seguridad en la generación de documentos aportado por la Guía Metodológica en el sistema informático de la Municipalidad Provincial de Recuay?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

9. ¿Cómo calificas el nivel de seguridad del sistema informático de la Municipalidad Provincial de Recuay?

   a. Malo b. Regular c. Normal d. Bueno e. Excelente

10. ¿Cómo consideras el aporte de mejora nivel de seguridad en el procesamiento de documentos generado por la guía metodológica en el sistema informático de la Municipalidad Provincial de Recuay?

    a. Malo b. Regular c. Normal d. Bueno e. Excelente

11. ¿Cómo califica las contribuciones de la norma ISO/IEC 27001:2013 en la estructuración de la información en la Municipalidad Provincial de Recuay?

a. Malo b. Regular c. Normal d. Bueno e. Excelente

12. ¿Cuáles son las contribuciones de la norma NTP ISO/IEC 27001:2014 en la estructuración en la información en la Municipalidad Provincial de Recuay?

a. Malo b. Regular c. Normal d. Bueno e. Excelente

CUESTIONARIOS

A continuación, se presenta un cuestionario que va a permitir verificar aspectos relacionados con el uso, estado y situación de la seguridad en el sistema informático de la municipalidad.

Tabla 13: Aspectos relacionados con el uso, estado y situación de la seguridad en el sistema informático de la municipalidad.

PREGUNTAS	SI	NO	N/A
ASPECTOS RELACIONADOS CON INFORMÁTICA			
1. ¿Existe dentro de la Municipalidad un área de informática o de sistemas?			
2. ¿Rinde cuentas de su gestión sobre el manejo de información?			
3. ¿Conoce muy bien los procesos que se realizan en la generación de documentos dentro de la municipalidad?			
4. ¿Está identificada dicha área dentro del organigrama general de la Municipalidad?			
5. ¿Se tiene un organigrama específico de dicha área?			
6. ¿Existe manual de organización y funciones aplicables a la seguridad de la información?			
7. ¿Están delimitadas las funciones de cada integrante del área de informática?			
8. ¿Cada empleado del área de informática conoce la persona ante la que tiene que rendir cuentas de su labor?			
9. ¿Los gerentes y otros funcionarios de nivel superior pueden dar órdenes directas a cualquier empleado sobre el uso de la información o del sistema informático?			
10. ¿Cada empleado es especialista en aspectos de la seguridad de la información?			
ASPECTOS RELACIONADOS AL HARDWARE			
11. ¿Existen problemas de hardware en la generación de documentos, mantenimiento y envío de archivos?			
12. ¿El sistema de red brinda seguridad de protección de datos o de información?			

PREGUNTAS	SI	NO	N/A
13. ¿Considera adecuado el hardware instalado para el trabajo realizado?			
14. ¿Cada usuario utiliza el hardware bajo responsabilidad?			
15. ¿Existe política de protección de hardware a nivel físico y lógico?			
ASPECTOS RELACIONADOS AL SOFTWARE			
16. ¿Se han presentado problemas en el registro de los documentos?			
17. ¿hay una persona responsable de resguardar la información de acuerdo a lo previsto en las normas de la Municipalidad?			
18. ¿Permite el sistema el ingreso de datos de documentos de acuerdo a lo previsto en las normas de la Municipalidad?			
19. ¿Los reportes obtenidos de los documentos son aceptables por los usuarios y/o la Municipalidad?			
20. ¿Los pedidos de copias de documentos ofrecen todos los datos de la documentación?			
ASPECTOS RELACIONADOS AL PERSONAL			
21. ¿Cuál es su nivel de manejo de seguridad de la información?			
22. ¿Se siente satisfecho de laborar en la Municipalidad?			
23. ¿Se siente satisfecho trabajando con el uso de la computadora?			
24. ¿Alguna vez ha participado de un proceso de seguridad de la información?			
25. ¿Cree usted que la seguridad de la información es de vital importancia?			
26. ¿Ha sido evaluado alguna vez en un proceso de seguridad de la información?			
27. ¿Has recibido capacitaciones en llevar a cabo procesos de seguridad de la información?			
28. ¿Se ha capacitado en su momento para manejar y administrar información de forma segura y confiable?			
29. ¿Cree usted que es importante disponer de una Guía Metodológica de seguridad de la información?			
ASPECTOS RELACIONADOS AL MANTENIMIENTO DE LA INFORMACION			

PREGUNTAS	SI	NO	N/A
30. ¿Cada cuanto tiempo se realiza mantenimiento correctivo al sistema informático con que trabaja?			
31. ¿Dispone de una copia de seguridad de los instaladores del sistema?			
32. ¿Dispone de programas antivirus para proteger al sistema y a la información?			
33. ¿El acceso al sistema informático con el que trabaja esta normado?			
34. ¿Realiza copia de seguridad de los datos o información con los cuales trabaja?			
ASPECTOS RELACIONADOS A LA SEGURIDAD			
35. ¿Considera usted que existe amenaza o riesgo interno respecto a la seguridad de los datos e información?			
36. ¿Considera usted que existe amenaza o riesgo externo respecto a la seguridad de los datos e información?			
37. ¿Está contemplado la seguridad en las normas de registro de datos de bienes dentro de la Municipalidad?			
38. ¿Existe una política de acceso al sistema de la municipalidad?			
39. ¿Le han dado clave para ingresar al sistema?			
40. ¿La clave que ha recibido le da acceso a documentos y archivos de la municipalidad de acuerdo al nivel establecido?			
41. ¿Alguna vez ha sido testigo de cambio de información por parte del usuario o del cliente?			
42. ¿El acceso a internet está regulado en función del nivel de autoridad y responsabilidad en el cargo?			
43. ¿Está permitido a un empleado usar cualquier computadora?			
44. ¿Ha presentado alguna vez actos de piratería, Hackerismo o cualquier otro tipo de delito informático?			

Fuente: Elaboración propia

Tabla 14: Sobre la Guía metodológica

N°	PREGUNTAS	SI	NO	N/A
1	¿Cuenta la Municipalidad con una Guía metodológica que oriente a sus servidores públicos en la seguridad de la información?			
2	¿Desarrolla la Municipalidad Provincial de Recuay un Plan de seguridad de información?			
3	¿Ha realizado la Municipalidad acciones sobre la seguridad de la información?			
4	¿Dispone la Municipalidad de un organigrama estructural actualizado que esté aprobado y en funcionamiento?			
5	¿Cuenta la Municipalidad con un Manual de Organización y Funciones actualizado?			
6	¿Están disponibles y en aplicación manuales de Normas y procedimientos e instructivos para el uso del sistema informático?			
7	¿Estos manuales están aprobados por la autoridad de la Municipalidad?			
8	¿La Municipalidad cuenta con un reglamento Interno de trabajo autorizado?			
9	¿Cuenta la Municipalidad con programas permanentes de capacitación informática a servidores públicos?			
10	¿Es política de la administración de la Municipalidad contratar al personal conforme a los requisitos de idoneidad que exige cada puesto?			
11	¿Se realizan evaluaciones del personal en forma frecuente?			
12	¿Todo personal que hace uso del sistema informático de la Municipalidad ha recibido el adecuado entrenamiento para el manejo del sistema informático?			

Fuente: Elaboración propia