UNIVERSIDAD SAN PEDRO

FACULTAD DE INGENIERÍA

ESCUELA DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

Sistema de gestión de seguridad de la información para la Municipalidad Distrital de Independencia 2017

Tesis para obtener el título profesional de Ingeniero en Informática y de Sistemas

AUTOR

Robles Aguirre, Merkhyn Leonardo Manomi

ASESOR

Marlene Paredes, Jacinto

HUARAZ – PERU

2019

INDICE

PALABRAS CLAVE:

Tema	Seguridad de la información
Especialidad	Gestión

KEY WORDS:

Topic	Information Security
Specialization	Management

LÍNEA DE INVESTIGACIÓN:

Área	Ingeniería Tecnológicas
Sub Área	Ingeniería Eléctrica, Electrónica e Informático
Disciplina	Ingeniería de Sistemas y Comunicación

TÍTULO

Sistema de Gestión de Seguridad de la Información para de la Municipalidad Distrital de Independencia 2017

RESUMEN

El propósito de la investigación fue desarrollar un plan para un sistema de gestión de seguridad de la información en la Municipalidad Distrital de Independencia de la Provincia de Huaraz.

Para la investigación se utilizó la Norma Técnica Peruana NTP ISO/IEC 27001:2014, en la que se establece los dominios y controles a tomar en cuenta para el desarrollo del Sistema de Gestión de Seguridad de la Información; y también, el marco de referencia de Objetivos de Control para Información y Tecnologías Relacionadas - COBIT para evaluar la eficacia respecto a los controles de seguridad física y lógica y los procesos informáticos implementados en la municipalidad y así poder detectar vulnerabilidades existentes en lo relativo a controles de seguridad.

Se obtuvo como resultado de la investigación un plan del Sistema Gestión de Seguridad de la Información, la cual dependerá de la organización certificar según conveniencias y alineados al estándar ISO/IEC 27001:2013.

ABSTRACT

The purpose of the research was to develop a plan for an information security management system in the District Municipality of Independence for the Province of Huaraz.

For the research was used NTP Peruvian Technical Standard ISO/IEC 27001:2014, which sets out the domains and controls to be taken into account for the development of the Information Security Management System; and also, the frame of reference for Control Objectives for Information and Related Technologies - COBIT to evaluate the effectiveness with regard to the controls of physical and logical security and processes implemented in the municipality and thus be able to detect vulnerabilities existing in regard to security controls.

Was obtained as a result of the research plan of the System Information Security Management, which will depend on the organization certify according to conveniences and aligned to the standard ISO/IEC 27001:2013.

1. INTRODUCCIÓN

De los trabajos revisados que guardan relación en el estudio de tesis se ha tomado a los más relevantes como son:

El proyecto desarrollado en España del Ayuntamiento de Málaga (2010), se implementaron políticas de seguridad de la información para su municipio desde el enfoque de la ISO 27001:2005, uno de los objetivos fundamentales de la implantación de un marco de referencia para asentar las bases sobre las cuales los trabajadores públicos y los ciudadanos relacionados con la municipalidad puedan acceder a los servicios en un entorno de gestión seguro, anticipándose a las necesidades, y preservando los derechos. Metodológicamente la implementación de política se ha basado en la asignación de roles y responsabilidades, así como normas internas y externas ligadas a las políticas de seguridad de la información. Concluyó que la gestión de la seguridad de la información ha de garantizar el adecuado funcionamiento de las actividades de control, monitorización y mantenimiento de las infraestructuras e instalaciones generales, necesarias para la adecuada prestación de servicios, así como de la información derivada del funcionamiento de los mismos. Esta investigación aporta conocimiento de cómo los objetivos de control se implementan de acuerdo a ISO y de cómo se adecuan a los objetivos de la organización y estas a la vez con las personas involucradas.

En Venezuela, De Pablo (2007), en la tesis de grado "Evaluación de seguridad de información para la plataforma de Banca Virtual en una entidad financiera", evalúa la seguridad de información para la plataforma de Banca Virtual en una entidad financiera bajo el enfoque COBIT. El problema que estudia es específicamente la revelación, manipulación y accesos no autorizados. Se trazó como objetivo general evaluar y probar los controles establecidos en la plataforma tecnológica que respalda la Banca Virtual, así como proponer soluciones para la reducción de riesgos del negocio implícitos en la utilización de tecnologías de información de la Entidad Financiera. Propuso soluciones a las diferentes oportunidades de mejoras identificadas, en función de reducir los riesgos implícitos en la utilización de tecnologías y sistemas de información, así como alcanzar un nivel de seguridad aceptable que les permita hacer frente a las nuevas amenazas informáticas. Se tomó

en cuenta esta investigación, porque demuestra a través de como el marco de COBIT a través de sus dominios, se pueden determinar roles en los responsables, y procesos que ayuden a evaluar y solucionar problemas con el uso de las tecnologías de información y gobierno de TI.

Así mismo en la investigación Villasmil (2006), tesis de postgrado, "Análisis de los riesgos de seguridad informática para las pequeñas y medianas empresas usando el Estándar ISO 17799 para la definición de políticas de seguridad que protejan sus sistemas de información" realizado en la Universidad Centro Occidental Lisandro Alvarado de Venezuela, analiza los riesgos de seguridad informática para las pequeñas y medianas empresas usando el Estándar ISO 17799 en la definición de políticas de seguridad para proteger sistemas de información. Planteó los objetivos de identificar las situaciones de riesgo que afecten la seguridad informática de empresa Pymes, además de determinar las herramientas de control para reducir y monitorear dichos riesgos, asimismo la propuesta de un conjunto de lineamientos basados en el estándar ISO-17799, que permitan establecer políticas de seguridad para los sistemas de información de las Pymes. Utilizó un instrumento de recolección de datos, que se aplica a los administradores de los sistemas de información dentro de las empresas seleccionadas, la información recaudada, fue analizada desde el punto de vista estadístico, la investigación concluyó que existen riesgos generados por trabajadores, por instalaciones, por acceso a la información y alcanza un conjunto de políticas de como las Pymes deben enfrentar estos riesgos. Esta tesis aporta conocimiento de que tan importante es tener implementada una política de seguridad, ya que enmarca tanto a los objetivos de la organización como los objetivos a tomar en cuenta según el estándar ISO.

Mendoza (2005) por su lado, trata en su Tesis "Impacto de la Tecnología de Información en la Competitividad de las Pequeñas y Medianas Industrias", los aspectos relacionados con la implementación y aceptación de las Tecnologías de la información y comunicación, por parte de las pequeñas y medianas industrias, donde su incorporación es lenta pero progresiva, lo que contribuye a que este tipo de empresas mejoren su grado de competitividad dentro de su entorno. La investigación antes mencionada, aporta información sobre el uso que le da este grupo empresarial a las TIC's, las cuales motivado a los constantes cambios

tecnológicos de actualidad, han tomado gran relevancia para las organizaciones que se sirven de ellas.

Borghello (2001), en su tesis titulada "Seguridad Informática: sus implicancias e implementación", describe los aspectos que abarca la seguridad informática. Este trabajo proporciona importantes definiciones sobre el tema, además de explicar todos los componentes de un sistema de seguridad de la información. Concluyó con los aspectos que influyen de manera contundente sobre el desempeño de la seguridad en la actualidad como lo son: Aislamiento y globalización, legislación vigente, tecnología existente, daños minimizables, riesgos manejables, costos, personas involucradas. Esta tesis se relaciona con la investigación, porque el estudio proporciona información teórica, la cual es una base para el manejo e implementación de la seguridad en un sistema informático además del establecimiento de los riesgos que podrían afectarlo, lo que favorece al logro de los objetivos de esta investigación.

En Perú, **Córdova (2003),** en sus tesis de grado sobre "Plan de seguridad informática para una entidad financiera, realizada en la Universidad Nacional Mayor de San Marcos de Lima Perú", recopiló información que trata lo relacionado con gestión y políticas de seguridad para la información. Entre los aspectos resaltantes menciona: usar una metodología comprobada para el diseño de un plan de seguridad de la información, el cual debe adaptarse a la empresa que lo requiera. El mismo debe incluirse en plan presupuestario de la organización, establecer los deberes y derechos de cada una de la personas que utilizan los sistemas de información, determinar qué información se protegerá y donde se encuentra; para aplicar los controles que garanticen su seguridad; el diseño de las políticas de seguridad de la información debe ser claro y jurídicamente viable, debe incluir todos los factores involucrados: tecnología, marco legal, compatible con la organización y su personal. Esta tesis aporta a la investigación en estudio, conocimientos sobre las políticas o normativas que se pueden usar para el aseguramiento de la información dentro de una organización.

Se puede decir entonces que hoy en día la información ha dejado de ser algo sin valor y se ha convertido en un activo para cualquier organización, especialmente para una municipalidad; ya que esta administra datos e información de todos los contribuyentes y personas que residen dentro de la jurisdicción de esta, en los que se gestiona la información en distintos procesos.

La investigación, es relevante en lo social porque permite a la Municipalidad Distrital de Independencia que toda la información obtenida de los contribuyentes, se maneje de manera adecuada con el estándar ISO 27001, y esta al tener objetivos de control, se cumplan estos objetivos asegurando la información de cualquier contribuyente o administrado por parte de la municipalidad.

Así mismo, la investigación tiene un aporte al conocimiento ya hablamos que la información, contiene 3 pilares importantes que son: Confidencialidad, Integridad y Disponibilidad que permiten que la información sea confiable durante el procesamiento de esta. Si alguna de estos pilares falla, se compromete la información final del usuario afectando directamente en la credibilidad de la información.

La Municipalidad Distrital de Independencia, al ser un ente del estado dispone y maneja demasiada información, y mucha de esta es información sensible.

La información manejada a través de precarios sistemas informáticos, desconocimientos de los roles básicos de la seguridad del personal y archiveros sin los controles de seguridad básicos; a esto se suma, la desorganización de toda la documentación y el uso indebido de los ordenadores que contienen valiosa información.

Por tanto, el principal problema que se obtiene, es que, al no tener los controles, el estándar de seguridad sobre la información, esta puede verse afectada ocasionando problemas sobre el proceso de esta misma. Generando atraso y errores en la información final obtenida. De lo expuesto se formula el problema de manera interrogativa:

¿Cómo desarrollar un sistema de gestión de seguridad de la información para la Municipalidad Distrital de Independencia?

La investigación es de carácter descriptivo, en el que se planeta el estudio de las variables sistema de gestión y control de la información.

Se define al **sistema de gestión** como un conjunto de etapas unidas en un proceso continuo, que permite trabajar ordenadamente una idea hasta lograr mejoras y su continuidad. Y el modo en que va a operar esta variable será a través de objetivos de control de seguridad, los cuales tendrán que cumplirse.

Por otro lado, se define el **control de la información** como actividades organizadas y estructuradas que se realizan con el objetivo de asegurar los mecanismos que alcancen a la entrada, salida, proceso, almacenamiento y salida de la información. (Gema, 2014).

Se dice que SGSI es la abreviatura utilizada para referirse a un Sistema de Gestión de la Seguridad de la Información. ISMS es el concepto equivalente en idioma inglés, siglas de *Information Security Management System*.

En el contexto aquí tratado, se entiende por información todo aquel conjunto de datos organizados en poder de una entidad que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

Para garantizar que la seguridad de la información es gestionada correctamente se

debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

En base al conocimiento del ciclo de vida de cada información relevante se debe adoptar el uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

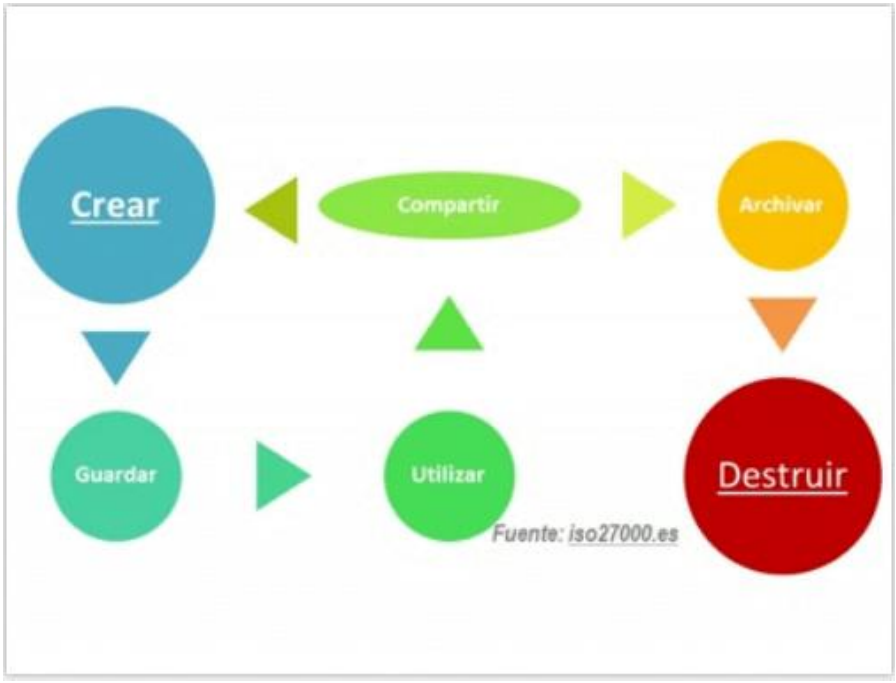


Figura 1: Estados de la Información

FUENTE: www.iso27000.es

Uno de los principales activos que poseen las empresas es la información que manejan. Un correcto tratamiento de la información requiere la adopción de las medidas que sean necesarias para proteger los tres aspectos básicos de la misma: integridad, confidencialidad y disponibilidad.

Un Sistema de Gestión de la Seguridad de la Información o SGSI sería, por tanto, un conjunto de medidas destinadas a preservar estos tres elementos de la información que maneja una empresa, independientemente del soporte, tipo, etc., de la misma. Para que estas medidas sean efectivas, deben llevarse a cabo a través de procesos estandarizados, documentados, conocidos y aplicados por toda la empresa. Para sistematizar estos procesos, existe un conjunto de normas conocidas como **ISO 27000**, encaminadas a la gestión de la seguridad. Una empresa puede elegir implementar estas normas o bien establecer su propia política de gestión de la seguridad, aunque el uso de estándares normalizados le permite acceder a certificaciones independientes. (Gema, 2014).

Norma	Contenido
ISO/IEC 27000	Ofrece una visión general de las normas de toda la serie 27000, una introducción a los SGSI, terminología utilizada, etc.
ISO/IEC 27001	Es la norma principal y contiene los requisitos del sistema de gestión de seguridad de la información. Es la norma utilizada por los auditores externos para certificar los SGSI de las empresas.
ISO/IEC 27002	Guía de buenas prácticas en la que se describen los objetivos de control y controles recomendables relativos a la seguridad de la información. No es certificable.
ISO/IEC 27003	Se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI de acuerdo ISO/IEC 27001. No es certificable.
ISO/IEC 27004	Guía para medir eficacia de un SGSI. No es certificable.
ISO/IEC 27005	Proporciona las directrices para la gestión del riesgo en la seguridad de la información. No es certificable.
ISO/IEC 27006	Especifica los requerimientos para la acreditación de entidades de auditoría y certificación de SGSI.
ISO/IEC 27007 ISO/IEC TR 27008	Guías de auditoría.
ISO/IEC 27011	Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

Figura 2: Familia ISO 27000
Fuente: Gema (2014)

Mientras por su parte, la Norma Técnica Peruana que abarca a todos los tipos de organizaciones (empresas comerciales, agencias de gobierno y organizaciones sin fines de lucro). Esta 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. (INDECOPI, 2014)

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 Nº 197-2007-PCM, Sobre la fecha límite para diversas entidades de la Administración Publica implementen el Plan de Seguridad del a Información Dispuesto en la NTP 17799:2007 EDI, Resolución de Contraloría General Nº 320-2006 CG Normas de control Interno y Resolución Ministerial Nº 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 SGSI 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 SGSI ha sido diseñado para garantizar y proporcionar controles de seguridad adecuados que protejan los activos de información, brindando confianza a las partes interesadas.4

Siguiendo los lineamientos establecidos se asegurará mejorar la seguridad de la información al dar tratamiento a los riesgos más críticos.

Entre los principales beneficios que se tienen está:

- El establecimiento de una metodología de gestión de la seguridad y estructura.
- Reducción de riesgos de pérdida, robo o corrupción de la información.
- Los clientes tienen acceso a la información a través de medidas de seguridad.
- Los riesgos y sus controles son continuamente revisados.
- Confianza de usuarios y los regidores estratégicos por la garantía y confidencialidad de la información.
- Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- Posibilidad de integrarse con otros sistemas de gestión.
- Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- Imagen de la institución a nivel nacional, internacional y elemento diferenciador.
- Confianza y reglas claras para las personas de la organización.
- Aumento de la seguridad en base a la gestión de procesos en vez de la compra sistemática de productos y tecnologías.

Por otro lado, en la investigación también se usó COBIT, que es un marco de gobierno de las tecnologías de información que proporciona una serie de herramientas para que la gerencia pueda conectar los requerimientos de control con los aspectos técnicos y los riesgos del negocio. Permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías en toda la organización. Enfatiza el cumplimiento regulatorio, ayuda a las organizaciones a incrementar su valor a través de las tecnologías, y permite su alineamiento con los objetivos del negocio. (Prandini y Szuster, 2012).

Una de las directivas en COBIT 5 es la distinción hecha entre gobierno y gestión. En línea con este principio, se espera que todas las empresas implementen varios procesos de gobierno y varios procesos de gestión para proporcionar un gobierno y una gestión del entorno IT exhaustivos.

Los procesos de gobierno tratan de los objetivos de gobierno de las partes interesadas entrega de valor, optimización del riesgo y de recursos – e incluye prácticas y actividades orientadas a evaluar opciones estratégicas, proporcionando la dirección de TI y supervisando la salida (Evaluar, orientar y supervisar [EDM] – en línea con los conceptos del estándar ISO/IEC 38500).

Mientras que las prácticas y actividades de los procesos de gestión cubren las áreas de responsabilidad de PBRM de TI de la empresa y tienen que proporcionar cobertura de TI extremo a extremo.(ISACA, 2012)

En la presente investigación, la hipótesis que se determina es que se mejorará la gestión de la información luego de haber desarrollado el SGSI.

La investigación tiene como objetivo general, desarrollar un Sistema de Gestión de Seguridad de la Información para la Municipalidad Distrital de Independencia, en la Gerencia de Administración Tributaria y Rentas del Distrito de Independencia de la ciudad de Huaraz, y como objetivos específicos se planteó:

1. Analizar el estado actual en que se encuentra la seguridad de la información en la Municipalidad Distrital de Independencia en la Gerencia de Administración Tributaria y Rentas.

2. Estudiar las características de riesgos, vulnerabilidades y sus formas de prevención de todos los activos de información desde el enfoque de NTP ISO/IEC 27001:2014, y COBIT 5 a los que se encuentra expuesta la información de la Municipalidad Distrital de Independencia.

3. Evaluar el nivel de conocimiento del personal de las áreas involucradas sobre

SGSI y seguridad de la información.

4. Desarrollar el Sistema de Gestión de Seguridad de la Información desde el enfoque de la NTP ISO/IEC 27001:2014 y COBIT 5.

2. METODOLOGÍA

En la formulación de la investigación, se tiene un componente investigativo de tipo descriptivo, considerando el objetivo fue necesario la recopilación de información relacionada con las variables de estudio para el desarrollo de un Sistema Gestión de Seguridad de la Información para la municipalidad Distrital de Independencia.

El diseño de Investigación es no experimental, respecto a la toma de datos para la construcción del sistema con corte transversal aplicándose técnicas e instrumentos de recolección de datos en el tiempo que dura el desarrollo del sistema, así mismo es propositiva, de innovación incremental, porque se trata de desarrollar un sistema de gestión para salvaguardar la información existente y evaluar los controles necesarios y mantenerlos actualizados.

La muestra a considerar será de 15 personas de un total de 25 que es la población; estas personas laboran en el área de rentas de la municipalidad y están involucradas con el proceso del desarrollo del SGSI. Las técnicas de recolección de datos en las que la investigación se apoyó son: análisis documental, encuestas y entrevista y como instrumentos: textos, tesis de estudios previos y cuestionarios.

Uno de los aspectos más destacados del ISO 27001 es la descripción del proceso de implantación de un SGSI. Básicamente se resume en un proceso cíclico continuo que pasa por las fases ***Plan-Do-Check-Act*** y vuelta a empezar.

Jimeno (2013) que también es conocido como ciclo de mejora continua o circulo de Deming, por ser Edwards Deming su autor. Esta metodología describe los cuatro pasos esenciales que se deben de llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallo, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales, etc.) El círculo de Deming lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para incorporar nuevas mejoras. La aplicación de esta metodología está enfocada principalmente para ser usada en empresas y organizaciones.

La NTP ISO/IEC 27001:2014, nos dice que debemos usar tantos objetivos de control como sean necesarios para la organización que implantará el SGSI, pero este paso se llega haciendo el estudio preliminar para identificar todos los activos de información que se verán afectados por el SGSI; y haciendo uso de indicadores como Licker en donde llegué a una valorización final de que tan importante es el activo para la organización, para posteriormente analizar en un cuadro de análisis de riesgo y ver que activos ya tienen controles aplicados por la organización y también que tan seguros son estos frente a las amenazas existentes. A esto sumarle, los activos que no cuentan con controles adecuados; para luego darles una valorización final y estimar si el nivel de riesgo es muy alto y poder tomar acciones inmediatas. Finalmente, los activos pasarán a un último análisis en donde se verán descritas las acciones a tomar en cuenta de acuerdo a los controles ya descritos en la ISO 27002 Anexo A y analizar también los riesgos residuales luego de aplicado los controles.

Luego de analizado todos estos procesos poder determinar la política de seguridad que será aplicada y que será el eje fundamental del SGSI; ya que en esta se describe como se lograrán los objetivos de la organización con los controles a implementar en todos los activos de información y el compromiso de la organización con el SGSI.

Por otro lado, se tomará en cuenta también la Guía COBIT para hacer un mapeo de procesos existentes entre esta y los objetivos relacionados a Tecnologías de Información en donde se determinarán que procesos de gobierno son primarios o secundarios determinando así, su importancia y que implicancia tendrán en 4 aspectos de la organización como Financiera, Cliente, Interna y de Aprendizaje y Conocimiento, serán necesarios para la implementación del SGSI en la municipalidad. Luego de ello hacer un mapeo entre los dominios necesarios a implementar de COBIT con los controles existentes en la ISO 27002; y de aquí obtener que dominios de gobierno se tomarán directamente con la guía COBIT y que no tienen controles en la ISO 27002 para ser aplicados.

Y finalmente, llegar a describir los procesos que se llevan a cabo, con cada dominio de la guía COBIT; para determinar a través de una matriz RACI (Responsible –

Accountable – Consulted – Informed) quien será el responsable, encargado, consultado e informado de las personas involucradas directamente durante el desarrollo del SGSI. Ya que, en esta matriz se asigna el rol que el recurso debe desempeñar para cada actividad dada. No es necesario que en cada actividad se asignen los cuatro roles, pero sí por lo menos el de responsable y el de encargado.

3. RESULTADOS

Para el logro de los objetivos se aplicó la metodología PDCA, llegando a los siguientes resultados.

a) Resultados de Pre-Test

Tabla 1: Resultados de pre-test

PRE-TEST: Nivel de conocimiento del personal en aspectos de SGSI y seguridad de la información																										TOTAL
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
1	1	1	2	1	2	2	1	1	1	1	1	2	2	2	1	1	2	1	1	1	2	1	2	1	2	35
2	1	3	1	2	1	2	2	2	1	1	1	1	2	2	1	1	2	2	2	2	2	2	1	1	2	40
3	1	2	1	1	1	1	2	1	1	2	2	1	1	1	1	2	2	2	2	1	1	2	1	2	2	36
4	2	2	1	1	1	2	2	2	2	2	2	2	1	2	1	1	2	2	1	2	2	1	2	1	2	41
5	1	1	2	2	1	1	2	1	2	1	1	2	1	1	2	1	1	2	1	2	2	2	2	1	1	36
6	1	2	2	1	2	1	2	2	2	1	1	1	1	1	2	1	1	1	1	2	1	1	2	1	1	34
7	1	1	2	2	1	2	2	1	1	1	1	2	2	1	2	2	1	2	2	2	2	3	1	1	1	39
8	1	1	1	1	1	2	1	1	2	1	2	1	1	2	1	1	2	1	1	2	2	2	2	1	1	34
9	1	2	2	2	1	2	1	2	2	2	1	1	2	2	1	1	2	1	2	1	2	2	1	1	2	39
10	2	2	2	2	1	3	2	1	1	1	1	3	1	1	3	2	1	2	1	2	1	2	2	2	2	43
11	1	2	2	1	1	1	2	2	2	1	1	2	1	2	1	1	2	1	2	2	1	2	1	1	1	36
12	1	1	1	1	1	1	2	2	2	1	2	1	2	1	1	1	2	1	1	2	2	2	2	1	2	36
13	1	2	2	2	2	1	1	1	1	2	3	2	2	2	2	2	1	1	2	2	2	1	2	1	2	42
14	1	2	2	1	2	1	1	1	1	2	1	2	2	2	2	1	1	2	1	1	1	1	1	2	2	36
15	1	2	1	2	1	2	1	1	2	1	2	2	1	2	1	2	1	1	2	1	1	2	2	2	2	38

Fuente: Elaboración Propia

b) Resumen de resultados post-test

Tabla 2: Resumen de pre-test

N°	NIVEL DE CONOCIMIENTO DEL PERSONAL SOBRE SGSI Y SEGURIDAD DE LA INFORMACIÓN	
	TOTAL	BAREMO
1	35	BAJO
2	40	BAJO
3	36	BAJO
4	41	BAJO
5	36	BAJO

6	34	BAJO
7	39	BAJO
8	34	BAJO
9	39	BAJO
10	43	MEDIO
11	36	BAJO
12	36	BAJO
13	42	MEDIO
14	36	BAJO
15	38	BAJO

Fuente: Elaboración Propia

De la consolidación de datos obtenidos desarrollado el pre-test al personal de la gerencia de administración tributaria y rentas, se puede deducir que el nivel de conocimiento del personal en relación al tema de seguridad de la información y seguridad informática, previo al desarrollo del SGSI, es bajo en promedio. Por tanto, a través de la hipótesis planteada y el desarrollo del SGSI se espera que este mejore y así cumplir con los objetivos planteados.

Esto también se afianza con la entrevista de tono informal realizada al gerente de administración tributaria y rentas en las que se realizaron preguntas muy puntuales sobre el estado actual de la seguridad de la información que posee esta gerencia, en las que las respuestas no fueron muy alentadoras, teniendo un déficit en temas de seguridad de la información.

c) Mapeo de procesos de COBIT con objetivos relacionado con TI

Tabla 3: Mapeo de objetivos de TI con COBIT

			OBJETIVO RELACIONADO CON TI														
			Alineamiento de TI y la estrategia de organización.	Cumplimento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas.	Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.	Riesgos de negocio relacionadas con las TI gestionadas	Transparencia de los costes, beneficios y riesgos de las TI.	Entrega de servicios de TI de acuerdo a los requisitos de la organización.	Uso adecuado de aplicaciones, información y soluciones tecnológicas.	Agilidad de las TI	Seguridad de la información infraestructura de procesamiento y aplicaciones.	Optimización de activos, recursos y capacidades de las TI	Capacitación y soporte de procesos de la organización integrado aplicaciones y tecnologías en procesos de negocio.	Disponibilidad de información útil y relevante para la toma de decisiones.	Cumplimiento de las políticas internas por parte de las TI	Personal de la organización y de las TI competente y motivado	Conocimiento, experiencia e iniciativas para la innovación de negocio.
			01	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**	**14**	**15**
Procesos de COBIT 5			**Financiera**					**Cliente**		**Interna**						**Aprendizaje y Crecimiento**	
Evaluar, Orientar y Monitorizar	**EDM03**	Asegurar la Optimización del Riesgo	**S**	**S**	**S**	**P**	**P**	**P**	**S**		**P**			**S**	**P**	**S**	**S**
	EDM04	Asegurar la Optimización de los Recursos	**S**		**S**	**S**	**S**	**S**	**S**	**P**		**P**				**P**	**S**
	EDM05	Asegurar la Transparencia hacia las partes interesadas	**S**	**S**	**P**		**P**	**P**						**S**	**S**		**S**

Alinear, Planificar y Organizar	**APO02**	Gestionar la Estrategia	**P**		**S**	**S**		**P**	**S**	**S**		**S**	**S**	**S**	**S**	**S**	**P**
	APO06	Gestionar el Presupuesto y los Costes	**S**		**S**	**S**	**P**	**S**	**S**			**S**					
	APO07	Gestionar los Recursos Humanos	**P**	**S**	**S**	**S**		**S**		**S**	**S**	**P**			**S**	**P**	**P**
	APO12	Gestionar el Riesgo		**P**		**P**	**P**	**S**	**S**	**S**	**P**			**S**	**S**	**S**	**S**
	APO13	Gestionar la Seguridad		**P**		**P**	**P**	**S**	**S**		**P**				**P**		
Construcción, Adquisición e Implementación	**BAI05**	Gestionar la introducción de Cambios Organizativos	**S**		**S**			**S**	**P**	**S**		**S**	**S**				**P**
	BAI06	Gestionar los cambios			**S**	**P**		**P**	**S**	**S**	**P**	**S**	**S**	**S**	**S**		**S**
	BAI09	Gestionar los Activos		**S**		**S**	**P**	**S**		**S**	**S**	**P**		**S**	**S**		
Entregar, Dar Servicio y Soporte	**DSS02**	Gestionar las Peticiones y los Incidentes del Servicio				**P**		**P**	**S**		**S**			**S**	**S**		**S**
	DSS03	Gestionar los Problemas		**S**		**P**		**P**	**S**	**S**		**P**	**S**	**P**	**S**		**S**
	DSS04	Gestionar la Continuidad	**S**	**S**		**P**		**P**	**S**	**S**	**S**	**S**	**S**	**P**	**S**	**S**	**S**
	DSS05	Gestionar los Servicios de Seguridad	**S**	**P**		**P**		**S**	**S**		**P**	**S**	**S**		**S**	**S**	
	DSS06	Gestionar los Controles de los Procesos del Negocio		**S**		**P**		**P**	**S**		**S**	**S**	**S**	**S**	**S**	**S**	**S**

Fuente: Elaboración Propia

d) Mapeo de procesos COBIT 5 con la NTP ISO/IEC 27001:2014 (ANEXO A)

Tabla 4: Mapeo de Dominio APO y NTP ISO/IEC 27001:2014

COBIT 5 SEGURIDAD DE LA INFORMACIÓN	NTP ISO/IEC 27001:2014
Dominio: APO (Alinear, Planificar y Organizar)	
APO02: Gestionar la Estrategia	4 Contexto de la organización 5.2 Política 6 Planeación
APO06: Gestionar el presupuesto y los costes	No existe
APO07: Gestionar los recursos humanos	7.2 Competencia 7.3 Concientización A.7 Seguridad de los recursos humanos
APO12: Gestionar el riesgo	5.2 Política 6.1 Acciones para abordar los riesgos y las oportunidades. 7.5 Información documentada 8.1 Plan operacional y de control 8.3 Tratamiento al riesgo de seguridad de información 9.1 Monitoreo, medición, análisis y evaluación 9.3 Revisión gerencial
APO13: Gestionar la seguridad	Considerado en todo el estándar

Fuente: Elaboración Propia

Tabla 5: Mapeo de Dominio BAI y NTP ISO/IEC 27001:2014

COBIT 5 SEGURIDAD DE LA INFORMACIÓN	NTP ISO/IEC 27001:2014
Dominio: BAI (Construir, Adquirir e Implementar)	
BAI05: Gestionar la introducción de Cambios Organizativos	No existe
BAI06: Gestionar los Cambios	A.12.1.2 Administración de Cambios
BAI09: Gestionar los Activos	A.8 Administración de Activos

Fuente: Elaboración Propia

Tabla 6: Mapeo de Dominio DSS y NTP ISO/IEC 27001:2014

COBIT 5 SEGURIDAD DE LA INFORMACIÓN	NTP ISO/IEC 27001:2014
Dominio: DSS (Entregar, Dar servicio y Soporte)	
DSS02: Gestionar las Peticiones y los Incidentes del Servicio	A.16 Administración de incidentes de seguridad de la información
DSS03: Gestionar los Problemas	No existe
DSS04: Gestionar la Continuidad	4.1 Entendiendo la organización y su

	contexto 6.1 Acciones para abordar riesgos y oportunidades 7.4 Comunicación 7.5 Información documentada 10 Mejoramiento
DSS05: Gestionar los servicios de seguridad	Considerado en todo el estándar
DSS06: Gestionar los controles de los procesos del negocio	6.1.2 Evaluación de riesgo de seguridad de la información 9 Evaluación del rendimiento A.8.2 Clasificación de la información A.9.4 Control de acceso a los sistemas y aplicaciones

Fuente: Elaboración Propia

e) Política de Seguridad

Teniendo en cuenta el alcance y los objetivos (del proyecto y de la organización); se describirá a continuación la política de seguridad según el anexo A.5 de la NTP ISO/IEC 27001:2014.

"La Gerencia de Administración Tributaria y Rentas de la Municipalidad Distrital de Independencia reconoce la importancia de identificar y proteger sus activos de información, evitando la destrucción, la divulgación, modificación y utilización no autorizada de toda información relacionada con usuarios, empleados, bases de conocimiento, estrategia, gestión, y otros conceptos; comprometiéndose a desarrollar, implantar, mantener y mejorar continuamente el Sistema de Gestión de Seguridad de la Información."

f) Roles

Tabla 7: Matriz RACI para EDM03

EDM03 **Asegurar la optimización del riesgo**			**Dominio: Evaluar, Orientar y supervisar**	
Descripción del proceso Asegurar que el apetito y la tolerancia al riesgo de la organización son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
EDM 03.01 Evaluar la gestión de Riesgos	**A**	**C**	**I**	**R**
EDM 03.02 Orientar la gestión de riesgos			**I**	**R**
EDM 03.03 Supervisar la gestión de riesgos	**R**		**I**	**C**

Fuente: Elaboración Propia

Tabla 8: Matriz RACI para EDM04

EDM04 **Asegurar la optimización de recursos**			**Dominio: Evaluar, Orientar y supervisar**	
Descripción del proceso Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
EDM 04.01 Evaluar la gestión de recursos	**A**	**C**	**I**	**R**
EDM 04.02 Orientar la gestión de recursos	**R**		**A**	**I**
EDM 04.03 Supervisar la gestión de recursos	**A**		**R**	**I**

Fuente: Elaboración Propia

Tabla 9: Matriz RACI para EDM03

EDM05 **Asegurar la transparencia hacia las partes interesadas**			**Dominio: Evaluar, Orientar y supervisar**	
Descripción del proceso Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de TI de la empresa son transparentes, con aprobación por parte de las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
EDM 05.01 Evaluar los requisitos de elaboración de informes de las partes interesadas.	**A**	**C**	**I**	**R**
EDM 05.02 Orientar la comunicación con las partes interesadas y la elaboración de informes.	**A**	**C**	**I**	**R**
EDM 05.03 Supervisar la comunicación con las partes interesadas.	**R**		**I**	**C**

Fuente: Elaboración Propia

Tabla 10: Matriz RACI para APO02

APO02 **Asegurar la transparencia hacia las partes interesadas**			**Dominio:** **Alinear, Planificar y Organizar**	
Descripción del proceso Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
APO 02.01 Comprender la dirección de la empresa.	**C**		**C**	**R**
APO 02.02 Evaluar el entorno, capacidades y rendimientos actuales.		**C**		**R**
APO 02.03 Definir el objetivo de las capacidades de TI	**I**	**A**		**R**
APO 02.04 Realizar un análisis de diferencias	**A**			**R**
APO 02.05 Definir un plan estratégico y la hoja de ruta	**A**		**I**	**R**
APO 02.06 Comunicar la estrategia y la dirección de TI	**I**	**A**	**I**	**R**

Fuente: Elaboración Propia

Tabla 11: Matriz RACI para APO06

APO06 **Gestionar el presupuesto y costes**			**Dominio:** **Alinear, Planificar y Organizar**	
Descripción del proceso Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
APO 06.01 Gestionar las finanzas y contabilidad	**R**		**A**	
APO 06.02 Priorizar la asignación de recursos	**R**		**A**	**I**
APO 06.03 Crear y mantener presupuestos			**R**	**I**
APO 06.04 Modelar y asignar costes	**R**		**A**	**I**
APO 06.05 Gestionar costes	**R**		**A**	**I**

Fuente: Elaboración Propia

Tabla 12: Matriz RACI para APO07

APO07 **Gestionar los recursos humanos**			**Dominio:** **Alinear, Planificar y Organizar**	
Descripción del proceso Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
APO 07.01 Mantener la dotación de personal suficiente y adecuada	**A**		**R**	
APO 07.02 Identificar personal clave de TI		**R**	**A**	
APO 07.03 Mantener las habilidades y competencias del personal	**R**		**A**	
APO 07.04 Evaluar el desempeño laboral de los empleados			**R**	
APO 07.05 Planificar y realizar un seguimiento del uso de recursos humanos y de TI del negocio	**A**	**R**		**R**

APO 07.06 Gestionar el personal contratado			**R**	**I**

Fuente: Elaboración Propia

Tabla 13: Matriz RACI para APO12

APO12 **Gestionar el riesgo**			**Dominio:** **Alinear, Planificar y Organizar**	
Descripción del proceso Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
APO 12.01 Recopilar datos	**C**		**I**	**R**
APO 12.02 Analizar el riesgo			**I**	**R**
APO 12.03 Mantener un perfil de riesgo	**A**		**I**	**R**
APO 12.04 Expresar el riesgo	**A**		**I**	**R**
APO 12.05 Definir un portafolio de acciones para la gestión de riesgos	**A**			**R**
APO 12.06 Responder al riesgo			**R**	**A**

Fuente: Elaboración Propia

Tabla 14: Matriz RACI para APO13

APO13 **Gestionar la seguridad**			**Dominio:** **Alinear, Planificar y Organizar**	
Descripción del proceso Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
APO 13.01 Establecer y mantener un SGSI	**A**	**C**		**R**
APO 13.02 Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información	**A**		**I**	**R**
APO 13.03 Supervisar y revisar el SGSI	**R**		**R**	**A**

Fuente: Elaboración Propia

Tabla 15: Matriz RACI para BAI05

BAI05 **Gestionar la facilitación del cambio organizativo**			**Dominio:** **Construir, Adquirir e Implementar**	
Descripción del proceso Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todas las partes interesadas del negocio y de TI.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
BAI 05.01 Establecer el deseo de cambiar	**R**		**A**	
BAI 05.02 Formar un equipo de implementación efectivo		**A**		**R**
BAI 05.03 Comunicar la visión deseada	**R**		**I**	**C**
BAI 05.04 Facilitar la operación y el uso			**R**	**A**
BAI 05.05 Integrar nuevos enfoques	**I**	**I**	**A**	**R**
BAI 05.06 Mantener los cambios	**I**	**I**	**R**	**A**

Fuente: Elaboración Propia

Tabla 16: Matriz RACI para BAI09

BAI09 **Gestionar los activos**			**Dominio:** **Construir, Adquirir e Implementar**	
Descripción del proceso Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
BAI 09.01 Identificar y registrar activos reales				**R**
BAI 09.02 Gestionar activos críticos	**A**		**I**	**R**
BAI 09.03 Gestionar el ciclo de vida de los activos	**I**		**A**	**R**
BAI 09.04 Optimizar el coste de los activos	**R**		**A**	
BAI 09.05 Administrar licencias		**R**		**A**

Fuente: Elaboración Propia

Tabla 17: Matriz RACI para DSS02

DSS02 **Gestionar Peticiones e incidentes de servicio**			**Dominio:** **Entrega, Servicio y Soporte**	
Descripción del proceso Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
DSS 02.01 Definir esquemas de clasificación de incidentes y peticiones de servicio	**C**		**A**	**R**
DSS 02.02 Registrar, clasificar y priorizar peticiones e incidentes		**R**	**A**	**C**
DSS 02.03 Verificar, aprobar y resolver peticiones de servicio	**R**		**A**	**C**
DSS 02.04 Investigar, diagnosticar y localizar incidentes		**C**		**R**
DSS 02.05 Resolver y recuperarse de incidentes			**R**	**A**

DSS 02.06 Cerrar peticiones de servicio e incidentes	**R**		**A**	**C**
DSS 02.07 Seguir el estado y emitir informes	**R**		**A**	**C**

Fuente: Elaboración Propia

Tabla 18: Matriz RACI para DSS03

DSS03 **Gestionar Problemas**			**Dominio:** **Entrega, Servicio y Soporte**	
Descripción del proceso Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
DSS 03.01 Identificar y clasificar problemas	**A**		**I**	**R**
DSS 03.02 Investigar y diagnosticar problemas	**A**		**I**	**R**
DSS 03.03 Levantar errores conocidos	**C**		**A**	**R**
DSS 03.04 Resolver y cerrar	**A**		**I**	**R**

problemas				
DSS 03.05 Realizar una gestión de problemas proactiva	**A**		**I**	**R**

Fuente: Elaboración Propia

Tabla 19: Matriz RACI para DSS04

DSS04 **Gestionar la Continuidad**			**Dominio:** **Entrega, Servicio y Soporte**	
Descripción del proceso Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
DSS 04.01 Definir la política de continuidad del negocio, objetivos y alcance	**I**		**A**	**R**
DSS 04.02 Mantener una estrategia de continuidad	**R**	**C**	**R**	**I**
DSS 04.03 Desarrollar e implementar una respuesta a la continuidad del negocio	**A**		**I**	**R**

DSS 04.04 Ejercitar, probar y revisar el plan de continuidad			**R**	**A**
DSS 04.05 Revisar, mantener y mejorar el plan de continuidad			**A**	**R**
DSS 04.06 Proporcionar formación en el plan de continuidad			**R**	**A**
DSS 04.07 Gestionar acuerdos de respaldo	**R**		**A**	**C**
DSS 04.08 Ejecutar revisiones post-reanudación	**R**		**A**	**C**

Fuente: Elaboración Propia

Tabla 20: Matriz RACI para DSS05

DSS05 **Gestionar Servicios de Seguridad**			**Dominio:** **Entrega, Servicio y Soporte**	
Descripción del proceso Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
DSS 05.01 Proteger contra software		**R**	**A**	**I**

malicioso (malware)				
DSS 05.02 Gestionar la seguridad de la red y las conexiones		**R**	**A**	**I**
DSS 05.03 Gestionar la seguridad de los puestos de usuario final	**I**	**R**	**A**	**I**
DSS 05.04 Gestionar la identidad del usuario y el acceso lógico		**R**	**A**	**C**
DSS 05.05 Gestionar el acceso físico a los activos de TI		**R**	**I**	**A**
DSS 05.06 Gestionar documentos sensibles y dispositivos de salida	**I**	**R**	**I**	**A**
DSS 05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad	**I**	**R**	**I**	**A**

Fuente: Elaboración Propia

Tabla 21: Matriz RACI para DSS05

DSS05 **Gestionar Controles de Proceso de Negocio**			**Dominio:** **Entrega, Servicio y Soporte**	
Descripción del proceso Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información. Identificar los requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.				
Práctica Clave de gobierno	**Gerente del área de Administración Tributaria**	**Gerente de TI**	**Administración Municipal**	**Implementador ISO**
DSS 05.01 Alinear las actividades de control embebidas en los procesos de negocio con los objetivos corporativos.			**A**	**R**
DSS 05.02 Controlar el proceso de la información	**R**		**I**	**A**
DSS 05.03 Gestionar roles, responsabilidades, privilegios de acceso y niveles de autorización	**C**	**I**	**R**	**C**
DSS 05.04 Gestionar errores y excepciones			**A**	**R**
DSS 05.05 Asegurar la trazabilidad de los eventos y	**R**		**A**	**C**

responsabilidades de información				
DSS 05.06 Asegurar los activos de información	**C**		**I**	**R**

Fuente: Elaboración Propia

g) Inventario de activos

Tabla 22: Valoración de activos

Id Activo de Información	Nombre Activo de Información	Categoría Activo	Breve Descripción Activo de Información	Ubicación	Propietario del Activo de Información	Custodio del Activo de Información	Normativa asociada en la organización	Tipo de Activo de Información	Clasificación de Uso del Activo de Información	Valor del Activo de Información				
										Confidencialidad	Integridad	Disponibilidad	TOTAL	TASACIÓN
1	PC Escritorio	Activo Físico	PC para la atención de los contribuyentes	Área de rentas (área de atención)	Operador de caja de rentas	Área de TI	No aplica	Equipo de procesamiento	Interno	3.0	3.0	3.0	3.0	MEDIO
2	Archivero	Activo Físico	Contiene Documentos de los contribuyentes y documentos varios	Área de rentas (área de atención)	Operadores de caja de rentas	Operadores de caja de rentas	No aplica	Medio de Almacenamiento	Interno	2.0	2.0	3.0	2.0	MEDIO
3	Gerente de Rentas	Personal	Encargado de realizar informes, balances contables, etc. sobre el área	Área de rentas	Gerente de Rentas	Administración Municipal	MOF	Personal interno	Interno	3.0	3.0	4.0	3.3	MEDIO

4	Secretaria	Personal	Encargada de realizar la documentación necesaria del área	Área de Fiscalización	Gerente de Rentas	Gerente de Rentas	MOF	Personal Interno	Interno	2.0	2.0	3.0	2.7	MEDIO
5	PC Escritorio	Activo Físico	PC para la atención de los contribuyentes	Área de rentas (área de atención)	Operador de caja de rentas	Área de TI	No aplica	Equipo de procesamiento	Interno	3.0	3.0	4.0	3.3	MEDIO
6	PC Escritorio	Activo Físico	PC para la atención de los contribuyentes	Área de rentas (área de atención)	Operador de caja de rentas	Área de TI	No aplica	Equipo de procesamiento	Interno	3.0	3.0	4.0	3.3	MEDIO
7	PC Escritorio	Activo Físico	Documentación de los contribuyentes y de gerencia	Área de rentas (Oficina de Gerencia	Secretaria	Área de TI	No aplica	Equipo de procesamiento	Interno	3.0	3.0	4.0	3.3	MEDIO
8	PC Escritorio	Activo Físico	Documentación legislativa de los contribuyentes sobre el área de rentas	Área de rentas (Oficina de Gerencia	Abogado	Área de TI	No aplica	Equipo de procesamiento	Interno	3.0	3.0	3.0	3.0	MEDIO
9	Base de Datos	Información Documental	Data de los contribuyentes	Área de informática	Gerente	Administrador de base de datos	No aplica	Información Digital	Confidencial	4.0	4.0	5.0	4.3	ALTO
10	Software de Gestión de Rentas	Software	SW para administrar la información de los contribuyentes	Informática	Operadores de caja de rentas	Área de TI	Manual de uso	SW in house	Interno	3.0	3.0	5.0	3.7	ALTO

11	Cajas con Documentos	Información Documental	Información sobre los contribuyentes	Área de rentas	Secretaria	Gerente	No aplica	Información impresa	Interno	4.0	3.0	2.0	3.0	MEDIO
12	Operador de Caja	Personal	Encargado de facilitar a los contribuyentes toda la información sobre sus estados de cuenta	Área de rentas	Gerente de Rentas	Gerente de Rentas	MOF	Personal interno	Interno	3.0	3.0	4.0	3.5	ALTO
13	Laptop	Activo Físico	Contiene información sobre todos los contribuyentes y documentación sensible sobre los estados de cuenta de la municipalidad	Oficina de Gerencia	Gerente de Rentas	Área de TI	No aplica	Equipo de procesamiento	Confidencial	4.0	3.0	5.0	4.0	ALTO
14	Impresora	Activo Físico	Imprime los Estados de Cuenta y HR	Área de rentas (área de atención)	Operador de caja de rentas	Área de TI	No aplica	Equipo de procesamiento	Interno	2.0	2.0	3.0	2.3	MEDIO
15	Impresora	Activo Físico	Imprime los Estados de Cuenta y HR	Área de rentas (área de atención)	Operador de caja de rentas	Área de TI	No aplica	Equipo de procesamiento	Interno	2.0	2.0	3.0	2.3	MEDIO
16	Impresora	Activo Físico	Imprime los Estados de Cuenta y HR	Área de rentas (oficina de gerencia)	Operador de caja de rentas	Área de TI	No aplica	Equipo de procesamiento	Interno	2.0	2.0	3.0	2.3	MEDIO

17	Operador de Caja	Personal	Encargado de facilitar a los contribuyentes toda la información sobre sus estados de cuenta	Área de rentas	Gerente de Rentas	Gerente de Rentas	MOF	Personal interno	Interno	3.0	3.0	4.0	3.5	ALTO
18	Operador de Caja	Personal	Encargado de facilitar a los contribuyentes toda la información sobre sus estados de cuenta	Área de rentas	Gerente de Rentas	Gerente de Rentas	MOF	Personal interno	Interno	3.0	3.0	4.0	3.5	ALTO
19	Abogado	Personal	Encargado de ver toda la parte legislativa del área de rentas	Área de rentas (Oficina de Gerencia)	Gerente de Rentas	Gerente de Rentas	MOF	Personal interno	Interno	3.0	3.0	4.0	3.5	ALTO
20	Sub-Gerente de Fiscalización	Personal	Encargado de gestionar y generar reportes sobre las fiscalizaciones realizadas	Área de Fiscalización	Gerente de Rentas	Gerente de Rentas	MOF	Personal Interno	Interno	2.0	3.0	4.0	3.0	MEDIO
21	Secretaria	Personal	Encargada de realizar la documentación necesaria del área	Área de Fiscalización	Sub-Gerente de Fiscalización	Sub-Gerente de Fiscalización	MOF	Personal Interno	Interno	2.0	2.0	3.0	2.7	MEDIO
22	Fiscalizador	Personal	Persona encargada de fiscalizar los predios declarados	Área de Fiscalización	Sub-Gerente de Fiscalización	Gerente de Rentas	MOF	Personal Interno	Interno	2.0	2.0	1.0	1.7	BAJO

23	Fiscalizador	Personal	Persona encargada de fiscalizar los predios declarados	Área de Fiscalización	Sub-Gerente de Fiscalización	Gerente de Rentas	MOF	Personal Interno	Interno	2.0	2.0	1.0	1.7	BAJO
24	Fiscalizador	Personal	Persona encargada de fiscalizar los predios declarados	Área de Fiscalización	Sub-Gerente de Fiscalización	Gerente de Rentas	MOF	Personal Interno	Interno	2.0	2.0	1.0	1.7	BAJO
25	Fiscalizador	Personal	Persona encargada de fiscalizar los predios declarados	Área de Fiscalización	Sub-Gerente de Fiscalización	Gerente de Rentas	MOF	Personal Interno	Interno	2.0	2.0	1.0	1.7	BAJO
26	Fiscalizador	Personal	Persona encargada de fiscalizar los predios declarados	Área de Fiscalización	Sub-Gerente de Fiscalización	Gerente de Rentas	MOF	Personal Interno	Interno	2.0	2.0	1.0	1.7	BAJO
27	Laptop	Activo Físico	Contiene información sobre los predios fiscalizados	Área de Fiscalización	Sub-gerente de Fiscalización	Gerente de Rentas	No aplica	Equipo de procesamiento	Interno	3.0	3.0	4.0	3.3	MEDIO
28	Laptop	Activo Físico	Contiene información diversa sobre los predios fiscalizados	Área de Fiscalización	Fiscalizador	Sub-Gerente de Fiscalización	No aplica	Equipo de procesamiento	Interno	3.0	3.0	3.0	3.0	MEDIO
29	Laptop	Activo Físico	Contiene información diversa sobre los predios fiscalizados	Área de Fiscalización	Fiscalizador	Sub-Gerente de Fiscalización	No aplica	Equipo de procesamiento	Interno	3.0	3.0	3.0	3.0	MEDIO

30	PC Escritorio	Activo Físico	PC para la atención de los contribuyentes	Área de Fiscalización	Secretaria	Sub-Gerente de Fiscalización	No aplica	Equipo de procesamiento	Interno	3.0	3.0	3.0	3.0	MEDIO
31	Archivero	Activo Físico	Documentación variada sobre el área (Reportes, etc)	Área de Fiscalización	Área de fiscalización	Sub-Gerente de Fiscalización	No aplica	Medio de Almacenamiento	Interno	2.0	3.0	2.0	2.3	MEDIO
32	Archivero	Activo Físico	Documentación sobre los contribuyentes	Área de Fiscalización	Área de fiscalización	Sub-Gerente de Fiscalización	No aplica	Medio de Almacenamiento	Interno	2.0	3.0	2.0	2.3	MEDIO
33	Impresora	Activo Físico	Impresión de Documentos	Área de Fiscalización	Sub-Gerencia de Fiscalización	Área de TI	No aplica	Equipo de procesamiento	Interno	1.0	2.0	3.0	2.0	MEDIO
34	Cajas con Documentos	Información Documental	Información sobre los contribuyentes	Área de fiscalización	Área de Fiscalización	Gerente	No aplica	Información impresa	Interno	4.0	3.0	2.0	3.0	MEDIO
35	PC Escritorio	Activo Físico	Información sobre los contribuyentes y documentación de la sub-gerencia	Área de Ejecución Coactiva	Secretaria	Sub-Gerente de Ejecución Coactiva	No aplica	Equipo de Procesamiento	Interno	3.0	3.0	3.0	3.0	MEDIO
36	Secretaria	Personal	Encargada de realizar la documentación necesaria del área	Área de ejecución coactiva	Sub-Gerente de Ejecución Coactiva	Sub-Gerente de Ejecución Coactiva	MOF	Personal Interno	Interno	2.0	3.0	2.0	2.3	MEDIO

37	Sub-Gerente de Ejecución Coactiva	Personal	Encargado de realizar documentos y planear los planes de ejecución coactiva	Área de ejecución coactiva	Gerente de rentas	Gerente de rentas	MOF	Personal Interno	Interno	3.0	3.0	3.0	3.0	MEDIO
38	Archivero	Activo Físico	Contiene Documentos de los contribuyentes y documentos varios	Área de ejecución coactiva (área de atención)	Área de ejecución coactiva	Sub-gerente de Ejecución coactiva	No aplica	Medio de Almacenamiento	Interno	2.0	3.0	3.0	2.7	MEDIO
39	PC Escritorio	Activo Físico	Almacena y procesa información sobre los contribuyentes	Área de ejecución coactiva	Secretaria	Área de TI	No aplica	Equipo de procesamiento	Interno	3.0	3.0	3.0	3.0	MEDIO
40	Software de Ejecución Coactiva	Software	Sistema que ayuda a la gestión del área de ejecución coactiva	Área de ejecución coactiva	Área de Ejecución Coactiva	Área de TI	No aplica	SW in house	Confidencial	4.0	4.0	4.0	4.0	ALTO
41	Coordinador de planes de ejecución coactiva	Personal	Coordina y gestiona el plan de ejecución coactiva que se llevarán acabo	Área de ejecución coactiva	Sub-Gerente de Ejecución Coactiva	Gerente de rentas	MOF	Personal Interno	Interno	3.0	3.0	3.0	3.0	MEDIO
42	Sub-Gerente de Recaudación	Personal	Encargado de la administración de cobros realizados en caja	Área de Recaudación	Gerente de rentas	Gerente de rentas	MOF	Personal Interno	Interno	3.0	3.0	3.0	3.0	MEDIO

43	Secretaria	Personal	Realiza documentos e informes sobre el área de recaudación	Área de recaudación	Sub-Gerente de Recaudación	Gerente de Rentas	MOF	Personal Interno	Interno	3.0	2.0	3.0	2.7	MEDIO
44	Cajero	Personal	Realiza los cobros generados por impuestos o trámites	Área de recaudación	Sub-Gerente de Recaudación	Gerente de Rentas	MOF	Personal Interno	Interno	3.0	3.0	4.0	3.3	MEDIO
45	Cajero	Personal	Realiza los cobros generados por impuestos o trámites	Área de recaudación	Sub-Gerente de Recaudación	Gerente de Rentas	MOF	Personal Interno	Interno	3.0	3.0	4.0	3.3	MEDIO
46	PC Escritorio	Activo Físico	Almacena toda la información sobre los cobros realizados	Área de recaudación	Cajero	Área de TI	No aplica	Equipo de procesamiento	Interno	4.0	4.0	4.0	4.0	ALTO
47	PC Escritorio	Activo Físico	Almacena toda la información sobre los cobros realizados	Área de recaudación	Cajero	Área de TI	No aplica	Equipo de procesamiento	Interno	4.0	4.0	4.0	4.0	ALTO
48	PC Escritorio	Activo Físico	Almacena documentación del área y archivos.	Área de recaudación	Secretaria	Área de TI	No aplica	Equipo de procesamiento	Interno	4.0	4.0	3.0	3.7	ALTO
49	Laptop	Activo Físico	Almacena documentación e informes sobre el área	Área de recaudación	Sub-Gerente de Recaudación	Área de TI	No aplica	Equipo de procesamiento	Interno	4.0	4.0	4.0	4.0	ALTO

50	Software de Recaudación	Software	Sistema que ayuda a la gestión de pagos de los contribuyentes	Área de recaudación	Cajeras	Área de TI	No aplica	SW in house	Confidencial	5.0	4.0	4.0	4.3	ALTO
51	Impresora	Activo Físico	Imprime boletas facturas y recibos	Área de recaudación	Cajero	Área de TI	No aplica	Equipo de procesamiento	Interno	2.0	2.0	3.0	2.3	MEDIO
52	Impresora	Activo Físico	Imprime documentos y oficios del área	Área de recaudación	Área de recaudación	Área de TI	No aplica	Equipo de procesamiento	Interno	2.0	2.0	3.0	2.3	MEDIO
53	Archivero	Activo Físico	Documentación sobre el área	Área de recaudación	Área de recaudación	Sub-Gerente de Fiscalización	No aplica	Medio de Almacenamiento	Interno	2.0	3.0	2.0	2.3	MEDIO

Fuente: Elaboración Propia

h) Análisis de riesgos, impacto y cálculo de riesgos

Tabla 23: Análisis de riesgo de cada activo

Id Activo de Información	Nombre Activo de Información	Categoría Activo	Amenaza		Controles		Riesgo	Id Riesgo	Impacto			Cálculo del Riesgo				
			Descripción	Frecuencia	Controles Actuales	Nivel de Vulnerabilidad			Legal	Operativo	Económico	Probabilidad de Ocurrencia	Impacto	NIVEL DE EXPOSICIÓN AL RIESGO	NIVEL DE RIESGO	Aceptable / No aceptable
1	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico e intrusión de malware al activo	2.0	UPS, SW antivirus	1.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	3.0	2.0	1.5	2.7	4.0	Moderado	Aceptable
2	Archivero	Activo Físico	Antigüedad del activo y contacto directo con cableado no protegido.	2.0	No existe	3.0	La información contenida no está debidamente protegida por tanto puede haber pérdida de esta, en caso de un problema con el cableado se podría ver afectado inmediatamente.	**2**	3.0	3.0	3.0	2.5	3.0	7.5	Alto	No aceptable

3	Gerente de Rentas	Personal	No pueda venir a trabajar	2.0	Delegar la función a Sub-Gerente Fiscalización	2.0	El personal de respaldo no está totalmente capacitado.	**3**	1.0	4.0	1.0	2.0	2.0	4.0	Moderado	Aceptable
4	Secretaria	Personal	No pueda venir a trabajar	2.0	No existe	2.0	No existe personal de respaldo	**4**	1.0	4.0	1.0	2.0	2.0	4.0	Moderado	Aceptable
5	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	UPS, SW antivirus	2.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	3.0	2.0	2.0	2.7	5.3	Moderado	Aceptable
6	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	SW antivirus	2.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	2.0	3.0	2.0	2.7	5.3	Moderado	Aceptable

7	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	SW antivirus	2.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	2.0	3.0	2.0	2.7	5.3	Moderado	Aceptable
8	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	SW antivirus	2.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	2.0	3.0	2.0	2.7	5.3	Moderado	Aceptable
9	Base de Datos	Información Digital	Falta de Fluido Eléctrico, Intrusión de terceros al sistema y modificación de la información	2.0	UPS, firewall	2.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico y a la desactualización de controles actuales por falta de mantenimiento	**1**	3.0	4.0	3.0	2.0	3.3	6.7	Alto	No aceptable
10	Software de Gestión de Rentas	SW in House	Antigüedad del sistema, contraseñas débiles	2.0	Clave de acceso	3.0	Un ingreso no autorizado por contraseñas poco robustas	**5**	4.0	3.0	4.0	2.5	3.7	9.2	Muy Alto	No aceptable

11	Cajas con Documentos	Información Impresa	Que la información se extravíe o el ambiente la deteriore	2.0	No existe	3.0	Que se pierda información o que se vea afectada por factores ambientales	**6**	4.0	3.0	2.0	2.5	3.0	7.5	Alto	No aceptable
12	Operador de Caja	Personal	El operador de caja no vaya a trabajar	3.0	No existe	2.0	Que no exista personal de respaldo, por tanto no se podrá a toda capacidad en la atención al público	**7**	1.0	3.0	3.0	2.5	2.3	5.8	Moderado	Aceptable
13	Laptop	Activo Físico	Intrusión de malware al activo	1.0	SW antivirus	3.0	Debido a la falta de constante de actualización del sw antivirus puede implantarse sw inadecuado sobre el activo, que permita robar y/o modificar información sensible	**8**	4.0	3.0	4.0	2.0	3.7	7.3	Alto	No aceptable
14	Impresora	Activo Físico	Que deje de operar por la antigüedad del mismo activo	3.0	No existe	3.0	Debido a la falta constante de mantenimiento genera que no opere adecuadamente, esto conlleva a que se demore en la atención de los contribuyentes generando un malestar	**9**	1.0	4.0	3.0	3.0	2.7	8.0	Alto	No aceptable

15	Impresora	Activo Físico	Que deje de operar por la falta de mantenimiento	3.0	No existe	3.0	Debido a la falta constante de mantenimiento genera que no opere adecuadamente, esto conlleva a que se demore en la atención de los contribuyentes generando un malestar	**9**	1.0	4.0	3.0	3.0	2.7	8.0	Alto	No aceptable
16	Impresora	Activo Físico	Que deje de operar por la falta de mantenimiento	3.0	No existe	3.0	Debido a la falta constante de mantenimiento genera que no opere adecuadamente, esto conlleva a que se demore en la atención de los contribuyentes generando un malestar	**9**	1.0	4.0	3.0	3.0	2.7	8.0	Alto	No aceptable
17	Operador de Caja	Personal	No pueda venir a trabajar	3.0	No existe	2.0	No existe personal de respaldo	**4**	1.0	4.0	2.0	2.5	2.3	5.7	Moderado	Aceptable
18	Operador de Caja	Personal	No pueda venir a trabajar	3.0	No existe	2.0	No existe personal de respaldo	**4**	1.0	4.0	2.0	2.5	2.3	5.7	Moderado	Aceptable
19	Abogado	Personal	No pueda venir a trabajar	2.0	No existe	1.0	No existe personal de respaldo	**4**	1.0	2.0	1.0	1.5	1.3	2.0	Bajo	Aceptable

20	Sub-Gerente de Fiscalización	Personal	No pueda venir a trabajar	2.0	No existe	1.0	No existe personal de respaldo	**4**	1.0	3.0	1.0	1.5	1.7	3.3	Moderado	
21	Secretaria	Personal	No pueda venir a trabajar	2.0	No existe	2.0	No existe personal de respaldo	**4**	1.0	4.0	1.0	2.0	2.0	4.0	Moderado	Aceptable
22	Fiscalizador	Personal	No pueda venir a trabajar	2.0	No existe	2.0	Existe personal de respaldo, pero impacta en la productividad	**10**	1.0	3.0	1.0	2.0	1.7	3.3	Moderado	Aceptable
23	Fiscalizador	Personal	No pueda venir a trabajar	2.0	No existe	2.0	Existe personal de respaldo, pero impacta en la productividad	**10**	1.0	3.0	1.0	2.0	1.7	3.3	Moderado	Aceptable
24	Fiscalizador	Personal	No pueda venir a trabajar	2.0	No existe	2.0	Existe personal de respaldo, pero impacta en la productividad	**10**	1.0	3.0	1.0	2.0	1.7	3.3	Moderado	Aceptable
25	Fiscalizador	Personal	No pueda venir a trabajar	2.0	No existe	2.0	Existe personal de respaldo, pero impacta en la productividad	**10**	1.0	3.0	1.0	2.0	1.7	3.3	Moderado	Aceptable
26	Fiscalizador	Personal	No pueda venir a trabajar	2.0	No existe	2.0	Existe personal de respaldo, pero impacta en la productividad	**10**	1.0	3.0	1.0	2.0	1.7	3.3	Moderado	Aceptable

27	Laptop	Activo Físico	Intrusión de malware al activo	1.0	SW antivirus	3.0	Debido a la falta de constante de actualización del sw antivirus puede implantarse sw inadecuado sobre el activo, que permita robar y/o modificar información sensible	**8**	4.0	3.0	4.0	2.0	3.7	7.3	Alto	No aceptable
28	Laptop	Activo Físico	Intrusión de malware al activo	1.0	SW antivirus	3.0	Debido a la falta de constante de actualización del sw antivirus puede implantarse sw inadecuado sobre el activo, que permita robar y/o modificar información sensible	**8**	4.0	3.0	4.0	2.0	3.7	7.3	Alto	No aceptable
29	Laptop	Activo Físico	Intrusión de malware al activo	1.0	SW antivirus	3.0	Debido a la falta de constante de actualización del sw antivirus puede implantarse sw inadecuado sobre el activo, que permita robar y/o modificar información sensible	**8**	4.0	3.0	4.0	2.0	3.7	7.3	Alto	No aceptable

30	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	UPS, SW antivirus	1.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	3.0	2.0	1.5	2.7	4.0	Moderado	Aceptable
31	Archivero	Activo Físico	Antigüedad del activo y contacto directo con cableado no protegido.	2.0	No existe	3.0	La información contenida no está debidamente protegida por tanto puede haber pérdida de esta, en caso de un problema con el cableado se podría ver afectado inmediatamente.	**2**	3.0	3.0	3.0	2.5	3.0	7.5	Alto	No aceptable
32	Archivero	Activo Físico	Antigüedad del activo y contacto directo con cableado no protegido.	2.0	No existe	3.0	La información contenida no está debidamente protegida por tanto puede haber pérdida de esta, en caso de un problema con el cableado se podría ver afectado inmediatamente.	**2**	3.0	3.0	3.0	2.5	3.0	7.5	Alto	No aceptable

33	Impresora	Activo Físico	Que deje de operar por la falta de mantenimiento	3.0	No existe	3.0	Debido a la falta constante de mantenimiento genera que no opere adecuadamente, esto conlleva a que se demore en la atención de los contribuyentes generando un malestar	**9**	1.0	4.0	3.0	3.0	2.7	8.0	Alto	No aceptable
34	Cajas con Documentos	Información Impresa	Que la información se extravíe o el ambiente la deteriore	2.0	No existe	3.0	Que se pierda información o que se vea afectada por factores ambientales	**6**	4.0	3.0	2.0	2.5	3.0	7.5	Alto	No aceptable
35	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	UPS, SW antivirus	1.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	3.0	2.0	1.5	2.7	4.0	Moderado	Aceptable
36	Secretaria	Personal	No pueda venir a trabajar	2.0	No existe	2.0	No existe personal de respaldo	**4**	1.0	4.0	1.0	2.0	2.0	4.0	Moderado	Aceptable
37	Sub-Gerente de Ejecución Coactiva	Personal	No pueda venir a trabajar	2.0	No existe	2.0	Existe personal de respaldo, pero impacta en la productividad	**10**	1.0	3.0	1.0	2.0	1.7	3.3	Moderado	Aceptable

38	Archivero	Activo Físico	Antigüedad del activo y contacto directo con cableado no protegido.	2.0	No existe	3.0	La información contenida no está debidamente protegida por tanto puede haber pérdida de esta, en caso de un problema con el cableado se podría ver afectado inmediatamente.	**2**	3.0	3.0	3.0	2.5	3.0	7.5	Alto	No aceptable
39	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	UPS, SW antivirus	1.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	3.0	2.0	1.5	2.7	4.0	Moderado	Aceptable
40	Software de Ejecución Coactiva	SW in House	Antigüedad del sistema, contraseñas débiles	2.0	Clave de acceso	3.0	Un ingreso no autorizado por contraseñas poco robustas	**5**	4.0	3.0	4.0	2.5	3.7	9.2	Muy Alto	No aceptable
41	Coordinador de planes de ejecución coactiva	Personal	No pueda venir a trabajar	2.0	No existe	2.0	Existe personal de respaldo, pero impacta en la productividad	**10**	1.0	3.0	1.0	2.0	1.7	3.3	Moderado	Aceptable
42	Sub-Gerente de Recaudación	Personal	No pueda venir a trabajar	2.0	No existe	2.0	No existe personal de respaldo capacitado	**11**	1.0	3.0	1.0	2.0	1.7	3.3	Moderado	

43	Secretaria	Personal	No pueda venir a trabajar	2.0	No existe	2.0	No existe personal de respaldo	**4**	1.0	4.0	1.0	2.0	2.0	4.0	Moderado	Aceptable
44	Cajero	Personal	El operador de caja no vaya a trabajar	3.0	No existe	2.0	Que no exista personal de respaldo, por tanto, no se podrá a toda capacidad en la atención al público	**10**	1.0	4.0	3.0	2.5	2.7	6.7	Alto	Aceptable
45	Cajero	Personal	El operador de caja no vaya a trabajar	3.0	No existe	2.0	Que no exista personal de respaldo, por tanto, no se podrá a toda capacidad en la atención al público	**10**	1.0	4.0	3.0	2.5	2.7	6.7	Alto	Aceptable
46	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	UPS, SW antivirus	1.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	3.0	2.0	1.5	2.7	4.0	Moderado	Aceptable
47	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	UPS, SW antivirus	1.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	3.0	2.0	1.5	2.7	4.0	Moderado	Aceptable

48	PC Escritorio	Activo Físico	Falta de Fluido Eléctrico, Intrusión de malware al activo	2.0	UPS, SW antivirus	1.0	La posibilidad de que no se pueda acceder a los servicios debido al corte de fluido eléctrico, falta de mantenimiento de los controles actuales	**1**	3.0	3.0	2.0	1.5	2.7	4.0	Moderado	Aceptable
49	Laptop	Activo Físico	Intrusión de malware al activo	1.0	SW antivirus	3.0	Debido a la falta de constante de actualización del sw antivirus puede implantarse sw inadecuado sobre el activo, que permita robar y/o modificar información sensible	**8**	4.0	3.0	4.0	2.0	3.7	7.3	Alto	No aceptable
50	Software de Recaudación	SW in House	Antigüedad del sistema, contraseñas débiles	2.0	Clave de acceso	3.0	Un ingreso no autorizado por contraseñas poco robustas	**5**	4.0	3.0	4.0	2.5	3.7	9.2	Muy Alto	No aceptable
51	Impresora	Activo Físico	Que deje de operar por la falta de mantenimiento	3.0	No existe	3.0	Debido a la falta constante de mantenimiento genera que no opere adecuadamente, esto conlleva a que se demore en la atención de los contribuyentes generando un malestar	**9**	1.0	4.0	3.0	3.0	2.7	8.0	Alto	No aceptable

52	Impresora	Activo Físico	Que deje de operar por la falta de mantenimiento	3.0	No existe	3.0	Debido a la falta constante de mantenimiento genera que no opere adecuadamente, esto conlleva a que se demore en la atención de los contribuyentes generando un malestar	**9**	1.0	4.0	3.0	3.0	2.7	8.0	Alto	No aceptable

Fuente: Elaboración Propia

i) Tratamiento de riesgos

Tabla 24: Control de cada activo

Id Activo de Información	Nombre Activo de Información	Categoría de Activo	Id de Riesgo	Nivel Riesgo	Riesgo	Estrategia de Tratamiento	Control de mitigación		Responsable	Comentarios
							Control de mitigación	Control ISO 27001		
1	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento
2	Archivero	Activo Físico	**2**	Alto	Revisar Cuadro de Matriz de Riesgo	Asegurar que la información contenida sea protegida	Mantener en un lugar seguro y protegido	A.11.2.1 Emplazamiento y protección de los equipos A.11.1.4 Protección contra amenazas externas y ambientales	Área correspondiente	

3	Gerente de Rentas	Personal	**3**	Moderado	Revisar Cuadro de Matriz de Riesgo	Que se generen citas para atención	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
4	Secretaria	Personal	**4**	Moderado	Revisar Cuadro de Matriz de Riesgo	Que se generen citas para atención	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
5	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento
6	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento
7	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento

8	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento
9	Base de Datos	Información Digital	**1**	Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantener en constante monitoreo para descartar fallos	A.9.2 Gestión de Acceso de Usuario A.9.4 Control de acceso a sistema y aplicación	Área de TI	
10	Software de Gestión de Rentas	SW in House	**5**	Muy Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Generar un plan para contraseñas más robustas	A.9.4.3 Sistema de gestión de contraseñas	Área de TI	Solicitar un nuevo software de gestión
11	Cajas con Documentos	Información Impresa	**6**	Alto	Revisar Cuadro de Matriz de Riesgo	Asegurar que la información contenida sea protegida	Mantener en un lugar seguro que pueda resguardar la información	A.11.1.4 Protección contra amenazas externas y ambientales	Área correspondiente	
12	Operador de Caja	Personal	**7**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
13	Laptop	Activo Físico	**8**	Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantener los controles actuales y mejorarlos	A.11.2.1 Emplazamiento y protección de los equipos A.12.2.1 Controles contra códigos	Área de TI	Se tiene que planificar un calendario de mantenimiento

								maliciosos		
14	Impresora	Activo Físico	**9**	Alto	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener en constante monitoreo por posibles fallos	A.11.2.4. Mantenimiento de Equipos A.11.2.1 Emplazamiento y protección de los equipos	Área de TI	Se tiene que planificar un calendario de mantenimiento
15	Impresora	Activo Físico	**9**	Alto	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener en constante monitoreo por posibles fallos	A.11.2.4. Mantenimiento de Equipos A.11.2.1 Emplazamiento y protección de los equipos	Área de TI	Se tiene que planificar un calendario de mantenimiento
16	Impresora	Activo Físico	**9**	Alto	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener en constante monitoreo por posibles fallos	A.11.2.4. Mantenimiento de Equipos A.11.2.1 Emplazamiento y protección de los equipos	Área de TI	Se tiene que planificar un calendario de mantenimiento
17	Operador de Caja	Personal	**4**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	

18	Operador de Caja	Personal	**4**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
19	Abogado	Personal	**4**	Bajo	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
20	Sub-Gerente de Fiscalización	Personal	**4**	Moderado	Revisar Cuadro de Matriz de Riesgo	Que se generen citas para atención	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
21	Secretaria	Personal	**4**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
22	Fiscalizador	Personal	**10**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	

23	Fiscalizador	Personal	**10**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
24	Fiscalizador	Personal	**10**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
25	Fiscalizador	Personal	**10**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
26	Fiscalizador	Personal	**10**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
27	Laptop	Activo Físico	**8**	Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantener en constante monitoreo por posibles fallos	A.11.2.1 Emplazamiento y protección de los equipos A.12.2.1 Controles contra códigos maliciosos	Área de TI	Se tiene que planificar un calendario de mantenimiento

28	Laptop	Activo Físico	**8**	Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantener en constante monitoreo por posibles fallos	A.11.2.1 Emplazamiento y protección de los equipos A.12.2.1 Controles contra códigos maliciosos	Área de TI	Se tiene que planificar un calendario de mantenimiento
29	Laptop	Activo Físico	**8**	Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantener en constante monitoreo por posibles fallos	A.11.2.1 Emplazamiento y protección de los equipos A.12.2.1 Controles contra códigos maliciosos	Área de TI	Se tiene que planificar un calendario de mantenimiento
30	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento
31	Archivero	Activo Físico	**2**	Alto	Revisar Cuadro de Matriz de Riesgo	Asegurar que la información contenida sea protegida	Mantener en un lugar seguro y protegido	A.11.2.1 Emplazamiento y protección de los equipos A.11.1.4 Protección contra amenazas externas y ambientales	Área correspondiente	

32	Archivero	Activo Físico	**2**	Alto	Revisar Cuadro de Matriz de Riesgo	Asegurar que la información contenida sea protegida	Mantener en un lugar seguro y protegido	A.11.2.1 Emplazamiento y protección de los equipos A.11.1.4 Protección contra amenazas externas y ambientales	Área correspondiente	
33	Impresora	Activo Físico	**9**	Alto	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener en constante monitoreo por posibles fallos	A.11.2.4. Mantenimiento de Equipos A.11.2.1 Emplazamiento y protección de los equipos	Área de TI	Se tiene que planificar un calendario de mantenimiento
34	Cajas con Documentos	Información Impresa	**6**	Alto	Revisar Cuadro de Matriz de Riesgo	Asegurar que la información contenida sea protegida	Mantener en un lugar seguro y protegido	A.11.1.4 Protección contra amenazas externas y ambientales	Área correspondiente	
35	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento
36	Secretaria	Personal	**4**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	

37	Sub-Gerente de Ejecución Coactiva	Personal	**10**	Moderado	Revisar Cuadro de Matriz de Riesgo	Que se generen citas para atención	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
38	Archivero	Activo Físico	**2**	Alto	Revisar Cuadro de Matriz de Riesgo	Asegurar que la información contenida sea protegida	Mantener en un lugar seguro y protegido	A.11.1 Áreas seguras	Área correspondiente	
39	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.11.2.4. Mantenimiento de Equipos	Área de TI	Se tiene que planificar un calendario de mantenimiento
40	Software de Ejecución Coactiva	SW in House	**5**	Muy Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Generar un plan para contraseñas más robustas	A.9.4.3 Sistema de gestión de contraseñas	Área de TI	
41	Coordinador de planes de ejecución coactiva	Personal	**10**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	

42	Sub-Gerente de Recaudación	Personal	**11**	Moderado	Revisar Cuadro de Matriz de Riesgo	Que se generen citas para atención	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
43	Secretaria	Personal	**4**	Moderado	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
44	Cajero	Personal	**10**	Alto	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
45	Cajero	Personal	**10**	Alto	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener comunicado cualquier incidente de falta.	A.7.1.2 Términos y condiciones del empleo A.7.2.1 Responsabilidades de Gerencia	Administración Municipal	
46	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento

47	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento
48	PC Escritorio	Activo Físico	**1**	Moderado	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantenimiento preventivo del UPS y actualización adecuada de las firmas de virus del SW Antivirus	A.12.2.1 Controles contra códigos maliciosos A.11.2.2 Servicios de suministro	Área de TI	Se tiene que planificar un calendario de mantenimiento
49	Laptop	Activo Físico	**8**	Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Mantener en constante monitoreo por posibles fallos	A.11.2.1 Emplazamiento y protección de los equipos A.12.2.1 Controles contra códigos maliciosos	Área de TI	Se tiene que planificar un calendario de mantenimiento
50	Software de Recaudación	SW in House	**5**	Muy Alto	Revisar Cuadro de Matriz de Riesgo	Mantenimiento regular de los controles actuales.	Generar un plan para contraseñas más robustas	A.9.4.3 Sistema de gestión de contraseñas	Área de TI	

51	Impresora	Activo Físico	**9**	Alto	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener en constante monitoreo por posibles fallos	A.11.2.4. Mantenimiento de Equipos A.11.2.1 Emplazamiento y protección de los equipos	Área de TI	Se tiene que planificar un calendario de mantenimiento
52	Impresora	Activo Físico	**9**	Alto	Revisar Cuadro de Matriz de Riesgo	No existe	Mantener en constante monitoreo por posibles fallos	A.11.2.4. Mantenimiento de Equipos A.11.2.1 Emplazamiento y protección de los equipos	Área de TI	Se tiene que planificar un calendario de mantenimiento

Fuente: Elaboración Propia

j) Estado actual de conocimiento sobre seguridad de la información luego de aplicado el SGSI

Luego de concluido la etapa de desarrollo del SGSI se usó una encuesta, con todas las personas que estuvieron involucradas durante todo el proceso. Para ello tomamos nuestra población y muestra que son:

Población	Muestra
25	15

k) Resultados de post-test

Tabla 25: Resultados de post-test

POST-TEST: Nivel de conocimiento del personal en aspectos de SGSI y seguridad de la información																									TOTAL
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	
1	2	2	2	3	2	2	3	2	2	3	2	2	3	3	2	2	2	2	3	3	2	3	2	3	2	59
2	2	3	2	3	3	3	3	3	2	3	3	3	2	2	3	3	3	2	1	3	2	3	2	2	2	63
3	2	3	3	2	3	3	2	2	1	3	3	2	2	2	2	3	3	3	3	3	2	3	3	3	2	63
4	2	2	1	2	3	2	3	2	3	3	3	3	3	3	2	3	2	3	2	2	3	3	3	3	3	64
5	2	2	3	2	2	3	3	3	3	1	3	3	3	3	3	2	2	2	3	3	2	3	2	2	2	62
6	2	3	2	3	1	2	2	2	2	3	2	2	2	3	2	3	3	3	3	3	3	2	3	3	2	61
7	2	3	3	2	2	2	2	2	3	2	2	3	3	3	2	3	2	2	3	2	2	2	2	2	3	59
8	2	2	3	3	2	2	2	2	2	2	2	1	3	2	2	3	2	2	3	3	3	2	2	2	3	57
9	2	2	2	1	3	3	3	3	2	2	3	2	3	2	2	2	3	3	2	1	2	3	2	1	3	57
10	3	2	3	3	2	3	3	3	2	3	3	3	2	3	3	2	2	2	3	2	3	3	2	2	3	65
11	2	2	1	2	3	2	2	3	2	2	2	2	2	1	2	3	3	2	3	2	3	2	2	2	2	54
12	2	2	2	2	3	2	3	3	2	3	3	2	2	2	2	2	2	2	2	2	3	3	3	2	2	58
13	2	2	2	3	1	2	3	2	2	3	2	3	2	2	3	3	2	2	2	2	3	2	3	2	3	58
14	3	2	3	3	3	2	2	3	2	3	2	3	2	1	3	2	2	3	3	3	2	3	2	3	2	62
15	3	2	3	2	2	3	2	2	2	2	3	1	2	3	2	3	1	3	2	3	2	3	2	3	2	58

Fuente: Elaboración Propia

l) Resumen de resultados post-test

Tabla 26: Resumen de Resultados Post-test

N°	NIVEL DE CONOCIMIENTO DEL PERSONAL SOBRE SGSI Y SEGURIDAD DE LA INFORMACIÓN	
	TOTAL	BAREMO
1	59	MEDIO
2	63	ACEPTABLE
3	63	ACEPTABLE
4	64	ACEPTABLE
5	62	ACEPTABLE
6	61	ACEPTABLE
7	59	MEDIO
8	57	MEDIO
9	57	MEDIO
10	65	ACEPTABLE
11	54	MEDIO
12	58	MEDIO
13	58	MEDIO
14	62	ACEPTABLE
15	58	MEDIO

Fuente: Elaboración Propia

j.1 Cuadro que define el nivel de conocimiento

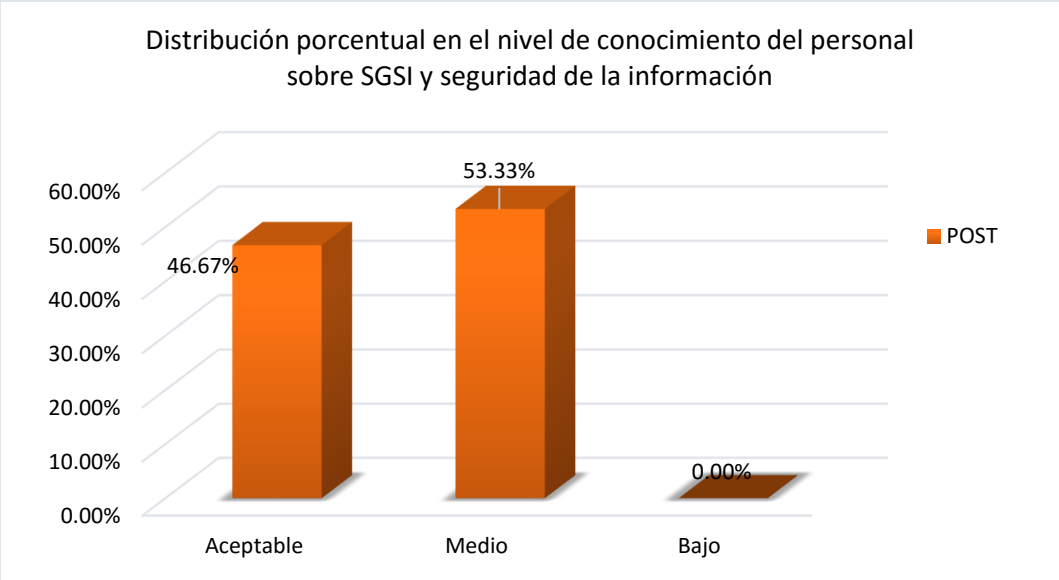
Tabla 27: Leyenda de nivel de conocimiento

NIVEL DE CONOCIMIENTO	
RANGO	CRITERIO
60 - 75	ACEPTABLE
43 - 59	MEDIO
25 - 42	BAJO

Fuente: Elaboración Propia

j.2 Gráfica de post-test

Gráfico 1: Gráfica de resultados



Fuente: Elaboración Propia

4. ANÁLISIS Y DISCUSIÓN

En referencia al proyecto realizado en el Ayuntamiento de Málaga (2005) en el cuál el objetivo era implantar una política de seguridad, en la que se consideraban objetivos de la entidad y se determinó usar la ISO 27001:2005 ya que estaba estrechamente relacionada con los procesos que se realizaban en la entidad, ya que ISO al ser un estándar que ayuda a orientar y simplificar procesos, y esto orientará en la investigación que servirá para mejorar los servicios en un entorno de gestión seguro en la entidad.

Así mismo, dentro del mismo proyecto se planteaba determinar roles en el personal de acuerdo a los procesos para que los controles sean más eficaces, esto se corrobora con la información encontrada en la investigación de, De Pablo (2007), en donde su objetivo era evaluar y corroborar controles ya existentes bajo la norma COBIT en la que asigna roles en cada proceso de la plataforma tecnológica de la banca virtual. Y esto, guarda relación con la presente investigación ya que se generan roles de acuerdo al grado de procesos que se realiza en la municipalidad.

Mientras que Villasmil (2006), hizo uso en su investigación del estándar ISO 17799 para estudiar y analizar los riesgos existentes e implicados en los sistemas de información de las pequeñas y medianas empresas y reducir los impactos que tuvieran a través de la implementación de una política de seguridad, y esta parte de la investigación guarda relación con la presente, ya que permitirá crear un conjunto de reglas y prácticas que regulan la manera en que se deben dirigir, proteger y distribuir los recursos en una organización para llevar a cabo los objetivos de esta, una vez establecida la política de seguridad.

Por otro lado, en la investigación de Mendoza (2005), nos habla que el impacto de las TIC's es mucho mayor al esperado en las organizaciones, esto por parte de la investigación refuerza la idea de ver que sobre este tipo de activos los controles implementados también tienen que ser adecuados.

La investigación de Borghello (2010), en la que finaliza con puntos importantes en la seguridad de la información sobre la organización como el aislamiento y globalización, legislación vigente, tecnología existente, daños minimizables, riesgos manejables, costos, personas involucradas; se relaciona en la investigación, de tal manera que todos los activos de información en la organización deben de ser totalmente involucrados para así mejorar la seguridad de toda la información que contienen estos activos y así reducir riesgos existentes.

Finalmente, Córdova (2003), concluyó en su tesis sobre un plan basado en una metodología en la que se reflejará todos los recursos usados en el desarrollo de un sistema que permitirá mejorar la seguridad acorde a la organización que lo requiera, a la vez de establecer roles de los usuarios involucrados en el plan. Esto se puede apreciar en el desarrollo de la presente investigación en la que se tiene que tener un control sobre los roles de las personas que se relacionan a la investigación, y también sobre los recursos usados durante todo el desarrollo del sistema de gestión de seguridad de la información.

5. CONCLUSIONES

a. Durante la etapa inicial de la investigación del estado actual de la organización, se tomó en cuenta los resultados obtenidos de la encuesta y entrevista realizada en la gerencia, al gerente y al personal; en la cual concluí, que la seguridad de la información no se toma muy en cuenta y no se siguen protocolos ni controles adecuados para el control de la información.
b. En base a todos los activos, se pudo determinar que la gran mayoría al no tener controles eficientes sobre ellos, provocaban la pérdida de información. Ya que los riesgos muchas veces se materializaban aprovechando las vulnerabilidades que ellos tenían. Para esto la matriz de control de riesgos nos ayudó a determinar cuáles eran los controles más eficientes que existían en base a la NTP ISO/IEC 27001:2014 y COBIT 5.
c. Se obtuvo el resultado esperado sobre el personal de la Gerencia de Administración Tributaria y Rentas, que se comprometió con el nuevo cambio y con el SGSI.

6. RECOMENDACIONES

a. Realizar una auditoría interna del SGSI para conocer cuáles podrían ser algunas falencias de los controles implementados.
b. Hacer un plan de sensibilización y compromiso con la política de seguridad en toda la Gerencia de Administración Tributaria.
c. Generar evaluaciones constantes a todo el personal involucrado en la implantación del SGSI.
d. Hacer de conocimiento público el SGSI a otras áreas para que puedan involucrarse con la correcta gestión de información.

REFERENCIA BIBLIOGRÁFICA

Alfaro, E. A. (2008). *Avance en la Implementación de las Normas Técnicas Peruanas de Gestión de Tecnología de Información*. Congreso Internacional Sudamericano de Ingeniería de Sistemas, Computación e Informática XII: Arequipa.

Ayuntamiento de Málaga (2010). *Política de seguridad de la información. España.* Citado en http://www.malaga.eu/inter/visor_contenido2/NRMDocumentDisplayer/665/DocumentoNormativa665

Borghello, C. (2001), *Seguridad Informática: sus implicancias e implementación*. Trabajo de Grado. Universidad Tecnológica Nacional de Argentina. http://cristianborghello.com/tesis/

Córdova, Rodríguez, Norma Edith. (2003). *Plan de Seguridad Informática para una Entidad Financiera. Trabajo de Grado. Universidad Nacional Mayor de San Marcos. Facultad de Ciencias Matemáticas*. EAP de Computación. Lima, Perú. URL: http://sisbib.unmsm.edu.pe/bibvirtual /Tesis/Basic/cordova_rn/contenido

De Pablo Arias, Samanta Andreina. (2007). *Evaluación de seguridad de información para la plataforma de Banca Virtual en una entidad financiera*. Tesis de Grado. Universidad Central de Caracas. Venezuela.

Escrivá Gascó, Gema (2014). *Seguridad Informática.* España: Macmillan Iberia, S.A.

INDECOPI (2014). *Norma técnica peruana NTP-ISO/IEC 27001 2014. Perú.* Documento encontrado en: www.pecert.gob.pe/_publicaciones/2014/ISO-IEC-27001-2014.pdf

ISACA (2008). Information Systems Audit and Control *Association*. URL: http://www.isaca.org/Template.cfm?Section=Downloads3&Template=/Contentmanagement/ContentDisplay.cfm&ContentID=19227

ISACA (2012). COBIT 5. Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. ISBN 978-1-60420-282-3. USA.

Jimeno Bernal, Jorge (2013). *Ciclo PDCA (Planificar, Hacer, Verificar y Actuar): El círculo de Deming de mejora continua*. Grupo PDCA HOME. Citado en: http://www.pdcahome.com/5202/ciclo-pdca/

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

Mamani Poma, O. J. et al (2002). *Auditoría informática Municipalidad Mariscal Nieto*. Universidad Privada José Carlos Mariátegui. Escuela de Ingeniería de Sistemas.

Mendoza, E. (2005). *Impacto de la Tecnología de Información en la Competitividad de las Pequeñas y Medianas Industrias*. Trabajo de Postgrado. Universidad Centroccidental Lisandro Alvarado. Decanato de Administración y Contaduría Barquisimeto. Venezuela.

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

Municipalidad Distrital de Independencia (2015). *Plan Estratégico Institucional – PEI, 2014 - 2021*. Recuperado de http://munidi.gob.pe/transparencia/category/pei/

Oz, E., (2001). *Administración de Sistemas de Información*, 2da Edic. México: Editorial Thomson Learning.

Prandini, Patricia y Szuster, Rodolfo (2012). *Segurinfo 2012*. Revolución Cobit 5. www.segurinfo.org. Buenos Aires. Argentina.

Villasmil, Fabiola (2006). *Análisis de los riesgos de seguridad informática para las pequeñas y medianas empresas usando el Estándar ISO 17799 para la definición de políticas de*

seguridad que protejan sus sistemas de información. Universidad Centro occidental Lisandro Alvarado. Barquisimeto. Venezuela

ANEXO

1. OBJETIVOS DE LA ORGANIZACIÓN

1.1. EJES Y OBJETIVOS ESTRATÉGICOS

1.1.1. Ejes estratégicos

1.1.1.1. EJE I: Oportunidades y acceso a los servicios públicos y sociales que brinda la MDI.

La MDI brinda una serie de servicios (exclusivas y/o compartidas) como: Saneamiento ambiental, salubridad y salud; Tránsito, circulación y transporte público; Educación, cultura, deporte y recreación; programas sociales, defensa y promoción de derechos ciudadanos; seguridad ciudadana; Abastecimiento y comercialización de productos y servicios; Registros Civiles, en mérito a convenio suscrito con el Registro Nacional de Identificación y Estado Civil, conforme a ley; Promoción del desarrollo económico local para la generación de empleo; Establecimiento, conservación y administración de parques zonales, parques zoológicos, jardines botánicos, bosques naturales, directamente o a través de concesiones.(PEI, 2016, P.45)

La situación actual de la oferta de referidos servicios es claramente menor, tanto en cantidad como en calidad, respecto a la demanda por parte de la población.

Es necesario ampliar la oferta de tales servicios a niveles aceptables, considerando indicadores relevantes de mejores prácticas de otros gobiernos locales.

Un buen punto de partida es el PDC 2014-2021 del distrito de Independencia, en donde se presentan indicadores, metas, así como programas y proyectos priorizados. En dicho estudio también se presentan los escenarios tendencial, deseable y probable por cada eje estratégico

1.1.1.2. EJE II: Estado, gobernabilidad e institucionalidad

En el distrito de Independencia se registra una débil gobernabilidad e institucionalidad, expresión de una inadecuada intervención del gobierno local, ello debilita las condiciones para avanzar de manera firme al desarrollo del distrito.

Proponemos como marco de análisis, el desarrollo de instituciones políticas y económicas inclusivas, es decir, que hacen respetar los derechos de propiedad, crean igualdad de oportunidades y fomentan la inversión en habilidades y nuevas tecnologías.

Las instituciones económicas inclusivas respaldan y reciben apoyo de las instituciones políticas inclusivas.

La institucionalidad es clave porque promueve cuatro objetivos centrales para todo país, región, provincia y distrito: *Democracia; Respeto de derechos humanos; Progreso económico; e, Inclusión social (cohesión social)*

Por ejemplo, el *democratizar la sociedad* (una sociedad más horizontal), contribuirá firmemente a lograr pasar de la simple democracia representativa (votas hoy por mí y luego te visito en 4 años, para que vuelves a votar por mí), y participativa formalista (te invito a participar en reuniones, pero tienes poca o ninguna decisión de cambiar las cosas según tus preferencias) a una democracia realmente representativa y participativa con transparencia (rendición de cuentas). Hay pues que fortalecer estos procesos, contribuyendo a desarrollar ciudadanía y gobernanza.

Así, en general, se fomentará de manera sinérgica, una democracia participativa (en donde la sociedad organizada pueda influir de manera efectiva en el proceso del desarrollo), una economía emprendedora y competitiva, articulando la academia con la empresa y el gobierno, y, con

un sector público moderno, que sea un real facilitador del desarrollo local, para ello deberá alcanzar niveles de eficiencia, eficacia y transparencia deseables.

La institucionalidad deberá ser una fuente de ventaja competitiva para el distrito de Independencia.

Un buen punto de partida es el PDC 2014-2021 del distrito de Independencia, en donde se presentan indicadores, metas, así como programas y proyectos priorizados. En dicho estudio también se presentan los escenarios tendencial, deseable y probable por cada eje estratégico. (PEI, 2014, P.47)

1.1.1.3. EJE III: Desarrollo Económico, competitividad y empleo

El ciclo emprendedor (generación de ideas de más y mejores negocios; innovación de producto, proceso, organización y marketing; productividad; y competitividad) está insuficiente desarrollado en el distrito de Independencia, generando pérdida de oportunidades de mercado y empleo.

La sociedad local no está aprovechando adecuadamente el bono demográfico que ocasiona una pérdida de potencial de empleo y riqueza.

No se han establecido las condiciones apropiadas para el desarrollo local.

Todo ello reflejaría el realizar el diseño e implementación de un "plan de desarrollo económico local", que identifique, articule y potencie las fortalezas productivas locales.

Un buen punto de partida es el PDC 2014-2021 del distrito de Independencia, en donde se presentan indicadores, metas, así como programas y proyectos priorizados. En dicho estudio también se presentan los escenarios tendencial, deseable y probable por cada eje estratégico. (PEI, 2014, P.48)

1.1.1.4. EJE IV: Desarrollo Local e Infraestructura.

No se evidencia una educada gestión del uso de suelos, expresado en desactualizado catastro urbano y rural; insuficiente habilitación urbana; inadecuado saneamiento físico legal de asentamientos humanos. Acondicionamiento territorial. Igualmente, deficiente Infraestructura urbana y rural básica, y deficiente vialidad.

Un buen punto de partida es el PDC 2014-2021 del distrito de Independencia, en donde se presentan indicadores, metas, así como programas y proyectos priorizados. En dicho estudio también se presentan los escenarios tendencial, deseable y probable por cada eje estratégico. (PEI, 2014, P.49)

1.1.1.5. EJE V: Recursos naturales y medio ambiente

Inadecuada promoción de la educación e investigación ambiental en la localidad, poco

incentivo para la participación ciudadana en todos sus niveles.

Coordinación insuficiente con gobierno regional, provincial y local sectorial sobre la correcta aplicación local de los instrumentos de planeamiento y de gestión ambiental, en el marco del sistema nacional y regional de gestión ambiental.

Un buen punto de partida es el PDC 2014-2021 del distrito de Independencia, en donde

se presentan indicadores, metas, así como programas y proyectos priorizados. En dicho

estudio también se presentan los escenarios tendencial, deseable y probable por cada eje

estratégico. (PEI, 2014, P.50)

1.1.2. Objetivos estratégicos y específicos

A continuación, se presentan determinados objetivos específicos por cada un

objetivo estratégico (OE):

Tabla 24: Objetivos Estratégicos y Específicos de la MDI

Objetivo Estratégico 1:	Objetivos Específicos:
Lograr la igualdad de oportunidades y acceso a los servicios públicos y sociales que brinda la MDI	1.1. Contribuir a mejorar la calidad en los servicios de salud. 1.2. Mejorar la seguridad ciudadana en cuanto a delitos y violencia. 1.3. Fortalecer la defensa y promoción de derechos y deberes ciudadanos. 1.4. Contribuir a la mejora de los aspectos cualitativos y cuantitativos de la educación en el distrito.
Objetivo Estratégico 2:	**Objetivos Específicos:**
Lograr que la MDI sea moderna, fortalezca la ciudadanía, la gobernanza e institucionalidad.	2.1 La MDI desarrolla los cinco pilares de la modernización de la gestión pública. 2.2 Desarrollar los ejes transversales para la gestión pública moderna.
Objetivo Estratégico 3:	**Objetivos Específicos:**
La municipalidad contribuye al desarrollo económico, competitividad y empleo a través del fomento de la diversificación productiva con valor agregado.	3.1. Facilitar a nivel local los negocios e inversiones privados a escala mediana y pequeña. 3.2. Fomentar las asociaciones público privadas en proyectos de interés local de tamaño mediano y grande. 3.3. Promoción de la formalización de las MYPE locales, que fortalezca la productividad y competitividad.

Objetivo Estratégico 4:	**Objetivos Específicos**
La municipalidad implementa el "plan de desarrollo urbano-distrital" con infraestructura y servicios básicos urbano y rural.	4.1. Mejoramiento de ingresos y de ordenamiento urbano a través de la actualización del catastro urbano (y rural). 4.2. Fomentar la infraestructura de servicios y de investigación y desarrollo. 4.3. Fortalecer la integración vial que reduzcan los costos de transacción.
Objetivo Estratégico 5:	**Objetivos Específicos**
Conservar y aprovechar sosteniblemente los recursos naturales y la biodiversidad.	5.1. Coordinar con los diversos niveles de gobierno provincial, regional y sectorial, la correcta aplicación local de los instrumentos de planeamiento y de gestión ambiental, en el marco del sistema nacional y regional de gestión ambiental. 5.2. Promover la educación e investigación ambiental en el distrito e incentivar la participación ciudadana en todos sus niveles. 5.3. Desarrollar un manejo integrado y eficiente del agua con enfoque de cuenca. 5.4. Considerar la gestión de riesgos y el cambio climático en las iniciativas de desarrollo.

Fuente: PEI – MDI 2014

ENCUESTA:

Por favor conteste con la mayor veracidad a la siguiente encuesta marcando con un aspa (x) una sola opción por cada pregunta.

PREGUNTAS	SI	NO	N/S
1. ¿Existe manual de organización y funciones aplicables a la seguridad de la información?			
2. ¿Usted tiene los conocimientos básicos en aspectos de la seguridad de la información?			
3. ¿El sistema de red brinda seguridad de protección de datos o de información?			
4. ¿Conoce si existe alguna política de protección de hardware a nivel físico y lógico?			
5. ¿Existe una persona responsable de resguardar la información de acuerdo a lo previsto en las normas de la Municipalidad?			
6. ¿Considera usted que maneja de manera adecuada la información?			
7. ¿Alguna vez ha participado de un proceso de seguridad de la información?			
8. ¿Cree usted que la seguridad de la información es de vital importancia?			
9. ¿Ha sido evaluado alguna vez en un proceso de seguridad de la información?			
10. ¿Has recibido capacitaciones en llevar a cabo procesos de seguridad de la información?			
11. ¿Se ha capacitado en su momento para manejar y administrar información de forma segura y confiable?			
12. ¿Dispone de programas antivirus para proteger al sistema y a la información?			
13. ¿El acceso al sistema informático con el que trabaja esta normado?			
14. ¿Realiza copia de seguridad de los datos o información			

PREGUNTAS	SI	NO	N/S
con los cuales trabaja?			
15. ¿Considera usted que existe amenaza o riesgo interno respecto a la seguridad de los datos e información?			
16. ¿Considera usted que existe amenaza o riesgo externo respecto a la seguridad de los datos e información?			
17. ¿Está contemplado la seguridad en las normas de registro de datos de bienes dentro de la Municipalidad?			
18. ¿Existe una política de acceso al sistema de la municipalidad?			
19. ¿Le han dado clave para ingresar al sistema?			
20. ¿La clave que ha recibido le da acceso a documentos y archivos de la municipalidad de acuerdo al nivel establecido?			
21. ¿Alguna vez ha sido testigo de cambio de información por parte del usuario o del cliente?			
22. ¿Está permitido a un empleado usar cualquier computadora?			
23. ¿Ha presentado alguna vez actos de piratería, *hacking* o cualquier otro tipo de delito informático?			
24. ¿Desarrolla la Municipalidad de Independencia un Plan de seguridad de información?			
25. ¿Ha realizado la Municipalidad acciones sobre la seguridad de la información?			