ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018.

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

Maestro en Ingeniería de sistemas con mención en tecnologías de la información.

AUTOR:

Br. Omar Yino, Jara Mendoza

ASESOR:

Mg. Luis Torres Cabanillas

SECCIÓN:

Ingeniería y tecnología

LÍNEA DE INVESTIGACIÓN:

Tecnologías de la información y comunicación

PERU-2018

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

DICTAMEN DE LA SUSTENTACIÓN DE TESIS

EL / LA BACHILLER (ES): **JARA MENDOZA, OMAR YINO**

Para obtener el Grado Académico de ***Maestro en Ingeniera de Sistemas con Mención en Tecnologías de la Información,*** ha sustentado la tesis titulada:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR EL PROCESO DE GESTIÓN DEL RIESGO EN UN GOBIERNO LOCAL, 2018

Fecha: 25 de enero de 2019 Hora: 6:00 p.m.

JURADOS:

PRESIDENTE: Dr. Noel Alcas Zapata **Firma:** .....

SECRETARIO: Dra. Flor de Maria Sanchez Aguirre **Firma:** .....

VOCAL: Mg. Luis Alberto Torres Cabanillas **Firma:** .....

El Jurado evaluador emitió el dictamen de:

..... APROBADO POR UNANIMIDAD .....

Habiendo encontrado las siguientes observaciones en la defensa de la tesis:

.....

.....

.....

.....

Recomendaciones sobre el documento de la tesis:

..... APA .....

.....

.....

.....

Nota: El tesista tiene un plazo máximo de seis meses, contabilizados desde el día siguiente a la sustentación, para presentar la tesis habiendo incorporado las recomendaciones formuladas por el jurado evaluador.

Dedicatoria

El presente trabajo de investigación lo dedico a mi madre la Sra. Honorata Mendoza Martel por acompañarme en todo momento, por brindarme su apoyo y confianza a lo largo de mi carrera y sobre todo por ser mi madre, mi vida, la razón de mi existir y por la oportunidad de tenerla a mi lado.

A mi padre, Isaac Jara Príncipe, que desde el cielo ilumina mi camino y me da fortaleza para seguir adelante con mis objetivos.

A mi hermana Gladys Jara, la quiero mucho y que desde temprana edad me supo guiar en mis estudios, dándome buenos ejemplos de vida y superación.

A mis Sobrinos Adán Isaac y Alba Lucero a quienes los quiero demasiado espero seguir siendo un ejemplo de persona para ellos y darle todo lo que necesiten.

A mis familiares por su confianza y apoyo incondicional.

Agradecimientos

En primer lugar agradecer a Dios, gracias señor por las bendiciones recibidas: En la salud, en mi familia y por los dones que me has dado.

A mis padres, Isaac y Honorata, por darme la vida, por sus bendiciones, gracias a ustedes soy un hombre de bien, con principios y valores.

A mi Hermana Gladys por todo su apoyo y consideración.

A mi tía Teófila por su esfuerzo y dedicación en mi infancia.

A mis compañeros de maestría gracias por su apoyo y ayuda, compartimos mutuamente: experiencias, conocimientos, habilidades, momentos de trabajo, risas y sobre todo el espíritu de compañerismo y cooperación entre nosotros.

Resolución de vicerrectorado académico Nº 00011-2016-UCV-VA

Lima, 31 de marzo de 2016

Declaración de Autoría

Yo **Omar Yino, Jara Mendoza**, estudiante del Programa de Maestría en ingeniería de sistemas con mención en tecnologías de la, de la Escuela de Postgrado de la Universidad César, sede/filial Lima Norte; declaro que el trabajo académico titulado **"Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018"**, es de mi autoría.

Por tanto, declaro lo siguiente:

- He mencionado todas las fuentes empleadas en el presente trabajo de investigación, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes, de acuerdo con lo estipulado por las normas de elaboración de trabajos académicos.
- No he utilizado ninguna otra fuente distinta de aquellas expresamente señaladas en este trabajo.
- Este trabajo de investigación no ha sido previamente presentado completa ni parcialmente para la obtención de otro grado académico o título profesional.
- Soy consciente de que mi trabajo puede ser revisado electrónicamente en búsqueda de plagios.
- De encontrar uso de material intelectual ajeno sin el debido reconocimiento de su fuente o autor, me someto a las sanciones que determinan el procedimiento disciplinario.

Lima, 21 de Diciembre del 2018

.....

Br. Jara Mendoza Omar Yino

DNI: 41168365

Presentación

Señores miembros del jurado:

En cumplimiento del reglamento de grados y títulos de la Universidad César Vallejo se presenta la tesis “Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018”, que tuvo como objetivo aplicar el sistema de gestión de seguridad de la información en la gestión del riesgo de la Municipalidad Distrital de Carabayllo.

El presente informe ha sido estructurado en nueve capítulos, de acuerdo con el formato proporcionado por la Escuela de Posgrado. En el capítulo I se presentan los antecedentes y fundamentos teóricos, la justificación, el problema, las hipótesis, y los objetivos de la investigación. En el capítulo II, se describen los criterios metodológicos empleados en la investigación y en el capítulo III, los resultados tanto descriptivos como inferenciales. El capítulo IV contiene la discusión de los resultados, el V las conclusiones y el VI las recomendaciones respectivas. Finalmente se presentan las referencias y los apéndices que respaldan la investigación.

La conclusión de la investigación fue la aplicación del sistema de gestión de seguridad de la información que mejoró la gestión del riesgo.

El autor

Índice

Índice de tablas

Índice de figuras

Resumen

La investigación titulada “Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018.”, tuvo como objetivo medir la influencia de la aplicación de un sistema de gestión de seguridad de la información en la gestión del riesgo.

Bajo un enfoque cuantitativo, basada en el método hipotético deductivo, se desarrolló una investigación aplicada, de diseño pre-experimental y corte longitudinal. La población estuvo constituida por registro de los activos, se validó el instrumento mediante se utilizó fichas de observación, mediante juicio de expertos.

Los resultados evidenciaron que existe una mejora al aplicar el Sistema de gestión de seguridad de la información sobre el proceso de gestión del riesgo en un gobierno local (Municipalidad Distrital de Carabayllo), evidenciándose a través del procedimiento estadístico de Wilcoxon.

Palabras clave: Seguridad de la información, riesgo, activos

Abstract

The research entitled "Information security management system to improve the risk management process in a local government, 2018.", aimed to measure the influence of the application of an information security management system in the risk management.

Under a quantitative approach, based on the hypothetical deductive method, an applied research was developed, with pre-experimental design and longitudinal cutting. The population was constituted by the registration of the assets, the instrument was validated through the use of observation sheets, through expert judgment.

The results showed that there is an improvement in applying the Information Security Management System on the risk management process in a local government (District Municipality of Carabayllo), evidenced through the Wilcoxon statistical procedure.

Keywords: Information security, risk, assets

I. Introducción

1. Realidad problemática

Casi todas las organizaciones públicas o privadas, al igual que las personas, dependen de alguna manera de la tecnología de la información como una herramienta esencial para lograr sus objetivos de negocio o para poder desarrollar actividades en su vida cotidiana; al mismo tiempo, todos tienen que enfrentarse con una amplia gama de amenazas y vulnerabilidades asociadas a los entornos informáticos de hoy

. El caso de Valencia (2016), en su tesis titulada “Metodología del SGSI Según La Norma ISO/IEC 27001 para el gobierno autónomo descentralizado de San Miguel de Urcuquí”, diseñó e implementó un sistema de gestión y seguridad de la información basado en la normas ISO/IEC 27001 para la red de datos en el GAD Municipal de Urcuquí, utilizaron la norma ISO 27005 para el análisis y gestión de riesgos y determinaron los activos más importantes con altos niveles de riesgos que deben ser reducidos, dando como resultado el cumplimiento obligatorio de las políticas y procesos de seguridad de la información para efectuar esta acción.

La gestión de seguridad de la información es de trascendencia mundial, así como lo definen algunos autores: Areitio (2008), La gestión de la seguridad de la información engloba todas las actividades relacionadas con la dirección y control de la seguridad de los activos de información. Estas actividades consisten en la valoración de las amenazas y del estado actual en el que se encuentra la seguridad de la información en la organización, el diseño y la implementación de controles de seguridad administrativos, como son las reglas de seguridad de la información para los empleados o los controles técnicos, como los sistemas de control de acceso y la operación de los esfuerzos del día a día para preservar la seguridad de la información, mediante la documentación y respuesta a incidentes, la información y concienciación de los empleados, etc.

Asimismo, a nivel local, la experiencia de Ayala (2017)**,** en su tesis investigación implantó la metodología del Sistema de Gestión de Seguridad de la Información (SGSI) para el proceso de gestión del riesgo en el Hospital Nacional de Policía

“Luis N. Sáenz. El autor formula las siguientes conclusiones más relevantes: encontrando resultados como la reduccion del nivel de riesgo se consigue disminuir de 3.72 a 3.09, representando un 16.96%.

La información es muy importante y debe estar debidamente protegida para poder darle un aprovechamiento correcto sin poner en riesgo la confidencialidad, disponibilidad e integridad.

En la Municipalidad Distrital de Carabayllo, no cuenta con políticas de seguridad de información para sus procesos de gestión del riesgo, por lo que existe un riesgo de seguridad, en mantener la confidencialidad, disponibilidad e integridad de la información de los contribuyentes, trabajadores, así como de los procesos de la entidad.

Por ello la importancia de la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI) para mejorar el proceso de gestión de riesgo, de tal manera, esta investigación se plantea mejorar los niveles de seguridad de la información en el gobierno local.

1.1. Trabajos previos

1.1.1. Antecedentes internacionales.

Rivero (2017), en su tesis titulada, “Diseño de un modelo de gestión del riesgo aplicado a una empresa manufacturera de autopartes”, tiene como objetivo el diseño de un modelo de gestión de riesgos que sea aplicable a empresas manufactureras. El autor formula las siguientes conclusiones más relevantes: Los beneficios de aplicar modelos de gestión del riesgo bien estructurados les permitirá a las organizaciones estimar ahorros o beneficios, cuando los impactos de los riesgos no sucedan, o que no afecten los objetivos y resultados esperados. Con la aplicación del modelo de gestión de riesgo en su totalidad será posible analizar los beneficios económicos que la organización puede tener, para ello es importante que se involucren las áreas administrativas de la organización. Lo más interesante del modelo fue cuando se aplicó la segunda etapa que fue el análisis y valoración del riesgo, para ello se debe

seleccionar la herramienta más adecuada para cada uno de los riesgos y para ello se debe tener experiencia en el rama de manufactura de autopartes así como de conocimiento para la selección de las herramientas adecuadas para analizar y valorar los riesgos de los 47 procedimientos. En el trabajo solo se presentan algunos procedimientos con sus herramientas a utilizar en el análisis. Finalmente, se les aplican las técnicas de análisis y evaluación de riesgo a los 2 subprocesos críticos. La investigación realizada por Rivero se ubica dentro del contexto de gestión de riesgos, las técnicas de evaluación de riesgos, tema que es de nuestro interés en la investigación realizada, además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación.

Rodríguez (2016), en su tesis titulada, “Diseño y formulación de un sistema de gestión de riesgos basados en los lineamientos establecidos por la norma NTC- ISO 31000 versión 2011 para la empresa Simma Ltda.”, tiene como objetivo diseñar y formular un sistema de gestión de riesgos en el área de producción y área administrativa de la empresa SIMMA Ltda, para la identificación, análisis y evaluación de riesgos operativos y estratégicos bajo lineamientos de la norma NTC-ISO 31000 versión 2011, para lo cual como objetivos específicos refiere evaluar los riesgos en los procesos que garanticen el cumplimiento de los requisitos establecidos por la NTC-ISO 31000:2011.Establecer las medidas de control y tratamiento para la organización en cada uno de los riesgos analizados. El autor formula las siguientes conclusiones más relevantes: Se realizó un sistema de gestión de riesgos, a partir de la identificación de contextos internos y externos que servirán como herramienta de apoyo para la toma de decisiones en la empresa SIMMA Ltda. Se desarrollan estrategias que permiten establecer un control frente a los riesgos a los que está expuesta la empresa, se aclara que el seguimiento y control de los mismos es una tarea continua en la organización. Mediante mesas de trabajo se desarrollaron capacitaciones a los trabajadores en relación a los riesgos en la empresa. Se inició el proceso de sensibilización respecto a la importancia que ellos tienen en crear cultura frente a la prevención de los riesgos en cada proceso dentro y fuera de la organización.

La investigación realizada por Rodríguez se ubica dentro del contexto de gestión de riesgos, capacitación a los trabajadores en relación a riesgos, tema que es de nuestro interés en la investigación realizada además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación.

Valencia (2016), en su tesis titulada “Metodología del SGSI Según La Norma ISO/IEC 27001 para el gobierno autónomo descentralizado de San Miguel de Urcuquí”, tiene como objetivo diseñar e implementar un sistema de gestión y seguridad de la información basado en la normas ISO/IEC 27001 para la red de datos en el GAD Municipal de Urcuquí, para garantizar el control de acceso a la información que maneja esta entidad. como objetivo específico menciona realizar el levantamiento de información de la situación actual de la red de datos del GAD Municipal de Urcuquí, para determinar su distribución, y los puntos más necesarios a ser protegidos. El autor formula las siguientes conclusiones más relevantes: Mediante la norma ISO 27005 para el análisis y gestión de riesgos se determinaron los activos más importantes con altos niveles de riesgos que deben ser reducidos, dando como resultado el cumplimiento obligatorio de las políticas y procesos de seguridad de la información para efectuar esta acción. En el análisis de riesgos se identifican el valor de los activos más importantes a ser protegidos, debido a que se encuentran propensos a sufrir algún daño, calificándolos en valores de dependencia, función, confidencialidad, integridad y disponibilidad. Por medio de la metodología del análisis y gestión de riesgos ISO 27005 se establecieron los controles para reducir los riesgos existentes, que fueron arrojados en el análisis de estos, asegurando el funcionamiento del SGSI.

La investigación realizada por Valencia se ubica dentro del contexto de gestión de riesgos y sistema de gestión de seguridad de la información, tema que es de nuestro interés en la investigación realizada, además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación.

Díaz (2015), en su tesis titulada, “Apoyo al proceso de implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:2013 en la alcaldía de Pasto”, tiene como objetivo apoyar el proceso de

implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:2013 que se ha venido trabajando en la Alcaldía de Pasto de acuerdo al manual 3.1 de la estrategia gobierno en línea para entidades del orden nacional de la República de Colombia. El autor formula las siguientes conclusiones más relevantes: En la Actualidad la implementación de un Sistema de Gestión de Seguridad de la Información es un proceso complejo y detallado que permite obtener grandes beneficios para una organización debido al constante control de riesgos y amenazas que puedan comprometer la seguridad de la información así mismo conseguir una potencial reducción de costos e inversiones. El correcto planteamiento de una política de seguridad permite mantener una correcta gestión de los procedimientos asociados a la política y también permite determinar responsabilidades con respecto a la protección y uso adecuado de los activos de información. Los constantes cambios de infraestructura, cambios tecnológicos y de talento humano a los que se ve acogida la Alcaldía de Pasto, requieren mantener una capacitación constante en seguridad de la información con el fin de minimizar los riesgos internos y externos a los que se exponen los activos de información.

La investigación realizada por Díaz se ubica dentro del marco del Sistema de gestión de seguridad de la Información, la protección y uso adecuado de los activos de información, tema que es de nuestro interés en la investigación realizada, lo cual es de aprovechamiento óptimo para esta investigación.

Arias, Díaz, & Vargas (2014), en su tesis titulada," Elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia", tiene como objetivo elaborar una guía de gestión de riesgos basados en la norma NTC-ISO 31000, para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda, de empresas de servicios de soporte de tecnología en Colombia. El autor formula las siguientes conclusiones más relevantes:

En todo proceso, área u organización siempre existirán riesgos, independientemente si estos son detectados o no, y es por este motivo que se debe implementar una gestión de riesgos eficiente para mitigarlos pues eliminarlos no es posible pero si ejercer un control adecuado sobre estos. Es necesario realizar campañas de concientización en todo tipo de empresa para que entiendan que la implementación de la gestión de riesgo y más cuando existen guías puntuales generadas es necesaria y que les ayudara a dar continuidad al negocio.De manera exacta se debe seguir el procedimiento desarrollado en la guía planteada, ajustándola en caso de ser necesario a los procesos del área de mesa de ayuda, para poder obtener una correcta gestión de los riesgos y de esta manera mitigar estos llevando a cumplir los objetivos del área.

La investigación realizada por los autores Arias, Díaz, & Vargas se ubica dentro del contexto de gestión de riesgos, la ISO 31000,tema que es de nuestro interés en la investigación realizada, además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación

1.2.1. Antecedentes nacionales.

Ayala (2017), en su tesis titulada, “Sistema de gestión de seguridad de información Para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017”, tiene como objetivo determinar el efecto de la implementación de la metodología del Sistema de Gestión de Seguridad de la Información (SGSI) para el proceso de gestión del riesgo en el Hospital Nacional de Policía “Luis N. Sáenz. El autor formula las siguientes conclusiones más relevantes: Mediante la implementación de la metodología del sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en el Hospital Nacional PNP “Luis N. Sáenz”, el nivel del riesgo se consigue disminuir de 3.72 a 3.09, representando un 16.96%. Por tanto, se determina que el nivel de riesgo de los activos críticos identificados en la presente investigación ha disminuido.

La investigación realizada por Ayala se ubica dentro del contexto de gestión de riesgos, tema que es de nuestro interés en la investigación realizada, además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación.

Bernaldo (2016), en su tesis titulada, “Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016”, tiene como objetivo determinar la relación significativa que existe entre el Sistema de Gestión de Seguridad de la Información y el Proceso de Registros Civiles del Reniec. San Borja. Lima. 2016. El autor formula las siguientes conclusiones más relevantes: En cuanto al objetivo general, la presente investigación demuestra que el Sistema de Gestión de Seguridad de la Información se relaciona de forma altamente significativa con el Proceso de Registros Civiles. Reniec. San Borja. Lima. 2016; siendo que el coeficiente de correlación Rho de Spearman de 0.781, representó una correspondencia positiva alta entre las variables. En cuanto al objetivo 1, la presente investigación demuestra que el Sistema de Gestión de Seguridad de la Información se relaciona de manera altamente significativamente con la dimensión Riesgos que afectan la seguridad de la información del proceso de registros civiles. Reniec. San Borja. Lima. 2016; siendo que el coeficiente de correlación Rho de Spearman de 0.781 representó afinidad positiva alta entre las variables. Se realizó un levantamiento de información de acuerdo a los requisitos que exige la Norma ISO 27001:2013, 10 cláusulas, se identificó los activos de la información asociados a sus riesgos, asimismo se evaluó los controles en el marco del ISO 27002:2005, identificándose la aplicación de 75 controles necesarios para el proceso de registros civiles del Reniec. San Borja, Lima. 2016.

La investigación realizada por Bernaldo se ubica dentro del marco del Sistema de gestión de seguridad de la Información, tema que es de nuestro interés en la investigación realizada, lo cual es de aprovechamiento óptimo para esta investigación.

De la Cruz (2016), en su trabajo de investigación “Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la

municipalidad provincial de Paita; 2016.“, tiene como objetivo realizar la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; en el año 2016, de tal forma que se minimice el riesgo de pérdida de información, para lo cual como objetivo específico refiere efectuar un diagnóstico de la situación actual de la seguridad de la información en la Municipalidad Provincial de Paita, en cumplimiento de los requisitos establecidos en la NTP-ISO/IEC 27001:2014. El autor formula las siguientes conclusiones: la Municipalidad Provincial de Paita carece de políticas y controles eficientes en cuanto a la protección de los activos de la información (los servidores públicos y/o contratistas, la creación de información, los procesos, las tecnologías de información incluido el hardware y el software y las instalaciones), por esta razón si resulta beneficioso el diseño e implementación de la propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la Municipalidad Provincial de Paita; 2016, el mismo que permitirá minimizar la pérdida de información, con lo que queda demostrado que la hipótesis general es aceptada.

La investigación realizada por De La cruz se ubica dentro del contexto minimizar el riesgo de pérdida de información, tema que es de nuestro interés en la investigación realizada, lo cual es de aprovechamiento óptimo para esta investigación.

Tarrillo (2016), en su trabajo de investigación titulado “Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015.”, tiene como objetivo general Conocer la influencia de la gestión de riesgos en la seguridad de activos de información de la Zona Registral III Sede Moyobamba. El autor formula las siguientes conclusiones más relevantes: Existe influencia de la gestión de riesgos en la seguridad de los activos de información de la Zona Registral III Sede Moyobamba, donde existe un Chí Cuadrado de Pearson es 15.712, mayor al Chí Cuadrado tabular con 4 grados de libertad (9.48), lo que indica que existe relación entre las variables de estudio. Asimismo, se encuentra en la zona probabilística de rechazo por lo que se acepta la hipótesis alternativa con un 95% de confianza. El nivel de riesgo de los activos de información de la zona Registral III Sede

Moyobamba es de nivel de riesgo “Alto”, con un 52%, este resultado se obtuvo en base a las dimensiones evaluadas en la variable Gestión de riesgo con los siguientes porcentajes: La dimensión cultura muestra un 54% de nivel de Gestión de riesgo de los activos de información, posicionando en un nivel “Alto”; la dimensión Gestión Gerencial tiene un nivel “Alto” con un 62% de nivel de riesgo; de la misma manera, la dimensión Recursos y Presupuesto tiene un nivel “Alto” con un 52% de nivel de riesgo; asimismo, la dimensión Infraestructura tecnología tiene un nivel “Alto” con un 48% de nivel de riesgo; y la dimensión Recursos Humanos tiene un nivel “Alto” con un 44% de nivel de riesgo. Los Factores de riesgo que afectan a los activos de información de la zona Registral N° III Sede Moyobamba, representa un 54% con un nivel “Alto” de riesgo que afectan a los activos de información.

La investigación realizada por Tarrillo se ubica dentro del marco del Sistema de gestión de riesgos, tema que es de nuestro interés en la investigación realizada, lo cual es de aprovechamiento óptimo para esta investigación.

Rios (2014), en su trabajo de investigación titulado “Diseño de un Sistema de Gestión de Seguridad de Información para una central privada de información de riesgos”, tiene como objetivo Diseño de un Sistema de Gestión de la Seguridad de Información (SGSI) el cual permita que una Central de Riesgo Privada pueda cumplir con las exigencias regulatorias a las que se haya sujeta, siguiendo las normas internacionales ISO/IEC 27001:2013, ISO/IEC 27002:2013 e ISO 31000:2009. El autor formula las siguientes conclusiones más relevantes: Contar con un adecuado SGSI es indispensable para la administración de la seguridad en una organización con alto nivel de complejidad como lo es una Central Privada de información de riesgo, para poder conseguir una mayor eficiencia y garantía en la protección de sus activos de información y en la calidad de la seguridad de la información. Es uno de los estándares más aceptados a nivel nacional e internacional y es base de iniciativas de cumplimiento. El SGSI necesita implicación de la Dirección y apoyo de toda la Organización.

La investigación realizada por Ríos se ubica dentro del contexto del sistema de gestión de seguridad de la información, tema que es de nuestro interés en la investigación realizada, además se precisa que es una de las mejoras herramientas para la gestión del riesgo y del cumplimiento en seguridad de la información.

1.2. Teorías relacionadas al tema

A continuación, se presentan las diferentes concepciones y teorías relacionadas sistema de gestión de seguridad de la información y procesos de gestión de riesgos.

Sistema de gestión de seguridad de la información (SGSI).

Según la Norma Técnica Peruana NTP-ISO/IEC 17799 -2007, define seguridad de la información:

> La información es un activo que, como otros activos importantes del negocio, tiene valor para la organización y requiere en consecuencia una protección adecuada. Como resultado de esta creciente interconectividad, la información está expuesta a un mayor rango de amenazas y vulnerabilidades. La información adopta diversas formas. Puede estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o por medios electrónicos, mostrada en video o hablada en conversación. Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene. La seguridad de la información protege a ésta de un amplio rango de amenazas para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocios. La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y

> mejorados donde sea necesario, para asegurar que se cumplan los objetivos específicos de seguridad y negocios de la organización. (p.2)

Miranda (2013), define Un sistema de gestión de la seguridad

> Es un enfoque gerencial para la seguridad. Se trata de un sistemático, explícito y amplio proceso de gestión de riesgos sobre la seguridad. Como con todos los sistemas de gestión, en un sistema de gestión de la seguridad se prevé la fijación de objetivos, planificación y medición del desempeño. Un sistema de gestión de la seguridad es parte de una organización. Se convierte en parte de la cultura, y de la forma en que realizamos un trabajo. Es necesario implantar Sistema de Gestión de la Seguridad, para apoyar a una organización, una forma eficaz la seguridad de la información, evitando las inversiones innecesarias, ineficientes o mal dirigidas que se producen por contrarrestar amenazas sin una evaluación previa. Por desestimar riesgos. Por la falta de contramedidas. Por el retraso en las medidas de seguridad en relación a la dinámica de cambio interno de la propia organización y del entorno. Por la falta de claridad en la asignación de funciones y responsabilidades sobre los activos de información. Por la ausencia de procedimientos que garanticen la respuesta puntual y adecuada ante incidencias o la propia continuidad del negocio, entre otros. (p..4)

Galindo (2014) de “La Segunda Cohorte del Doctorado en Seguridad Estratégica” define, como: “El conjunto de medidas preventivas y reactivas de las organizaciones y de los sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de la misma” (p. 100).

Existen diferencias da preventivas de las reactivas, las preventivas miden los riesgos identificados y las reactivas cuando se ha materializado el riesgo.

Rodríguez (2012) la define, como: “Conservación de confidencialidad, integridad y disponibilidad de la información” (p. 21).

En la seguridad de la información se busca proteger la información respecto a todas vulnerabilidades.

Cano (2011), define Seguridad de la información como:

> La disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información (p. 1).

Según la Norma Técnica Peruana NTP-ISO/IEC 27001:2014.

> Esta Norma Técnica Peruana ha sido preparado para proporcionar los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información. La adopción de un sistema de gestión de seguridad de la información es una decisión estratégica para una organización. El establecimiento e implementación de un sistema de gestión de seguridad de la información de la organización está influenciado por las necesidades y objetivos de la organización, los requisitos de seguridad, los procesos organizativos utilizados y el tamaño y estructura de la organización. Se espera que todos estos factores influyentes cambien con el tiempo. El sistema de gestión de la seguridad de información preserva la confidencialidad, integridad y disponibilidad de la información aplicando un proceso de gestión de riesgos y proporciona confianza a las partes interesadas en el sentido en que los riesgos se manejan adecuadamente.(p.8)

> Según la Norma Técnica Peruana NTP-ISO/IEC 17799 -2007, Los requisitos de seguridad
>
> Es esencial que la organización identifique sus requisitos de seguridad. Existen tres fuentes principales.

> 1. La primera fuente procede de la valoración de los riesgos de la organización, tomando en cuenta los objetivos y estrategias generales del negocio. Con ella se identifican las amenazas a los activos, se evalúa la vulnerabilidad y la probabilidad de su ocurrencia y se estima su posible impacto.
>
> 2. La segunda fuente es el conjunto de requisitos legales, estatutos, regulaciones y contratos que debería satisfacer la organización, sus socios comerciales, los contratistas y los proveedores de servicios.
>
> 3. La tercera fuente está formada por los principios, objetivos y requisitos que forman parte del tratamiento de la información que la organización ha desarrollado para apoyar sus operaciones. (p.2)

Según la Norma Técnica Peruana NTP-ISO/IEC 17799 -2007, Evaluación de los riesgos de seguridad.“Los requisitos de seguridad se identifican mediante una evaluación metódica de los riesgos. Las evaluaciones de riesgos deben repetirse periódicamente para tener en cuenta cualquier cambio que pueda influir en los resultados de la evaluación”. (p.3)

Según la Norma Técnica Peruana NTP-ISO/IEC 17799 -2007, Selección de controles

> Una vez que los requisitos de seguridad han sido identificados y las decisiones para el tratamiento de riesgos han sido realizadas, deberían elegirse e implantarse los controles que aseguren la reducción de los riesgos a un nivel aceptable. Pueden elegirse los controles partiendo de este documento, de otros conjuntos de controles o de nuevos controles que pueden diseñarse para cubrir adecuadamente las necesidades específicas. (p.3).Según la Norma Técnica Peruana NTP-ISO/IEC 17799 -2007, Punto de partida de la seguridad de la información.
>
> Cierto número de controles se consideran principios orientativos que proporcionan un punto de partida adecuado para implantar la seguridad

de la información. Se apoyan en requisitos legislativos esenciales o se considera la mejor práctica habitual para conseguir dicha seguridad.

Los controles que se consideran esenciales para una organización desde un punto de vista legislativo comprenden:

a) la protección de los datos de carácter personal y la intimidad de las personas (véase el inciso 15.1.4);

b) la salvaguarda de los registros de la organización (véase el inciso 15.1.3);

c) los derechos de la propiedad intelectual (véase el inciso 15.1.2).

Los controles que se consideran la mejor práctica habitual para conseguir la seguridad de la información comprenden:

a) la documentación de la política de seguridad de la información (véase el inciso 5.1.1);

b) la asignación de responsabilidades de seguridad (véase el inciso 6.1.3);

c) la formación y capacitación para la seguridad de la información (véase el inciso 8.2.2);

d) el procedimiento correcto en las aplicaciones (véase el inciso 12.2); e) la gestión de la vulnerabilidad técnica (véase el inciso 12.6);

f) la gestión de la continuidad del negocio (véase el inciso 14);

g) el registro de las incidencias de seguridad y las mejoras (véase el inciso 13.2).

Estos controles pueden aplicarse a la mayoría de las organizaciones y los entornos. Es conveniente señalar que pese a la importancia dada a los controles en este documento, la importancia de cualquier control debería determinarse a la luz de los riesgos específicos que afronta la organización. Por tanto y aunque el enfoque anterior se considere un

> buen punto de partida, no sustituye a la selección de controles basada en una evaluación del riesgo.

Según la Norma Técnica Peruana NTP-ISO/IEC 17799 -2007, Factores críticos de éxito.

> La experiencia muestra que los siguientes factores suelen ser críticos para el éxito de la implantación de la seguridad de la información en una organización: a) una política, objetivos y actividades que reflejen los objetivos del negocio de la organización; b) un enfoque para implantar, mantener, monitorear e improvisar la seguridad que sea consistente con la cultura de la organización; c) el apoyo visible y el compromiso de la alta gerencia; d) una buena comprensión de los requisitos de la seguridad, de la evaluación del riesgo y de la gestión del riesgo; e) la convicción eficaz de la necesidad de la seguridad a todos los directivos y empleados; f) la distribución de guías sobre la política de seguridad de la información de la organización y de normas a todos los empleados y contratistas; g) aprovisionamiento para financiar actividades de gestión de seguridad de la información; h) la formación y capacitación adecuadas; i) establecer un efectivo proceso de gestión de incidentes de la seguridad de información; j) un sistema integrado y equilibrado de medida que permita evaluar el rendimiento de la gestión de la seguridad de la información y sugerir mejoras. (p.23)

Riesgo

Areitio (2008), define

> El riesgo como la posibilidad de que se produzca un impacto determinado en un activo, en un dominio (o conjunto de activos) o en toda la organización. Este impacto se puede producir debido a que una amenaza

> explote vulnerabilidades para causar pérdidas o daños. Un entorno de riesgo es aquél en el que una amenaza concreta o un grupo de amenazas, pueden explotar una vulnerabilidad o grupo de vulnerabilidades determinado, exponiendo los activos a daños o pérdidas. El riesgo se caracteriza por una combinación de dos factores: la probabilidad de que ocurra el incidente no deseado y su impacto. Cualquier modificación en activos, amenazas, vulnerabilidades y salvaguardas puede tener efectos significativos en el riesgo. La rápida detección o el conocimiento de cambios en el entorno o en el sistema facilitan la toma de decisiones adecuadas. (p.200).

En el lenguaje común, el concepto de riesgo está asociado con diferentes consideraciones (el suceso es evaluado como negativo, la amenaza, su probabilidad de ocurrencia y/o impacto).

Sin embargo, los acontecimientos pueden tener unos impactos positivos, negativos o ambos. Uno puede simplemente tener una visión “neutral” como un científico y encontrar que se produce un evento sin practicar ninguna evaluación de valor. Por ejemplo, supongamos que un meteorólogo anuncia que hay un 80% de probabilidades de lluvia en las próximas semanas. Por lo tanto, el riesgo de lluvia es neutral en sí mismo. Es un hecho dado. Para la persona que quiere ir de vacaciones, es un acontecimiento perjudicial. Para un agricultor que está esperando irrigar sus campos, esta será una oportunidad.

Valoración de riesgos.

Areitio (2008), define:

> Esta fase prioriza las amenazas contra los objetivos, es decir, presenta los escenarios de ataque sobre objetivos específicos, de acuerdo al riesgo percibido. La caracterización del riesgo incorpora medidas frente a amenazas, vulnerabilidades y sus consecuencias, en un proceso de valoración repetible y sistemático. El resultado clave de esta fase es la identificación de la importancia relativa de las amenazas contra objetivos,

> de modo que se prioricen las cuestiones más importantes, que se planifique la gestión de riesgos más detallada y que los recursos necesarios implementen los controles de riesgo más apropiados. (p.203).

La valoración de los riesgos permite la identificación y el análisis de los riesgos que enfrenta la organización para la consecución de los objetivos, tanto de fuentes internas como externas.

Definición de ISO

> La ISO (Organización Internacional de Normalización) es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO). El trabajo de preparación de Normas Internacionales se lleva a cabo normalmente a través de comités técnicos de ISO. Cada organismo miembro interesado en una materia para la cual se ha establecido un comité técnico, tiene el derecho a estar representado en dicho comité, según la Norma Internacional ISO 31000.2009 (p.1).

La gestión de riesgos - Principios y directrices

Según la ISO 31000 (2009) explica lo siguiente:

> Todas las actividades de una organización implican un riesgo. Organizaciones a gestionar el riesgo mediante la identificación, análisis y evaluación si el riesgo debe ser modificado por el tratamiento del riesgo con el fin de satisfacer sus criterios de riesgo. Si bien todas las organizaciones a gestionar el riesgo en cierta medida, esta norma establece una serie de principios que deben ser satisfechas para que la gestión eficaz del riesgo.
>
> Esta Norma Internacional recomienda desarrollar, implementar y mejorar continuamente cuyo objetivo fuera integrar el proceso de gestión del riesgo en la administración general. La gestión del riesgo se puede aplicar a toda una organización, en sus muchas áreas y niveles, en cualquier momento, así como a las funciones, proyectos y actividades específicas.

Esta Norma Internacional proporciona los principios y directrices para la gestión de cualquier tipo de riesgo de una manera sistemática, transparente y creíble y dentro de cualquier ámbito y contexto.

La gestión de riesgos permite a la organización: aumentar la probabilidad de alcanzar los objetivos; fomentar una gestión proactiva; ser conscientes de la necesidad de identificar y tratar el riesgo en toda la organización; mejorar la identificación de oportunidades y amenazas; cumplir con los requisitos legales y reglamentarios pertinentes y las normas internacionales; mejorar la información obligatoria y voluntaria; mejorar la gestión pública; mejorar la confianza de los interesados y la confianza; establecer una base fiable para la toma de decisiones y la planificación; mejorar los controles; efectivamente asignar y utilizar recursos para el tratamiento del riesgo; mejorar la eficacia operativa y la eficiencia; mejorar la salud y la seguridad, así como la protección del medio ambiente; mejorar la prevención de pérdidas y gestión de incidencias; minimizar las pérdidas; mejorar el aprendizaje organizacional; y mejorar la resiliencia organizacional.

La Norma Internacional busca satisfacer las necesidades de partes interesadas, incluyendo: los responsables del desarrollo de políticas de gestión de riesgos dentro de su organización; los responsables de asegurar que el riesgo se gestiona con eficacia dentro de la organización como un todo o dentro de un área, proyecto o actividad específica; aquellos que necesitan para evaluar la efectividad de una organización en la gestión de riesgos; y los desarrolladores de normas, orientaciones, procedimientos y códigos de prácticas que, en su totalidad o en parte, se establece hasta qué riesgo es que se gestionan en el contexto específico de estos documentos.

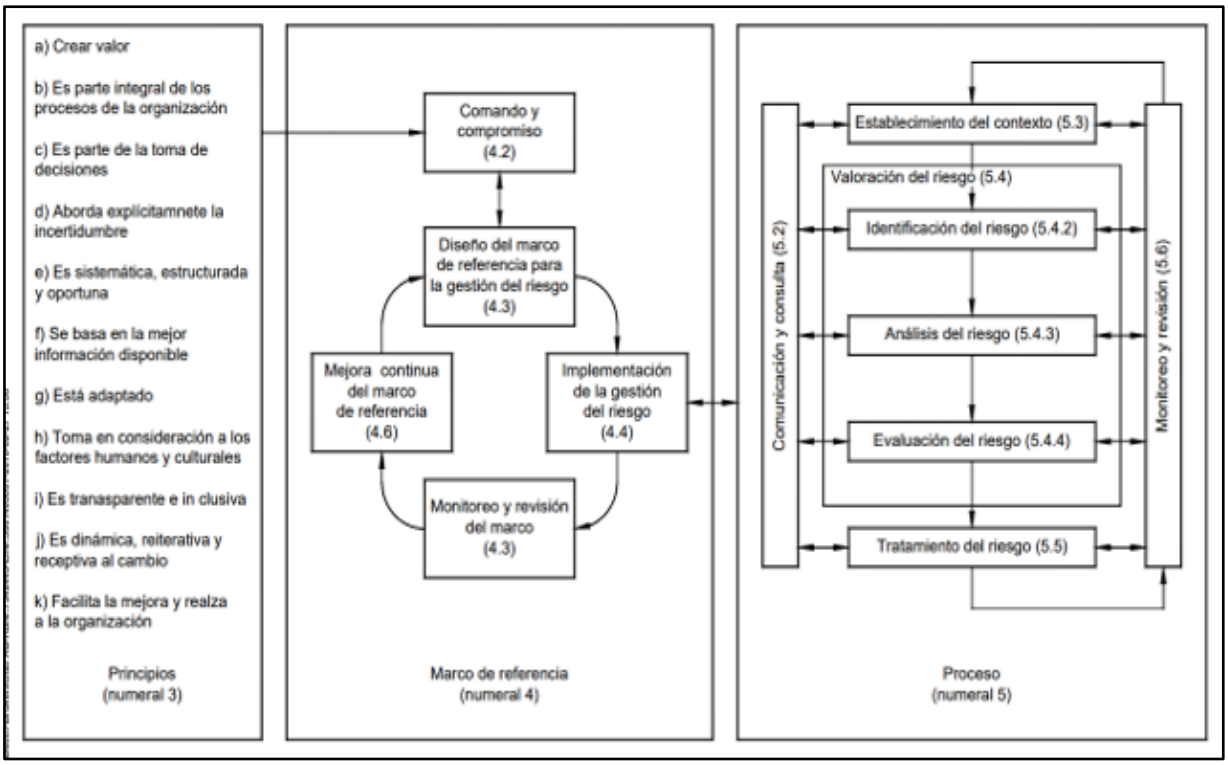


Figura 1 Relaciones entre los principios, el marco de referencia y los procesos para la gestión del riesgo

Fuente NORMA ISO 31000: 2009 - La gestión de riesgos - Principios y directrices (p.14).

Alcance de la Norma

Según la ISO 31000 (.2009), explica lo siguiente:

> Esta Norma Internacional proporciona principios y directrices genéricas sobre la gestión de riesgos, puede ser utilizado por cualquier empresa pública, privada o comunitaria, asociación, grupo o individuo. Esta norma no es específica para cualquier industria o sector, sino organización en general. Esta Norma Internacional puede ser aplicada en toda la vida de una organización, y para una amplia gama de actividades, incluidas las estrategias y decisiones, operaciones, procesos, funciones, proyectos, productos, servicios y activos. Esta norma internacional se puede aplicar a cualquier tipo de riesgo, cualquiera que sea su naturaleza, ya sea que tenga consecuencias positivas o negativas. (p.2)

Principios de la Norma

Según la ISO 31000 (2009) explica lo siguiente:

> Para la gestión del riesgo sea eficaz, una organización debe cumplir en todos los niveles con los principios siguientes.
>
> **La gestión del riesgo crea y protege el valor**.
>
> La gestión del riesgo contribuye al logro demostrable de objetivos y mejora del rendimiento, por ejemplo, la salud humana y la seguridad, la seguridad, el cumplimiento legal y normativo, la aceptación pública, la protección del medio ambiente, la calidad del producto, gestión de proyectos, la eficiencia en las operaciones, la gobernabilidad y la reputación.
>
> **La gestión de riesgos es una parte integral de todos los procesos de la organización**.
>
> La gestión del riesgo no es una actividad independiente que está separada de las principales actividades y procesos de la organización. La gestión de riesgos es parte de las responsabilidades de la dirección y una parte integral de todos los procesos de la organización, incluyendo la planificación estratégica y todos los procesos de gestión de cambios del proyecto.
>
> **La gestión del riesgo es parte de la toma de decisiones**.
>
> La gestión de riesgos ayuda a quienes toman las decisiones a tomar decisiones informadas, priorizar acciones y distinguen entre cursos alternativos de acción.
>
> **La gestión del riesgo aborda explícitamente la incertidumbre**.
>
> La gestión de riesgos tiene en cuenta explícitamente la incertidumbre, la naturaleza de esa incertidumbre, y cómo se puede tratar.
>
> **La gestión del riesgo es sistemática, estructurada y oportuna**.

Un enfoque sistemático, oportuno y estructurado para la gestión del riesgo contribuye a la eficiencia y resultados consistentes, comparables y fiables.

La gestión del riesgo se basa en la mejor información disponible.

Las entradas para el proceso de gestión de riesgos se basan en fuentes de información, tales como datos históricos, la experiencia, la retroalimentación de las partes interesadas, la observación, las previsiones y la opinión de expertos. Sin embargo, los tomadores de decisiones deben informarse, y deben tener en cuenta, cualquier limitación de los datos o de modelado utilizado o la posibilidad de divergencia entre los expertos. (p.7)

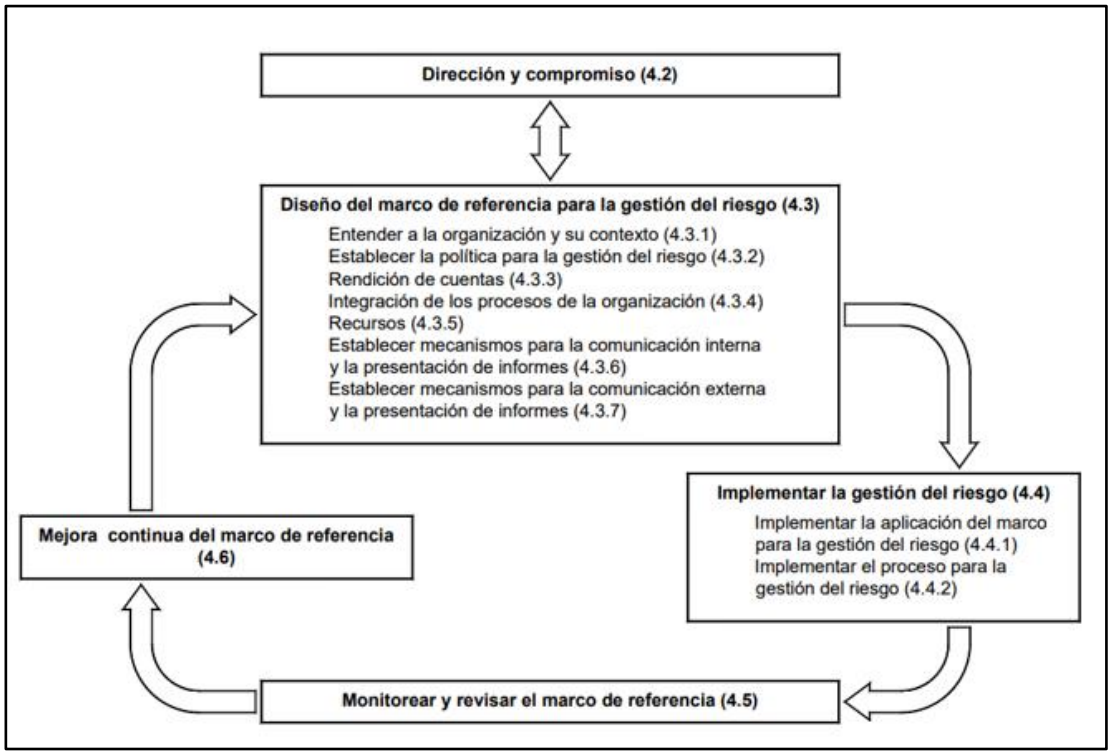


Figura 2 Relación entre los componentes del marco de referencia para la gestión del riesgo
Fuente NORMA ISO 31000: 2009 - La gestión de riesgos - Principios y directrices (p.8).

La implementación de la gestión de riesgos

Según la ISO 31000 (2009) explica lo siguiente:

Al poner en práctica el marco de la organización para la gestión de riesgos, la organización debe:

> Definir la sincronización y la estrategia apropiada para la aplicación del marco; Aplicar la política de gestión de riesgos y el proceso de los procesos de la organización; cumplir con los requisitos legales y reglamentarios; Asegurar que la toma de decisiones, incluyendo el desarrollo y establecimiento de objetivos, está alineado con los resultados de los procesos de gestión de riesgos; Realizar sesiones de información y formación; y Comunicarse y consultar con las partes interesadas para asegurar que su marco de gestión del riesgo sigue siendo apropiado. (p.13).

Para la implementación de la gestión de riesgo es fundamental considerar a la ISO 31000, que convierte la planificación en una futura buena gestión de riesgos. Esta norma y el Risk Management debería considerarse una parte estratégica de la organización, no aislada del resto. La finalidad es generar valor a través del cumplimiento de los objetivos estratégicos estipulados con antelación.

- Identificación en gestión de riesgos
- Análisis en Risk Management
- Evaluación en gestión de riesgos
- Tratamiento en Risk Management
- Comunicación y consulta en gestión de riesgos
- Revisión y monitoreo

Análisis de riesgo

Según la ISO 31000 (.2009) explica lo siguiente:

> El análisis de riesgos proporciona una entrada a la evaluación de riesgos y a las decisiones sobre si los riesgos necesitan ser tratados, y sobre las estrategias y los métodos de tratamiento de riesgo más apropiado. El análisis de riesgos también puede proporcionar elementos para la toma de decisiones, donde habrá que elegir y las opciones implican diferentes tipos y niveles de riesgo.
>
> El análisis de riesgos implica la consideración de las causas y las fuentes de riesgo, sus consecuencias positivas y negativas, y la probabilidad de que pueden ocurrir esas consecuencias. Los factores que afectan consecuencias y probabilidad deben ser identificados. Los controles existentes y su efectividad y la eficiencia también deben tenerse en cuenta.
>
> La confianza en la determinación del nivel de riesgo y su sensibilidad a las condiciones previas e hipótesis debe ser considerada en el análisis, y se comunica con eficacia a los tomadores de decisiones y, en su caso, otras partes interesadas. Factores tales como la divergencia de opiniones entre los expertos, la incertidumbre, la disponibilidad, la calidad, cantidad y relevancia de la información, o limitaciones en el modelado deben expresarse y pueden ser destacadas.
>
> El análisis de riesgos puede llevarse a cabo con diferentes grados de detalle, en función del riesgo, el propósito del análisis y la información, los datos y los recursos disponibles. El análisis puede ser cualitativa, semicuantitativa o cuantitativa, o una combinación de éstos, dependiendo de las circunstancias.

> Las consecuencias y sus probabilidades se pueden determinar mediante el modelado de los resultados de un evento o conjunto de eventos, o por extrapolación a partir de estudios experimentales o de los datos disponibles. Las consecuencias pueden ser expresadas en términos de impactos tangibles e intangibles. En algunos casos, se requiere más de un valor numérico o descriptor para especificar las consecuencias y la probabilidad de diferentes épocas, lugares, grupos o situaciones. (p.16).

El análisis de riesgo consiste en establecer actividades de monitoreo, de vigilancia, a través de un grupo multidisciplinario para evitar situaciones perjudiciales en una organización.

Para las decisiones se debería tener en cuenta el contexto más amplio del riesgo e incluir la consideración de la tolerancia del riesgo por otras partes diferentes de la organización, que se benefician del riesgo. Las decisiones se deberían tomar de acuerdo con requisitos legales, reglamentarios y requisitos de otro tipo.

En algunas circunstancias, la evaluación del riesgo puede llevar a la decisión de realizar un análisis en mayor profundidad. El análisis del riesgo también puede llevar a la decisión de no tratar el riesgo de ninguna otra manera que manteniendo los controles existentes. Esta decisión estaría influenciada por la actitud ante el riesgo por parte de la organización y por los criterios de riesgo que se hayan establecido.

EVALUACIÓN DE RIESGO

Según la ISO 31000 (.2009) explica lo siguiente:

> El propósito de la evaluación de riesgos es ayudar en la toma de decisiones, con base en los resultados de análisis de riesgos, sobre los cuales los riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento.

> La evaluación del riesgo implica comparar el nivel de riesgo encontrado durante el proceso de análisis con criterios de riesgo establecidos cuando se consideró el contexto. Sobre la base de esta comparación, la necesidad de tratamiento puede ser considerado.
>
> Las decisiones deben tener en cuenta el contexto más amplio del riesgo y de incluir la consideración de la tolerancia de los riesgos asumidos por las partes distintas de la organización que se beneficia del riesgo. Las decisiones deben tomarse de conformidad con los requisitos legales, reglamentarios y otros.
>
> En algunas circunstancias, la evaluación del riesgo puede conducir a una decisión de realizar un análisis más detallado. La evaluación de riesgos también puede conducir a una decisión de no tratar el riesgo de cualquier manera distinta del mantenimiento de los controles existentes. Esta decisión se verá influido por la actitud de riesgos de la organización y los criterios de riesgo que se han establecido. (p.18).

Metodología de gestión de riesgos de Ti

Según el Instituto Nacional de Normas y Tecnología (NIST) SP 800-30, se interpreta lo siguiente:

La metodología utilizada por el Gobierno local extrae los conceptos de metodologías de administración de riesgos de TI reconocidas mundialmente, como la ASNZ 4360, NIST 800-30, ISO 31000 e ISO 27005 donde la gestión de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones.

El término “Gestión de Riesgos” se refiere a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar,

> monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. Gestionar riesgos significa tanto identificar oportunidades como evitar o mitigar pérdidas.(p.8).

Glosario

Tomado de la tesis Análisis y diseño de controles de seguridad personal en redes sociales:

Aceptación de riesgo: una decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Amenaza: evento inesperado con el potencial para causar daños. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente.

Análisis de riesgo: un uso sistemático de la información disponible para determinar cuan frecuentemente puede ocurrir eventos especificados y la magnitud de sus consecuencias.

Consecuencia: el producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia. Podría haber un rango de productos posibles asociados a un evento.

Control de riesgos: la parte de administración de riesgos que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.

Análisis de riesgos: el proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgo objetivos u otro criterio.

Frecuencia: una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado.

Gestión de riesgos: la cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.

Identificación de riesgos: el proceso de determinar qué puede suceder, por qué y cómo.

Probabilidad: la probabilidad de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación a la cantidad total de posibles eventos o resultados.

Proceso de gestión de riesgos: la aplicación sistemática de políticas, procedimientos y prácticas de administración a las tareas de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos.

Riesgo residual: el nivel restante de riesgo luego de tomar medidas de tratamiento del riesgo.

Riesgo: la posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se le mide en términos de consecuencias y probabilidades.

Tratamiento de riesgos: selección e implementación de opciones apropiadas para tratar el riesgo.

Vulnerabilidad: es una debilidad (vacío) que se puede activar accidentalmente o explotar intencionalmente.

Etapas de la metodología de gestión de riesgos

1. Análisis de Riesgos
2. Gestión de Riesgos

Etapa 1: Análisis de riesgos

El análisis de riesgos es el primer proceso de la metodología de gestión de riesgos. El Gobierno local usa el análisis de riesgos para determinar la extensión de amenazas potenciales y riesgos asociados con sistemas de TI. La salida de este proceso ayuda a identificar apropiados controles para reducir o eliminar riesgos durante el proceso de mitigación.

Para determinar la probabilidad de un evento adverso futuro, las amenazas de los sistemas de TI deben ser analizadas en conjunto con las vulnerabilidades potenciales y los controles existentes en los mismos. El impacto se refiere a la magnitud del daño que podría ser causado porque las amenazas exploten una vulnerabilidad. El nivel de impacto es determinado por el impacto potencial en el logro de la misión y el valor relativo de los activos de TI que resulten afectados (por ejemplo, la criticidad y sensibilidad de componentes de sistemas de TI y datos). La metodología de análisis de riesgos está compuesta por once (11) pasos primarios:

Paso 1 - Caracterización de sistemas
Paso 2 - Identificación de amenazas
Paso 3 - Identificación de vulnerabilidades
Paso 4 – Determinación del evento del riesgo
Paso 5 - Determinación de probabilidades
Paso 6 - Análisis de impacto
Paso 7 – Cálculo del riesgo inherente
Paso 8 – Evaluación de controles existentes
Paso 9 – Calculo del riesgo residual
Paso 10 - Recomendaciones o mejoras de control
Paso 11 - Documentación de resultados
A continuación, se describen cada uno de estos pasos:

Paso 1: Caracterización de Sistemas

> En el análisis de riesgos para un sistema de TI, el primer paso es definir el alcance del esfuerzo. En este paso, se identifican los límites del sistema de TI, la información y los recursos que componen dicho sistema. La caracterización de un sistema de TI establece el alcance del esfuerzo de análisis de riesgos, establece los límites de la autorización operacional (acreditación) y provee información relacionada con el hardware, software, conectividad, personal de soporte y áreas responsables, esenciales para la definición de los riesgos.

Paso 2: Identificación de Amenazas

Una amenaza es la posibilidad que una situación o evento inesperado explote exitosamente una vulnerabilidad en particular. Una vulnerabilidad es una debilidad (vacío) que se puede activar accidentalmente o explotar intencionalmente. Una fuente de amenaza no representa un riesgo cuando no existe una vulnerabilidad que pueda ser explotada.

Una fuente de amenaza se define como cualquier circunstancia o evento con el potencial para causar daños a un sistema de TI. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente.

Amenazas naturales: Inundaciones, terremotos, tornados, deslizamientos de tierra, avalanchas, tormentas eléctricas y otros eventos similares.

Amenazas humanas: Eventos activados o causados por las personas, tales como actos no intencionados (errores en la entrada de datos) o malintencionados (ataques a la red, activación de software malicioso, acceso no autorizado a información confidencial).

Amenazas ambientales: Faltas prolongadas de energía eléctrica, polución, químicos, dispersión de líquidos.

Paso 3: Identificación de Vulnerabilidades

El análisis de las amenazas de un sistema de TI incluye el análisis de las vulnerabilidades asociadas al ambiente del sistema. La meta de este paso es desarrollar una lista de vulnerabilidades del sistema (defectos o debilidades) que podrían ser explotadas por fuentes de amenazas potenciales.

Paso 4: Determinación del Evento del Riesgo

Se describe el evento en el cual la amenaza se materializa debido a la vulnerabilidad existente. Los siguientes pasos evaluaran el evento del riesgo para obtener su cálculo inherente.

Paso 5: Determinación de Probabilidad

Se hace el análisis para cada amenaza de cuál es la probabilidad de ocurrencia de la misma. La probabilidad de que una vulnerabilidad pueda ser explotada por una fuente de amenaza se puede describir como Alto, Medio y Bajo.

Tabla 1

Probabilidad de ocurrencia

Probabilidad de Ocurrencia	Descripción
Bajo	Una vez al año / Un caso entre 6 y 12 meses
Medio	Entre 1 y 3 veces al año / Un caso entre 1 y 6 meses
Alto	Más de 3 veces al año / Entre 1 y 10 casos en 15 días

Paso 6: Análisis de Impacto

En esta actividad se establece impacto adverso para el negocio resultante de que una amenaza explote exitosamente una vulnerabilidad.

El impacto adverso de un evento de seguridad se puede describir en términos de la degradación de una o varias de las metas de seguridad: Integridad, Disponibilidad, Confidencialidad y No repudiación; se puede describir como Alta, Media y Baja.

Tabla 2

Nivel de Impacto

Nivel de Impacto	Descripción
Bajo	– Genera molestias en las usuarios internos – Inoperativo menos de 5 minutos – Sin lesiones o con lesiones leves – Pérdidas económicas menores al 5% del patrimonio. – Genera quejas de los usuarios (insatisfacción del cliente externo).
Medio	– Inoperativo entre 5 minutos y 1 hora – Genera traumas físicos o psicológicos – Pérdidas económicas entre el 5% y 20 % del patrimonio.
Alto	– Genera impacto negativo en la mayoría de los usuarios (externo). – Inoperativo más a 1 hora – Genera pérdidas de vidas humanas e invalidez – Pérdidas económicas superiores al 20 % del patrimonio.

Paso 7: Calculo del Riesgos Inherente

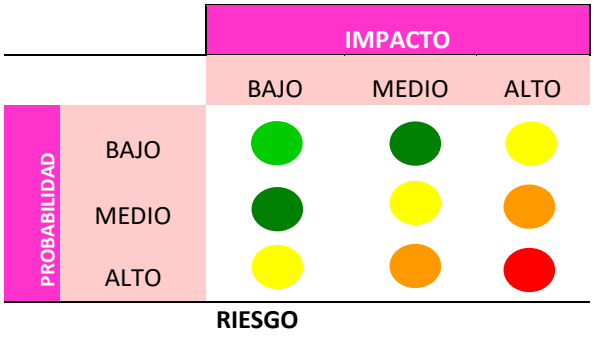
El propósito de este paso es valorar el nivel de riesgo de un sistema de TI. Ver Anexo 2. La determinación del riesgo inherente para una amenaza/vulnerabilidad en particular se expresa en función de:

- La probabilidad que una fuente de amenaza intente explotar una vulnerabilidad.
- La magnitud del impacto resultante de la explotación exitosa de una vulnerabilidad.

- Lo apropiado de los controles existentes o planeados para reducir o eliminar los riesgos.
- Se utiliza la siguiente tabla de valoración del riesgo:

Tabla 3

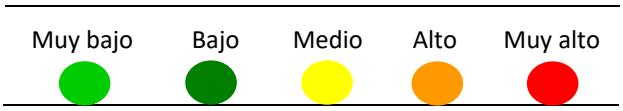
Matriz de valoración de riesgo



Siendo el nivel del riesgo:

Tabla 4

Nivel de riesgo



Etapa 2: Gestión de riesgos

La gestión de riesgos comprende la priorización, evaluación e implementación de controles que reduzcan los riesgos de acuerdo con las recomendaciones emanadas del proceso de análisis de riesgos.

Considerando que eliminar todos los riesgos es algo imposible de llevar a cabo, es responsabilidad de la Alta Dirección, de los administradores funcionales y del negocio utilizar el enfoque del menor costo e implementar los controles más apropiados para reducir la exposición a riesgos a un nivel aceptable, con un mínimo impacto adverso sobre los recursos y la misión de la entidad.

Opciones de gestión de riesgos

La mitigación de riesgos es una metodología sistemática utilizada por la Alta Dirección para reducir los riesgos que afecten la misión del negocio. La reducción de riesgos se puede alcanzar siguiente alguna o varias de las siguientes opciones:

- **Asumir el riesgo:** Consiste en aceptar el riesgo y continuar operando o implementar controles para bajar el nivel de exposición.
- **Evitar el riesgo:** No proceder con la actividad que tiene probabilidad de generar riesgo
- **Mitigar el riesgo:** Consiste en implementar controles que reduzcan los impactos negativos de la explotación exitosa de las vulnerabilidades (implementar controles preventivos y detectivos).
- **Transferir riesgos:** Es acudir a medidas contingentes para compensar las pérdidas, el ejemplo clásico es la compra de pólizas de seguros.

Las metas y objetivos de la entidad se deben tener en cuenta en la selección de opciones de mitigación de riesgos. La mitigación de riesgos requiere que la entidad implemente tecnologías de diferentes proveedores de seguridad junto con controles no técnicos y medidas administrativas.

Tabla 5

Evaluación del Riesgo

Evaluación del riesgo – Nivel de riesgo	Opciones de Gestión del Riesgo en función del Nivel de riesgo Admisible
– Muy bajo	– Asumir el riesgo
– Bajo	– Asumir el riesgo
– Medio	– Mitigar el riesgo
– Alto	– Evitar el riesgo – Transferir el riesgo
– Muy Alto	– Mitigar el riesgo – Evitar el riesgo – Transferir el riesgo

Apetito de riesgo

El Gobierno local ha considerado que el máximo nivel de riesgo aceptable es MEDIO, en el caso que el cálculo del riesgo sea ALTO o MUY ALTO se tomaran acciones pertinentes, es decir, implementación o mejoras de control para reducir el riesgo a un nivel aceptable.

Tabla 6

Evaluación del apetito del riesgo

Evaluación del Apetito del Riesgo	Descripción
– Alto 	– La Municipalidad **acepta oportunidades** que tienen inherentemente un riesgo alto que puede resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.
– Moderado 	– La Municipalidad está dispuesta a **aceptar riesgos** que puedan resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.
– Tolerable	– La Municipalidad está dispuesta a **aceptar algunos riesgos en ciertas circunstancias** que puedan resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.
– Bajo 	– La Municipalidad **NO está dispuesta a aceptar riesgos** en la mayoría de las circunstancias que puedan resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.
– Cero 	– La Municipalidad **NO está dispuesta a aceptar riesgos bajo ninguna circunstancia** que puedan resultar en daños a su reputación, pérdida financiera, averías graves en los sistemas de información, accidentes significativos, incumplimientos regulatorios, riesgo potencial de lesiones al personal.

Identificación de nuevos riesgos

El Gobierno local puede identificar nuevos riesgos mediante las siguientes fuentes:

- Controles de seguridad de la información deficientes identificadas en los informes de monitoreo.
- Observaciones de auditoria sobre el SGSI y SGCN.

- Incidentes de seguridad de la información.
- Reuniones periódicas trimestrales.
- Riesgos identificados por el área de riesgos, áreas usuarias o por el coordinador de seguridad de la información.

Para cada nuevo riesgo identificado por las fuentes mencionadas se deberá de realizar un análisis y evaluación del mismo, en caso, el riesgo sea intolerable (ALTO o MUY ALTO) se aplicaran nuevos controles o se mejoraran los actuales para disminuirlo.
El Gobierno local puede asumir un riesgo ALTO o MUY ALTO, en caso, considere que el costo de implementación del control es superior al riesgo evaluado.

Los riesgos de la información están presentes cuando confluyen dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones.

Las vulnerabilidades son una debilidad en la tecnología o en los procesos relacionados con la información, y como tal, se consideran características propias de los sistemas de información o de la infraestructura que la contiene. Una amenaza, en términos simples, es cualquier situación o evento que puede afectar la posibilidad de que las organizaciones o las personas puedan desarrollar sus actividades afectando directamente la información o los sistemas que la procesan.

El gestor de seguridad de la información es un empleado que tiene asignada la función de responsable de la gestión de seguridad de la información en una organización. Un sistema de gestión de la seguridad de la información (SGSI) es parte del sistema de gestión global, basado en el enfoque en los riesgos del negocio y que establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. El sistema de gestión incluye la estructura organizacional, las políticas, las actividades de planificación, las responsabilidades, las prácticas, los

procedimientos, los procesos y los recursos. Por tanto, este concepto hace referencia a los esfuerzos sistemáticos y organizados destinados a preservar la seguridad de la información en las organizaciones.

El interés de actuar en la seguridad de la información es muy importante, necesario y atractiva en los gobiernos locales, ya que la protección de la información que estas instituciones manejan es crítica. La información que tienen dichos gobiernos locales debe tener los cuidados apropiados, para garantizar los principios de seguridad de la información como confidencialidad, integridad y disponibilidad (conocida como la Tríada CIA, del inglés: "Confidentiality, Integrity, Availability") son los principios básicos de la seguridad de la información. Estos principios garantizaran un adecuado servicio de atención al ciudadano, protegiendo su intimidad y privacidad personal. Convergen los activos como recursos de información físicos, recursos de información digitales, recurso de software, activos físicos, servicios y recursos humanos.

Los procesos de gestión del riesgo en un gobierno local, implican los riesgos propiamente dichos de la seguridad de la información, que contemplan desde el uso inadecuado de la información de los contribuyentes y/o trabajadores, ataques externos a la entidad (ciberataques), peligro a la integridad, confidencialidad y disponibilidad de la información, pérdida de información por robo o como consecuencia de un desastre natural. La ausencia de controles adecuados y procedimientos, conlleva a una situación perjudicial de la información, dejando a la Municipalidad en un contexto de pérdida o alteración de la información, afectando la continuidad del servicio. Por tales afirmaciones, en la presente investigación se determinaron la evaluación, tratamiento del riesgo, mediante la implementación del Sistema de Gestión de Seguridad de la información en el proceso de gestión del riesgo del gobierno local, incrementando el grado de seguridad y justificando su implementación.

Cabe mencionar sobre la protección de datos personales según la ley N° 29733,que establece que en atención al principio de seguridad, en el tratamiento de los datos personales deben adoptarse las medidas de seguridad que resulten necesarias a fin de evitar cualquier tratamiento contrario a la Ley o al presente reglamento, incluyéndose en ellos a la adulteración, la pérdida, las desviaciones de

información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado. Toda información relativa a una persona debe tratarse como un dato personal, por lo que el objeto de la mencionada ley es el de garantizar y proteger el derecho fundamental a la privacidad de los datos personales, por tanto, debe dársele un tratamiento adecuado La norma también precisa las obligaciones que debe tener el titular de los bancos de datos personales, entre los que mencionan los siguientes: solicitar al titular un consentimiento expreso previo para realizar el tratamiento de información (salvo las excepciones); recabar los datos personales necesarios y pertinentes que exprese la ley, de acuerdo a la finalidad de la institución, el titular debe tener la posibilidad de ejercer sus derechos según la información que brinda la institución por tanto ésta debe facilitarlo, gestionar la inscripción en el Registro Nacional de Protección de Datos Personales y por último, lo más importante preservar la confidencialidad de los datos personales.

Metodología MAGERIT

La metodología para el proceso de gestión del riesgo es desarrollada para identificar la falta de aplicación de controles y la instauración de un plan de salvaguardas o medidas. La metodología que la presente investigación adopta es MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información),

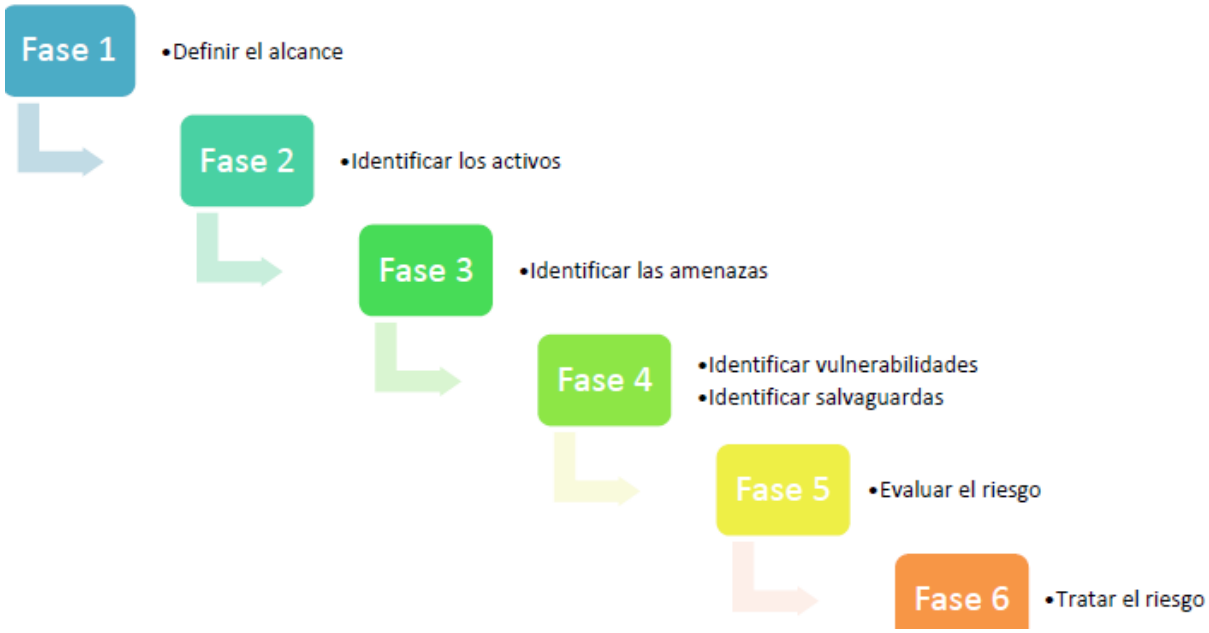


Figura 3 Fases del proceso MAGERIT

Fuente Tomado de Ayala (2017)

Según Ayala (2017), indicó que:

> La fase de la definición del alcance, es parte del establecimiento del contexto de la información relevante de la institución. Se determina hasta qué punto se intervendrá, se especificará que áreas y personal estarán comprometidos.
>
> La fase de la identificación de los activos, determina todos los activos en base a una encuesta al personal comprometido o en base a la recolección de información, tales pueden ser: Procesos del negocio, actividades e información, que incluyen hardware (equipos de procesamiento de datos, periféricos y medios de comunicación), software

(sistema operativo, servicio, software de aplicación), red, personal (directores, usuarios, personal de operación y desarrolladores), lugar y infraestructura de la organización (centro de datos, servidores).

La fase de identificación de amenazas implica identificar las causas potenciales de un incidente contra un activo, pueden ser de origen natural (inundación, lluvias, terremotos), de entorno (incendio, sobrecarga eléctrica), defecto de aplicaciones o software desarrollado, causadas por personas de forma accidental o deliberada.

La fase de identificación de vulnerabilidades y salvaguardas, implica clasificar las amenazas midiendo la degradación que le supone a un activo, a su vez, se determina que salvaguarda se empleará para disminuir el riesgo a un nivel aceptable.

La fase principal de evaluación del riesgo, identifica de forma cuantitativa o cualitativa los riesgos y les da prioridad a los criterios de evaluación que están inmersamente comprometidos dentro de los objetivos estratégicos de la organización.

Como última fase, se encuentra el tratamiento del riesgo, tiene como objetivo identificar las medidas de seguridad para reducir los riesgos y establecer un plan de tratamiento del riesgo. El proceso recibe como entrada la salida del proceso de evaluación de riesgos y produce como salida el plan de tratamiento de riesgos. (p.30)

Evaluación del riesgo

Para Peltier (2014), explica que:

[…] el proceso de evaluación de riesgos ayuda a la gestión en el cumplimiento de sus obligaciones de proteger los activos de la organización. Al ser un activo en el proceso de evaluación de riesgos, la gestión, cuando actúa en su condición de propietario, tiene la oportunidad de ver lo que las amenazas están al acecho en todo el proceso de negocio. (p.21)

Tratamiento del riesgo

Además, al definir el nivel de riesgo como algo que tiene que ser aceptado por la alta dirección de una organización, el Ministerio de Hacienda y Administraciones Pública (2012)16, indica:

El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema. En coordinación con los objetivos, estrategia y política de la Organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección.

1.4. Formulación del problema

Problema General.

¿De qué manera la implementación del Sistema de Gestión de la Seguridad de la Información influye en el proceso de gestión del riesgo en un gobierno local, 2018?

Problemas específicos.

Problema específico 1.

¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en la evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018?

Problema específico 2.

¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el tratamiento del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018?

1.5. Justificación.

La presente investigación es importante porque responde a las necesidades organizacionales de nuestro país.

Justificación teórica.

La presente investigación aplica el estándar ISO 31000-2009 para mejorar el proceso de gestión del riesgo en un gobierno local, sostiene el proceso de gestión de riesgos en una serie de acciones, para identificar el riesgo, efectos de producirse y aplicar medidas para reducirlos a un nivel aceptable, de tal manera que los resultados de la investigación incorporaron conocimientos a la comunidad científica sobre seguridad de la información.

Justificación metodológica

Con la finalidad de conseguir los objetivos de estudio, se utilizarán un instrumento validado y confiable, el cual mide el nivel de proceso de gestión del riesgo. Para lo cual se utilizará la técnica de encuesta y el procesamiento de las respuestas utilizando el software IBM SPSS Statistics, versión 25. Dentro de la entidad materia de estudio.

Justificación práctica.

Debido a la actual carencia de una metodología que permita la seguridad de la información en la institución de estudio, además de la falta de modelamiento de los procesos, fue necesario que se realice el inventario de activos de información, el análisis de riesgos y la implantación de controles que sirvieron como protección ante posibles amenazas internas y externas. En tal sentido, se requiere mejorar la seguridad de la información a través de mejorar los niveles de riesgo.

1.6. Hipótesis

1.6.1. Hipótesis General.

Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en el proceso de gestión del riesgo de un gobierno local.

1.6.2. Hipótesis Específicas.

Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.

Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en el tratamiento de en el proceso de gestión del riesgo en un gobierno local.

1.7. Objetivos

1.7.1. Objetivo general.

Determinar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un gobierno local, 2018.

Objetivos específicos.

- Determinar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en la evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.

- Determinar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el tratamiento del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.

II. Método

2.1. Diseño de estudio

Enfoque

El enfoque de la presente investigación es de enfoque cuantitativo.

Para Gómez (2010), “El enfoque cuantitativo emplea la recolección de datos para responder a las preguntas de investigación y probar hipótesis establecidas al inicio, desarrolla un plan para probar las hipótesis, mide las variables en un determinado contexto, analiza las mediciones obtenidas y establece una serie de conclusiones respecto de las hipótesis” (p.78).

Metodología

La metodología por excelencia que usan los investigadores científicos es el método deductivo, ya que consiste en hacer observaciones manipulativas y análisis, a partir de las cuales se pueden realizar formulaciones de hipótesis que serán comprobadas mediante experimentos que en su mayoría son controlados. En la presente investigación por lo antes ya expuesto, la metodología que se utilizara es la del método hipotético-deductivo, ya que es un proceso iterativo, es decir que se repite constantemente, donde en el trayecto se analizan las hipótesis de los datos que arrojan después del experimento.

Tipo de estudio

La investigación realizada es del tipo de estudio aplicada, Landau (2007), explicó que el estudio aplicado requiere información teórica y empírica que le permita la formulación precisa de problemas y sus prioridades en futuras investigaciones; así como también el desarrollo progresivo de teorías e hipótesis, con la finalidad de poder proporcionar una visión más específica o general de una determinada realidad. (p.14).

Diseño

Para la presente investigación se utilizó un diseño de investigación pre-experimental con un diseño post-test acompañado de un grupo que se deja intacto de alguna manipulación. Se han realizado los Test necesarios con dos grupos del mismo tamaño y con características similares; uno es el grupo experimental

Dónde:

G1 : Es el grupo de procesos de seguridad

G2: Es el grupo

X : Experimento de mejora de procesos

O1 : Es el resultado de realizar las pruebas con el proceso tradicional:

O2 : Es el resultado de realizar las pruebas utilizando la mejora continua de procesos

2.2 Variables, operacionalización

Identificación de variables

Variable independiente: Sistema de gestión de seguridad de la información.

Según Areitio, J (2008), el sistema de gestión de seguridad de la información es un sistema que se basa en el enfoque de los riesgos del negocio y que establece, implementa, opera, monitoriza, sostiene y optimiza la seguridad de la información. Esto implica generar una estructura organizacional dentro de la institución, establecer políticas de seguridad de la información, responsabilidades, procesos procedimientos y recursos.

Variable dependiente: Proceso de Gestión del riesgo.

Para definir la variable dependiente de esta investigación, se toma el concepto de Peltier, T (2014)28, quien sostiene:

"El proceso de gestión de riesgos consiste en identificar riesgos, evaluar la probabilidad de que se produzcan y, a continuación, tomar medidas para reducir todos los riesgos a un nivel aceptable. Todos los procesos de evaluación de riesgos utilizan la misma metodología. Determinar el activo a ser revisado. Identificar las amenazas, problemas o vulnerabilidades. Evaluar la probabilidad de que ocurra la amenaza y el efecto en el activo o en la organización si se realiza la amenaza (así se determina el riesgo). A continuación, identifique los controles que llevarían el efecto a un nivel aceptable".

Definición operacional

Variable independiente: Sistema de gestión de seguridad de la información.

Según Pacheco (2010), “Un SGSI es un elemento para la administración relacionado con la seguridad de la información, aspecto fundamental de cualquier empresa. Un SGSI implica crear un plan de diseño, implementación y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información”. Al implementar la metodología del estándar ISO 31000, en la administración de base de datos del gobierno local” se estará realizando una serie de actividades con la finalidad de mejorar la seguridad de la información y por consiguiente asegurar su confiabilidad, integridad y disponibilidad.

Variable dependiente: Proceso de Gestión del riesgo.

El proceso de gestión del riesgo es un conjunto de fases sucesivas, que implican evaluar el riesgo y tratar el riesgo en el contexto de la organización, estas acciones involucran llevar el nivel de riesgo a un grado aceptable y determinar el número de controles aplicados para su reducir el riesgo, respectivamente, para ello, es necesario la aplicación de un instrumento de recopilación directa de datos, como es la Ficha de Observación.

Operacionalización de variables

Variable independiente: Sistema de gestión de seguridad de la información.

Según la metodología del ISO 31000, requiere la elaboración de la documentación básica que será establecida como las dimensiones, a saber:

Del SGSI.

- Políticas de seguridad de información.
- Identificación de activos.
- Mecanismos de control SGSI.
- Análisis y evaluación del riesgo
- Plan de tratamiento del riesgo.
- Documentación de procedimientos.

Declaración de aplicabilidad.

Los indicadores para estas dimensiones, serán medidas como el resultado positivo de cumplimiento en la elaboración de los documentos (check list) con los valores o escala: si / no (si entregado o no entregado, respectivamente).

Variable dependiente: Proceso de Gestión del riesgo.

Según las dimensiones ya definidas para la variable dependiente, serán medibles, según los siguientes criterios:

▪ Dimensión: Evaluación del Riesgo

Como indicador tendremos el nivel de riesgo, cuya medida será cuantitativa y estará dada por la siguiente fórmula:

NR = (P x I)

En donde:

NR = Nivel de riesgo.

I = Nivel de impacto sobre el activo.

P = Probabilidad de ocurrencia

La técnica utilizada para obtener el nivel de riesgo será el de observación directa, cuyo instrumento de recolección será la Ficha de Observación.

▪ Dimensión: Tratamiento del riesgo

Como indicador tendremos el número de controles aplicados, cuya medida será cuantitativa y estará dada por la siguiente fórmula:

CA = Ciso – (CNE + CNA)

En donde:

CA = N° de controles aplicados.

Ciso = N° de controles ISO 31000

CNE = N° de controles no existentes.

CNA = N° de controles no aplicables.

La técnica utilizada para obtener el número de controles aplicados será el de observación directa, cuyo instrumento de recolección será la Ficha de Observación.

Tabla 7:Matriz de operacionalización de las variables

Variable	Dimensión	Indicador	Instrumento	Escala de Medición
PROCESO DE GESTIÓN DEL RIESGO	Evaluación del riesgo	Nivel de riesgo	Ficha de Observación	Razón
	Tratamiento del riesgo	Número de controles aplicados	Ficha de Observación	Nominal

Fuente: Ayala(2017).

2.3. Población y muestra

Población

Según el estándar ISO 31001, se identificarán los activos dentro de los procesos e información más sensibles del gobierno local, por lo que los activos se identificarán y evaluarán en base a un proceso de levantamiento de información que será recogida en la documentación en base a consultas al personal profesional y técnico comprendido dentro de las funciones operativas de desarrollo de sistemas, control y seguridad de la información de la organización.

Por tanto, si la población, por la cantidad de unidades que la conforman, alcanza su accesibilidad en su totalidad, no será necesario extraer una muestra. De tal manera que se han considerado 31 activos, y 114 controles de acuerdo a la norma establecida.

2.4 Técnicas e instrumentos de recolección de datos

Técnica de recolección de datos.

La técnica utilizada en la presente investigación para medir las variables de estudio**,** fue la encuesta, que una técnica basada en preguntas dirigidas a un número considerable de personas, la cual emplea cuestionarios para indagar sobre las características que se desea medir o conocer (Hernández, *et al.,* 2010).

Validación y confiabilidad de los instrumentos

Validación de los instrumentos.

La validación de un instrumento, en términos generales, se refiere al grado en que un instrumento realmente mide la variable que pretende medir (Hernández, Fernández y Baptista, 2014). Mediante el juicio de expertos consiste en preguntar a personas expertas acerca de la pertinencia, relevancia, claridad y suficiencia de cada uno de los ítems, en el caso del instrumento.

Tabla 8

Validez del instrumento para la Ficha de observación de nivel de riesgo

Experto	El instrumento presenta				Condición final
	Pertinencia	Relevancia	Claridad	Suficiencia	
Juez 1	si	si	si	si	Aplicable
Juez 2	si	si	si	si	Aplicable
Juez 3	si	si	si	si	Aplicable

La tabla muestra que los expertos consideraron que los cuestionarios de niveles de controles es un cuestionario esta por contener ítems pertinentes, relevantes, claros y suficientes para garantizar la medición válida de la variable gestión del riesgo.

Confiabilidad de los instrumentos

Los instrumentos de recolección de datos que presentaron ítems con opciones politómicas, fueron evaluados a través del coeficiente alfa de Cronbach con el fin de determinar su consistencia interna, analizando la correlación media de cada ítem con todas las demás que integran dicho instrumento. Se aplicó la prueba piloto y después de analizó mediante el Alfa de Cronbach con la ayuda del software estadístico SPSS versión 25.

Tabla 9

Escala de valores para determinar la confiabilidad (Hogan, 2004)

Valor	Confiabilidad
Alrededor de 0.9	Nivel elevado de confiabilidad
0.8 o superior	Confiable
Alrededor de 0.7, se considera	Baja
Inferior a 0.6, indica una confiabilidad	Inaceptablemente baja.

Tabla 10

Estadísticas de fiabilidad

Alfa de Cronbach	Parte 1	Valor	1,000
		N de elementos	1[a]
	Parte 2	Valor	1,000
		N de elementos	1[b]
	N total de elementos		2
Correlación entre formularios			1,000
Coeficiente de Spearman-Brown	Longitud igual		1,000
	Longitud desigual		1,000
Coeficiente de dos mitades de Guttman			1,000

a. Los elementos son: VAR00009

b. Los elementos son: VAR00010

El utilizó el coeficiente de dos mitades para evaluar la confiablidad de la ficha de observación de los controles, se empleó el método de dos mitades, se halló un valor de 1.000 para el instrumento indicando que la escala presentaba una confiabilidad muy alta.

2.5 Métodos de análisis de datos

El procedimiento para la recolección de datos siguió los siguientes pasos:

Se utilizaron las fichas de observación de niveles de riesgo y para los controles que se aplican para la recolección de datos.

Posteriormente, con los datos obtenidos se elaboró la matriz de datos, se transformaron los valores según las escalas establecidas y se procedió con el debido análisis con la finalidad de presentar las conclusiones y recomendaciones y de esta manera preparar el informe final.

Para el análisis y presentación de los datos obtenidos en la investigación, se empleó la estadística descriptiva e inferencial. Estos resultados fueron representados utilizando figuras estadísticas para poder visualizar y comprender

mejor la investigación. Para contrastar las hipótesis se utilizó la estadística inferencial el procedimiento de Wilcoxon. .

2.5 Aspectos Éticos

Los datos indicados en esta investigación fueron recogidos del grupo de investigación y se procesaron de forma adecuada sin adulteraciones.

Los trabajadores que han participado en esta encuesta, no fueron mencionados, se han tomado las reservas del caso para evitar información dañina en contra de las personas o instituciones que han colaborado con esta investigación.

De igual forma el marco teórico se recolectó de acuerdo a los parámetros establecidos e indicados para realizare este tipo de estudio, evitando copia de otras investigaciones.

Finalmente los resultados de la investigación no han sido adulteradas o plagiadas de otras investigaciones haciéndose un buen uso de la investigación en beneficio de todos.

III. Resultados

3.1 Resultados de la Estadística Descriptiva

En el estudio realizado sobre como el Sistema de Gestión de Seguridad de la Información influyó en el nivel de riesgo, a través de la evaluación de los niveles de riesgo y la aplicación de controles en el proceso de gestión de la Municipalidad Distrital de Carabayllo; por tanto, se aplicó una evaluación en los niveles de riesgo, tanto, en la evaluación y tratamiento de los niveles, se implementó la metodología propuesta para estimar los indicadores.

Valoración de los activos

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la importancia para la organización:

Tabla 11

Escala de puntuaciones de los activos

Escala de valoración	Descripción	Valor
Muy alta	De vital importancia para los objetivos que persigue la organización	5
Alta	Altamente importante para la organización	4
Media	Importante para la organización	3
Baja	Importancia menor para el desarrollo de la organización	2
Muy baja	Irrelevante para efectos prácticos	1

Valoración de la degradación

Los activos serán puntuados dependiendo de una tabla de ponderaciones en las que se evalúa la confidencialidad, integridad, disponibilidad de cada uno de los activos.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera.

Tabla 12

Escala de puntuaciones de valores de la degradación

Puntuación	Disponibilidad	Integridad	Confidencialidad
5	Siempre	Extrema	Uso confidencial
4	Exenta por horas	Importante	Uso restringido
3	Exenta por 24 horas	Media	Semi restringido
2	Exenta por 48 horas	No importante	Uso interno
1	Exenta por varios días	Insignificante	Acceso público

Degradación máxima- Al obtener cada uno de los puntajes asignados en la degradación, se determina el máximo valor de la degradación, dato que nos servirá para calcular el nivel de riesgo.

Valoración del impacto- El valor del impacto se determina según la tabla de estimación del impacto.

Tabla 13

Estimación del impacto

Valor	Descripción
Muy bajo (1)	Riesgo que puede tener un pequeño o nulo efecto en la institución.
Bajo (2)	Causa un daño en el patrimonio o imagen, que se puede corregir en el corto tiempo, y no afecta el cumplimiento de los objetivos estratégicos.
Medio (3)	Causaría, ya sea una pérdida importante en el patrimonio, incumplimientos normativos, problemas operativos o de impacto ambiental o un deterioro significativo de la imagen. Además, se referiría una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños.
Alto (4)	Dañaría significativamente el patrimonio, incumplimientos normativos, problemas operativos o impacto ambiental o deterioro de la imagen o logro de objetivos institucionales. Además, se referiría a una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños.
Muy alto (5)	Influye directamente en el cumplimiento de la misión, pérdida patrimonial incumplimientos normativos, problemas operativos o de impacto ambiental o deterioro de la imagen, dejando además sin funcionar totalmente o por un periodo importante de tiempo los programas o servicios que entrega la institución.

Probabilidad

La probabilidad es la posibilidad de que se lleve a cabo una amenaza. Para la presente investigación, se determina en la siguiente escala:

Tabla14

Escala de puntuaciones de la probabilidad

Escala de valoración	Descripción	Valor
Muy alta	La amenaza se materializa a lo sumo una vez cada día.	5
Alta	La amenaza se materializa a lo sumo una vez cada semana.	4
Media	La amenaza se materializa a lo sumo una vez cada mes.	3
Baja	La amenaza se materializa a lo sumo una vez cada semestre.	2
Muy baja	La amenaza se materializa a lo sumo una vez cada año.	1

Valoración del riesgo

El valor del riesgo se determina por la multiplicación del impacto y la probabilidad:

Riesgo = (Impacto x Probabilidad).

Los resultados del análisis descriptivo se detallan a continuación.

Indicador: Nivel de riesgo (Pre test y Post test)

Tabla 15

Evaluación del riesgo

N°	CÓDIGO ACTIVO	ACTIVOS	RIESGO PROMEDIO PRE TEST	RIESGO PROMEDIO POST TEST
1	A002	SISMUN	17	8
2	A005	Servidor Aplicaciones/BD (Sauce)	9.33	5.33
3	A009	Firewall	6	3.2
4	A004	SISMUN Fox	10.25	5.5
5	A010	Switch de Borde	6	2.67
6	A011	Switch de Distribución	8.67	2.33
7	A012	Switch Core	8.67	3.33
8	A029	Computadora de Escritorio (Técnico Liquidador de Fiscalización Tributaria)	13	5.33
9	A052	Subgerente de Informática	10.67	4.67
10	A003	SISMUN Web	10.25	6
11	A051	Computadora de Escritorio del Subgerente de Informática	12	7
12	A001	Analista Programador	10.16	3.33
13	A017	Supervisor de Plataforma	10	6
14	A026	Computadora de Escritorio (Técnico en Plataforma de Fiscalización Tributaria)	12.33	7.33
15	A044	Declaración Jurada de Predio Rustico	12.5	8
16	A046	Subgerente de Administración Tributaria	10	6
17	A048	Resolución de determinación predial - Fiscalización	12	7.5
18	A050	Hoja de Resumen de Declaración Jurada	10	6
19	A041	Subgerente de Fiscalización Tributaria	10	6
20	A043	Declaración Jurada de Predio Urbano	10	6
21	A047	Requerimiento de fiscalización	10	6
22	A049	Resolución de determinación de arbitrios - Fiscalización	12	7.5
23	A006	UPS de Switchs de Gabinete de Comunicación	7	6
24	A007	UPS de Switch Core	7	6
25	A008	UPS Servidor (Aplicaciones/BD)	7	6
26	A013	UPS (Analista Programador)	7	6
27	A028	Técnico Liquidador de Fiscalización Tributaria	10	8
28	A038	Técnico de Fiscalización Tributaria	10	8
29	A039	Técnico en Plataforma de Recaudación	10	8
30	A045	Estado de cuenta	10	6
31	A053	Cargo de Notificación de Fiscalización	10	6
NIVEL DE RIESGO			9.96	5.90

Fuente: Elaboración propia

Tabla 16

Resultados descriptivos del nivel de riesgo en fase pre y post test

Test	n	Rango	Mínimo	Máximo	Media	Desviación estándar
Pre test	31	11	6	17	9.96	2.27
Post test	31	5.67	2.33	8	5.90	1.60

Interpretación:

Según la Tabla 12 y figura 4, se determina que hay una disminución del nivel de riesgo de (9.96+-2.27) a (5.90+-1.60) en promedio, asimismo, en la figura 4, se visualiza la caja de bigotes, donde la mediana del pretest es mayor que la mediana del post test.

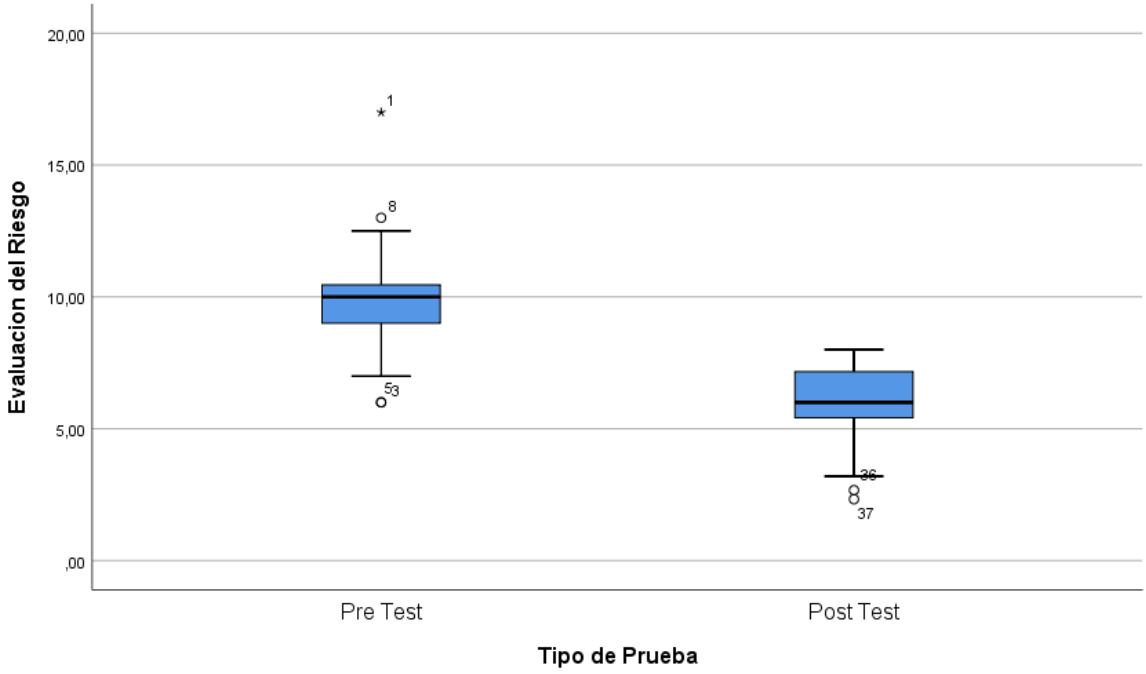


Figura 4. Diagrama de cajas por tipo de prueba

Indicador: Número de controles aplicados (Pre y Post test)

Los resultados descriptivos del número de controles aplicados, se aprecian en la Siguiente tabla.

Tabla 17

Tabla cruzada Existencia de controles por Tipo de prueba

			Tipo de prueba	
			Pre Test	Post Test
Existencia del control	No aplica	Recuento	105	1
		% dentro de Tipo de prueba	92,1%	0,9%
	Si aplica	Recuento	9	113
		% dentro de Tipo de prueba	7,9%	99,1%
Total		Recuento	114	114
		% dentro de Tipo de prueba	100,0%	100,0%

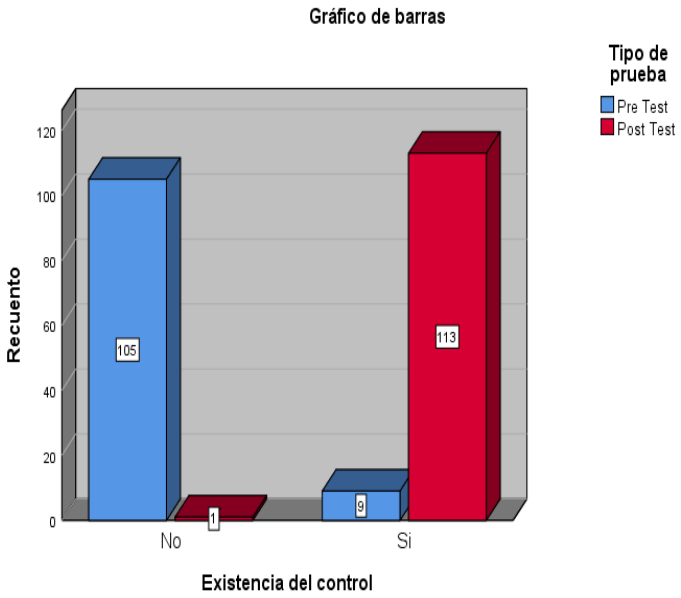


Figura 5. Existencia de Control

Interpretación

Según la tabla 13 y figura 5, existencia de controles aplicados, no se aplican en el 92.1% en el pre test, sin embargo, el 99.1% (114), se aplican en el post test. Asimismo, solo se aplican 9 controles (7.9%), al inicio del proceso (pretest)

3.2. CONTRASTE DE HIPOTESIS

Prueba de hipótesis especifica

H_o No Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.

H_a: Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.

Nivel de Significación Se ha considerado α= 0.05

Regla de decisión: Si p **≥** α, se acepta H_0; Si p < α, se rechaza H_0

Prueba de estadística: Debido a que las variables tienen escala de razón, primero realizamos la prueba de normalidad para determinar el procedimiento estadístico adecuado.

Tabla 18

Prueba de Normalidad de Shapiro -Wilk

	Estadístico	gl	Sig.
Evaluación del Riesgo (Pre test)	,901	31	,008
Evaluación del Riesgo (Post test)	,882	31	,003

De acuerdo a los resultados obtenidos en la prueba de normalidad, para menos de 50 observaciones, los resultados indican que no existe normalidad en ninguna de las distribuciones de la evaluación del riesgo del pre y post test, considerando que el pvalor=0.008 <0.05 (pre test) y pvalor=0.003<0.05 (post test).

Tabla 19

Prueba Wilcoxon para la evaluación del riesgo del pre y post test

Rangos

		N	Rango promedio	Suma de rangos
Evaluación del Riesgo (Post Test) - Evaluación del Riesgo (Pre Test)	Rangos negativos	31[a]	16,00	496,00
	Rangos positivos	0[b]	,00	,00
	Empates	0[c]		
	Total	31		

a. Evaluación del Riesgo (Post Test) < Evaluación del Riesgo (Pre Test)

b. Evaluación del Riesgo (Post Test) > Evaluación del Riesgo (Pre Test)

c. Evaluación del Riesgo (Post Test) = Evaluación del Riesgo (Pre Test)

Tabla 20

Estadísticos de prueba[a]

	Evaluación del Riesgo (Post Test) - Evaluación del Riesgo (Pre Test)
Z	-4,876[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos positivos.

En la tabla 16, que en la prueba de Wilcoxon respecto a la evaluación del riesgo, tuvo un pvalor=0.000 <0.05, de tal manera, que la prueba es significativa, por lo tanto existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en la evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.

Prueba de hipótesis especifica

H_O No Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva aumentando tratamiento del riesgo aplicados en el proceso de gestión del riesgo en un gobierno local.

H_a: Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva aumentando tratamiento del riesgo aplicados en el proceso de gestión del riesgo en un gobierno local.

Nivel de Significación Se ha considerado α= 0.05

Regla de decisión: Si p **≥** α, se acepta H_0; Si p < α, se rechaza H_0

Prueba de estadística: Debido a que las variables tienen escala de nominal, las distribuciones no son normales, para determinar la diferencia de dos grupos relacionados, se utilizó la prueba de Wilcoxon.

Tabla 21

Rangos

		N	Rango promedio	Suma de rangos
Existencia del Control (Post test) - Existencia del control (Pre test)	Rangos negativos	0[a]	,00	,00
	Rangos positivos	104[b]	52,50	5460,00
	Empates	10[c]		
	Total	114		

a. Existencia del Control (Post test) < Existencia del control (Pre test)
b. Existencia del Control (Post test) > Existencia del control (Pre test)
c. Existencia del Control (Post test) = Existencia del control (Pre test)

Tabla 22

Estadísticos de prueba[a]

	Existencia del Control (Post test) - Existencia del control (Pre test)
Z	-10,198[b]
Sig. asintótica(bilateral)	,000

a. Prueba de rangos con signo de Wilcoxon
b. Se basa en rangos negativos.

En la tabla 11, que en la prueba de Wilcoxon respecto a la tratamiento del riesgo, tuvo un pvalor=0.000 <0.05, de tal manera, que la prueba es significativa, de tal manera que, existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información influye de manera positiva aumentando etratamiento del riesgo aplicados en el proceso de gestión del riesgo en un gobierno local.

IV. Discusiones

En este capítulo los resultados de la presente investigación, permitió obtener el objetivo de la investigación, considerando que la implementación del Sistema de Gestión de Seguridad de la Información influyó en el proceso de gestión del riesgo en un gobierno local, 2018. En ese sentido, la investigación realizada por Rivero (2017), se ubica dentro del contexto de gestión de riesgos, las técnicas de evaluación de riesgos, tema que es de nuestro interés en la investigación realizada, además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación. En el caso de Rodríguez (2016), en su tesis titulada, “Diseño y formulación de un sistema de gestión de riesgos basados en los lineamientos establecidos por la norma NTC- ISO 31000 versión 2011 para la empresa Simma Ltda.”, de tal manera que, la investigación realizada por Rodríguez se ubica dentro del contexto de gestión de riesgos, capacitación a los trabajadores en relación a riesgos, tema que es de nuestro interés en la investigación realizada además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación. En ese sentido, Ayala (2017), en su tesis titulada, “Sistema de gestión de seguridad de información Para mejorar el proceso de gestión del riesgo en un hospital nacional, 2017”, se ubica dentro del contexto de gestión de riesgos, tema que es de nuestro interés en la investigación realizada, además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación. El objetivo logrado, establece que lo que indica Cano (2011), la disciplina que nos habla de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y esquemas normativos, que nos exigen niveles de aseguramiento de procesos y tecnologías para elevar el nivel de confianza en la creación, uso, almacenamiento, transmisión, recuperación y disposición final de la información. Según la ISO 31000 (2009) indico que las actividades de una organización implican un riesgo. Organizaciones a gestionar el riesgo mediante la identificación, análisis y evaluación si el riesgo debe ser modificado por el tratamiento del riesgo con el fin de satisfacer sus criterios de riesgo, en ese sentido, se ha logrado el objetivo general, de tal manera, que se pueda mitigar los riesgos a través de la implantación del sistema de seguridad de la información.

Respecto a la evaluación del riesgo, la ISO 31000 (2009) explica que una entrada a la evaluación de riesgos y a las decisiones sobre si los riesgos necesitan ser tratados, y sobre las estrategias y los métodos de tratamiento de riesgo más apropiado. Lo que nos indica que el análisis de riesgos implica la consideración de las causas y las fuentes de riesgo, sus consecuencias positivas y negativas, y la probabilidad de que pueden ocurrir esas consecuencias. Arias, Díaz, & Vargas (2014), en su tesis titulada," Elaboración de una guía de gestión de riesgos basados en la norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia", en la investigación realizada, corrobora los resultados obtenidos, además se precisa la importancia del análisis de riesgos, lo cual es de aprovechamiento óptimo para esta investigación.

Respecto al tratamiento del riesgo en el proceso de gestión, coinciden los resultados con el trabajo de Rios (2014), en su trabajo de investigación titulado "Diseño de un Sistema de Gestión de Seguridad de Información para una central privada de información de riesgos.", esta herramienta coincide respecto a que es una de las mejoras herramientas para la gestión del riesgo y del cumplimiento en seguridad de la información.

V. Conclusiones

Primera

La implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un gobierno local, 2018.

Segunda

La implementación del Sistema de Gestión de Seguridad de la Información influye en la evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018, basadas en evidencias estadísticas, con respecto al pvalor de la prueba siendo menor que el error.

Tercera

La implementación del Sistema de Gestión de Seguridad de la Información influye en el tratamiento del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018. Se corrobora a través del procedimiento de Wilcoxon, donde la comparación de ambos grupos, se evaluó a través de la prueba de wilcoxon, siendo ella significativa.

VI. Recomendaciones

Primera

En los gobiernos locales, se recomienda alinear a la Gerencia de TI con las estrategias del negocio(es decir lo que quiere el negocio). Se debe mantener información de calidad para apoyar las decisiones empresariales, para ello es necesario que la institución tenga mapeado todo sus activos y a cada activo gestionar sus riesgos(amenazas y vulnerabilidades), de tal manera se pueda aplicar un adecuado control y mantener los riesgos en un nivel aceptable.

Segunda

Se recomienda realizar evaluaciones periódicas de los niveles de riesgo, de tal manera se pueda monitorear correctamente la efectividad de los controles aplicados, a su vez se puede usar varias metodologías estándar para salvaguardar los activos de información.

Tercera

Se recomienda que los responsables de la seguridad de la información (oficial de seguridad) formulen los planes de acción o mejora de controles necesarios para el tratamiento de los riesgos según su criticidad, para el caso de la Dunicipalidad Distrital de Carabayllo se recomienda gestionar los riesgos, para evaluar los riesgos, impactos . Deben de seguir un procedimiento de tratamiento de los riesgos, de tal manera la gerencia pueda definir la opción de tratamiento a implementar (transferir, evitar, reducir o asumir el riesgo).

VII. Referencias

Avalos. C. (2012). *Análisis. diseño e implementación del sistema de riesgo operacional para entidades financieras – SIRO* (Tesis para Maestría). Pontificia Universidad Católica Del Perú. Perú. Recuperada de: http://tesis.pucp.edu.pe/repositorio/handle/123456789/4454

Celí. E. (2016). La gestión de riesgo TI y la efectividad de los sistemas de seguridad de información: caso de procesos críticos en las pequeñas entidades financieras de Lambayeque. Pueblo Cont. *27*(1). 73-84. Recuperado de:http://journal.upao.edu.pe/PuebloContinente/article/download/395/360

Alvizuri. G. (2014). *Implementación de Itil v3.0 y su influencia en el proceso de gestión de incidencias y cambios en el área de ti de la consultora ESPROTEC* (Tesis de Maestría). Universidad Peruana Unión. Perú. Recuperada de: http://repositorio.upeu.edu.pe/handle/UPEU/359?show=full

Areitio, J. (2008). Seguridad de la información Redes, informática y sistemas de información. (C. L. Carmona, Ed.) Madrid España: Ediciones Paraninfo.

Arias, Y., Díaz, M., & Vargas, J. (2014). Elaboración De Una Guía De Gestión De Riesgos Basados En La Norma NTC-ISO 31000 para el proceso de gestión de incidentes y peticiones de servicio del área de mesa de ayuda de empresas de servicios de soporte de tecnología en Colombia. Tesis, Universidad Católica de Colombia, Colombia.

Ayala , M. (2017). Sistema de gestión de seguridad de información Para mejorar el proceso de gestión del riesgo En un hospital nacional, 2017. Tesis, Universidad César Vallejo, Lima Perú.

Bernaldo, N. (2016). Sistema de gestión de seguridad de la Información en el Proceso de Registros Civiles de RENIEC. San Borja. Lima 2016. Tesis, Universidad César Vallejo, Lima.

De La cruz, R. (2016). Propuesta de políticas, basadas en buenas prácticas, para la gestión de seguridad de la información en la municipalidad provincial de Paita; 2016. Tesis, Universidad Católica Los Ángeles Chimbote, Piura.

Díaz, R. (2015). Apoyo al proceso de implementación de un sistema de gestión de la seguridad de la información basado en la norma ISO 27001:2013 en la alcaldía de Pasto. Tesis, Universidad de Nariño , Colombia.

Mera. A. (2014). *Diseño del modelo de gestión de seguridad de la información del sistema ERP de EP PETROECUADOR de acuerdo a norma ISO/IEC 27002 y COBIT 5*. (Tesis de Maestría). Universidad. Ecuador. Recuperado de:http://repositorio.espe.edu.ec/bitstream/21000/8073/1/T-ESPE-047641.pdf

Rios , J. (2014). Diseño de un Sistema de Gestión De Seguridad de Información para una Central Privada de Información de riesgos. Tesis, Pontificia Universidad Católica del Perú, Lima Perú.

Rivero, P. (2017). Diseño de un modelo de gestión del riesgo aplicado a una empresa manufacturera de autopartes. Tesis, Instituto Politécnico Nacional, México.

Rodríguez, Y. (2016). Diseño y formulación de un sistema de gestión de riesgos basados en los lineamientos establecidos por la norma NTC- ISO 31000 versión 2011 para la empresa Simma Ltda. Tesis, Universidad Industrial de Santander, Colombia.

Ramírez. A. y Ortiz. Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. Ingeniería. *16*(2). 56- 66. Recuperado de:https://dialnet.unirioja.es/descarga/articulo/4797252.pdf

Ramírez. G. y Álvarez. E. (2003). Auditoría a la gestión de las Tecnologías y sistemas de Información. Industrial Data. 6(1). 99-102. Recuperado de: http://sisbib.unmsm.edu.pe/bibvirtualdata/publicaciones/indata/Vol6_n1/pf/auditoria.pdf

Tarrillo, E. (2016). Influencia de la Gestión de Riesgo en la seguridad de Activos de Información de la zona Registral III Sede Moyobamba, 2015. Tesis, Universidad César Vallejo, Tarapoto.

Valencia, H. (2016). Metodología del SGSI Según La Norma ISO/IEC 27001 para el gobierno autónomo descentralizado de San Miguel de Urcuquí. Tesis, Universidad Técnica del Norte, Ibarra- Ecuador.

VIII. Anexos

ANEXO 1

MATRIZ DE CONSISTENCIA

<table>
<tr><th colspan="6">TITULO : Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018.</th></tr>
<tr><th rowspan="2">PROBLEMA</th><th rowspan="2">OBJETIVO</th><th rowspan="2">HIPÓTESIS</th><th colspan="3">DEFINICIÓN OPERACIONAL</th><th rowspan="2">METODOLOGÍA</th></tr>
<tr><th>Variable</th><th>Dimensiones</th><th>Indicadores</th></tr>
<tr>
<td>PRINCIPAL

¿De qué manera la implementación del Sistema de Gestión de la Seguridad de la Información influye en el proceso de gestión del riesgo en un gobierno local, 2018?

ESPECÍFICOS

1.- ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en la evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018?

2.- ¿Cómo se relaciona la ¿De qué manera la implementación del Sistema de Gestión de Seguridad de la Información influye en el tratamiento del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018?</td>
<td>PRINCIPAL

Determinar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el proceso de gestión del riesgo en un gobierno local, 2018

ESPECÍFICOS

1. Determinar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en la evaluación del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.

2. Determinar la manera en que la implementación del Sistema de Gestión de Seguridad de la Información influye en el tratamiento del riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.</td>
<td>PRINCIPAL
Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en el proceso de gestión del riesgo de un gobierno local.
.ESPECIFICOS

1. Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en la evaluación de riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.

2. Existen diferencias en la implementación del Sistema de Gestión de Seguridad de la Información en el tratamiento de riesgo en el proceso de gestión del riesgo en un gobierno local, 2018.</td>
<td>Variable

X

SGSI</td>
<td></td>
<td></td>
<td rowspan="3">Tipo

de investigación es de tipo Aplicada

El diseño de investigación es pre –experimental

- De corte longitudinal.
- Método deductivo

Población

La población está comprendida por los activos críticos de informacion.</td></tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Variable

Y

PROCESO DE GESTION DE RIESGO</td>
<td>Y1: Evaluación de Riesgo</td>
<td>Nivel de Riesgo</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Y2. Tratamiento de riesgo</td>
<td>Número de controles</td>
</tr>
</table>

ANEXO 2 – Ficha de observación para el indicador Nivel de Riesgo en fase Pre Test

	FICHA DE OBSERVACIÓN N° 01: **INDICADOR:** NIVEL DEL RIESGO (SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES) **FASE:** PRE TEST		
	CÓDIGO:	**VERSIÓN:**	**PÁGINA:**
	CLASIFICACIÓN: **CONFIDENCIAL**	**FECHA DISEÑO:**	
Proceso:	Gestión de riesgos		
Investigador:	Jara Mendoza Omar Yino		
Fecha de recolección:			
Puesto:			

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	Sección	Objetivo de control / control						

ANEXO 3 – Ficha de observación para el indicador Número de Controles Aplicados en fase Pre Test

	FICHA DE OBSERVACIÓN N° 02: **INDICADOR:** NÚMERO DE CONTROLES APLICADOS **(**DECLARACIÓN DE APLICABILIDAD DE CONTROLES) **FASE**: PRE TEST		
	CÓDIGO:	**VERSIÓN:**	**PÁGINA:**
	CLASIFICACIÓN: **CONFIDENCIAL**	**FECHA DISEÑO:**	
Proceso:	Gestión de riesgos		
Investigador:	Jara Mendoza Omar Yino		
Fecha de recolección:			

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	Sección	Objetivo de control / control						

ANEXO 4. Relación de activos críticos de información identificados para la presente investigación

N°	CÓDIGO	NOMBRE DEL ACTIVO	TIPO	PROPIETARIO
1	A002	SISMUN	Datos	Subgerente de Informática
2	A005	Servidor Aplicaciones/BD (Sauce)	Datos	Subgerente de Informática
3	A009	Firewall	Infraestructura	Subgerente de Informática
4	A004	SISMUN Fox	Datos	Subgerente de Informática
5	A010	Switch de Borde	Infraestructura	Subgerente de Informática
6	A011	Switch de Distribución	Infraestructura	Subgerente de Informática
7	A012	Switch Core	Infraestructura	Subgerente de Informática
8	A029	Computadora de Escritorio (Técnico Liquidador de Fiscalización Tributaria)	Equipamiento	Técnico Liquidador
9	A052	Subgerente de Informática	Recursos humanos	Subgerente de Informática
10	A003	SISMUN Web	Datos	Subgerente de Informática
11	A051	Computadora de Escritorio del Subgerente de Informática	Equipamiento	Subgerente de Informática
12	A001	Analista Programador	Recursos humanos	Subgerente de Informática
13	A017	Supervisor de Plataforma	Recursos humanos	SG. de Administración Tributaria y Recaudación
14	A026	Computadora de Escritorio (Técnico en Plataforma de Fiscalización Tributaria)	Equipamiento	Secretaria
15	A044	Declaración Jurada de Predio Rustico	Documentos	SG. de Administración Tributaria y Recaudación
16	A046	Subgerente de Administración Tributaria	Recursos humanos	SG. de Administración Tributaria y Recaudación
17	A048	Resolución de determinación predial - Fiscalización		G. de Administración Tributaria
18	A050	Hoja de Resumen de Declaración Jurada	Documentos	SG. de Administración Tributaria y Recaudación
19	A041	Subgerente de Fiscalización Tributaria	Recursos humanos	G. de Administración Tributaria
20	A043	Declaración Jurada de Predio Urbano	Documentos	SG. de Administración Tributaria y Recaudación

N°	CÓDIGO	NOMBRE DEL ACTIVO	TIPO	PROPIETARIO
21	A047	Requerimiento de fiscalización	Documentos	G. de Administración Tributaria
22	A049	Resolución de determinación de arbitrios - Fiscalización	Documentos	G. de Administración Tributaria
23	A006	UPS de Switchs de Gabinete de Comunicación	Equipamiento	Subgerente de Informática
24	A007	UPS de Switch Core	Equipamiento	Subgerente de Informática
25	A008	UPS Servidor (Aplicaciones/BD)	Equipamiento	Subgerente de Informática
26	A013	UPS (Analista Programador)	Equipamiento	Analista/Desarrollador
27	A028	Técnico Liquidador de Fiscalización Tributaria	Recursos humanos	SG. Fiscalización Tributaria
28	A038	Técnico de Fiscalización Tributaria	Recursos humanos	SG. Fiscalización Tributaria
29	A039	Técnico en Plataforma de Recaudación	Recursos humanos	SG. Fiscalización Tributaria
30	A045	Estado de cuenta	Documentos	SG. de Administración Tributaria y Recaudación
31	A053	Cargo de Notificación de Fiscalización	Documentos	SG. Fiscalización Tributaria

FICHA DE OBSERVACIÓN: INDICADOR NÚMERO DE CONTROLES APLICADOS
DECLARACIÓN DE APLICABILIDAD DE CONTROLES
FASE: PRE TEST

La selección de controles y objetivos de control se realizaron a través de los siguientes criterios:

- LR: requerimientos legales
- CO: obligaciones contractuales
- BR/BP: requerimientos del negocio/mejores prácticas adoptadas
- RRA: resultado de la valoración de riesgos;

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	**Sección**	**Objetivo de control / control**						
5 Políticas de Seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información						
	5.1.1	Políticas de seguridad de la información	SI	NO			X	
	5.1.2	Revisión de las políticas de seguridad de la información	SI	NO			X	
6 Organización de la Seguridad de la Información	6.1	Organización interna						
	6.1.1	Roles y responsabilidad de seguridad de la información	SI	NO			X	
	6.1.2	Segregación de deberes	SI	NO			X	
	6.1.3	Contacto con autoridades	NO	NO				
	6.1.4	Contacto con grupos de interés especial	NO	NO				
	6.1.5	Seguridad de la información en la gestión de proyectos	SI	NO			X	
	6.2	Dispositivos móviles y teletrabajo						
	6.2.1	Política de dispositivos móviles	SI	NO			X	
	6.2.2	Teletrabajo	NO	NO				
7 Seguridad en los Recursos Humanos	7.1	Previo al empleo						
	7.1.1	Verificación de antecedentes	SI	NO				X
	7.1.2	Términos y condiciones del empleo	SI	SI				X
	7.2	Durante el empleo						
	7.2.1	Responsabilidades de la Alta Gerencia	SI	NO			X	
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	SI	NO				X
	7.2.3	Proceso disciplinario	SI	NO			X	
	7.3	Terminación y cambio de empleo						
	7.3.1	Termino de responsabilidades o cambio de empleo	SI	NO			X	
8 Gestión de Activos	8.1	Responsabilidad de los activos						
	8.1.1	Inventario de activos	SI	NO				X
	8.1.2	Propiedad de activos	SI	NO				X
	8.1.3	Uso aceptable de los activos	SI	NO			X	

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	Sección	Objetivo de control / control						
	8.1.4	Devolución de activos	SI	NO			X	
	8.2	Clasificación de la información						
	8.2.1	Clasificación de la información	SI	NO				X
	8.2.2	Etiquetado de la información	SI	NO				X
	8.2.3	Manejo de activos	SI	NO			X	
	8.3	Manejo de medios						
	8.3.1	Gestión de medios removibles	SI	NO				X
	8.3.2	Eliminación de medios	SI	NO				X
	8.3.3	Transporte de medios físicos	SI	NO				X
9 Control de Acceso	9.1	Requerimientos de negocio para el control de acceso						
	9.1.1	Política de control de acceso	SI	NO				X
	9.1.2	Acceso a redes y servicios de red	SI	NO				X
	9.2	Gestión de accesos de usuario						
	9.2.1	Registro y baja del usuario	SI	NO				X
	9.2.2	Provisión de acceso a usuarios	SI	NO				X
	9.2.3	Gestión de derechos de acceso privilegiados	SI	NO				X
	9.2.4	Gestión de información de autenticación secreta de usuarios	SI	NO				X
	9.2.5	Revisión de derechos de acceso de usuarios	SI	NO				X
	9.2.6	Eliminación o ajuste de derechos de acceso	SI	NO				X
	9.3	Responsabilidades del usuario						
	9.3.1	Uso de información de autenticación secreta	SI	NO			X	
	9.4	Control de acceso de sistemas y aplicaciones						
	9.4.1	Restricción de acceso a la información	SI	NO				X
	9.4.2	Procedimientos de inicio de sesión seguro	SI	NO				X
	9.4.3	Sistema de gestión de contraseñas	SI	NO				X
	9.4.4	Uso de programas y utilidades privilegiadas	SI	NO			X	
	9.4.5	Control de acceso al código fuente del programa	SI	NO				X
10 Criptografía	10.1	Controles criptográficos						
	10.1.1	Política en el uso de controles criptográficos	SI	NO				X
	10.1.2	Gestión de llaves	SI	NO			X	
11 Seguridad Física y del Entorno	11.1	Áreas seguras						
	11.1.1	Perímetro de seguridad físico	SI	NO				X
	11.1.2	Controles físicos de entrada	SI	SI			X	
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	SI	SI			X	
	11.1.4	Protección contra amenazas externas y del ambiente	SI	NO			X	
	11.1.5	Trabajo en áreas seguras	SI	NO			X	

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	Sección	Objetivo de control / control						
	11.1.6	Áreas de entrega y carga	SI	NO			X	
	11.2	Equipo						
	11.2.1	Instalación y protección de equipo	SI	NO			X	
	11.2.2	Servicios de soporte	SI	SI			X	
	11.2.3	Seguridad en el cableado	SI	NO				X
	11.2.4	Mantenimiento de equipos	SI	SI				X
	11.2.5	Retiro de activos	SI	NO			X	
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	SI	NO			X	
	11.2.7	Eliminación segura o reuso del equipo	SI	NO			X	
	11.2.8	Equipo de usuario desatendido	SI	NO			X	
	11.2.9	Política de escritorio limpio y pantalla limpia	SI	NO				X
12 Seguridad en las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades						
	12.1.1	Documentación de procedimientos operacionales	SI	SI				X
	12.1.2	Gestión de cambios	SI	SI				X
	12.1.3	Gestión de la capacidad	SI	NO				X
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	NO				X
	12.2	Protección de Software Malicioso						
	12.2.1	Controles contra software malicioso	SI	NO				X
	12.3	Respaldo						
	12.3.1	Respaldo de información	SI	NO				X
	12.4	Bitácoras y monitoreo						
	12.4.1	Bitácoras de eventos	SI	NO			X	
	12.4.2	Protección de información en bitácoras	SI	NO			X	
	12.4.3	Bitácoras de administrador y operador	SI	NO			X	
	12.4.4	Sincronización de relojes	SI	NO			X	
	12.5	Control de software operacional						
	12.5.1	Instalación de software en sistemas operacionales	SI	NO			X	
	12.6	Gestión de vulnerabilidades técnicas						
	12.6.1	Gestión de vulnerabilidades técnicas	SI	NO				X
	12.6.2	Restricciones en la instalación de software	SI	NO				X
	12.7	Consideraciones de auditoria de sistemas de información						
	12.7.1	Controles de auditoría de sistemas de información	SI	NO			X	
13 Seguridad en las Comunicaciones	13.1	Gestión de seguridad en red						
	13.1.1	Controles de red	SI	SI			X	
	13.1.2	Seguridad en los servicios en red	SI	NO				X
	13.1.3	Segregación en redes	SI	NO				X

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	**Sección**	**Objetivo de control / control**						
	13.2	Transferencia de información						
	13.2.1	Políticas y procedimientos para la transferencia de información	SI	NO			X	
	13.2.2	Acuerdos en la transferencia de información	SI	NO			X	
	13.2.3	Mensajería electrónica	SI	NO			X	
	13.2.4	Acuerdos de confidencialidad o no-revelación	SI	NO			X	
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de seguridad en sistemas de información						
	14.1.1	Análisis y especificación de requerimientos de seguridad	SI	NO			X	
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	SI	NO			X	
	14.1.3	Protección de transacciones en servicios de aplicación	SI	NO			X	
	14.2	Seguridad en el proceso de desarrollo y soporte						
	14.2.1	Política de desarrollo seguro	SI	NO			X	
	14.2.2	Procedimientos de control de cambios del sistema	SI	NO			X	
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	SI	NO			X	
	14.2.4	Restricción de cambios en paquetes de software	SI	NO			X	
	14.2.5	Principios de seguridad en la ingeniería de sistemas	SI	NO			X	
	14.2.6	Entorno de desarrollo seguro	SI	NO			X	
	14.2.7	Desarrollo tercerizado	SI	NO			X	
	14.2.8	Pruebas de seguridad del sistema	SI	NO			X	
	14.2.9	Pruebas de aceptación del sistema	SI	NO			X	
	14.3	Datos de prueba						
	14.3.1	Protección de datos de prueba	SI	NO			X	
15 Relaciones con Proveedores	15.1	Seguridad de la información en relaciones con el proveedor						
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	SI	NO		X		
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	SI	NO		X		
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	SI	NO			X	
	15.2	Gestión de entrega de servicios de proveedor						
	15.2.1	Monitoreo y revisión de servicios del proveedor	SI	NO		X		
	15.2.2	Gestión de cambios a los servicios del proveedor	SI	NO		X		
16 Gestión de Incidentes de Seguridad de la Información	16.1	Gestión de incidentes de seguridad de la información y mejoras						
	16.1.1	Responsabilidades y procedimientos	SI	NO			X	
	16.1.2	Reporte de eventos de seguridad de la información	SI	NO			X	
	16.1.3	Reporte de debilidades de seguridad de la información	SI	NO			X	

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	Sección	Objetivo de control / control						
	16.1.4	Valoración y decisión de eventos de seguridad de la información	SI	NO			X	
	16.1.5	Respuesta a incidentes de seguridad de la información	SI	NO			X	
	16.1.6	Aprendizaje de incidentes de seguridad de la información	SI	NO			X	
	16.1.7	Colección de evidencia	SI	NO			X	
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17.1	Continuidad de la seguridad de la información						
	17.1.1	Planeación de la continuidad de la seguridad de la información	SI	NO				X
	17.1.2	Implementación de la continuidad de la seguridad de la información	SI	NO				X
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	NO				X
	17.2	Redundancias						
	17.2.1	Disponibilidad de facilidades de procesamiento de información	SI	NO			X	
18 Cumplimiento	18.1	Cumplimiento con Requerimientos Legales y Contractuales						
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	SI	SI	X			
	18.1.2	Derechos de propiedad intelectual (IPR)	SI	NO	X			
	18.1.3	Protección de registros	SI	NO	X			
	18.1.4	Privacidad y protección de información personal identificable (PIR)	SI	NO	X			
	18.1.5	Regulación de controles criptográficos	SI	NO			X	
	18.2	Revisiones de seguridad de la información						
	18.2.1	Revisión independiente de seguridad de la información	SI	NO			X	
	18.2.2	Cumplimiento con políticas y estándares de seguridad	SI	NO			X	
	18.2.3	Revisión del cumplimiento técnico	SI	NO			X	

FICHA DE OBSERVACIÓN: INDICADOR NÚMERO DE CONTROLES APLICADOS
DECLARACIÓN DE APLICABILIDAD DE CONTROLES
FASE: POST TEST

La selección de controles y objetivos de control se realizaron a través de los siguientes criterios:

- LR: requerimientos legales
- CO: obligaciones contractuales
- BR/BP: requerimientos del negocio/mejores prácticas adoptadas

RRA: resultado de la valoración de riesgos

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	**Sección**	**Objetivo de control / control**						
5 Políticas de Seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información						
	5.1.1	Políticas de seguridad de la información	SI	SI			X	
	5.1.2	Revisión de las políticas de seguridad de la información	SI	SI			X	
6 Organización de la Seguridad de la Información	6.1	Organización interna						
	6.1.1	Roles y responsabilidad de seguridad de la información	SI	SI			X	
	6.1.2	Segregación de deberes	SI	SI			X	
	6.1.3	Contacto con autoridades	NO	NO				
	6.1.4	Contacto con grupos de interés especial	NO	NO				
	6.1.5	Seguridad de la información en la gestión de proyectos	SI	SI			X	
	6.2	Dispositivos móviles y teletrabajo						
	6.2.1	Política de dispositivos móviles	SI	SI			X	
	6.2.2	Teletrabajo	NO	NO				
7 Seguridad en los Recursos Humanos	7.1	Previo al empleo						
	7.1.1	Verificación de antecedentes	SI	SI				X
	7.1.2	Términos y condiciones del empleo	SI	SI				X
	7.2	Durante el empleo						
	7.2.1	Responsabilidades de la Alta Gerencia	SI	SI			X	
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	SI	SI				X
	7.2.3	Proceso disciplinario	SI	SI			X	
	7.3	Terminación y cambio de empleo						
	7.3.1	Termino de responsabilidades o cambio de empleo	SI	SI			X	
8 Gestión de Activos	8.1	Responsabilidad de los activos						
	8.1.1	Inventario de activos	SI	SI				X
	8.1.2	Propiedad de activos	SI	SI				X
	8.1.3	Uso aceptable de los activos	SI	SI			X	
	8.1.4	Devolución de activos	SI	SI			X	
	8.2	Clasificación de la información						
	8.2.1	Clasificación de la información	SI	SI				X
	8.2.2	Etiquetado de la información	SI	SI				X
	8.2.3	Manejo de activos	SI	SI			X	

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	Sección	Objetivo de control / control						
	8.3	Manejo de medios						
	8.3.1	Gestión de medios removibles	SI	SI				X
	8.3.2	Eliminación de medios	SI	SI				X
	8.3.3	Transporte de medios físicos	SI	SI				X
9 Control de Acceso	9.1	Requerimientos de negocio para el control de acceso						
	9.1.1	Política de control de acceso	SI	SI				X
	9.1.2	Acceso a redes y servicios de red	SI	SI				X
	9.2	Gestión de accesos de usuario						
	9.2.1	Registro y baja del usuario	SI	SI				X
	9.2.2	Provisión de acceso a usuarios	SI	SI				X
	9.2.3	Gestión de derechos de acceso privilegiados	SI	SI				X
	9.2.4	Gestión de información de autenticación secreta de usuarios	SI	SI				X
	9.2.5	Revisión de derechos de acceso de usuarios	SI	SI				X
	9.2.6	Eliminación o ajuste de derechos de acceso	SI	SI				X
	9.3	Responsabilidades del usuario						
	9.3.1	Uso de información de autenticación secreta	SI	SI			X	
	9.4	Control de acceso de sistemas y aplicaciones						
	9.4.1	Restricción de acceso a la información	SI	SI				X
	9.4.2	Procedimientos de inicio de sesión seguro	SI	SI				X
	9.4.3	Sistema de gestión de contraseñas	SI	SI				X
	9.4.4	Uso de programas y utilidades privilegiadas	SI	SI			X	
	9.4.5	Control de acceso al código fuente del programa	SI	SI				X
10 Criptografía	10.1	Controles criptográficos						
	10.1.1	Política en el uso de controles criptográficos	SI	SI				X
	10.1.2	Gestión de llaves	SI	SI			X	
11 Seguridad Física y del Entorno	11.1	Áreas seguras						
	11.1.1	Perímetro de seguridad físico	SI	SI				X
	11.1.2	Controles físicos de entrada	SI	SI			X	
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	SI	SI			X	
	11.1.4	Protección contra amenazas externas y del ambiente	SI	SI			X	
	11.1.5	Trabajo en áreas seguras	SI	SI			X	
	11.1.6	Áreas de entrega y carga	SI	SI			X	
	11.2	Equipo						
	11.2.1	Instalación y protección de equipo	SI	SI			X	
	11.2.2	Servicios de soporte	SI	SI			X	

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	Sección	Objetivo de control / control						
	11.2.3	Seguridad en el cableado	SI	SI				X
	11.2.4	Mantenimiento de equipos	SI	SI				X
	11.2.5	Retiro de activos	SI	SI			X	
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	SI	SI			X	
	11.2.7	Eliminación segura o reuso del equipo	SI	SI			X	
	11.2.8	Equipo de usuario desatendido	SI	SI			X	
	11.2.9	Política de escritorio limpio y pantalla limpia	SI	SI				X
12 Seguridad en las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades						
	12.1.1	Documentación de procedimientos operacionales	SI	SI				X
	12.1.2	Gestión de cambios	SI	SI				X
	12.1.3	Gestión de la capacidad	SI	SI				X
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	SI				X
	12.2	Protección de Software Malicioso						
	12.2.1	Controles contra software malicioso	SI	SI				X
	12.3	Respaldo						
	12.3.1	Respaldo de información	SI	SI				X
	12.4	Bitácoras y monitoreo						
	12.4.1	Bitácoras de eventos	SI	SI			X	
	12.4.2	Protección de información en bitácoras	SI	SI			X	
	12.4.3	Bitácoras de administrador y operador	SI	SI			X	
	12.4.4	Sincronización de relojes	SI	SI			X	
	12.5	Control de software operacional						
	12.5.1	Instalación de software en sistemas operacionales	SI	SI			X	
	12.6	Gestión de vulnerabilidades técnicas						
	12.6.1	Gestión de vulnerabilidades técnicas	SI	SI				X
	12.6.2	Restricciones en la instalación de software	SI	SI				X
	12.7	Consideraciones de auditoria de sistemas de información						
	12.7.1	Controles de auditoría de sistemas de información	SI	SI			X	
13 Seguridad en las Comunicaciones	13.1	Gestión de seguridad en red						
	13.1.1	Controles de red	SI	SI			X	
	13.1.2	Seguridad en los servicios en red	SI	SI				X

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	**Sección**	**Objetivo de control / control**						
	13.1.3	Segregación en redes	SI	SI				X
	13.2	Transferencia de información						
	13.2.1	Políticas y procedimientos para la transferencia de información	SI	SI			X	
	13.2.2	Acuerdos en la transferencia de información	SI	SI			X	
	13.2.3	Mensajería electrónica	SI	SI			X	
	13.2.4	Acuerdos de confidencialidad o no-revelación	SI	SI			X	
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de seguridad en sistemas de información						
	14.1.1	Análisis y especificación de requerimientos de seguridad	SI	SI			X	
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	SI	SI			X	
	14.1.3	Protección de transacciones en servicios de aplicación	SI	SI			X	
	14.2	Seguridad en el proceso de desarrollo y soporte						
	14.2.1	Política de desarrollo seguro	SI	SI			X	
	14.2.2	Procedimientos de control de cambios del sistema	SI	SI			X	
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	SI	SI			X	
	14.2.4	Restricción de cambios en paquetes de software	SI	SI			X	
	14.2.5	Principios de seguridad en la ingeniería de sistemas	SI	SI			X	
	14.2.6	Entorno de desarrollo seguro	SI	SI			X	
	14.2.7	Desarrollo tercerizado	SI	SI			X	
	14.2.8	Pruebas de seguridad del sistema	SI	SI			X	
	14.2.9	Pruebas de aceptación del sistema	SI	SI			X	
	14.3	Datos de prueba						
	14.3.1	Protección de datos de prueba	SI	SI			X	
15 Relaciones con Proveedores	15.1	Seguridad de la información en relaciones con el proveedor						
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	SI	SI		X		
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	SI	SI		X		
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	SI	SI			X	
	15.2	Gestión de entrega de servicios de proveedor						
	15.2.1	Monitoreo y revisión de servicios del proveedor	SI	SI		X		
	15.2.2	Gestión de cambios a los servicios del proveedor	SI	SI		X		
16	16.1	Gestión de incidentes de seguridad de la información y mejoras						

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	JUSTIFICACION DE LA APLICACIÓN			
					LR	CO	BR/BP	RRA
Cláusula	**Sección**	**Objetivo de control / control**						
Gestión de Incidentes de Seguridad de la Información	16.1.1	Responsabilidades y procedimientos	SI	SI			X	
	16.1.2	Reporte de eventos de seguridad de la información	SI	SI			X	
	16.1.3	Reporte de debilidades de seguridad de la información	SI	SI			X	
	16.1.4	Valoración y decisión de eventos de seguridad de la información	SI	SI			X	
	16.1.5	Respuesta a incidentes de seguridad de la información	SI	SI			X	
	16.1.6	Aprendizaje de incidentes de seguridad de la información	SI	SI			X	
	16.1.7	Colección de evidencia	SI	SI			X	
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17.1	Continuidad de la seguridad de la información						
	17.1.1	Planeación de la continuidad de la seguridad de la información	SI	SI				X
	17.1.2	Implementación de la continuidad de la seguridad de la información	SI	SI				X
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	SI				X
	17.2	Redundancias						
	17.2.1	Disponibilidad de facilidades de procesamiento de información	SI	SI			X	
18 Cumplimiento	18.1	Cumplimiento con Requerimientos Legales y Contractuales						
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	SI	SI	X			
	18.1.2	Derechos de propiedad intelectual (IPR)	SI	SI	X			
	18.1.3	Protección de registros	SI	SI	X			
	18.1.4	Privacidad y protección de información personal identificable (PIR)	SI	SI	X			
	18.1.5	Regulación de controles criptográficos	SI	SI			X	
	18.2	Revisiones de seguridad de la información						
	18.2.1	Revisión independiente de seguridad de la información	SI	SI			X	
	18.2.2	Cumplimiento con políticas y estándares de seguridad	SI	SI			X	
	18.2.3	Revisión del cumplimiento técnico	SI	SI			X	

ANEXO N° 5 – Tabla resumen para el indicador Nivel de Riesgo en fases Pre y Post Test

TABLA RESUMEN: INDICADOR: EVALUACIÓN DEL RIESGO				
FASES: PRE Y POST TEST				
N°	CÓDIGO ACTIVO	ACTIVOS	RIESGO PROMEDIO PRE TEST	RIESGO PROMEDIO POST TEST
1	A002	SISMUN	12.5	8.33
2	A005	Servidor Aplicaciones/BD (Sauce)	9.17	6.67
3	A009	Firewall	4.4	3.3
4	A004	SISMUN Fox	11.25	7.5
5	A010	Switch de Borde	5.67	2.5
6	A011	Switch de Distribución	5.67	2.5
7	A012	Switch Core	6.33	2.67
8	A029	Computadora de Escritorio (Técnico Liquidador de Fiscalización Tributaria)	8.67	5.5
9	A052	Subgerente de Informática	9.33	6
10	A003	SISMUN Web	7.5	5.88
11	A051	Computadora de Escritorio del Subgerente de Informática	7.88	6.38
12	A001	Analista Programador	8.94	2.33
13	A017	Supervisor de Plataforma	10	6
14	A026	Computadora de Escritorio (Técnico en Plataforma de Fiscalización Tributaria)	8.33	5.83
15	A044	Declaración Jurada de Predio Rustico	15.5	8
16	A046	Subgerente de Administración Tributaria	10	6
17	A048	Resolución de determinación predial - Fiscalización	12	7.5
18	A050	Hoja de Resumen de Declaración Jurada	10	6
19	A041	Subgerente de Fiscalización Tributaria	10	6
20	A043	Declaración Jurada de Predio Urbano	10	6
21	A047	Requerimiento de fiscalización	10	6
22	A049	Resolución de determinación de arbitrios - Fiscalización	12	7.5
23	A006	UPS de Switchs de Gabinete de Comunicación	7	6
24	A007	UPS de Switch Core	7	6
25	A008	UPS Servidor (Aplicaciones/BD)	7	6
26	A013	UPS (Analista Programador)	7	6
27	A028	Técnico Liquidador de Fiscalización Tributaria	10	8
28	A038	Técnico de Fiscalización Tributaria	10	8
29	A039	Técnico en Plataforma de Recaudación	10	8
30	A045	Estado de cuenta	10	6
31	A053	Cargo de Notificación de Fiscalización	10	6
NIVEL DE RIESGO			9.13	5.95

Fuente: Elaboración propia

ANEXO 6– Tabla resumen para el indicador Número de Controles Aplicados en fases Pre y Post Test

TABLA RESUMEN:					
INDICADOR: NÚMERO DE CONTROLES APLICADOS FASES: PRE Y POST TEST					
		TOTAL PRE TEST		TOTAL POST TEST	
N° CONTROLES QUE APLICAN	TOTAL	NO EXISTENTE	SI EXISTENTE	NO EXISTENTE	SI EXISTENTE
/EXISTEN SI APLICA /EXISTE	114	105	9	3	111
	100%	92.11%	7.89%	2.63%	97.37%
	DIFERENCIA			-89.47%	89.47%
NO APLICA	3				

Fuente: Elaboración propia

PLAN DE IMPLANTACION DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR EL PROCESO DE GESTIÓN DEL RIESGO EN UN GOBIERNO LOCAL, 2018.

DIAGNÓSTICO DE SEGURIDAD INFORMÁTICA

1. OBJETIVOS

1.1 Identificar el nivel de cumplimiento de la NTP ISO/IEC 27001:2014.

1.2 Revisar el nivel de efectividad de controles implementados.

2. ALCANCE

El alcance de la revisión se basa en los procesos de negocio:

- Inscripción de predios
- Fiscalización

Inscripción de predios: El ciudadano solicita a la Municipalidad de Carabayllo la inscripción del predio con documentación mínimo exigida por la Municipalidad y realiza un pago por la inscripción. La municipalidad hace entrega de un cronograma de pagos mensuales de tributos.

Fiscalización: Los fiscalizadores extraen del Sistema Sismun

3. PROCEDIMIENTOS REALIZADOS

Para el desarrollo de éste proyecto se han realizado las siguientes actividades:

3.1 Revisión de documentación

Se solicitó al área de tecnología los documentos relacionados al quehacer de los procesos en revisión. Se entregó la siguiente documentación, que fue revisada por el equipo consultor que crea el presente documento:

- Organigrama Municipal
- Documento de comité de seguridad de la información
- Plan Estratégico Municipal

3.2 Entrevistas al Personal

Se han desarrollado entrevistas con las personas encargadas de los procesos comprendidos en nuestro alcance:

- Jefe de TI
- Personal clave del proceso de Inscripción de predios
- Personal clave del proceso Fiscalización

Las entrevistas estuvieron orientadas a identificar los flujos de información y servicios de tecnología de los cuales dependen los procesos que ellos gestionan.

5. RESULTADOS DE DIAGNOSTICO

Se identificó que la Municipalidad de Carabayllo no cuenta con la siguiente información documentada obligatoria para el cumplimiento de la NTP ISO/IEC 27001:2014

- Alcance del SGSI (Clausula 4.3)
- Políticas y objetivos de seguridad de la información (Clausula 5.2, 6.2).
- Metodología de evaluación y tratamiento de riesgos (Clausula 6.1.2)
- Declaración de aplicabilidad (Clausula 6.1.3 d)
- Plan de tratamiento del riesgo (Clausulas 6.1.3.e, 6.2)
- Informe de evaluación de riesgos (Clausulas 8.2)
- Definición de funciones y responsabilidades de seguridad (Clausula A.7.1.2, A.13.2.4)
- Inventario de activos (Clausula A.8.1.1)
- Uso aceptable de los activos (Clausula A.8.1.3)
- Política de control de acceso (Clausula A.9.1.1)
- Procedimientos operativos para gestión de TI (Clausula A.12.1.1)
- Principios de ingeniería para sistema seguro (Clausula A.14.2.5)
- Política de seguridad para proveedores (Clausula A.15.1.1)
- Procedimiento para gestión de incidentes (Clausula A.16.1.5)
- Procedimientos de la continuidad del negocio (Clausula A.17.1.2)
- Requisitos legales, normativos y contractuales (Clausula A.18.1.1)

En la revisión no se identificó los siguientes registros mandatorios:

- Registros de capacitación, habilidades, experiencia y Calificaciones (Clausula 7.2).
- Resultados de supervisión y medición (Clausula 9.1)
- Programa de auditoría interna (Clausula 9.2)
- Resultados de las auditorías internas (Clausula 9.2)

- Resultados de la revisión por parte de la dirección (Clausula 9.3)
- Resultados de acciones correctivas (Clausula 10.1)
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (Clausulas A.12.4.1, A.12.4.3)

Sobre los controles NTP ISO/IEC 27001:2014:

- A.5 Política de Seguridad: No existe
- A.6 Organización de Seguridad: Si existe. Se definió la responsabilidad de Seguridad de la Información y del comité
- A.7 Seguridad de los Recursos Humanos: Si existe inducción y solicitud de antecedentes.
- A.8 Administración de Activos: No existe
- A.9 Control de Accesos: Si existe pero no es efectivo
- A.10 Criptografía: No existe
- A.11 Seguridad Física y Ambiental: Si existe pero no es efectivo
- A.12 Gestión de Operaciones: Solo existe estrategias de respaldo
- A.13 Seguridad de Comunicaciones: No existe
- A.14 Adquisición, Desarrollo y Mantenimiento de Sistemas de Información: No existe
- A.15 Relaciones con el proveedor: No existe

- A.16 Gestión de Incidentes de Seguridad de la Información: No existe
- A.17 Gestión de Continuidad del Negocio: No existe. Solo existe estrategias de respaldo.
- A.18 Cumplimiento: No existe

6. CONCLUSIONES

- Se concluye que el nivel de cumplimiento seguridad de la información basado en la NTP ISO/IEC 27001:2014 es **deficiente** no se cumple con la información documentada requerida no con los controles de seguridad mínimos requeridos.
- En la Municipalidad Distrital de Carabayllo se encontraron vulnerabilidades técnicas como resultado de las penetraciones externas que exponen a la Entidad ha ataques que pueden vulnerar la información procesada en su red interna. Se identificó que un atacante externo mediante Inyección SQL puede explotar la página web de la Municipalidad Distrital de Carabayllo.
- En la Municipalidad Distrital de Carabayllo en su análisis de controles, se pudo corroborar que no cuentan con controles adecuados que le permitan cumplir con los principios de Confidencialidad, Integridad y Disponibilidad de su información.
- En la Municipalidad Distrital de Carabayllo no posee procedimientos formalizados y estandarizados para la Gestión de Activos, Organización de Seguridad, Gestión de Cambios, Gestión de Operaciones, Gestión de Acceso, Seguridad Físico, Gestión de Proveedores, Gestión de Adquisición, Mantenimiento y Desarrollo de Sistemas, Gestión de Proveedores, Gestión de Gestión de Incidentes, Gestión de Continuidad de Negocio y Cumplimiento.

7. GLOSARIO

Amenaza: evento inesperado con el potencial para causar daños. Las fuentes comunes de amenazas son las personas, la naturaleza y el ambiente.

Análisis de riesgo: un uso sistemático de la información disponible para determinar cuan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

Consecuencia: el producto de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia. Podría haber un rango de productos posibles asociados a un evento.

Control de riesgos: la parte de administración de riesgos que involucra la implementación de políticas, estándares, procedimientos y cambios físicos para eliminar o minimizar los riesgos adversos.

Análisis de riesgos: el proceso utilizado para determinar las prioridades de administración de riesgos comparando el nivel de riesgo respecto de estándares predeterminados, niveles de riesgo objetivos u otro criterio.

Frecuencia: una medida del coeficiente de ocurrencia de un evento expresado como la cantidad de ocurrencias de un evento en un tiempo dado.

Gestión de riesgos: la cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos.

Identificación de riesgos: el proceso de determinar qué puede suceder, por qué y cómo.

Probabilidad: la probabilidad de un evento específico o resultado, medido por el coeficiente de eventos o resultados específicos en relación a la cantidad total de posibles eventos o resultados. La probabilidad se expresa como un número entre 0 y 1, donde 0 indica un evento o resultado imposible y 1 indica un evento o resultado cierto.

Proceso de gestión de riesgos: la aplicación sistemática de políticas, procedimientos y prácticas de administración a las tareas de establecer el

contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar riesgos.

Riesgo: la posibilidad de que suceda algo que tendrá un impacto sobre los objetivos. Se le mide en términos de consecuencias y probabilidades.

Vulnerabilidad: es una debilidad (vacío) que se puede activar accidentalmente o explotar intencionalmente.

Requerimientos de Seguridad de la Información- Alcance de Seguridad de la Información

1. Objetivo del documento

El objetivo de éste documento es definir el alcance de la seguridad de la información y los requisitos de seguridad de las partes interesadas.

2. Alcance

Este procedimiento aplica a los activos de información de los siguientes procesos críticos de Municipalidad Distrital de Carabayllo.

Procesos de Negocio	1. Inscripción de Predios 2. Fiscalización de Predios
Procesos de Soporte	3. Tecnologías de la Información

Sub Proceso de Inscripción de Predios, responsable de la inscripción de los predios de los contribuyentes en forma veraz y confiable por parte del responsable de la Subgerencia de Administración tributaria y recaudación.

Sub Proceso de Fiscalización de Predios, responsable de la fiscalización de los predios, validando y verificando si lo consignado por los contribuyentes está de acorde a lo declarado ante la Municipalidad, siendo responsabilidad de la Subgerencia de Fiscalización tributaria.

Para cada uno de los procesos críticos se ha identificado los servicios de TI de los cuales dependen y los activos de información que soportan dichos servicios:

3. Objetivo del SGSI

Proporcionar seguridad a la información que se maneja dentro de los procesos que se llevan a cabo en la MUNICIPALIDAD, sobre la base de la aplicación de la NTP ISO/IEC 27001:2014.

4. Partes Interesadas (Stakeholders)

El Sistema de Gestión de Seguridad de la Información es el punto de convergencia de varios entes interesados en la seguridad de la información del negocio y del éxito en la implementación del sistema, se han identificado y clasificado las partes interesadas o stakeholders en:

Stakeholders internos:

Comité de Seguridad de Información:

- Gerente Municipal
- Gerente de Fiscalización
- Gerente de Tributación
- Jefe de TI
- Oficial de Seguridad de la Información
- Empleados de la Municipalidad

Stakeholders externos:

- ONGEI
- Ministerio de Economía
- Contraloría
- Ciudadanía

Todos las partes interesadas deberán cumplir con todos los requisitos de seguridad, legales, regulatorios y obligaciones contractuales según sea el caso.

Recursos necesarios para Implementar el SGSI

1. Objetivos

1.1 Planificar los recursos necesarios para la implementación del SGSI.

1.2 Asignar los recursos necesarios para la implementación del SGSI.

1.3 Aprobar los recursos necesarios.

2. Recursos necesarios Implementar el SGSI

A continuación detallamos los recursos necesarios para la implementación del SGSI en aquellos proyectos identificados como resultado del Plan de Tratamiento de Riesgos, y que se listan a continuación:

Breve Descripción de Plan de Mitigación	Responsable	Recursos necesarios para implementar el SGSI
Proyecto: Documentar metodología de desarrollo, estándar de desarrollo funcional y seguro que sea aplicado por personal interno y por proveedores	Sistemas	Se necesitara contratar un servicio de consultoria para la elaboración de una metodología para el desarrollo de sistemas informáticos.
Proyecto: Implementar un sistema de continuidad de negocio que incluya análisis de impacto, tiempos de recuperación, estrategias de recuperación, planes de contingencia y pruebas	Sistemas	Se necesitara contratar un servicio de consultoria para la elaboración de una metodología para el desarrollo de sistemas informáticos.
Proyecto: documentar procedimiento de control de cambio operativo y capacitar sobre el mismo.	Sistemas	Se deberá elaborar un procedimiento de control de cambio operativo; asimismo, el mismo que deberá ser aprobado en forma formal y ser distribuido al personal informático para su conocimiento y aplicación.
Proyecto: Rediseño de gestión de acceso y programa de concientización	Sistemas	Se deberá elaborar un procedimiento de gestión de control de accesos, y además, elaborar un Programa de Concientización.
Proyecto: Capacitación en codificación segura y revisión de código	Sistemas	Se deberá contratar un servicio de capacitación en codificación segura y revisión de código.
Proyecto: Hardening o aseguramiento de servidores mediante buenas practicas NIST	Sistemas	Se deberá contratar un servicio de capacitación en buenas prácticas NIST para el personal informático.
Proyecto: Implementación de sistemas de certificados	Sistemas	Se deberá contratar el servicio de capacitacion para un sistema de certificación.
Segregar funciones de TI. Contratación de Personal.	Sistemas	Se deberá implementar la segregación de funciones del personal del ambiente de desarrollo, pruebas y producción, definiendo sus funciones a cada uno.
Contratación del CAS como Oficial de Seguridad de la Información para segregar funciones	Sistemas	Se debe generar la contratación de un Oficial de Seguridad de la Información, para lo cual se deberá generar las funciones a realizar por este personal.
Proyecto de “documentación de un sistema de gestión de seguridad de la información: políticas y procedimientos”	Sistemas	Se diseñará un documento denominado Política de Seguridad de la Información y sus procedimientos que sustenten las políticas definidas.

Breve Descripción de Plan de Mitigación	Responsable	Recursos necesarios para implementar el SGSI
Proyecto: Establecer políticas de password en sistemas de información bajo los mismo requisitos de la política de seguridad	Sistemas	Se deberá elaborar una Política para la gestión de los password en el acceso a los sistemas de información de acorde a los perfiles definidos.
Proyecto: Segregación de red TI y Administrativa	Sistemas	Se deberá generar un servicio de consultoria para la segregación de la red de Ti en la municipalidad.
Proyecto: Implementación de Sistema de Gestión de respaldo adquirido y establecer política de respaldo insite y offsite	Sistemas	a) Se deberá elaborar una Política de Respaldo y Restauración de la información definiendo la custodia de una copia de Respaldo fuera de la Municipalidad- b) Contratación de un servicio de custodia de una copia de Respaldo de la información fuera de la Municipalidad.
Proyecto: documentar procedimiento de control de cambio operativo y capacitar sobre el mismo.	Sistemas	a) Se deberá elaborar la generación de un Procedimiento para el control de cambio operativo. B) Se deberá diseñar la capacitación del procedimiento al personal involucrado en el control de cambios operativo.
Proyecto: Implementar un sistema manual o automatizado de control de versiones como SUBVERSION.	Sistemas	Se deberá contratar el servicio de adquisición de un sistema automatizado para el control de versionamiento de los sistemas de información.
Actualización del organigrama de TI y establecer un comité de seguridad de la información. El responsable de red debe monitorear tanto el firewall como las anomalías de red	Sistemas	Se deberá implementar una actualización del organigrama de TI de acorde a la segregación de funciones establecida en el área informática.
Proyecto: Adquisición e implementación de controles físicos para centro de datos (Cámaras, Controles ambientales)	Sistemas	Se deberá contratar el servicio de consultoria para la implementación de controles de seguridad del Centro de Datos de TI de la Municipalidad.
Proyecto: Adquisición e implementación de sistema de capacidad de servidores y aplicaciones (CPU, Memoria, Disco)	Sistemas	Se deberá contratar un servicio de consultoría para la adquisición e implementación de un sistema de capacidad de los servidores y aplicaciones.

DIAGRAMA

CRONOGRAMA DE IMPLEMENTACIÓN		
	INICIO	**FIN**
Implementación de controles del SGSI		
Definición de roles y responsabilidades de seguridad	2/02/2018	4/04/2018
Inventario de activos		
Uso aceptable de activos		
Plan de tratamiento de riesgos		
Controles de seguridad		
Política de control de acceso		
Políticas y procedimientos del SGSI		
Procedimientos operativos para la gestión de TI	5/04/2018	2/09/2018
Asegurar los principios de ingeniería del sistema		
Procedimiento para el control de documentos		
Política de seguridad del proveedor		
Política de dispositivos móviles (BYOD)		
Política de clasificación de la información		
Política de contraseñas		
Política de eliminación y destrucción		
Política clara de escritorio y pantalla clara		
Política de gestión del cambio		
Política de copia de seguridad		
Política de transferencia de información		
Dispositivo móvil y política de teletrabajo		
Controles para la gestión de registros		
Procedimiento para la acción correctiva		
Procedimientos para trabajar en áreas seguras		
Plan de continuidad del Negocio		
Procedimiento de gestión de incidentes	3/09/2018	20/012/2018
Procedimientos de continuidad del negocio		
Requisitos legales, reglamentarios y contractuales		
Análisis del impacto en los negocios		
Plan de ejercicios y pruebas		
Plan de mantenimiento y revisión		
Estrategia de continuidad del negocio		

ANEXOS

Capacitación a la alta gerencia

Capacitación al personal técnico


CETIS GROUP
www.cetis-group.com
Taller Seguridad de la Información
ISO/IEC 27001 para el personal de la
Subgerencia de Informática
Expositores:
Ing. Huangal Quiroz, Cristhian Pierre
Ing. Jara Mendoza, Omar Yino
ISO 27001

Capacitación al personal administrativo

Plan de Tratamiento de Riesgos

1. Objetivo

Fortalecer la implementación y desarrollo de las prácticas de la administración del riesgo en la Municipalidad Distrital de Carabayllo a través del adecuado tratamiento de los riesgos, controlando las situaciones que puedan impactar en el cumplimiento de la misión y los objetivos de la Municipalidad.

2. Objetivos Específicos

- Generar una visión sistémica acerca de la administración y evaluación de riesgos, consolidada en un ambiente de control adecuado a la Municipalidad distrital de Carabayllo.
- Continuar con el Direccionamiento Estratégico que fije la orientación clara y planeada de la gestión dando las bases para el adecuado desarrollo de las Actividades de Control.
- Proteger los recursos de la Municipalidad distrital de Carabayllo, resguardándolos contra la materialización de los riesgos de gestión y corrupción.
- Asegurar el cumplimiento de normas, leyes y regulaciones vigentes sobre administración del Riesgo.
- Involucrar y comprometer a todo el personal que labora en la Municipalidad Distrital de Carabayllo en la búsqueda de acciones encaminadas a prevenir y controlar los riesgos.
- Fomentar entre el personal la actitud preventiva encaminada a identificar, analizar su contexto y administrar los riesgos.

3. Alcance

El presente plan de tratamiento de riesgos aplica para la identificación, análisis, valoración, tratamiento, monitoreo, control y comunicación de los riesgos de gestión y de corrupción de los procesos del Sistema de Gestión Integrado de la Municipalidad Distrital de Carabayllo e incluye las políticas para la administración del riesgo.

4. Responsabilidades

Todos los funcionarios de la Municipalidad Distrital de Carabayllo, deben conocer y poner en práctica las disposiciones dadas por la presente guía.

5. Generalidades

Conocer la criticidad de los activos información que cada funcionario manipula a fin de darle el trato adecuado, de esta manera mitigando los riesgos de seguridad de la información que se puedan presentar en los mismos.

6. Políticas para el uso aceptable de los activos

1. Todas las actividades de administración y operación que se realicen en los activos de información deben ser orientadas a garantizar el correcto cumplimiento de la misión de la Municipalidad Distrital de Carabayllo.
2. Todos los funcionarios deben aplicar los controles de seguridad de la Información definidos en el Sistema de Gestión de Seguridad de la Información de la Municipalidad Distrital de Carabayllo para reducir los riesgos que afectan a la seguridad de la información.

7. Gestión del riesgo

La gestión de riesgos implica seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible. Un resultado del análisis de riesgos habrá sido el criterio para determinar cuáles van a ser los niveles de riesgo aceptables y en consecuencia, cuáles van a ser los niveles inaceptables y que por lo tanto son susceptibles de ser gestionados. La gestión de los riesgos tiene como objetivo reducir los riesgos que estén por

encima de los niveles aceptables, a niveles que puedan ser asumidos por la organización.

Una vez que conocemos los riesgos de la Municipalidad y decidido el tratamiento que se le va a dar para cada uno de los activos, se deben tomar acciones en consecuencia. Los cuatro tipos de tratamiento requieren de acciones de distinta naturaleza:

- **Mitigar el riesgo:** Reducirlo mediante la implantación de controles que reduzcan el riesgo a un nivel aceptable, implica seleccionar dichos controles, definir y documentar los métodos para ponerlos en marcha y gestionarlos.
- **Asumir el riesgo:** La Dirección asume el riesgo ya que está por debajo de un valor de riesgo aceptable, simplemente requiere que quede documentado que la dirección conoce y acepta estos riesgos. Los riesgos que se han asumido han de ser controlados y revisados periódicamente de cara a evitar que evolucionen y se conviertan en riesgos mayores.
- **Transferir el riesgo a un tercero:** Como por ejemplo, asegurando el activo que tiene el riesgo o subcontratando el servicio. Deben evaluarse las opciones y tomar las acciones pertinentes para ejecutar la opción escogida, en función del valor del activo y del coste de realizar esta transferencia (no sólo coste económico sino también los riesgos que conlleva esta transferencia en cuanto a la inclusión de un tercero).

- **Eliminar el riesgo:** Aunque no suele ser la opción más viable, ya que puede resultar difícil o demasiado costoso, si se cree posible o necesario, habrá que establecer los pasos para conseguirlo: eliminar el activo, eliminar el proceso o incluso el área de negocio que es la fuente del riesgo.

Seleccionar la opción de tratamiento del riesgo más adecuada consiste en equilibrar los costos y los esfuerzos de aplicación frente a los beneficios obtenidos, asimismo, es necesario considerar los aspectos legales y normativos en la respuesta que se dé al riesgo.

Mitigación del riesgo:

En el caso de se decida mitigar el riesgo, los pasos a seguir son:

1. Seleccionar los controles apropiados para los riesgos a los que se quiere hacer frente, en principio del Catálogo de Buenas Prácticas de la ISO/IEC 27002 (133 controles posibles), pero pueden añadirse otros que la organización considere necesario.
2. Implantar los controles para lo que deben desarrollarse procedimientos. Aunque sean controles tecnológicos deben desarrollarse para su instalación, uso y mantenimiento.
3. Verificar que los controles están correctamente implantados.
4. Establecer indicadores para saber en qué medida la implantación de los controles seleccionados reduce el riesgo a un nivel aceptable.

Los controles se seleccionarán e implementarán para minimizar en lo posible la posibilidad de que los riesgos detectados en el análisis de riesgos dañen los activos.

Existen dos grandes grupos de controles. Por un lado, los técnicos, tales como sistemas de cifrado, copias de seguridad, sistemas de detección de intrusos, actualizaciones de software, antivirus o cortafuegos, y por otro los organizativos que son medidas organizativas tales como la Política de Seguridad, procedimientos de uso de los sistemas de información para los usuarios, los planes de formación o los planes de continuidad del negocio.

ZONA DE RIESGO	COLOR	OPCIONES DE TRATAMIENTO DE RIESGOS			
		Evitar	Reducir	Compartir o transferir	Asumir
Inaceptable	**Rojo**	X	X	X	
Importante	**Naranja**	X	X	X	
Tolerable	**Amarillo**	X	X	X	X
Aceptable	**Verde**				X

Cuadro 1: Opciones de tratamiento de riesgos de acuerdo con la zona de ubicación.

Nota 1: Cuando no se definen acciones para riesgos ubicados en zona tolerable, la opción de tratamiento es asumir.

Valoración del riesgo para cada uno de los activos.

A continuación, se presenta una matriz de la valoración del riesgo según cada activo informático en él se analiza en cada activo su clasificación, la clasificación del riesgo, la manera como se presenta, la valoración del riesgo y dentro de él probabilidad, impacto y riesgo determinando una aplicación de controles y el riesgo residual.

Para entender la matriz se deben tener en cuenta las siguientes tablas:

Estimación de probabilidad

TABLA PARA ESTIMAR LA PROBABILIDAD	
Valor	**Descripción**
Muy bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Bajo (2)	La amenaza se materializa a lo sumo una vez cada semestre.
Medio (3)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (4)	La amenaza se materializa a lo sumo una vez cada semana.
Muy alto (5)	La amenaza se materializa a lo sumo una vez cada día.

Estimación del impacto

TABLA PARA ESTIMAR EL IMPACTO	
Valor	**Descripción**
Muy bajo (1)	Riesgo que puede tener un pequeño o nulo efecto en la institución.
Bajo (2)	Causa un daño en el patrimonio o imagen, que se puede corregir en el corto tiempo, y no afecta el cumplimiento de los objetivos estratégicos.
Medio (3)	Causaría, ya sea una pérdida importante en el patrimonio, incumplimientos normativos, problemas operativos o de impacto ambiental o un deterioro significativo de la imagen. Además, se referiría una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños.
Alto (4)	Dañaría significativamente el patrimonio, incumplimientos normativos, problemas operativos o impacto ambiental o deterioro de la imagen o logro de objetivos institucionales. además, se referiría a una cantidad importante de tiempo de la alta dirección en investigar y corregir los daños.
Muy alto (5)	Influye directamente en el cumplimiento de la misión, pérdida patrimonial incumplimientos normativos, problemas operativos o de impacto ambiental o deterioro de la imagen, dejando además sin funcionar totalmente o por un periodo importante de tiempo los programas o servicios que entrega la institución.

Tipos de impacto:

- Impacto financiero
- Reputacional o legal

Identificar fuentes generadoras de riesgo que puedan afectar el cumplimiento de los objetivos planteados para los procesos (PECB, 2008).

1. Recurso humano
2. Externo
3. Infraestructura
4. Medioambiental
5. Operativo
6. Tecnológico

Para determinar la valoración del riesgo en cada uno de los activos se debe tener en cuenta la tabla de valoración del riesgo mostrada a continuación la cual ha sido elaborada teniendo en cuenta las 5 dimensiones de valoración del riesgo.

Tabla: Análisis del riesgo

Probabilidad (Posibilidad / Frecuencia / Amenaza)										
	Muy Alto	5	20%	5	40%	10	60%	15	80%	20	100%	25
	Alto	4	16%	4	32%	8	48%	12	64%	16	80%	20
	Medio	3	12%	3	24%	6	36%	9	48%	12	60%	15
	Bajo	2	8%	2	16%	4	24%	6	32%	8	40%	10
	Muy Bajo	1	4%	1	8%	2	12%	3	16%	4	20%	5
	Valoración		1		2		3		4		5	
			Muy Bajo		Bajo		Medio		Alto		Muy Alto	
			Impacto (Consecuencia / Daño / Pérdida)									

Tabla: Guía de valoración del riesgo

IMPACTO						
	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	8	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
	PROBABILIDAD					

MUY ALTO
ALTO
MEDIO
BAJO

Una vez analizadas las vulnerabilidades se establece la valoración del riesgo, esto permitirá definir la aplicación de controles ISO 27001 – 27002 los cuales tendrán un nivel de eficacia según la tabla que se muestra a continuación:

ZONA DE RIESGO	
Valor	**Descripción**
Bajo (1)	Riesgos de baja exposición y severidad, para lo cual se recomienda monitoreo permanente
Medio (2)	Dada su menor intensidad, se recomienda que estos riesgos sean gestionados en niveles básicos de la Municipalidad, pero con supervisión directa del responsable
Alto (3)	Riesgos que requieren de controles y alertas permanentes que permitan su gestión constante
Muy Alto (4)	Riesgos de alta severidad y exposición, para los cuales se deben implementar sistemas de control para su adecuado tratamiento, los cuales por su importancia y criticidad son de máxima prioridad para la Municipalidad

Tabla: Eficacia del control

EFICIENCIA DE CONTROL	
Alto	4
Medio	3
Bajo	2
Inexistente	1

Tras la implementación de controles y aplicación de los mismos se genera una mitigación del riesgo, lo anterior significa que el riesgo no ha sido erradicado por completo por lo que se genera una valoración de riesgo residual.

Tabla: Valoración del riesgo residual.

VALORACIÓN DEL RIESGO RESIDUAL	
NIVEL DEL RIESGO RESIDUAL	**CALIFICACIÓN**
INACEPTABLE	>16
IMPORTANTE	11 a 15
MODERADO	6 a 10
TOLERABLE	2 a 5
ACEPTABLE	<2

Teniendo en cuenta lo anterior a continuación se relaciona la matriz de valoración del riesgo por activo informático.

Para calcular o estimar el valor o calificación del riesgo residual tendremos la siguiente formula:

$$Riesgo\ residual = \frac{Valor\ del\ riesgo\ inherente}{Valor\ eficacia\ del\ control}$$

8. Tratamiento del Riesgo

TRATAMIENTO DEL RIESGO	
Acción	**Descripción**
Evitar	Implica tomar medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los procesos se genera cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
Reducir	Implica tomar medidas encaminadas a disminuir tanto la probabilidad como el impacto, a través de la optimización de los procedimientos y la implementación de controles eficientes, eficaces y efectivos.
Compartir o Transferir	Implica reducir su efecto a través de posibles impactos a otras organizaciones, como el caso de los seguros o a través de otros medios que permitan distribuir una porción del riesgo con otra entidad.

Asumir	Una vez el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el comité de Seguridad de la Información o de Riesgos, puede aceptar el riesgo residual.

Anexo N° 7– Políticas de seguridad de la información

<table>
<tr><td> 
</td><td colspan="2">DOCUMENTOS</td></tr>
<tr><td rowspan="3">POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN DE LA “MUNICIPALIDAD DISTRITAL DE CARABAYLLO”</td><td>CÓDIGO:</td><td>VERSIÓN:</td></tr>
<tr><td>FECHA:</td><td>PÁGINA:</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td></td><td colspan="2">Revisado por: Jara Mendoza Omar Yino</td></tr>
</table>

1. Introducción

La política de seguridad de la información es el pilar fundamental del Sistema de Gestión de Seguridad de la Información (SGSI) en una organización, la administración establece un programa de seguridad, las metas del programa, asigna responsabilidades, muestra el valor estratégico y táctico de la seguridad y describe cómo se debe llevar a cabo la ejecución. A partir de ellas se pueden desarrollar procedimientos detallados y guías de acción para casos de brechas y violaciones de seguridad.

Las políticas tratan los aspectos de manera genérica y dan base a las normas, las cuales hacen referencia específica a tecnologías, metodologías, procedimientos de implementación y otros aspectos de detalle, además las políticas pueden servir para evitar responsabilidades legales, ya que permiten aplicar controles para evitar contingencias de negligencia o violación de confidencialidad, fallas en el uso de medidas de seguridad, mala práctica, contra personas particulares u organizaciones que podrían reclamar por daños o perjuicios.

La implementación de las políticas en la MUNICIPALIDAD DISTRITAL DE CARABAYLLO, tiene como propósito reducir el riesgo, que en forma accidental o intencional se divulgue, modifique, destruya o use de manera indebida la información crítica de la institución. Al mismo tiempo las políticas habilitan a las áreas responsables de la administración de seguridad en orientar y mejorar la gestión de los activos de información y proveer las bases para el monitoreo a través de toda la institución.

2. Propósito

Las políticas de Seguridad de la Información que se enuncian se alinean al objetivo estratégico Nº 4 (OE 4) del Plan de Desarrollo Local Concertado del Distrito de

Carabayllo al 2021, dando cumplimiento a la Resolución Ministerial Nº 004-2016 – PCM, cuyos propósitos son:

1. Comprometer a toda la organización con la seguridad de la información, desde la alta dirección de funcionarios hasta el personal de todas las unidades orgánicas y proveedores. La política de seguridad de la información proporciona las reglas, responsabilidades y requerimientos para salvaguardar la información.
2. Proteger los recursos de información de la Municipalidad Distrital de Carabayllo y la tecnología utilizada para su procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.
3. Asegurar la implementación de las medidas de seguridad comprendidas en esta política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.
4. Mantener la política de seguridad actualizada de la Municipalidad Distrital de Carabayllo, a efecto de asegurar su vigencia y nivel de eficacia.

3. Alcance

Esta Política de Seguridad de la Información aplica a los activos de información de los siguientes procesos críticos de LA MUNICIPALIDAD DISTRITAL DE CARABAYLLO.

Procesos de Negocio	1. Inscripción de Predios 2. Fiscalización de Predios
Procesos de Soporte	3. Gestión de la Tecnología Informática

Proceso de Inscripción de Predios, responsable de la inscripción de los predios de los contribuyentes en forma veraz y confiable por parte del responsable de la Subgerencia de Administración Tributaria y Recaudación.

Proceso de Fiscalización de Predios, responsable de la fiscalización de los predios, validando y verificando, si lo consignado por los contribuyentes está acorde a lo declarado ante la Municipalidad Distrital de Carabayllo, siendo responsabilidad de la Subgerencia de Fiscalización Tributaria.

Proceso de Gestión de la Tecnología Informática, responsable de el uso apropiado de los dispositivos tecnológicos (computadoras de escritorio, portátiles, etc.), recursos administrativos, personal, suministro de energía, servicios como internet y correo electrónico, brindando al personal pautas para la utilización apropiada de dichos recursos, permitiendo así minimizar los riesgos de una eventual pérdida de información sensible de la institución.

4. Público Objetivo

Esta política deberá ser aplicada por todo el personal, terceros (contratistas y/o proveedores), responsables de los activos de información de los procesos involucrados en las unidades orgánicas de la Municipalidad Distrital de Carabayllo.

5. Políticas

5.1. Política de Seguridad de Información

La Política de Seguridad de la Información la constituye el presente documento y define los lineamientos que deben cumplir el personal y terceros (contratistas y/o proveedores) de la Municipalidad Distrital de Carabayllo, con el fin de establecer adecuados niveles de confidencialidad, integridad y disponibilidad en la información.

El comité de seguridad de la información de la Municipalidad Distrital de Carabayllo debe aprobar, comunicar, publicar y mantener el presente documento de políticas de la seguridad de la información.

La Política de Seguridad de la Información debe ser comunicada en forma efectiva y relevante a todo el personal de la MUNICIPALIDAD DISTRITAL DE CARABAYLLO, y a los terceros que se relacionen a través de los contratos y/o acuerdos que formalicen el vínculo.

5.2. Revisión de la Política de Seguridad de la Información

La Política de Seguridad de la Información debe ser revisada para asegurar su aplicabilidad, suficiencia, efectividad y actualización. Esta actualización también es necesaria en caso de que existan nuevas exigencias regulatorias en la materia o en caso de un cambio significativo dentro de la Municipalidad Distrital de Carabayllo.

Las revisiones de la política deben incluir:

a) El proceso de mejora continua, considerando el comportamiento del proceso de seguridad en marcha, tales como datos históricos, estadísticas, acciones correctivas y preventivas realizadas, incumplimientos, incidentes de seguridad y recomendaciones según la normatividad vigente.
b) El enfoque de gestión para responder adecuadamente a los cambios organizacionales, circunstancias políticas y sociales, condiciones legales y/o la evolución tecnológica y del conocimiento.

Las revisiones de la política pueden resultar en decisiones y acciones tendientes a:

a) Mejorar la forma en la que Municipalidad Distrital de Carabayllo administra el proceso de seguridad.
b) Perfeccionar las Directivas de seguridad y los controles.
c) Optimizar la asignación de recursos y/o responsabilidades.

El comité de seguridad de la información debe efectuar, como mínimo, una revisión por año, y toda vez que se identifique la ocurrencia de cambios significativos y debe emitir un informe a la alta dirección.

5.3. Organización y Gestión de la Seguridad de la Información

5.3.1. Roles y Responsabilidades en seguridad de la información

La Municipalidad Distrital de Carabayllo constituye el **"Comité de Gestión de Seguridad de la Información"**, el cual estará integrado por los siguientes funcionarios:

- Gerente Municipal
- Gerente de Administración y Finanzas
- Gerente de Planeamiento, Presupuesto y Cooperación Internacional
- Sub Gerente de Informática
- Gerente de Asesoría Jurídica
- El Oficial de Seguridad de la Información

5.3.2. Oficial de Seguridad de la Información

La Municipalidad Distrital de Carabayllo establece y designa el rol del Oficial de Seguridad de la Información, quien debe liderar todas las iniciativas relacionadas a la seguridad de la información.

5.3.3. Comité de Gestión de la Seguridad de la Información

Establecen reuniones periódicas para:

- Asegurar el cumplimiento de la política de seguridad de la información.
- Coordinar y Monitorear la implementación de los controles de seguridad de la información.
- Desarrollar actividades de concienciación y capacitación en seguridad de la información.
- Evaluar los incidentes de seguridad de la información y recomendar las acciones apropiadas.

5.4. Política de dispositivos móviles

Se deben establecer las normas y las medidas de seguridad que se deben aplicar al uso de los dispositivos móvil.

La existencia de usuarios remotos y el uso de computadoras portátiles que contengan información de la Municipalidad Distrital de Carabayllo deben tener la aprobación del Subgerente de Informática. Las computadoras portátiles asignadas al personal de la Municipalidad Distrital de Carabayllo deben ser configuradas con los controles técnicos de seguridad al igual que las estaciones de trabajo.

El Comité de Seguridad de la Información debe definir y documentar las normas y procedimientos para el uso de los dispositivos móviles, tomando en cuenta las siguientes consideraciones:

a) Evaluar los riesgos de trabajar con equipos de computación móvil en entornos no protegidos.
b) Requerimientos de
c) protección física de los equipos.
d) Requerimientos especiales en el control de acceso.
e) Utilización de sistemas criptográficos.
f) Respaldo de la información y las aplicaciones.
g) Protección contra el malware.
h) Reglas y advertencias para la conexión de dispositivos móviles a las redes públicas y privadas.
i) Reglas y normas de uso de dispositivos móviles en sitios públicos
j) Capacitación de los usuarios que utilice computación móvil

5.5. Teletrabajo

Establecer las medidas de seguridad para la protección de los activos de información accedidos, procesados o almacenados desde los accesos habilitados para realizar trabajo fuera de la oficina, y que resulten de la evaluación de los riesgos.

5.6. Politica de Seguridad del Personal

Esta politica se aplica a todo el personal de la Municipalidad Distrital de Carabayllo, terceros (contratistas y/o proveedores), que efectúen tareas dentro del ámbito de la Municipalidad.

El responsable del areá de Recursos Humanos, incluirá las funciones relativas a la seguridad de la información en las descripciones del personal e informará a los mismos cuando se establezca el vinculo laboral, respecto del cumplimiento de la politica de seguridad de la información, gestionará los compromisos de

confidencialidad con el personal y coordinará las tareas de capacitación de usuarios respecto de la presente política.

El comite de seguridad de la información es responsable de implementar los medios y canales necesarios para que el oficial de seguridad de la información, maneje los reportes de incidentes y anomalías de los sistemas. Asi mismo dicho comite tomará conocimiento, efectuará el seguimiento de la información, controlará la evolución e impulsará la solución de los incidentes relativos a la seguridad.

El funcionario responsable de la Gerencia de Asesoria Legal, participará en la elaboración del compromiso de confidencialidad a firmar por el personal de la Municipalidad Distrital de Carabayllo, terceros (contratistas y/o proveedores), que desarrollen funciones en la Municipalidad, en el asesoramiento sobre las sanciones que deben ser aplicadas por incumplimiento de la presente politica y en el tratamiento de incidentes de seguridad que requieran su intervención.

5.6.1. Política antes de la contratación de personal

La Subgerencia de Recursos Humanos establece la necesidad de verificar los antecedentes de las personas que sean contratados para laborar en la Municipalidad Distrital de Carabayllo. En ese sentido se establece la necesidad de solicitar los siguientes documentos:

- Certificado de antecedentes penales y policiales
- Copias de los certificados de educación superior. En caso de practicantes presentar constancia de estudios vigente.
- Copias de los certificados laborales de los trabajos anteriores

Como parte del proceso de ingreso de una persona a laborar en la institución, ésta debe firmar un Acuerdo de Cumplimiento de la Seguridad de Información.

Los funcionarios deberán asegurar que todo el personal, terceros (contratistas y/o proveedores) bajo su área de responsabilidad:

a) Están apropiadamente capacitados en sus roles y responsabilidades de seguridad en el contexto de la labor que desempeñan.
b) Están motivados para satisfacer la Política de Seguridad de la Información.
c) Conforman los términos y condiciones de empleo.
d) Mantienen las aptitudes y calificaciones apropiadas.

5.6.2. Politica durante el periodo laboral del personal

El comité de Seguridad de la Información y el Subgerente de Recursos Humanos deben planificar las actividades de concienciación, capacitación, entrenamiento y actualización en materia de seguridad de la información, para asegurar que no se rompa el esquema de seguridad debido a falta de capacitación o desconocimiento del SGSI.

Los derechos y obligaciones del personal relativos a la Seguridad de la Información, por ejemplo en relación con las leyes de Propiedad Intelectual o la legislación de protección de datos, se encontrarán aclarados e incluidos en los términos y condiciones de empleo.

El personal que labora en la institución debe firmar una vez al año, un Acuerdo de Cumplimiento de la Seguridad de Información.

Los procesos disciplinarios, en caso de incumplimiento de la política, deben ser contemplados en una DIRECTIVA aprobada por la Alta Dirección, que considere como mínimo las siguientes faltas:

Tipo de Falta	Faltas
Faltas Leves	• Utilización de internet para acceder a páginas web no apropiadas en el contexto laboral (contenido para adultos, sitios de entretenimiento, música y video en demanda, etc.). • Instalar software no autorizado en las computadoras personales asignadas (freeware, shareware, juegos, etc).
Faltas Moderadas	• Utilización del correo electrónico para envío de cadenas, mensajes publicitarios, bromas.

	• No reportar incidentes de seguridad de información (accesos no autorizados, virus, uso inapropiado de la información, etc.)
Faltas Graves	• Divulgación de las contraseñas de acceso a algún sistema de información o a cualquier otra plataforma computacional de la Municipalidad. • Divulgación de información de la institución a terceros sin la autorización correspondiente. • Utilización de cuentas de usuario que no le hayan sido asignadas (usurpación de identidad) para acceder a los sistemas de información o a cualquier otra plataforma computacional de la Municipalidad. • Pérdida de computadora portátil u algún otro medio de almacenamiento externo con información de la Municipalidad. • Acciones que comprometan la integridad de la información (Borrado, alteración de los datos) sin autorización.

5.6.3. Politica de la salida del personal de la institución

Se deben definir y asignar con claridad las responsabilidades ante la finalización o cambio de las relaciones contractuales con el personal, terceros (contratistas y/o proveedores).

Las responsabilidades y obligaciones subsistentes con posterioridad a la culminación del vínculo laboral, deben estar incluidas en los contratos del personal, terceros (contratistas y/o proveedores).

El cambio de responsabilidad o empleo dentro del ámbito de Municipalidad Distrital de Carabayllo no significa que deban superponerse los privilegios de ambas funciones, sino que debe manejarse como la finalización de una responsabilidad y el inicio de una nueva bajo los términos de los controles de la Declaración 5.6.1.

El Subgerente de Recursos Humanos debe coordinar con los funcionarios responsables de las unidades orgánicas donde se desempeñen los que

egresan, las responsabilidades y obligaciones establecidas en los acuerdos y contratos correspondientes.

La terminación del contrato de trabajo del personal exige el llenado de un formato de entrega de cargo que asegure la entrega de activos y remoción de los accesos a los sistemas de información de la Municipalidad Distrital de Carabayllo.

5.7. Política de Uso Aceptable de los Activos

Esta política se aplica a todos los activos de información administrados en la Municipalidad Distrital de Carabayllo, cualquiera sea su forma (físico y/o lógico) en que se encuentre, a fin de cumplir lo siguiente:

a) Garantizar que los activos de información reciban un apropiado nivel de protección
b) Clasificar la información para señalar su sensibilidad y criticidad
c) Definir niveles de protección y medidas de tratamiento especial acordes a su clasificación

El oficial de seguridad es el responsable de asegurar que, para la utilización de los activos contemplen los requerimientos de seguridad establecidos según la criticidad de la información que procesan.

5.7.1. Inventario de activos

Todos los funcionarios de la Municipalidad Distrital de Carabayllo en conjunto con el oficial de la seguridad de la información deben identificar e inventariar todos los activos significativos bajo su custodia y que estén bajo su responsabilidad.

Los funcionarios deben mantener plena responsabilidad sobre los activos asignados y validar el inventario con una periodicidad no mayor a 1 año.

5.7.2. Propiedad de los activos

Los activos identificados en el inventario de activos deben poseer un propietario.

Se reconoce como propietario a todo funcionario que posee responsabilidad administrativa aprobado por la Municipalidad Distrital de Carabayllo, para controlar el uso y seguridad de los activos.

5.7.3. Devolución de los activos

Todos los empleados y usuarios de las partes externas devolverán todos los activos de la organización en su poder al finalizar su empleo, contrato o acuerdo.

- Se debe contar con la aprobación del responsable de la unidad para devolver un activo fijo a Control Patrimonial.
- En caso el activo se encuentre en condiciones reutilización, Control Patrimonial coordinará con la sección Compras la posibilidad de reasignación a otra unidad.
- Control Patrimonial gestionará la baja del activo fijo recibido si por sus condiciones ya no puede ser reasignado para su uso en otras unidades.

5.7.4. Clasificación de los Activos

Los propietarios de los activos, son los responsables de clasificar, documentar y actualizar el nivel de criticidad de los mismos, indicando el nivel de riesgo existente para la Municipalidad, así como las medidas apropiadas de control que deben asociarse a las clasificaciones

Los propietarios de los activos deben clasificar según la confidencialidad, integridad y disponibilidad de los mismos.

Solo los propietarios de los activos pueden asignar o cambiar el nivel de criticidad y sensibilidad de los activos.

5.7.5. Etiquetado de los activos

Los activos se etiquetan de acuerdo al nivel de confidencialidad, lo mismo que se aplica a los recursos de información tanto en formato físico como electrónico.

5.7.6. Manipulado de los activos

Deben definirse procedimientos para la manipulación de los activos, de acuerdo con el esquema de clasificación definido. Los mismos deben contemplar los recursos de información tanto en formatos físicos como electrónicos.

Los medios considerados incluyen:

a) Información impresa

b) Información en pantalla

c) Información almacenada (discos portátiles, CDs, DVDs, USBs etc)

d) Mensajes electrónicos

e) Transferencia de archivos

f) Fax

g) Envío postal

5.8. Política de autenticación

La Sub Gerencia de Informática de la Municipalidad Distrital de Carabayllo será responsable del acceso a los sistemas de información internos y externos, equipos electrónicos, unidades y servicios de red, basados en un modelo de acceso por roles, mediante la identificación y puede clasificar de la siguiente manera:

- Algo que el usuario conoce (por ejemplo: una clave de identificación)
- Algo que el usuario posee (por ejemplo: una tarjeta)
- Algo que el usuario es (por ejemplo: características biométricas)

5.9. Política de Control de acceso

La Sub Gerencia de Informática de la Municipalidad Distrital de Carabayllo será responsable de que el acceso a los sistemas de información internos y externos, equipos electrónicos, unidades de red y servicios de red estarán basados en un Modelo de acceso por roles y por medio de la identificación de cuentas con usuario y contraseñas personales e intransferibles.

5.9.1. Administración de accesos de usuarios

Se implementaran procedimientos formales para controlar la asignación de derechos de acceso a los sistemas, datos y servicios de información

5.9.2. Registro de usuarios

El Subgerente de Informática de la Municipalidad Distrital de Carabayllo definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario.

5.9.3. Administración de privilegios

Se limitará y controlara la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios del sistema resulta frecuentemente el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos

no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

5.9.4. Administración de contraseñas de usuarios

La asignación de contraseñas se controlara a través de un proceso de administración formal.

5.9.5. Revisión de derechos de acceso de usuarios

Al fin de mantener un control eficaz del acceso a los datos y servicios de información, el responsable del área de TI, llevará acabo un proceso formal de no mayor a cuatro meses, a fin de revisar los derechos de acceso de los usuarios.

5.9.6. Responsabilidades del usuario

5.9.6.1. Uso de contraseñas

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas. Las contraseñas constituyen un medio de validación y autenticación de la identidad de un usuario, y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información. Los usuarios deben cumplir las directivas que se impartan a tal efecto.

5.9.6.2. Acceso a los servicios de red

Se controlará el acceso a los servicios de red tanto internos como externos. El Subgerente de Informática de la Municipalidad de Carabayllo tendrá a cargo el otorgamiento de accesos a los servicios y recursos de red, únicamente de acuerdo al pedido formal del titular de una unidad orgánica que lo solicite para personal de su incumbencia.

5.9.6.3. Acceso a Internet

El acceso a Internet será utilizado con propósitos autorizados o con el destino por el cual fue provisto. El responsable de seguridad informática definirá procedimientos para solicitar y aprobar accesos a internet. Los accesos serán autorizados formalmente por el Responsable de la unidad orgánica a cargo del personal que lo solicite. Asimismo, se definirán las pautas de utilización de internet para todos los usuarios.

5.9.6.4. Limitación del Horario de conexión

Se implementara un control de esta índole para aplicaciones informáticas sensibles especialmente aquellas terminales instaladas en ubicaciones de alto riesgo

5.9.6.5. Registro de eventos

Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha, hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema, acceso a datos y otros recursos.

5.9.6.6. Sincronización de Relojes

A fin de garantizar la exactitud de los registros de auditoría, al menos los equipos que realicen estos registros, deberán tener una correcta configuración de sus relojes para ello, se dispondrá de un procedimiento de ajuste de relojes, el cual indicará también la verificación de los relojes contra una fuente externa del dato y la modalidad de corrección ante cualquier variación significativa.

5.10. Política de computación móvil

Se desarrollaran procedimientos adecuados para estos dispositivos, que abarquen la protección física necesaria, el acceso seguro a los dispositivos, la

utilización de los dispositivos en lugares públicos, el acceso a los sistemas de información y servicios de la Municipalidad de Carabayllo a través de dichos dispositivos, las técnicas criptográficas a utilizar para la transmisión de información clasificada, los mecanismos de resguardo de la información contenida en los dispositivos y la protección contra software malicioso.

5.11. Política de backup

La Municipalidad Distrital de Carabayllo establece que todos los días se deben ejecutar obligatoriamente una copia de respaldo total de las bases de datos en producción. Las copias diarias deben de mantenerse en un lugar alejado del centro de cómputo; mensualmente se debe mantener una copia de respaldo off-site, asimismo de las fuentes de los sistemas cada vez que exista una modificación y actualización.

5.12. Política de datos confidenciales

La Municipalidad Distrital de Carabayllo debe adoptar medidas que aseguren razonablemente la privacidad de la información que reciben de los contribuyentes y administrados, conforme a la ley N° 29733 (ley de protección de datos personales).

En circunstancias muy excepcionales, la Municipalidad Distrital de Carabayllo podría verse en la obligación legal de comunicar información confidencial, si dicha información es necesaria para identificar, detener o colaborar con una acción judicial contra cualquier individuo que pudiera perjudicar, intencionalmente o no:

a) Los derechos o la propiedad de la Municipalidad.
b) A otros contribuyentes o administrados de la Municipalidad.

A cualquier otra persona que podría verse penalizada por dichas actividades.

5.13. Política de cifrado

Se utilizarán sistemas y técnicas criptográficas para la protección de la información en base a un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

5.13.1. Política de Utilización de controles criptográficos

Se utilizan controles criptográficos en los siguientes casos:

- Para la protección de claves de acceso a sistemas, datos y servicios.
- Para la transmisión de información clasificada, fuera del ámbito del Organismo.

Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el propietario de la información y el Oficial de seguridad

5.14. Política de Correo Electrónico

El responsable de la Sub Gerencia de Informática definirá y documentara normas y procedimientos claros con respecto al uso de correo electrónico y debe ser aprobado como parte del proceso de concesión de accesos.

La Municipalidad Distrital de Carabayllo establece que el uso del correo electrónico de la institución debe limitarse exclusivamente a temas laborales.

5.15. Política de Internet

La Municipalidad Distrital de Carabayllo establece que el uso del internet debe limitarse a temas laborales. En ese sentido queda establecido que el usuario está sujeto a monitoreo de sus actividades en internet.

5.16. Política de Proveedores o Contratistas

Es responsabilidad del subgerente de Informática que las conexiones a la red de la institución por parte de proveedores o contratistas sean autorizadas.

La Gerencia de Asesoría Jurídica es responsable de los contratos que se suscriban entre la Municipalidad Distrital de Carabayllo y los proveedores o contratistas, estos deberán incluir el acuerdo para cumplir las Políticas de Seguridad de la Información y una cláusula de confidencialidad de la información a la que tienen acceso.

Los funcionarios de la municipalidad son responsables de que los proveedores llenen un formulario, cuando estos soliciten el uso o acceso a un activo de la Municipalidad Distrital de Carabayllo, este formulario deberá contener como mínimo lo siguiente:

a) El tipo de acceso requerido (físico/lógico y a que activo)
b) Los motivos para los cuales se solicita el acceso
c) El valor de la información
d) Los controles empleados por la tercera parte
e) La incidencia de este acceso en la seguridad de la información

5.17. Política de respuesta a incidentes

5.17.1. Registro de Incidentes

El personal, terceros (contratistas y/o proveedores), deben reportar los incidentes de seguridad de información al propietario del activo, mediante un formulario que contenga como mínimo lo siguiente:

a) Fecha y Hora
b) Nombre de la persona que reporta
c) Ubicación
d) Descripción del incidente
e) Efecto del incidente
f) Como se descubrió

Por cada uno de los incidentes se debe asignar un responsable que realice el seguimiento hasta su resolución.

5.17.2. Revisión de Incidentes

Periódicamente, se debe revisar los incidentes de seguridad ocurridos en un periodo de tiempo con la finalidad de identificar tendencias o mayor ocurrencia

de determinados incidentes y tomar las acciones necesarias para corregirlos y prevenirlos.

5.18. Política de seguridad de red

La Municipalidad Distrital de Carabayllo establece el uso de registros de auditoría en la red, en los sistemas de información y en el uso de internet, de tal manera que las actividades de los usuarios puedan ser monitoreadas y las posibles responsabilidades puedan ser seguidas e identificadas.

La Municipalidad Distrital de Carabayllo establece que la revisión de registros de auditoría se realizará en forma reactiva, en caso de ser necesaria debido a algún incidente de seguridad de la información.

5.19. Política de Contraseñas

Municipalidad Distrital de Carabayllo establece que el uso de contraseñas robustas (con periodicidad de cambio, mínimo de 8 caracteres, uso de caracteres alfanuméricos, historial de contraseñas y bloqueo luego de intentos fallidos de acceso).

Está prohibido intentar ingresar a la infraestructura tecnológica con la cuenta de usuario de otro empleado.

5.20. Política de seguridad física y ambiental

El oficial de seguridad de la información debe implementar controles para prevenir pérdidas, daños o robos de los activos, incluyendo la protección de los equipos frente a amenazas físicas y ambientales.

5.20.1. Acceso físico no autorizado al Data Center

Las puertas de acceso deberán permanecer cerradas en todo momento.

El personal, terceros (contratistas y/o proveedores) que ingresen, deberán llenar un formulario de ingreso que deberá tener los siguientes datos como mínimo:

a) Fecha y Hora de ingreso y salida
b) Nombre de la persona
c) Entidad a la que pertenece
d) Personal que autoriza
e) Descripción del motivo

Ninguna persona debe ingresar sin ser supervisado por un miembro de la Sub Gerencia de Informática de la Municipalidad Distrital de Carabayllo. Este lineamiento es válido inclusive para el personal de limpieza y mantenimiento.

El Data Center de la Municipalidad Distrital de Carabayllo debe contar con aire acondicionado y medidores de temperatura, así como sensores de calor y humedad.

5.20.2. Protección de Oficinas, Recintos e Instalaciones

Para la selección y el diseño de un área protegida se tendrá en cuenta la posibilidad de daño producido por incendio, inundación, explosión, agitación civil, y otras formas de desastres naturales o provocados por el hombre. También se tomaran en cuenta las disposiciones y normas (estándares) en materia de sanidad y seguridad. Asimismo, se considerarán las amenazas a la seguridad que representan los edificios y zonas aledañas.

5.20.3. Aislamiento de Áreas de Trabajo

El oficial de seguridad de la información debe implementar controles para evitar el acceso físico no autorizado, daños o interferencias a los locales y a la información de la Municipalidad Distrital de Carabayllo.

5.20.4. Suministro de Energía

El equipamiento debe estar protegido con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía estará de acuerdo con las especificaciones del fabricante o proveedor de cada equipo.

5.20.5. Seguridad del cableado

El cableado de energía y de comunicaciones que transporta datos o brinda apoyo a los servicios de información estará protegido contra intercepción o daño.

5.20.6. Mantenimiento de Equipos

Se realizará el mantenimiento del equipamiento para asegurar su disponibilidad, confidencialidad e integridad, teniendo en cuenta a tal efecto:

a) La realización de tareas de mantenimiento preventivo, de acuerdo con los intervalos de servicio y especificaciones recomendados por el proveedor y con la autorización formal del sub gerente de Informática.
b) El establecimiento de la práctica de que sólo el personal de mantenimiento autorizado puede brindar mantenimiento y llevar a cabo reparaciones del equipamiento.
c) El registró de todas las fallas supuestas y/o reales y de todo el mantenimiento preventivo y correctivo realizado.
d) El registro del retiro de equipamiento para su mantenimiento de la sede central y agencias municipales.
e) La eliminación de toda información confidencial que contenga cualquier equipamiento que sea necesario retirar, realizándose previamente las respectivas copias de resguardo.

5.20.7. Seguridad de los equipos fuera de las instalaciones

El uso de equipamiento destinado al procesamiento de información, fuera del ámbito de la Municipalidad Distrital de Carabayllo será autorizado por el sub

gerente de Logística, Control Patrimonial y Maestranza. En el caso de que en el mismo se almacene información clasificada, deberá ser aprobado además por el propietario de la misma. La seguridad provista debe ser equivalente a la suministrada dentro del ámbito de la Municipalidad Distrital de Carabayllo para un propósito similar, teniendo en cuenta los riesgos de trabajar fuera de la misma.

5.20.8. Desafectación o reutilización segura de los equipos

La información puede verse comprometida por una desafectación o reutilización descuidada del equipamiento. Los medios de almacenamiento conteniendo material sensible, por ejemplo discos rígidos no removibles, serán físicamente destruidos o sobrescritos en forma segura en lugar de utilizar las funciones de borrado estándar, según corresponda.

5.20.9. Políticas de escritorios y pantallas limpias

Se adopta una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles y una política de pantallas limpias en las instalaciones de procesamiento de información, a fin de reducir los riesgos de acceso como fuera del mismo.

5.20.10. Retiro de los bienes

El equipamiento, la información y el software no serán retirados de la sede principal o agencia de la Municipalidad Distrital de Carabayllo sin autorización formal. Periódicamente, se llevarán a cabo comprobaciones puntuales para detectar el retiro no autorizado de activos de la institución.

5.21. Política de acceso remoto

El trabajo remoto sólo será autorizado por el responsable de la unidad organizativa, o superior jerárquico correspondiente, a la cual pertenezca el usuarios solicitante, conjuntamente con el oficial de seguridad de la información, cuando se verifique que son adoptadas todas las medidas que correspondan en

materia de seguridad de la información, de modo de cumplir con la política, normas y procedimientos existentes.

5.22. Política de retención de datos

Los propietarios de los activos de información deben proponer los periodos de retención y eliminación de los activos, estos deben ser aprobados por el comité de Gestión de Seguridad de la Información de la Municipalidad Distrital de Carabayllo.

Esta Política está diseñada para identificar los plazos por los que deben conservarse ciertos tipos de información, al tiempo que prescribe la eliminación periódica de información que no sea indispensable.

El comité de Gestión de Seguridad de la Información es responsable de clasificar los activos de información en función de su retención y criticidad.

5.23. Política de conexión con un proveedor

El comité de Gestión de Seguridad de la Información de la Municipalidad Distrital de Carabayllo, es responsable de implementar los controles necesarios para asegurar una conexión segura y estable con los proveedores de servicios de internet, energía, agua, etc.

Los funcionarios de la municipalidad son responsables de exigir que los proveedores llenen un formulario cuando éstos soliciten el uso o acceso a un activo de la Municipalidad, este formulario deberá contener como mínimo lo siguiente:

a) El tipo de acceso requerido (físico/lógico y a que activo)
b) Los motivos para los cuales se solicita el acceso
c) El valor de la información
d) Los controles empleados por la tercera parte
e) Los eventos de este acceso en la seguridad de la información.

5.24. Política de VPN

El comité de Gestión de la Seguridad de la Información es responsable de autorizar a los usuarios propuestos por los responsables de los activos sobre los cuales se realizará el acceso mediante VPN, además de aprobar las medidas de seguridad, controles y protocolos que aseguren la confidencialidad e integridad de los activos.

Es responsabilidad de la Sub Gerencia de informática; capacitar al personal, preparar y configurar los equipos con las medidas de seguridad, controles, protocolos aprobados y llevar un registro auditable de todas las conexiones vía VPN que deberán contener como mínimo lo siguiente:

a) Usuario
b) Fecha y Hora
c) Equipo donde se conecta
d) Equipos a los que se conecta

Los usuarios son responsables del uso inapropiado de la VPN con sus credenciales y serán motivos de sanción de acuerdo al Reglamento de Ética interno.

5.25. Política de acceso inalámbrico

El oficial de seguridad de la información es responsable de diseñar los controles de acceso inalámbrico y estos deben ser aprobados por el comité de Gestión de Seguridad de la Información.

Las redes inalámbricas están disponibles y debe limitarse al servicio de atención a los contribuyentes de la Municipalidad Distrital de Carabayllo, siendo responsabilidad del usuario no realizar un uso ilícito de la red. No se puede hacer uso de esta red con fines privados ni en ninguna forma que viole la legislación vigente.

La Municipalidad Distrital de Carabayllo se reserva el derecho a monitorear y registrar la actividad que se realice a través de estas redes. Además el acceso a Internet podrá ser filtrado y controlado por la Sub Gerencia de

Informática, no estando permitido el uso de técnicas, sistemas o aplicaciones que permitan evitar dicho control.

5.26. Gestión de Controles de Seguridad de la Información

Trimestralmente se debe realizar la revisión de controles de acuerdo a su nivel de cumplimiento y efectividad tomando en consideración los informes de monitoreo anteriores, informes de vulnerabilidades, revisiones del SGSI, informes de auditoría o cualquier cambio que afecte el SGSI. En caso se identifique controles ineficientes que generen nuevos riesgos se deberán revisar en el siguiente monitoreo trimestral a pesar que su frecuencia sea semestral o anual y se deberá actualizar la matriz de riesgos.

5.27. Gestión de la continuidad de los servicios

El comité de Gestión de Seguridad de la información será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de las actividades de la Municipalidad Distrital de Carabayllo.

Se debe establecer la necesidad de contar con un plan de continuidad de las actividades de la Municipalidad Distrital de Carabayllo que contemple los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del periodo de recuperación
- Identificar los controles preventivos

Esta actividad será llevada a cabo con la activa participación de los propietarios de los procesos y recursos de información de que se trate y el Oficial de Seguridad de la Información.

5.27.1. Elaboración e implementación de los planes de continuidad de las actividades.

Los propietarios de procesos y activos de información, con la asistencia del Oficial de Seguridad de la Información, elaboran planes de contiengencia necesarios para garantizar la continuidad de las actividades de la Municipalidad Distrital de Carabayllo

5.27.2. Marco para la Planificación de la Continuidad de las Actividades

Se mantendrá un solo marco para los planes de continuidad de las actividades, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo. Cuando se identifiquen nuevos requerimientos se modificarán los procedimientos de emergencia establecidos, por ejemplo, los planes de evacuación o los activos de emergencia existentes.

5.27.3. Ensayo, mantenimiento y reevaluación de los Planes de Continuidad.

El comité de seguridad de la información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia.

Anexo N° 8 – Declaración de Aplicabilidad

<table>
<tr><td> 
</td><td colspan="2">DOCUMENTO</td></tr>
<tr><td rowspan="3">DECLARACIÓN DE APLICABILIDAD DE LA “MUNICIPALIDAD DISTRITAL DE CARABAYLLO”</td><td>CÓDIGO:</td><td>VERSIÓN:</td></tr>
<tr><td>FECHA:</td><td>PÁGINA:</td></tr>
<tr><td colspan="2"></td></tr>
<tr><td></td><td colspan="2">Revisado por: Jara Mendoza Omar Yino</td></tr>
</table>

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
5 Políticas de Seguridad	5.1	Dirección de la alta gerencia para la seguridad de la información			
	5.1.1	Políticas de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado:
	5.1.2	Revisión de las políticas de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100% Documento elaborado:
6 Organización de la Seguridad de la Información	6.1	Organización interna			
	6.1.1	Roles y responsabilidad de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	6.1.2	Segregación de deberes	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	6.1.3	Contacto con autoridades	NO	NO	-
	6.1.4	Contacto con grupos de interés especial	NO	NO	-
	6.1.5	Seguridad de la información en la gestión de proyectos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	6.2	Dispositivos móviles y teletrabajo			
	6.2.1	Política de dispositivos móviles	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	6.2.2	Teletrabajo	NO	NO	-
7 Seguridad en los Recursos Humanos	7.1	Previo al empleo			
	7.1.1	Verificación de antecedentes	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	7.1.2	Términos y condiciones del empleo	SI	SI	Porcentaje de cumplimiento: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
					Meta: 100%
	7.2	Durante el empleo			
	7.2.1	Responsabilidades de la Alta Gerencia	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	7.2.2	Conciencia, educación y entrenamiento de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	7.2.3	Proceso disciplinario	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	7.3	Terminación y cambio de empleo			
	7.3.1	Termino de responsabilidades o cambio de empleo	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
8 **Gestión de Activos**	8.1	Responsabilidad de los activos			
	8.1.1	Inventario de activos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.1.2	Propiedad de activos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.1.3	Uso aceptable de los activos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.1.4	Devolución de activos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.2	Clasificación de la información			

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
	8.2.1	Clasificación de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.2.2	Etiquetado de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.2.3	Manejo de activos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.3	Manejo de medios			
	8.3.1	Gestión de medios removibles	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.3.2	Eliminación de medios	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	8.3.3	Transporte de medios físicos	SI	SI	
9 **Control de Acceso**	9.1	Requerimientos de negocio para el control de acceso			
	9.1.1	Política de control de acceso	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.1.2	Acceso a redes y servicios de red	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2	Gestión de accesos de usuario			
	9.2.1	Registro y baja del usuario	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2.2	Provisión de acceso a usuarios	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
	9.2.3	Gestión de derechos de acceso privilegiados	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2.4	Gestión de información de autenticación secreta de usuarios	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2.5	Revisión de derechos de acceso de usuarios	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.2.6	Eliminación o ajuste de derechos de acceso	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.3	Responsabilidades del usuario			
	9.3.1	Uso de información de autenticación secreta	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.4	Control de acceso de sistemas y aplicaciones			
	9.4.1	Restricción de acceso a la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.4.2	Procedimientos de inicio de sesión seguro	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.4.3	Sistema de gestión de contraseñas	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.4.4	Uso de programas y utilidades privilegiadas	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	9.4.5	Control de acceso al código fuente del programa	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
10 Criptografía	10.1	Controles criptográficos			
	10.1.1	Política en el uso de controles criptográficos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	10.1.2	Gestión de llaves	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
11 Seguridad Física y del Entorno	11.1	Áreas seguras			
	11.1.1	Perímetro de seguridad físico	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.1.2	Controles físicos de entrada	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.1.3	Seguridad de oficinas, habitaciones y facilidades	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.1.4	Protección contra amenazas externas y del ambiente	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.1.5	Trabajo en áreas seguras	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.1.6	Áreas de entrega y carga	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2	Equipo			
	11.2.1	Instalación y protección de equipo	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
	11.2.2	Servicios de soporte	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.3	Seguridad en el cableado	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.4	Mantenimiento de equipos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.5	Retiro de activos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.6	Seguridad del equipo y activos fuera de las instalaciones	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.7	Eliminación segura o reuso del equipo	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.8	Equipo de usuario desatendido	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	11.2.9	Política de escritorio limpio y pantalla limpia	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
12 Seguridad en las Operaciones	12.1	Procedimientos Operacionales y Responsabilidades			
	12.1.1	Documentación de procedimientos operacionales	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.1.2	Gestión de cambios	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
	12.1.3	Gestión de la capacidad	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.2	Protección de Software Malicioso			
	12.2.1	Controles contra software malicioso	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.3	Respaldo			
	12.3.1	Respaldo de información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.4	Bitácoras y monitoreo			
	12.4.1	Bitácoras de eventos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.4.2	Protección de información en bitácoras	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.4.3	Bitácoras de administrador y operador	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.4.4	Sincronización de relojes	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.5	Control de software operacional			
	12.5.1	Instalación de software en sistemas operacionales	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
	12.6	Gestión de vulnerabilidades técnicas			
	12.6.1	Gestión de vulnerabilidades técnicas	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.6.2	Restricciones en la instalación de software	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	12.7	Consideraciones de auditoria de sistemas de información			
	12.7.1	Controles de auditoría de sistemas de información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
13 Seguridad en las Comunicaciones	13.1	Gestión de seguridad en red			
	13.1.1	Controles de red	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	13.1.2	Seguridad en los servicios en red	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	13.1.3	Segregación en redes	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	13.2	Transferencia de información			
	13.2.1	Políticas y procedimientos para la transferencia de información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	13.2.2	Acuerdos en la transferencia de información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	13.2.3	Mensajería electrónica	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	**Sección**	**Objetivo de control / control**			
	13.2.4	Acuerdos de confidencialidad o no-revelación	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
14 Adquisición, Desarrollo y Mantenimiento de Sistemas	14.1	Requerimientos de seguridad en sistemas de información			
	14.1.1	Análisis y especificación de requerimientos de seguridad	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.1.2	Aseguramiento de servicios de aplicación en redes públicas	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.1.3	Protección de transacciones en servicios de aplicación	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2	Seguridad en el proceso de desarrollo y soporte			
	14.2.1	Política de desarrollo seguro	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.2	Procedimientos de control de cambios del sistema	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.3	Revisión técnica de aplicaciones después de cambios a la plataforma operativa	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.4	Restricción de cambios en paquetes de software	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.5	Principios de seguridad en la ingeniería de sistemas	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.6	Entorno de desarrollo seguro	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	**Sección**	**Objetivo de control / control**			
	14.2.7	Desarrollo tercerizado	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.8	Pruebas de seguridad del sistema	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.2.9	Pruebas de aceptación del sistema	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	14.3	Datos de prueba			
	14.3.1	Protección de datos de prueba	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
15 Relaciones con Proveedores	15.1	Seguridad de la información en relaciones con el proveedor			
	15.1.1	Política de seguridad de la información en las relaciones con el proveedor	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	15.1.2	Atención de tópicos de seguridad en los acuerdos con el proveedor	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	15.1.3	Cadena de suministros de tecnologías de la información y comunicaciones	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	15.2	Gestión de entrega de servicios de proveedor			
	15.2.1	Monitoreo y revisión de servicios del proveedor	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	15.2.2	Gestión de cambios a los servicios del proveedor	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
16 Gestión de Incidentes de Seguridad de la Información	16.1	Gestión de incidentes de seguridad de la información y mejoras			
	16.1.1	Responsabilidades y procedimientos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	16.1.2	Reporte de eventos de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	16.1.3	Reporte de debilidades de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	16.1.4	Valoración y decisión de eventos de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	16.1.5	Respuesta a incidentes de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	16.1.6	Aprendizaje de incidentes de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	16.1.7	Colección de evidencia	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
17 Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio	17.1	Continuidad de la seguridad de la información			
	17.1.1	Planeación de la continuidad de la seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	17.1.2	Implementación de la continuidad de la seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%

DECLARACIÓN DE APLICABILIDAD

ISO 27001:2014 Controles de Seguridad			Aplica o no Aplica	Existe SI/NO	DESCRIPCIÓN DE LA IMPLEMENTACIÓN INDICADOR
Cláusula	Sección	Objetivo de control / control			
	17.2	Redundancias			
	17.2.1	Disponibilidad de facilidades de procesamiento de información	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
18 Cumplimiento	18.1	Cumplimiento con Requerimientos Legales y Contractuales			
	18.1.1	Identificación de legislación aplicable y requerimientos contractuales	SI	SI	Porcentaje de cumplimiento: 60% Meta: 100%
	18.1.2	Derechos de propiedad intelectual (IPR)	SI	SI	Porcentaje de cumplimiento: 60% Meta: 100%
	18.1.3	Protección de registros	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	18.1.4	Privacidad y protección de información personal identificable (PIR)	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	18.1.5	Regulación de controles criptográficos	SI	SI	Porcentaje de cumplimiento: 100% Meta: 100%
	18.2	Revisiones de seguridad de la información			
	18.2.1	Revisión independiente de seguridad de la información	SI	SI	Porcentaje de cumplimiento: 80% Meta: 100%
	18.2.2	Cumplimiento con políticas y estándares de seguridad	SI	SI	Porcentaje de cumplimiento: 80% Meta: 100%
	18.2.3	Revisión del cumplimiento técnico	SI	SI	Porcentaje de cumplimiento: 80% Meta: 100%

FICHA DE OBSERVACIÓN: INDICADOR NIVEL DE RIESGO															
SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES FASE: PRE TEST															
	ACTIVOS CRÍTICOS						EVALUACIÓN DEL RIESGO							
N°	CÓDIGO ACTIVO	ACTIVO	Ubicación Física	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDADES	DEGRADACIÓN			DEGRADACIÓN MÁXIMA	IMPACTO	PROBABILIDAD	RIESGO	Riesgo promedio
							C	I	D					
1	A002	SISMUN	SGI-Datacenter	5	Acceso no autorizado	Política de controles de accesos	4	5	5	5	5	4	20	17
					Pérdida de información	Backup no periodico	4	5	5	5	5	3	15	
					Denegación del servicio	Registro de transacciones no actualizado	5	5	5	5	4	4	16	
2	A005	Servidor Aplicaciones/BD (Sauce)	SGI-Datacenter	5	Codigo malicioso	Actualizacion de antivirus	4	5	5	5	4	3	12	9.33
					Acceso de personas no autorizadas	Seguridad perimetral	4	5	5	5	3	4	12	
					Recuperación de informacion	Procedimiento de eliminación física de los datos alojados.	4	5	5	5	4	1	4	
3	A009	Firewall	SGI-Datacenter	4	Reglas mal implementadas	Soporte de TI in situ	4	5	5	5	5	1	5	6
					Desactualización de las reglas	Mantenimiento lógico	4	5	5	5	2	1	2	
					Ataques internos y externos	Mantenimiento lógico	4	5	5	5	4	4	16	
					Desconfiguracion de las políticas	Control de accesos	4	5	5	5	4	1	4	
					Ataques internos y externos	Gran numero de puertos abiertos	4	5	5	5	3	1	3	
4	A004	SISMUN Fox	SGI-Datacente	4	Acceso no autorizado	Control de accesos	4	4	5	5	3	5	15	10.25
					Incumplimiento de requerimientos del area usuaria	Capacitacion a programadores	4	4	5	5	3	4	12	
					Trasabilidad del codigo fuente	Backup de codigo fuente periodico	4	5	5	5	4	1	4	
					Mal uso del sistema	Ausencia de manual de uso del sistema	3	4	4	4	2	5	10	
5	A010	Switch de Borde	SGI-Datacenter	5	Sobre carga o corto circuito	El cableado de red y energía no cumple las normas de seguridad	3	4	4	4	2	2	4	6.00
					Manipulación de personal no autorizado	Seguridad física	3	4	4	4	2	2	4	
					Inestabilidad de la energia electrica	Falta de mantenimiento	3	4	4	4	5	2	10	
6	A011	Switch de Distribucion	SGI-Datacenter	4	Sobre carga o corto circuito	El cableado de red y energía no cumple las normas de seguridad	3	4	4	4	4	2	8	8.67
					Manipulación de personal no autorizado	Seguridad física	3	4	4	4	4	2	8	
					Inestabilidad de la energia electrica	Falta de mantenimiento	3	5	5	5	5	2	10	
7	A012	Switch Core	SGI-Datacenter	5	Sobre carga o corto circuito	El cableado de red y energía no cumple las normas de seguridad	3	4	5	5	4	2	8	8.67
					Manipulación de personal no autorizado	Seguridad física	3	4	4	4	4	2	8	
					Inestabilidad de la energia electrica	Falta de mantenimiento	4	5	5	5	5	2	10	
8	A029	Computadora de Escritorio (Técnico Liquidador de Fiscalizacion Tributaria)	SG. Fiscalización Tributaria	3	Uso indebido de las computadoras	Directiva para el uso de las computadoras	4	4	4	4	4	4	16	13.00
					Acceso no autorizado	Equipo desbloqueado	4	3	4	4	4	5	20	
					Acceso no autorizado	Control de accesos a recursos compartidos	4	3	3	4	3	1	3	

FICHA DE OBSERVACIÓN: INDICADOR NIVEL DE RIESGO														
SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES FASE: PRE TEST														
	ACTIVOS CRÍTICOS						EVALUACIÓN DEL RIESGO							
							DEGRADACIÓN			DEGRADACIÓN MÁXIMA	IMPACTO	PROBABILIDAD	RIESGO	Riesgo promedio
N°	CÓDIGO ACTIVO	ACTIVO	Ubicación Física	VALOR DEL ACTIVO	AMENAZA	VULNERABILIDADES	C	I	D					
9	A052	Subgerente de Informatica	SGI-Subgerencia	4	Decisiones incorrectas o errores involuntarios	Supervisión	4	3	3	4	4	4	16	10.67
					Proyectos inconclusos	Sobrecarga de tareas	4	3	3	4	4	2	8	
					Incumplimiento de normas vigentes	Desconocimiento de Normas vigentes	4	3	3	4	2	4	8	
10	A003	SISMUN Web	SGI-Datacenter	3	Acceso no autorizado	Control de accesos	3	3	3	3	3	5	15	10.25
					Incumplimiento de requerimientos del area usuaria	Capacitacion a programadores	3	3	3	3	3	4	12	
					Trasabilidad del codigo fuente	Backup de codigo fuente periodico	3	3	3	3	4	1	4	
					Mal uso del sistema	Ausencia de manual de uso del sistema	3	3	3	3	2	5	10	
11	A051	Computadora de Escritorio del Subgerente de Informatica	SGI-Subgerencia	3	Uso indebido de las computadoras	Directiva para el uso de las computadoras	3	3	3	3	2	5	10	12.00
					Acceso no autorizado	Equipo desbloqueado	3	3	3	3	2	5	10	
					Acceso no autorizado	Control de accesos a recursos compartidos	3	3	3	3	5	4	20	
					Inoperatividad de la computadora	Backup de información	3	3	3	3	4	2	8	
12	A001	Analista Programador	SGI-Área de Desarrollo	3	Errores involuntarios	Supervisión	3	3	2	3	4	2	8	10.17
					proyectos inconclusos	Sobrecarga de tareas	3	3	2	3	4	2	8	
					Compartir contraseña	Politicas de uso de contraseñas y falta de capacitacion sobre seguridad de la informacion	3	3	2	3	3	4	12	
13	A017	Supervisor de Plataforma	Plataforma	2	Perdida de infomacion	Reporte al jefe inmediato	3	3	2	3	3	4	12	10
14	A026	Computadora de Escritorio (Técnico en Plataforma de Fiscalizacion Tributaria)	SG. Fiscalización Tributaria	2	Uso indebido de las computadoras	Directiva para el uso de las computadoras	3	3	2	3	3	4	12	12.33
					Acceso no autorizado	Equipo desbloqueado	3	3	2	3	3	5	15	
					Acceso no autorizado	Control de accesos a recursos compartidos	3	3	2	3	2	5	10	
15	A044	Declaracion Jurada de Predio Rustico	Plataforma	2	Uso indebido	Protocolos de clasificacion de acuerdo a la confidencialidad	2	3	3	3	2	5	10	12.5
16	A046	Subgerente de Administracion Tributaria	Plataforma	2	Decisiones incorrectas o errores involuntarios	Supervision	3	3	2	3	2	4	8	10
17	A048	Resolución de determinación predial - Fiscalización	SG. Fiscalización Tributaria	3	Uso indebido	Protocolos de clasificacion de acuerdo a la confidencialidad	2	3	3	3	3	4	12	12

FICHA DE OBSERVACIÓN: INDICADOR NIVEL DE RIESGO														
SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES FASE: PRE TEST														
ACTIVOS CRÍTICOS					AMENAZA	VULNERABILIDADES	EVALUACIÓN DEL RIESGO							
							DEGRADACIÓN			DEGRADACIÓN MÁXIMA	IMPACTO	PROBABILIDAD	RIESGO	Riesgo promedio
N°	CÓDIGO ACTIVO	ACTIVO	Ubicación Física	VALOR DEL ACTIVO			C	I	D					
18	A050	Hoja de Resumen de Declaracion Jurada	Plataforma	2	Uso indebido	Protocolos de clasificacion de acuerdo a la confidencialidad	2	3	3	3	2	4	8	10
19	A041	Subgerente de Fiscalizacion Tributaria	SG. Fiscalización Tributaria	2	Decisiones incorrectas o errores involuntarios	Supervision	3	2	2	3	3	4	12	10
20	A043	Declaracion Jurada de Predio Urbano	Plataforma	2	Uso indebido	Protocolos de clasificacion de acuerdo a la confidencialidad	2	3	2	3	3	4	12	10
21	A047	Requerimiendo de fiscalización	SG. Fiscalización Tributaria	2	Uso indebido	Protocolos de clasificacion de acuerdo a la confidencialidad	2	3	2	3	2	4	8	10
22	A049	Resolución de determinación de arbitrios - Fiscalización	SG. Fiscalización Tributaria	3	Uso indebido	Protocolos de clasificacion de acuerdo a la confidencialidad	2	3	2	3	3	4	12	12
23	A006	UPS de Switchs de Gabinete de Comunicación	SGI-Datacenter	3	Corte de energia electrica	Regulador de voltaje	1	1	4	4	3	2	6	7
24	A007	UPS de Switch Core	SGI-Datacenter	3	Corte de energia electrica	Regulador de voltaje	1	1	4	4	3	2	6	7
25	A008	UPS Servidor (Aplicaciones/BD)	SGI-Datacenter	3	Corte de energia electrica	Regulador de voltaje	1	1	4	4	3	2	6	7
26	A013	UPS (Analista Programador)	SGI-Administrativo	3	Corte de energia electrica	Regulador de voltaje	1	1	4	4	3	2	6	7
27	A028	Técnico Liquidador de Fiscalizacion Tributaria	SG. Fiscalización Tributaria	2	Divulgación contraseña	Politicas de uso de contraseñas y falta de capacitacion sobre seguridad de la informacion	2	2	2	2	3	5	15	10
28	A038	Técnico de Fiscalización Tributaria	SG. Fiscalización Tributaria	2	Divulgación contraseña	Politicas de uso de contraseñas y falta de capacitacion sobre seguridad de la informacion	2	2	2	2	1	3	3	10
29	A039	Técnico en Plataforma de Recaudacion	SG. Administración Tributaria	2	Divulgación contraseña	Politicas de uso de contraseñas y falta de capacitacion sobre seguridad de la informacion	2	2	2	2	3	5	15	10
30	A045	Estado de cuenta	Plataforma	2	Uso indebido del activo	Protocolos de clasificacion de acuerdo a la confidencialidad	1	3	2	3	5	4	20	10
31	A053	Cargo de Notificacion de Fiscalizacion	Plataforma	2	Uso indebido del activo	Protocolos de clasificacion de acuerdo a la confidencialidad	2	3	3	3	2	4	8	10
													NIVEL DE RIESGO	9.96

FICHA DE OBSERVACIÓN: INDICADOR NIVEL DE RIESGO														
SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES FASE: POST TEST														
ACTIVOS CRÍTICOS					AMENAZA	VULNERABILIDADES	EVALUACIÓN DEL RIESGO							Riesgo promedio
							DEGRADACIÓN			DEGRADACIÓN MÁXIMA	IMPACTO	PROBABILIDAD	RIESGO	
N°	CÓDIGO ACTIVO	ACTIVO	Ubicación Física	VALOR DEL ACTIVO			C	I	D					
1	A002	SISMUN	SGI-Datacenter	5	Acceso no autorizado	Falta de restricción del acceso al DC.	4	4	4	4	3	3	9	8.00
					Pérdida de información	Falta o deficiencia en protección contra amenazas internas y externas	4	4	4	4	3	2	6	
					Denegación del servicio	Ambientales	4	4	5	5	3	3	9	
2	A005	Servidor Aplicaciones/BD (Sauce)	SGI-Datacenter	5	Codigo malicioso	Actualizacion de antivirus	3	4	5	5	3	2	6	5.33
					Acceso de personas no autorizadas	Falta de monitoreo de la Seguridad perimetral	4	4	4	4	2	3	6	
					Caída de servidor	Carencia de sistema de contingencia	4	4	4	4	2	2	4	
3	A009	Firewall	SGI-Datacenter	4	Reglas mal implementadas	Falla de mecanismos de monitoreo	3	4	4	4	3	1	3	3.20
					Manipulación de la Configuración	deficiente cumplimiento de los procedimientos operativos específicos, asi como las políticas	3	4	5	5	2	1	2	
					Ataques internos y externos	Falta de mantenimiento lógico del equipo	3	4	4	4	2	3	6	
					Errores de monitorización	Falla de los mecanismos de monitoreo	4	4	4	4	3	1	3	
					Ataques internos y externos	deficiencia en protección contra amenazas externas y	3	4	4	4	2	1	2	
4	A004	SISMUN Fox	SGI-Datacente	4	Errores de Configuración	Falta de capacitación	3	4	4	4	2	4	8	5.5
					Incumplimiento de requerimientos del area usuaria	Capacitacion a programadores	3	3	4	4	1	3	3	
					Trasabilidad del codigo fuente	Backup de codigo fuente periodico	3	4	4	4	3	1	3	
					Errores de Usuario	Falta de capacitación	3	3	3	3	2	4	8	
5	A010	Switch de Borde	SGI-Datacenter	5	Sobre carga o corto circuito	El cableado de red y energía no cumple las normas de seguridad	3	3	3	3	2	1	2	2.67
					Manipulación de personal no autorizado	Falta de procedimientos operativos	3	3	3	3	2	1	2	
					Errores de monitorización	Falla de mecanismos de monitoreo	3	3	4	4	4	1	4	
6	A011	Switch de Distribucion	SGI-Datacenter	4	Sobre carga o corto circuito	El cableado de red y energía no cumple las normas de seguridad	3	3	3	3	2	1	2	2.33
					Manipulación de personal no autorizado	Falta de procedimientos operativos	3	4	4	4	2	1	2	
					Inestabilidad de la energia electrica	Mantenimientos inadecuados	3	4	4	4	3	1	3	
7	A012	Switch Core	SGI-Datacenter	5	Sobre carga o corto circuito	El cableado de red y energía no cumple las normas de seguridad	3	3	4	4	3	1	3	3.33
					Manipulación de personal no autorizado	Falta de procedimientos operativos	3	3	3	3	3	1	3	
					Inestabilidad de la energia electrica	Mantenimientos inadecuados	4	4	4	4	4	1	4	

FICHA DE OBSERVACIÓN: INDICADOR NIVEL DE RIESGO														
SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES FASE: POST TEST														
ACTIVOS CRÍTICOS					AMENAZA	VULNERABILIDADES	EVALUACIÓN DEL RIESGO							Riesgo promedio
							DEGRADACIÓN			DEGRADACIÓN MÁXIMA	IMPACTO	PROBABILIDAD	RIESGO	
N°	CÓDIGO ACTIVO	ACTIVO	Ubicación Física	VALOR DEL ACTIVO			C	I	D					
8	A029	Computadora de Escritorio (Técnico Liquidador de Fiscalizacion Tributaria)	SG. Fiscalización Tributaria	3	Uso indebido de las computadoras	Desconocimiento de las Directivas para el uso de los equipos	3	3	3	3	2	3	6	5.33
					Acceso no autorizado	Equipos desbloqueados	3	2	3	3	2	4	8	
					Acceso no autorizado	Accesos compartidos	3	3	3	3	2	1	2	
9	A052	Subgerente de Informatica	SGI-Subgerencia	4	Deficiencias en la organización	Falta de control y supervisión en la organización	3	2	3	3	2	3	6	4.67
					Personal Indisponibilidad	Falta de personal para desempeñar el rol	3	3	3	3	1	2	2	
					Incumplimiento de normas vigentes	Desconocimiento de normas vigentes	3	3	3	3	2	3	6	
10	A003	SISMUN Web	SGI-Datacenter	3	Acceso no autorizado	Falta de restricción del acceso	2	3	3	3	2	4	8	6.00
					Abuso de Privilegios de Acceso	Falta de restricción de accesos a usuarios	2	2	3	3	2	3	6	
					Caída del Sistema	Carencia de sistema de contingencia	2	2	2	2	2	1	2	
					Manipulación de Programas	Incumplimiento de las políticas para la protección de los sistemas de información	2	3	2	3	2	4	8	
11	A051	Computadora de Escritorio del Subgerente de Informatica	SGI-Subgerencia	3	Uso indebido de las computadoras	Desconocimiento de las Directivas para el uso de los equipos	2	3	2	3	2	4	8	7.00
					Acceso no autorizado	Equipos desbloqueados	3	2	2	3	2	4	8	
					Acceso no autorizado	Accesos compartidos	2	3	3	3	2	3	6	
					Inoperatividad de la computadora	Backup de información	2	2	3	3	3	2	6	
12	A001	Analista Programador	SGI-Área de Desarrollo	3	Indisponibilidad del personal	Falta de personal para desempeñar el rol	2	2	2	2	2	1	2	3.33
					Acceso no autorizado	Sobrecarga de tareas	2	3	2	3	2	1	2	
					Acceso no autorizado	Falta de capacitacion sobre seguridad de la informacion	2	2	2	2	2	3	6	
13	A017	Supervisor de Plataforma	Plataforma	2	Pérdida de infomacion	Incumplimiento en el reporte al jefe inmediato	2	2	2	2	2	3	6	6
14	A026	Computadora de Escritorio (Técnico en Plataforma de Fiscalizacion Tributaria)	SG. Fiscalización Tributaria	2	Uso indebido de las computadoras	Desconocimiento de las Directivas para el uso de los equipos	2	3	2	3	2	3	6	7.33
					Acceso no autorizado	Equipos desbloqueados	2	2	2	2	2	4	8	
					Acceso no autorizado	Accesos compartidos	2	3	2	3	2	4	8	
15	A044	Declaracion Jurada de Predio Rustico	Plataforma	2	Uso indebido	Inadecuado cumplimiento de los Protocolos de clasificacion de acuerdo a la confidencialidad.	2	2	2	2	2	4	8	8

FICHA DE OBSERVACIÓN: INDICADOR NIVEL DE RIESGO														
SEGÚN LOS ACTIVOS DE INFORMACIÓN, AMENAZAS Y VULNERABILIDADES FASE: POST TEST														
	ACTIVOS CRÍTICOS				AMENAZA	VULNERABILIDADES	EVALUACIÓN DEL RIESGO							
							DEGRADACIÓN			DEGRADACIÓN MÁXIMA	IMPACTO	PROBABILIDAD	RIESGO	Riesgo promedio
Nº	CÓDIGO ACTIVO	ACTIVO	Ubicación Física	VALOR DEL ACTIVO			C	I	D					
16	A046	Subgerente de Administracion Tributaria	Plataforma	2	Decisiones incorrectas o errores involuntarios	Falta de monitoreo	2	2	2	2	2	3	6	6
17	A048	Resolución de determinación predial - Fiscalización	SG. Fiscalización Tributaria	3	Uso indebido	Inadecuado cumplimiento de los Protocolos de clasificacion de acuerdo a la confidencialidad.	2	2	2	2	2	3	6	7.5
18	A050	Hoja de Resumen de Declaracion	Plataforma	2	Uso indebido	Inadecuado cumplimiento de los Protocolos de clasificacion de acuerdo a la confidencialidad.	2	2	2	2	2	3	6	6
19	A041	Subgerente de Fiscalizacion Tributaria	SG. Fiscalización Tributaria	2	Decisiones incorrectas o errores involuntarios	Falta de monitoreo	2	2	2	2	1	3	3	6
20	A043	Declaracion Jurada de Predio Urbano	Plataforma	2	Uso indebido	Inadecuado cumplimiento de los Protocolos de clasificacion de acuerdo a la confidencialidad.	1	2	2	2	2	3	6	6
21	A047	Requerimiendo de fiscalización	SG. Fiscalización Tributaria	2	Uso indebido	Inadecuado cumplimiento de los Protocolos de clasificacion de acuerdo a la confidencialidad.	1	2	2	2	1	3	3	6
22	A049	Resolución de determinación de arbitrios - Fiscalización	SG. Fiscalización Tributaria	3	Uso indebido	Inadecuado cumplimiento de los Protocolos de clasificacion de acuerdo a la confidencialidad.	2	2	2	2	2	3	6	7.5
23	A006	UPS de Switchs de Gabinete de Comunicación	SGI-Datacenter	3	Corte de energia electrica	Regulador de voltaje	1	1	3	3	1	2	2	6
24	A007	UPS de Switch Core	SGI-Datacenter	3	Corte de energia electrica	Regulador de voltaje	1	1	3	3	1	2	2	6
25	A008	UPS Servidor (Aplicaciones/B	SGI-Datacenter	3	Corte de energia electrica	Regulador de voltaje	1	1	3	3	1	2	2	6
26	A013	UPS (Analista Programador)	SGI-Administrativo	3	Corte de energia electrica	Regulador de voltaje	1	1	3	3	1	2	2	6
27	A028	Técnico Liquidador de Fiscalizacion Tributaria	SG. Fiscalización Tributaria	2	Divulgación contraseña	Inadecuado uso de las políticas de uso de contraseñas y falta de capacitacion.	1	2	2	2	1	4	4	8
28	A038	Técnico de Fiscalización Tributaria	SG. Fiscalización Tributaria	2	Divulgación contraseña	Inadecuado uso de las políticas de uso de contraseñas y falta de capacitacion.	1	1	2	2	1	4	4	8
29	A039	Técnico en Plataforma de Recaudacion	SG. Administración	2	Divulgación contraseña	Inadecuado uso de las políticas de uso de contraseñas y falta de capacitacion.	1	2	1	2	1	4	4	8
30	A045	Estado de cuenta	Plataforma	2	Uso indebido del activo	Incumplimiento de los Protocolos de clasificacion de acuerdo a la confidencialidad	1	2	2	2	1	3	3	6
31	A053	Cargo de Notificacion de Fiscalizacion	Plataforma	2	Uso indebido del activo	Incumplimiento de los Protocolos de clasificacion de acuerdo a la confidencialidad	2	2	2	2	2	3	6	6
													NIVEL DE RIESGO	5.90

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTION DEL RIESGO

EVALUACION DEL RIESGO (Niveles)	Pertinencia [1]		Relevancia [2]		Claridad [3]	
	Si	No	Si	No	Si	No
1. Código de activo	X		X		X	
2. Activo críticos	X		X		X	
3. Vulnerabilidad	X		X		X	
4. Evaluación del riesgo	X		X		X	
Degradación	X		X		X	
Degradación Máxima	X		X		X	
Impacto	X		X		X	
Probabilidad	X		X		X	
Riesgo						
TRATAMIENTO DEL RIESGO (Controles)						
5. Clausula	X		X		X	
6. Sección	X		X		X	
7. Objetivo	X		X		X	
8. Aplicación	X		X		X	
9. Existencia	X		X		X	
10. Justificación	X		X		X	

Observaciones (precisar si hay suficiencia): Existe suficiencia para su aplicación

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: **Mg. Luis Torres Cabanillas** **DNI:08404690**

Especialidad del validador: Ing. Estadístico Nro. 49863

09 de Dic del 2018

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---

Firma del Experto Informante.

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTION DEL RIESGO

EVALUACION DEL RIESGO (Niveles)	Pertinencia [1]		Relevancia [2]		Claridad [3]	
	Si	No	Si	No	Si	No
1. Código de activo	X		X		X	
2. Activo críticos	X		X		X	
3. Vulnerabilidad	X		X		X	
4. Evaluación del riesgo	X		X		X	
Degradación	X		X		X	
Degradación Máxima	X		X		X	
Impacto	X		X		X	
Probabilidad	X		X		X	
Riesgo						
TRATAMIENTO DEL RIESGO (Controles)						
5. Clausula	X		X		X	
6. Sección	X		X		X	
7. Objetivo	X		X		X	
8. Aplicación	X		X		X	
9. Existencia	X		X		X	
10. Justificación	X		X		X	

Observaciones (precisar si hay suficiencia): Existe suficiencia para su aplicación

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: **Tito Chura Virgilio Fredy** **DNI:** 01333753

Especialidad del validador: Ing. Electrónico, Implementador Líder ISO 27001 en PECB **CIP N°:** 81469

11 de Dic del 2018

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia**: El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad**: Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---
Firma del Experto Informante.

UCV UNIVERSIDAD CÉSAR VALLEJO
ESCUELA DE POSTGRADO

CERTIFICADO DE VALIDEZ DE CONTENDO DEL INSTRUMENTO QUE MIDE LA GESTION DEL RIESGO

EVALUACION DEL RIESGO (Niveles)	Pertinencia [1]		Relevancia [2]		Claridad [3]	
	Si	No	Si	No	Si	No
1. Código de activo	X		X		X	
2. Activo críticos	X		X		X	
3. Vulnerabilidad	X		X		X	
4. Evaluación del riesgo	X		X		X	
Degradación	X		X		X	
Degradación Máxima	X		X		X	
Impacto	X		X		X	
Probabilidad	X		X		X	
Riesgo						
TRATAMIENTO DEL RIESGO (Controles)						
5. Clausula	X		X		X	
6. Sección	X		X		X	
7. Objetivo	X		X		X	
8. Aplicación	X		X		X	
9. Existencia	X		X		X	
10. Justificación	X		X		X	

Observaciones (precisar si hay suficiencia): Existe suficiencia para su aplicación

Opinión de aplicabilidad: **Aplicable [X]** **Aplicable después de corregir [ ]** **No aplicable [ ]**

Apellidos y nombres del juez validador. Dr/ Mg: **López Chávez Carlomagno** **DNI:** 42072348

Especialidad del validador: Ing. De Sistemas, Implementador Líder ISO 27001 en PECB **CIP N°:** 212126

12 de Dic del 2018

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

---

Firma del Experto Informante.

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

ACTA DE APROBACIÓN DE ORIGINALIDAD DE LOS TRABAJOS ACADÉMICOS DE LA UCV

Yo, Luis Torres Cabanillas, docente de la Escuela de Posgrado de la UCV y revisor del trabajo académico titulado "Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018" del estudiante: Jara Mendoza Omar Yino ; y habiendo sido capacitado e instruido en el uso de la herramienta Turnitin, he constatado lo siguiente: Que el citado trabajo académico tiene un índice de similitud constato 24% verificable en el reporte de originalidad del programa turnitin, grado de coincidencia mínimo que convierte el trabajo en aceptable y no constituye plagio, en tanto cumple con todas las normas del uso de citas y referencias establecidas por la universidad César Vallejo.

Lima, 20 de enero del 2019

Luis Torres Cabanillas

DNI: 08404690

ESCUELA DE POSGRADO
UNIVERSIDAD CÉSAR VALLEJO

Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018.

TESIS PARA OPTAR EL GRADO ACADÉMICO DE:

Maestro(a) en Ingeniería de sistemas con mención en tecnologías de la información.

AUTOR:

Br. Omar Yino, Jara Mendoza

ASESOR:

Mg. Luis Torres Cabanillas

SECCIÓN:

Ingeniería y tecnología

LÍNEA DE INVESTIGACIÓN:

Tecnologías de la información y comunicación

PERU-2018

INFORME_FINAL-V6_17-01-2019_version_de_turni_v2.docx

INFORME DE ORIGINALIDAD

24%	13%	0%	17%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	10%
2	openaccess.uoc.edu Fuente de Internet	5%
3	Submitted to Universidad ESAN -- Escuela de Administración de Negocios para Graduados Trabajo del estudiante	3%
4	repositorio.ucv.edu.pe Fuente de Internet	2%
5	repositorio.uladech.edu.pe Fuente de Internet	2%
6	tesis.pucp.edu.pe Fuente de Internet	2%

UNIVERSIDAD CÉSAR VALLEJO

Centro de Recursos para el Aprendizaje y la Investigación (CRAI)
"César Acuña Peralta"

FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN ELECTRÓNICA DE LAS TESIS

1. **DATOS PERSONALES**
Apellidos y Nombres: (solo los datos del que autoriza)
Jara Mendoza Omar Yino
D.N.I. : 41168365
Domicilio : Mz. I Lt. 11 Laderas de chillón – Puente Piedra
Teléfono : Fijo : ..... Móvil : 951357961
E-mail : omarjara2017@hotmail.com

2. **IDENTIFICACIÓN DE LA TESIS**
Modalidad:
☐ Tesis de Pregrado
Facultad : .....
Escuela : .....
Carrera : .....
Título : .....

☐ Tesis de Posgrado
☒ Maestría ☐ Doctorado
Grado : Maestro
Mención : Tecnologías de la información

3. **DATOS DE LA TESIS**
Autor (es) Apellidos y Nombres:
Jara Mendoza Omar Yino
.....
.....

Título de la tesis:
Sistema de gestión de Seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018

Año de publicación : 2019

4. **AUTORIZACIÓN DE PUBLICACIÓN DE LA TESIS EN VERSIÓN ELECTRÓNICA:**
A través del presente documento,
Si autorizo a publicar en texto completo mi tesis. ☒
No autorizo a publicar en texto completo mi tesis. ☐

Firma : ..... Fecha : 11/04/2019

UNIVERSIDAD CÉSAR VALLEJO

AUTORIZACIÓN DE LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN

CONSTE POR EL PRESENTE EL VISTO BUENO QUE OTORGA EL ENCARGADO DE INVESTIGACIÓN DE

ESCUELA DE POSGRADO

A LA VERSIÓN FINAL DEL TRABAJO DE INVESTIGACIÓN QUE PRESENTA:

JARA MENDOZA OMAR YINO

INFORME TÍTULADO:

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA MEJORAR EL PROCESO DE GESTIÓN DEL RIESGO EN UN GOBIERNO LOCAL, 2018

PARA OBTENER EL TÍTULO O GRADO DE:

Maestro en Ingeniería de Sistemas con mención en Tecnologías de la Información

SUSTENTADO EN FECHA: 25 de Enero del 2019

NOTA O MENCIÓN: Aprobado por unanimidad

ESCUELA DE POSGRADO UCV UNIVERSIDAD CÉSAR VALLEJO INVESTIGACIÓN CAMPUS NORTE

FIRMA DEL ENCARGADO DE INVESTIGACIÓN