



UNIVERSIDAD CATÓLICA LOS ÁNGELES
CHIMBOTE

FACULTAD DE INGENIERÍA
ESCUELA PROFESIONAL DE INGENIERÍA DE
SISTEMAS

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA
INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE PIRA
APLICANDO LA NORMA ISO/IEC 27001:2013

TESIS PARA OPTAR TÍTULO PROFESIONAL DE INGENIERA
DE SISTEMAS

AUTORA

CASTILLO COLLAZOS, ROXANA ELIDA

ASESOR

JAMANCA RAMÍREZ, MARCO ANTONIO

HUARAZ – PERÚ

2016

JURADO EVALUADOR DE TESIS

ING. KRAMER SILVERIO GARAY GÓMEZ

Presidente

ING. MIGUEL ÁNGEL SILVA ZAPATA

Secretario

MGTR. JUAN RAÚL CADILLO LEÓN

Miembro

AGRADECIMIENTO

Doy gracias a Dios por permitirme tener tan buena experiencia dentro de la universidad.

Gracias a la universidad por permitirme en ser un profesional en lo que tanto me apasiona.

Gracias a cada maestro que hizo parte de este proceso integral de formación, que deja como producto terminado a esta persona, y como recuerdo y prueba viviente en la historia; esta tesis, que perdurará dentro de los conocimientos y desarrollo de la demás generaciones.

Finalmente agradezco a quien lee este apartado y más de mi tesis, por permitir a mis experiencias, investigaciones y conocimiento, incurrir dentro de su repertorio de información mental.

Roxana C.

DEDICATORIA

A dios, por permitirme llegar a este momento tan especial en mi vida. Por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más.

A mis padres, quienes me vieron nacer; a sus enseñanzas y a sus buenas costumbres que han creado en mí sabiduría haciendo que hoy tenga el conocimiento para el desarrollo de mi carrera profesional.

A mi esfuerzo y dedicación, que gracias a ello logro alcanzar mis propósitos.

Para una gran persona quien me enseñó que en el trabajo los retos difíciles siempre deben de solucionarse.

Roxana C.

RESUMEN

El presente informe propone un SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA MUNICIPALIDAD DISTRITAL DE PIRA de acuerdo al estándar internacional ISO/IEC 27001:2013 debido a que las medidas de control para satisfacer los requisitos mínimos en seguridad han sido efectivas sólo parcialmente por lo que se diagnosticó la situación actual de la municipalidad.

Posteriormente se desarrolló el SGSI basado en la fase de planeación de la norma ISO/IEC 27001:2013 y en los controles. Como metodología de Análisis de Gestión del Riesgo se empleó MAGERIT versión 3.0. Orientado a todos los sectores de la organización, es decir, administradores de sistemas de gestión de seguridad de la información.

MAGERIT se aplica a los sistemas de información de toda la Municipalidad Distrital de Pira, incluyendo los computadores personales y las redes. Está basado en la filosofía de que los recursos que necesitan ser administrados por un conjunto de procesos agrupados para proveer la información pertinente y confiable que requiere una organización para lograr sus objetivos.

Concluida la tesis se dieron las recomendaciones con respecto al correcto uso y administración de los activos, a la seguridad de la información y los cambios que se requieran para lograr mejores resultados en los sistemas de gestión de seguridad de la información en la Municipalidad Distrital de Pira.

Palabras Clave: Sistema de gestión de seguridad de la información (SGSI),

ISO/IEC 27001:2013, MAGERIT versión 3.0

ABSTRACT

This research work proposes the use of the information security management system in the municipality in the district of Pira in accordance with the international standard ISO/IEC 27001:2013, since that the control measures that satisfies the minimum requirements in security information had been partially effective in that municipality. After finishing to obtain all the data about the situation at the municipality in the district of Pira; the ISMS (Information Security Management System) was applied based on the planning phase of ISO/IEC 27001:2013. It was also applied the methodology of analysis and risk management (MAGERIT version 3.0) which was oriented to all sectors of the organization; that is to say, to the administrators of the security management system.

MAGERIT versión 3.0 was applied to all the the information system at the municipality of Pira including to personal computers and social networking. MAGERIT is based on the philosophy that all the resources that are needed to be administered by a set of grouped processes and provides relevant and reliable information requires a good organization to achieve its goals.

When the thesis was finished recommendations and suggestions were given regarding to the correct use of administration assets, the security of information and the changes needed to achieve better results in the information security management system in the municipality in the district of Pira.

Key Words: Information Security Management System (ISMS), ISO/IEC 27001:2013, MAGERIT version 3.0

ÍNDICE DE CONTENIDO

JURADO EVALUADOR DE TESIS	II
AGRADECIMIENTO	III
DEDICATORIA	IV
RESUMEN	V
ABSTRACT	VI
ÍNDICE DE CONTENIDO	VII
ÍNDICE DE TABLAS	

IX ÍNDICE DE GRÁFICOS

.....	XI
I. INTRODUCCIÓN	XIII
II. REVISIÓN DE LA LITERATURA	21
2.1. ANTECEDENTES	21
2.1.1. Antecedentes internacionales	21
2.1.2. Antecedentes nacionales	24
2.2. BASES TEÓRICAS	27
2.2.1. Municipalidad	27
2.2.2. Seguridad	27
2.2.3. Información	28
2.2.4. Activos de información	28
2.2.5. Sistemas informáticos	28
2.2.6. Sistemas de información	29
2.2.7. Sistema de información para la administración	29

2.2.8. Seguridad informática	31
2.2.9. Seguridad de la información	32
2.2.10. Normativas de Seguridad	34
2.2.11. Sistema de gestión de seguridad de información (SGSI)	36
2.2.12. Estándar De Gestión De La Seguridad De La Información	43
2.2.13. La Normativa ISO/IEC 27001:2013	48
2.2.14. El modelo de madurez de la seguridad de la información	67
2.2.15. Gestión de Riesgos	68
2.2.16. Metodologías	72
2.2.16.1. MAGERIT V.03	73
2.3. HIPÓTESIS	101
III. METODOLOGÍA	102
3.1. DISEÑO DE LA INVESTIGACIÓN	102
3.2. POBLACIÓN Y MUESTRA	103
3.3. DEFINICIÓN Y OPERACIONALIZACIÓN DE VARIABLES E INDICADORES	105
3.4. TÉCNICAS E INSTRUMENTOS DE RECOLECCIÓN DE DATOS	106
3.5. PLAN DE ANÁLISIS	107
3.6. MATRIZ DE CONSISTENCIA	108
3.7. PRINCIPIOS ÉTICOS	109
IV. RESULTADOS	110
4.1. RESULTADOS	110
4.2. ANÁLISIS DE RESULTADOS	128
V. CONCLUSIONES	129

VI. RECOMENDACIONES	130
REFERENCIAS BIBLIOGRÁFICAS	131
ANEXOS	136
ÍNDICE DE TABLAS Tabla N° 01 : Diferencia entre seguridad de la información y protección de datos	¡Error! Marcador no definido.
Tabla N° 02 : Evolución de la organización British Standard Institute (BSI).....	34
Tabla N° 03 : Relación de serie de las normas ISO/IEC 27000	43
Tabla N° 04 : Relación de activos de seguridad de la información	75
Tabla N° 05 : Criterios de valoración de los activos.....	78
Tabla N° 06 : ¿Conoce las Políticas de seguridad de la Información?	110
Tabla N° 07 : ¿Usted cree que debe sentirse responsable e identificarse con el equipo	111
informático que usa o utilizará en algún momento dentro de la Municipalidad Distrital de Pira?.....	111
Tabla N° 08 : ¿Cuándo se ausenta de su oficina deja bloqueada la PC?	113
Tabla N° 09 : ¿Cuándo se ausenta de su oficina deja documentación visible en su	114
escritorio?Tabla N° 10 : ¿Has utilizado algún dispositivo externo para extraer algún tipo de	115
información de trabajo o de su interés?.....	115
Tabla N° 11 : ¿La clave de acceso es la misma para todos los sistemas con los que cuenta la Municipalidad Distrital de Pira?	116
Tabla N° 12 : ¿Comparte sus claves de acceso con sus compañeros de trabajo?....	117
Tabla N° 13 : ¿Ud. cambia con frecuencia sus Claves de acceso?.....	118
Tabla N° 14 : ¿Ud. Ha observado que algún compañero ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en cualquiera de las computadoras de la Municipalidad Distrital de Pira?.....	119
Tabla N° 15 : ¿Cuenta con correo electrónico?	120

Tabla N° 16 : ¿Reconoce Ud. Cuáles son los activos importantes de la Municipalidad Distrital de Pira?	121
Tabla N° 17 : ¿Usted ha detectado que el antivirus de la Municipalidad Distrital de Pira funciona adecuadamente y que se encuentra actualizado?	123
Tabla N° 18 : ¿Qué es lo que hace con la información que ya no necesita?	124
Tabla N° 19 : ¿Usted apaga los equipos informáticos correctamente después de utilizarlos?	126
Tabla N° 20 : ¿Existe alguna alarma contra incendios, robos, otros?.....	127
Tabla N° 21 : ¿Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información?	128

ÍNDICE DE GRÁFICOS

Ilustración N° 01: Modelo de las cuatro actividades básicas de un SI	31
Ilustración N° 02: Los 03 Pilares de Seguridad de la Información	34
Ilustración N° 03: Procesos de un Sistema de Gestión de Seguridad de Información	37
Ilustración N° 04: Ciclo PDCA para la implementación de SGSI	38
Ilustración N° 05: Evolución estructural del ISO 27001	46
Ilustración N° 06: Dominios de seguridad normativa ISO/ 27001:2013	48
Ilustración N° 07: Elementos del análisis de riesgos potenciales	74
Ilustración N° 08: MAR – Método de análisis de Riesgo	76
Ilustración N° 09: ¿Conoce las Políticas de seguridad de la Información?	110
Ilustración N° 10: ¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la Municipalidad Distrital de Pira?	111

Ilustración N° 11: ¿Cuándo se ausenta de su oficina deja bloqueada la PC?	112
Ilustración N° 12: ¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?	113
Ilustración N° 13: ¿Has utilizado algún dispositivo externo para extraer algún tipo de información de trabajo o de su interés?	114
Ilustración N° 14: ¿La clave de acceso es la misma para todos los sistemas con los que cuenta la Municipalidad Distrital de Pira?	115
Ilustración N° 15: ¿Comparte sus claves de acceso con sus compañeros de trabajo?	116
Ilustración N° 16: ¿Ud. cambia con frecuencia sus Claves de acceso?	117
Ilustración N° 17: ¿Ud. Ha observado que algún compañero ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en cualquiera de las computadoras de la Municipalidad Distrital de Pira?	118
Ilustración N° 18: ¿Cuenta con correo electrónico?	120
Ilustración N° 19: ¿Reconoce Ud. Cuáles son los activos importantes de la Municipalidad Distrital de Pira?	121
Ilustración N° 20: ¿Usted ha detectado que el antivirus de la Municipalidad Distrital de Pira funciona adecuadamente y que se encuentra actualizado?	122
Ilustración N° 21: ¿Qué es lo que hace con la información que ya no necesita?	124
Ilustración N° 22: ¿Usted apaga los equipos informáticos correctamente después de utilizarlos?	125
Ilustración N° 23: ¿Existe alguna alarma contra incendios, robos, otros?	126
Ilustración N° 24: ¿Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información?	127

I. INTRODUCCIÓN

En la actualidad, es un hecho que las Organizaciones utilizan la tecnología de la información y las comunicaciones para ampliar cobertura en sus servicios y competir ante un mercado globalizado, ofreciendo a sus clientes múltiples opciones para acceder a sus productos y servicios. Adicional a ello, las Tics también les han permitido llevar organizado todos sus procesos administrativos en línea, para poder operar y/o funcionar de manera alineada o distribuida, sus sistemas de información.

Lo anterior conlleva a que de alguna manera, las empresas tiendan a ser más vulnerables o atacadas por cualquier persona que tenga el conocimiento o tal vez por una organización delincriminal que utiliza diferentes herramientas tecnológicas para afectar a sus víctimas y obtener beneficios. Hoy en día las Organizaciones han tomado conciencia de la necesidad de implementar sistemas de seguridad informática para proteger su información y evitar el riesgo a un posible ataque. En este sentido, el Sistema de Gestión de la Seguridad de la información (SGSI) pretende mostrar las técnicas y metodologías apropiadas y actuales que se deben utilizar para que las empresas salvaguarden su información; igualmente se utilicen las normas ISO como

los estándares internacionales certificados para la implantación de Sistemas de Seguridad de la Información con alta calidad.

De acuerdo a lo anterior las organizaciones además de proteger sus activos físicos, están asegurando sus sistemas de información ya que estos le crean una dependencia considerablemente para el cumplimiento de su misión y visión empresarial y su estado económico. Hoy las empresas acuden a consultores y/o auditores especializados para que les realicen los estudios pertinentes para el análisis del funcionamiento de su empresa, las respectivas políticas de seguridad y certificaciones con el objetivo de obtener un alto nivel de seguridad en su empresa. Esta investigación, describe todos los aspectos que involucra un sistema de gestión de seguridad de la información (SGSI), además mirar como las empresas han evolucionado entorno a la necesidad de asegurar su información como uno de los activos más importantes para el correcto funcionamiento de su organización.

En tal sentido llevar de manera remota los procesos administrativos así como la comunicación entre sus trabajadores, necesarios para su funcionamiento es otro de los beneficios que la tecnología de la Información y las comunicaciones brinda a las empresas. El mismo servicio en la web que las empresas de hoy presta a sus trabajadores, los ha afectado a ellos de alguna manera, por cuanto a través de los pagos en línea que han realizado para la compra de servicios, consultas, actualización de datos, entre otros son aprovechados también por los delincuentes para acceder a sus claves o contraseñas, a sus computadoras personales para copia y/o eliminación de su información entre otras. Lo anterior hace que de alguna forma, las personas se nieguen a realizar transacciones a través de estos medios de comunicación masiva como internet perdiendo las organizaciones posibles clientes potenciales a nivel mundial. En

este orden, las empresas deben garantizar a sus clientes una transacción protegida, así como las orientaciones pertinentes para evitar fraudes interinaticos.

En concordancia con la necesidad de las empresas de asegurar su información además de sus dispositivos computacionales y de comunicación, de manera organizada, sistemática, documentada y conocida, que involucre todos los aspectos físicos, lógicos y humanos de la organización. ISO como organización Internacional de Estándares, ha definido el estándar ISO 27001 para La gestión de la seguridad de la información.

El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

En esta investigación se trabajara con seguridad informática, estándares de gestión de la seguridad de la información SGSI y Procesos de análisis de riesgos.

En el primer lugar enfocaremos los pilares de la seguridad informática y un estado del arte sobre la implementación de sistemas de gestión planteada por las empresas de hoy. Seguidamente se enfatizará los elementos contemplados por el estándar ISO para la implementación de un SGSI. Y el último capítulo enfoca un aspecto importante que permite a las empresas conocer el estado actual en que se encuentra sus activos de información a través del análisis de riesgos.

Hoy en día vivimos en un mundo globalizado, donde se necesita gestionar la seguridad de la información inicia de un ámbito cada día más globalizado donde las organizaciones deben enfrentar y tomar decisiones correctas y eficientes convirtiendo

la información en uno de los activos más importantes dentro de las organizaciones llegando a tener una estrategia ya que con ello les permite una ventaja competitiva frente a otras organizaciones.

La seguridad de la información se encarga de la búsqueda de la preservación de la Confidencialidad, integridad así como la disponibilidad de la información, es decir, cada vez más se busca proteger de los riesgos e inseguridades procedentes de una amplia variedad de fuentes tanto en ataques físicos, tales como robos, incendios o inundaciones, como de ataques cibernéticos que aprovechan las vulnerabilidades de los sistemas de información, así como fraudes basados en informática, espionaje, sabotaje, también ciertas fuentes de daños como virus informáticos y ataques de intrusión o de negación de servicios los cuales se están volviendo cada vez más comunes, ambiciosos y sofisticados.

Considerando que esta información esté disponible para diferentes usuarios e interacciones, ya sea para la toma de decisiones, realización de reportes, inventarios, planeamientos, estadísticas y entre otros.

Sin embargo, qué sucede si los activos de información no son utilizados según su objetivo y son usados para otros fines no autorizados y malintencionados.

Sabemos que toda información asume un riesgo sino existen las medidas necesarias y correctivas para evitarlo.

La municipalidad es una entidad pública que tiene como objetivo promover toda clase de actividades y prestar los servicios públicos que contribuyan a satisfacer las aspiraciones y necesidades de la comunidad. Esto ha originado un crecimiento constante y sostenido de su plataforma tecnológica, además de sus activos, tales como

la información, el hardware, el software y los recursos humanos entre otros, estando expuestos a situaciones de inseguridad.

Actualmente no cuenta con los controles adecuados en la seguridad de información orientado al resguardo y prevención de sus activos de información; tales como:

- Déficit de Criterios en la selección y contratación del personal así como la formación, cambio de puesto de trabajo o la finalización del mismo.
- Carencia de un control de acceso efectivo a las instalaciones de la Municipalidad.
- Existencia de usuarios que acceden a información que no es de su competencia.
- Sustracción indebida de información por parte del personal que ya no ejercen funciones dentro de la Municipalidad.
- Abandono de un Control continuo de la administración de los sistemas de antivirus pertenecientes a la red
- Falta de un sistema de control de inventarios.
- Falta de control de uso malintencionado de claves de accesos y dispositivos.
- Ausencia de un sistema de control de custodia de Expedientes.

Por lo antes expuesto es necesario establecer herramientas, procedimientos y controles que aseguren la confidencialidad, disponibilidad, e integridad de la información, con ellos garantizar a que accedan a la información quienes están designados para su uso, esté disponible cuando se requiera y permanezca tal como fue creada por sus propietarios y asegurar también la actualización de la misma.

Por lo anteriormente expresado, el enunciado del problema de investigación es el siguiente: ¿Cómo el desarrollo de un sistema de gestión de seguridad de la información basada en la norma ISO/IEC 27001:2013, permitirá una adecuada

administración en la seguridad de los activos de información en la Municipalidad Distrital de Pira?

Para dar respuesta al problema, se ha planteado el siguiente objetivo general: Evaluar el sistema de gestión de seguridad de la información en la Municipalidad Distrital de Pira basado en la norma ISO/IEC 27001:2013; la cual permitirá una mejor administración en los activos de información.

Para poder conseguir el objetivo general, se planteó los siguientes objetivos específicos:

- a) Identificar la existencia de los riesgos considerando la seguridad de la información.
- b) Evaluar los mecanismos de seguridad, localizando los problemas.
- c) Desarrollar el informe final en base a la Norma ISO 27001/2013, apoyado de metodología MAGERIT V.03.

Considerando la justificación de la investigación esta se justifica por la necesidad de tener una descripción clara del nivel de gestión del proceso, esto permitirá evaluar un Sistema de Gestión de Seguridad de la información aplicando la norma ISO/IEC 27001:2013 en la Municipalidad, que requiere de un sistema de seguridad de la información para salvaguardar sus activos. La información junto con los procesos que la administran además de cada una de las personas que hacen parte de los mismos siendo estos el pilar fundamental para la organización.

La importancia que tiene la seguridad de la información y el poder que implica manejar información es un tema muy delicado que no está en el conocimiento de muchas organizaciones las cuales hacen grandes inversiones en sistemas y dispositivos de seguridad como: firewalls, antivirus, sistemas de respaldo entre otros; Uno de los

parámetros fundamentales a medir y analizar en la seguridad de la información son los incidentes, es decir, los eventos no deseados que se detectan en la red o en los servicios y que pueden poner en riesgo la disponibilidad, la confidencialidad o la integridad de la información. Cada evento debe ser registrado y calificado para así poder determinar cómo reaccionar ante cada incidente. Por ello, los mecanismos de seguridad necesitan de un sistema de gestión basada en el ISO/IEC 27001:2013 que los integre a las políticas generales de la Municipalidad.

Una evaluación del sistema de gestión de seguridad de la Información permite maximizar los esfuerzos desarrollados para asegurar la organización en todos sus niveles, aporta una metodología para el análisis y gestión del riesgo y garantiza la implantación de medidas de seguridad consistente, eficiente y apropiada al valor de la información protegida.

Es así como la Municipalidad se beneficiaría con la evaluación de un sistema de gestión de seguridad de la Información basada en el ISO/IEC 27001:2013 pues éste permitirá establecer políticas, procedimientos, objetivos y procesos claros que permitan determinar y establecer controles de seguridad que ayuden a tratar los riesgos en la Seguridad de la Información comprendiendo espacios físicos, procesos automáticos y manuales, gestión del personal, usuarios de los sistemas y equipos para optimizar la gestión de los incidentes que se detecten y generar resultados en concordancia con las políticas y objetivos generales de la Municipalidad.

Esta investigación tiene un alcance y limitaciones que busca proponer un sistema de gestión de seguridad de la Información en la Municipalidad del Distrito de Pira. El alcance y las limitaciones del proyecto se describen a continuación.

El alcance del presente proyecto, abarca un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001:2013, para resguardar la

confidencialidad, disponibilidad e integridad de los activos de información en la municipalidad distrital de Pira.

El alcance del proyecto solo estará precedido por un diagnóstico de la situación actual de la seguridad de la información, que permita un análisis comparativo de los controles a ser implantados o requeridos en la Municipalidad. Las limitaciones del proyecto de tesis consistirá solo en un sistema de gestión de la seguridad de la información basada en la norma ISO/IEC 27001:2013, pero no abarca la parte de la implementación del SGSI en la Organización.

II. REVISIÓN DE LA LITERATURA

2.1. Antecedentes

2.1.1. Antecedentes internacionales

Guachi Aucapiña, T.V., Guevara Aulestia D.O. (2012), en Ambato. Ecuador.⁽¹⁾, Elaboro la tesis “Norma De Seguridad Informática ISO 27001 Para Mejorar La Confidencialidad, Integridad Y Disponibilidad De Los Sistemas De Información Y Comunicación En El Departamento De Sistemas De La Cooperativa De Ahorro Y Crédito San Francisco Ltda.” – Universidad Técnica de Ambato. El presente proyecto reúne la información necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001, se ha concebido esta norma para garantizar la selección de controles de seguridad adecuados y proporcionales. Ello ayuda a proteger los activos de información y otorga confianza a cualquiera de las partes interesadas, sobre todo a los clientes. La norma adopta un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un SGSI.

La presente tesis ayudo a como implantar la norma de seguridad informática ISO 27001 para mejorar la confidencialidad, integridad y disponibilidad de los sistemas de información y comunicación en la municipalidad distrital de Pira.

Barragán, I., Góngora I., & Martínez, E. (2013), En Guayaquil. Ecuador.⁽²⁾, se presentó la tesis “Implementación de políticas de seguridad informática para la municipalidad de Guayaquil aplicando la norma ISO/IEC 27002”, su objetivo fue formular un modelo de política de seguridad de la información que sirva de punto de partida para la elaboración de políticas correspondientes tomando como base estándares internacionales, se decidió basar el modelo en la norma ISO/IEC 27002, como un marco de referencias para la gestión de la seguridad de la información ,

concluyendo que la forma de conseguir el mayor beneficio en seguridad de la información es contar con una adecuada evaluación de riesgos, que oriente las inversiones, que minimicen el impacto en caso de incidentes , dando a conocer que la seguridad de la información no es una responsabilidad únicamente del área de tecnología , debe fluir desde la alta gerencia hacia todos los procesos de negocios.

La presente tesis apoyo en el alcance del objetivo de sus políticas generales en relación a la consideración de los accesos de los usuarios y de las condiciones del uso de las claves de acceso.

Aguirre Cardona, J. D., & Aristizabal Betancourt, C. (2013), en Pereira. Ecuador.⁽³⁾ se presentó la tesis “Diseño del sistema de gestión de seguridad de la información para el Grupo Empresarial La Ofrenda”, su propósito fue diseñar el sistema de gestión de seguridad de la información para el grupo Empresarial La ofrenda ya que dicha organización no contaba con un SGSI, para así poder determinar los riesgos que se presentan con la información que se maneja en la empresa, utilizando herramientas tecnológicas y de desarrollo que permitan la gestión de los procesos que avalen la SI, aplicar los controles de la Norma ISO 27001 que permitan administrar el funcionamiento de un sistema de detección de intrusos dentro de un SGSI, se aplicó el modelo COBIT que se basa en un conjunto de herramientas de soporte del gobierno TI que les permitió a los gerentes cubrir la brecha entre los requerimientos de control , los aspectos técnicos y riesgos del negocio, concluyo que actualmente se vive en una época en que la información y los datos poseen una importancia decisiva en la gran mayoría de las organizaciones, convirtiéndose así en su activo más importante, se debe tener en cuenta que hay que recalcar que de nada sirve contar con un SGSI, que consideren todos los posibles riesgos y controles para mitigarlos o contar con toda la

tecnología posible para asegurar la información de la compañía si no se da una debida importancia a la seguridad de la información por parte de la alta gerencia y no se cumplen las políticas y procedimientos establecidos por parte del personal de la empresa.

La presente investigación nos sirvió como orientación en el Sistema de Gestión de Seguridad de la Información; el cual considera a la Norma ISO 27001:2005 para salvaguardar la Información.

Yagual Del Valle, C., & Chilán, L. (2014), en Guayaquil. Ecuador.⁽⁴⁾, se presentó la tesis “Análisis para la integración de un Sistema de Gestión de Seguridad de Información (SGSI) ISO-27001 Utilizando OSSIM para empresa Industrial” – Universidad Politécnica SALESIANA, su objetivo general de esta tesis fue minimizar los riesgos de seguridad de la información mediante el análisis previo a la implementación de la norma ISO 27001 combinando las herramientas de seguridad que ofrece OSSIM logrando así el fortalecimiento de un sistema de gestión de control eficiente para el área de Tecnología de información, como también proponer políticas y objetivos para la seguridad de la información, identificar los activos más críticos de los diferentes procesos de la empresa, donde aplicara controles adecuados previniendo riesgos encontrados, permitirá la visualización de análisis de eventos de vulnerabilidad que pudieran presentarse dentro de la infraestructura de la empresa mediante la consola de aplicación OSSIM.

El presente proyecto nos sirvió como orientación en el Sistema de Gestión de Seguridad de la Información; el cual considera minimizar los riesgos de seguridad de la información mediante el análisis previo a la implementación de la norma ISO 27001.

2.1.2. Antecedentes nacionales

Montoya Pachas, N. K. (2012), en Lima. Perú.⁽⁵⁾, presentó la tesis “Diseño de un sistema de gestión de seguridad de información para un centro cultural binacional”, su propósito fue proteger los activos de la información ante las amenazas a las cuales están expuestas, y de esta manera dar un tratamiento a los riesgos de información en los procesos de la Municipalidad , este proyecto se realizó siguiendo lo propuesto en la Norma ISO/IEC 27001:2005 para elaborar el diseño de un SGSI donde se establezcan una política, objetivos , procesos y procedimientos ,concluyendo así que el Centro Cultural, y las organizaciones en general deben tomar en cuenta la seguridad de la información de la empresa y de esa forma proteger su activo más valioso que es la información.

La presente investigación brindó un apoyo en la consideración del Sistema de Gestión de Seguridad de la Información el cual se basó bajo la misma Norma ISO 27001 de nuestra investigación, por lo que les permitió gestionar la seguridad de sus activos con el objetivo de darles un tratamiento adecuado.

Espinoza Aguinaga, H. R. (2013), En Lima. Perú. ⁽⁶⁾, realizó una tesis titulada: “Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo – Pontifica Universidad Católica del Perú”, el problema presentado en la empresa es en cuanto al manejo de la seguridad de la información. En el cual se planteó el análisis y diseño de un sistema de gestión de seguridad de información, basado en la norma ISO/IEC 27001:2005 para una empresa dedicada a la producción y comercialización de alimentos de consumo masivo. De las cuales era Inventariar los procesos de negocio, los procesos de

tecnologías de información (TI) que dan soporte al proceso de negocio y finalmente los activos relacionados con estos procesos. Además era Identificar y analizar los riesgos de seguridad de información de los principales procesos identificados y Elaborar el sistema de gestión de seguridad de información (SGSI) en base a la norma ISO/IEC 27001:2005 para el SGSI que se quiere diseñar, y elegir los controles basándose en la norma ISO/IEC 27002. Los resultados esperados es el inventariado de los procesos la cual se verificará en el documento en sí y con la matriz de riesgo determinar y entender qué procesos son esenciales para la continuidad de las operaciones, calcular su posible impacto y los tiempos máximos tolerables de interrupción así como sus tiempos estimados de recuperación. Para ello se realiza el análisis de riesgos. Documento con la declaración de aplicabilidad de la norma ISO 27001 para el SGSI que se quiere diseñar. Documentación obligatoria exigida por la norma ISO 27001 para implantar un SGSI.

El proyecto concluye con la adecuada gestión de la seguridad de información teniendo en cuenta el diseño de SGSI basado en la norma ISO/IEC 27001:2005, lo que se relaciona directamente con esta propuesta ya que se basó en la aplicación de un SGSI según la norma ISO 27001, versión actualizada.

Aguirre Mollehuanca, D.A. (2014), En Lima. Perú. ⁽⁷⁾, realizó una tesis titulada “Diseño De Un Sistema De Gestión De Seguridad De Información Para Servicios Postales Del Perú S.A.” La exigencia de la implementación de la norma técnica peruana NTP-ISO/IEC 27001:2008 en las entidades públicas nace de la necesidad de gestionar adecuadamente la seguridad de la información en cada una de estas empresas. Sin embargo, el desconocimiento de estos temas por parte de la alta dirección, ha ocasionado que no se tomen las medidas necesarias para asegurar el éxito de este proyecto en el tiempo estimado por la Oficina Nacional de Gobierno

Electrónico e Informática (ONGEI), entidad responsable de apoyar a las entidades públicas durante el proceso de implementación de la norma. Debido a ello, para la realización de este proyecto de fin de carrera, se decidió trabajar con una entidad pública como caso de estudio, a fin de diseñar un Sistema de Gestión de Seguridad de Información o SGSI que se acople a la normativa a la cual está sujeta la organización y que pueda, en un futuro, servir como referencia para la implementación del mismo. Por último, se presenta un documento llamado Declaración de Aplicabilidad en el cual se indica que controles de la NTP ISO/IEC 17799:2007 se pueden implementar dentro de la organización basado en el trabajo realizado dentro de la organización.

El proyecto concluye con la adecuada gestión de la seguridad de información, fue imprescindible, debido a que fue necesaria su intervención para ayudar a concientizar a los jefes y demás responsables de área a participar de las entrevistas de levantamiento de información y ayudó a que entendieran que el SGSI no solo busca proteger la información digital, sino toda la información crítica del negocio independientemente del medio que la contenga.

Talavera Álvarez, V. R. (2016), En Lima. Perú. ⁽⁸⁾, realizó una tesis titulada: “Diseño de un Sistema de Gestión de Seguridad de la Información para una Entidad Estatal de Salud de Acuerdo a la ISO/IEC 27001:2013”. En respuesta a este proyecto, las instituciones públicas han sido llamadas a realizar la implementación de diversos controles a través de un Sistema de Gestión de Seguridad de la Información y de diferentes normas, entre ellas la Norma Técnica NTP ISO/IEC 27001 con la finalidad de asegurar el buen uso y protección de la información crítica que manejen, ya sea de clientes o información estratégica interna. En la actualidad los sistemas que se utilizan para almacenar, procesar y transmitir información se encuentran en toda clase de

instituciones de diferentes rubros y funciones. Los sistemas de información se han vuelto más complejos debido a la globalización que tiene por consecuencia que las distancias geográficas ya no supongan un obstáculo. De esta forma se tiene que existe una cantidad cada vez mayor de personas que tienen acceso a información que podría ser crítica para las diferentes empresas e instituciones en las que trabajan. Adicionalmente a este riesgo interno, siempre se tiene presente el riesgo que supone la fuga de información sensible ya sea por medio de personas que cuentan con acceso a dicha información, como por terceros que han accedido a ella mediante algún mecanismo de ataque.

La presente investigación se considera justificada porque pretende apoyar en la consideración de la metodología de análisis de riesgo y valoración de los activos de información, lo que se relaciona directamente con este proyecto.

2.2. Bases teóricas

2.2.1. Municipalidad

Es la organización que se encarga de la administración local en un pueblo o ciudad, compuesta por un alcalde y varios concejales para la administración de los intereses de un municipio. ⁽⁹⁾

2.2.2. Seguridad

Característica que indica que un sistema está libre de todo peligro, daño o riesgo. ⁽¹⁰⁾

2.2.3. Información

Conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. ⁽¹⁰⁾

2.2.4. Activos de información

Los activos de información son los recursos que tienen valor o utilidad para la organización, sus operaciones comerciales y su continuidad, los cuales son necesarios

para que la organización funcione y alcance los objetivos que propone su dirección.

(11)

Los activos de información se pueden clasificar en las siguientes categorías:

- Activos de información (Datos, manuales del usuario)
- Documentos de papel (contratos, resoluciones)
- Activos de software (aplicación, software de sistemas)
- Personal (trabajadores, población)
- Imagen de la empresa y reputación
- Servicios (comunicaciones)

2.2.5. Sistemas informáticos

Es el conjunto de elementos hardware, software y periféricos que conectados entre sí, forman un ordenador que permiten la digitalización de todo un volumen de información reduciendo el espacio ocupado, pero, sobre todo, facilitando su análisis y procesado. Se gana en 'espacio', acceso, rapidez en el procesado de dicha información y mejoras en la presentación de dicha información. ⁽¹²⁾

2.2.6. Sistemas de información

Un sistema de información es un conjunto de elementos orientados al tratamiento y administración de datos e información, organizados y listos para su uso posterior, generados para cubrir una necesidad o un objetivo. ⁽¹²⁾

2.2.7. Sistema de información para la administración

Es un sistema de información basado en computadora, que presenta una colección de personas, procedimientos, bases, tienen como objetivo principal mostrar una visión general de la situación de la empresa. Consecuentemente, estos muestran la situación

de las operaciones regulares de la empresa para que los directivos puedan controlar, organizar, planear y dirigir. ⁽¹³⁾

Actividades básicas:

a) Entrada de información: Es el proceso mediante el cual el sistema de información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas.

- Las manuales son aquellas que se proporcionan en forma directa por el usuario.
- Las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos. Esto último se denomina interfaces automáticas. Las unidades típicas de entrada de datos a las computadoras son las terminales, las cintas magnéticas, las unidades de disco, los códigos de barras, el escáner, la voz, los

monitores sensibles al tacto, el teclado y el mouse, entre otras. ⁽¹⁴⁾

b) Almacenamiento de información: A través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. La información suele ser almacenada en estructuras de información denominadas archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros. ⁽¹⁴⁾

c) Procesamiento de información: Es la capacidad del sistema de información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser utilizada para la toma de

decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general de un año base. ⁽¹⁴⁾

d) Salida de Información: Es la capacidad de un sistema de información para sacar la información procesada o los datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, discos y la voz, entre otros. Es importante aclarar que la salida de un sistema de información puede constituir la entrada a otro sistema de información o módulo. En este caso, también existe una interface automática de salida.

Por ejemplo, el sistema de control de clientes tiene una interface automática de salida con el sistema de contabilidad, ya que genera las pólizas contables con los movimientos de los clientes. ⁽¹⁴⁾

Ilustración N° 01

Modelo de las cuatro actividades básicas de un SI



Fuente: ulavirtual.tecnologicocomfenalcovirtual.edu.com

Cuando se habla de seguridad en el ámbito de las Tecnología de la Información y Comunicación a menudo se confunden los conceptos de seguridad de la información y seguridad informática. Y siendo ambos realmente importantes y similares, hay diferencias entre ellos.

2.2.8. Seguridad informática

Es la que permite lograr que todos los sistemas informáticos utilizados en cualquier contexto, se encuentren seguro de cualquier daño o riesgos, ya sea por parte de personas ajenas que en forma voluntaria o involuntaria lo pueda hacer o de cualquier desastre natural. En este sentido, la protección de la información requiere de un conjunto de software o aplicativos diseñados, documentos estándares y metodologías existentes que permitan aplicar las normativas certificables internacionalmente y técnicas apropiadas para llevar un control en la seguridad. Se expresa control en la seguridad, porque se considera un tanto difícil garantizar la seguridad de la información en forma completa o llevada a un 100%, por cuanto intervienen diferentes amenazas a las que las organizaciones y/o personas se encuentran continuamente expuestas. ⁽¹⁵⁾

Considerar aspectos de seguridad significa:

- a) Conocer el peligro
- b) Clasificarlo
- c) Protegerse de los impactos o daños de la mejor manera posible.

En este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella. ⁽¹⁵⁾

Tabla N° 01

Diferencia entre seguridad de la información y protección de datos

SEGURIDAD DE LA INFORMACIÓN	PROTECCIÓN DE DATOS
Protección contra pérdida y modificación de los activos de información de la organización.	Protección de la personalidad y los derechos personales de los individuos, que salen en los datos, para evitar consecuencias negativas en contra de ellos.

Elaborado por: Castillo. R.; 2016

2.2.9. Seguridad de la información

Son aquellas medidas preventivas y reactivas de efectúa una Organización que permitan resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e Integridad de la misma. ⁽¹⁶⁾

Importancia

Evaluar los riesgos asociados, estableciendo estrategias y controles adecuados que aseguren una permanente protección de la información y de sus sistemas.

Es así, que la gestión de seguridad de la información permitirá:

- Asegurar el acceso a la información, previniendo la divulgación de la misma a personas o sistemas no autorizados.
- Asegurar la información con métodos de proceso exactos y completos, buscando mantener los datos libres de modificaciones no autorizadas.
- Asegurar que usuarios autorizados tengan acceso a la información y activos asociados cuando lo requieran, es decir que pueden encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. ⁽¹⁶⁾ Lo que se persigue proteger en la información, son los cuatro pilares importantes que conlleva a que la información sea protegida a gran escala, son:

a) La Confidencialidad

Es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización. ⁽¹⁶⁾

b) La Integridad

Es la propiedad que busca mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados. ⁽¹⁶⁾

c) La Disponibilidad

Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

La disponibilidad al acceso de la información y a los sistemas por personas autorizadas en el momento que así lo requiera. ⁽¹⁶⁾

En la seguridad de la información es importante señalar que su manejo está basado en la tecnología y debemos saber que puede ser confidencial. Puede ser divulgada, mal utilizada, robada, borrada, sabotada, etc. La información es poder, y según las posibilidades estratégicas que ofrece tener acceso cierta información, esta se clasifica como:

Crítica: Es indispensable para la operación de la empresa.

Valiosa: Es un activo de la empresa y muy valioso.

Sensible: Debe ser conocida por las personas autorizadas.

Ilustración N° 02

Los 03 Pilares de Seguridad de la Información

2.2.10. Normativas

Existen diferentes seguridad que las implantan para la información. Todas persiguen los mismos diseñadas para incluir departamentos que para obtener una seguridad mínima de la información procesada y transferida por el personal que hace parte de ella.



Fuente: krizmichell.blogspot.pe

de Seguridad

normativas de empresas de hoy seguridad de la estas normativas objetivos, ya que están a todas las unidades o estructura a la empresa

Se trataran en forma general la normativa encargada de la gestión de la seguridad de la información, por lo que se enfatizará en la normativa ISO/IEC 27001, teniendo en cuenta que es las más actual certificable internacionalmente utilizada. ⁽¹⁷⁾

2.2.10.1. Estructura de las normativas de gestión de la seguridad

Las normativas de seguridad, tienen la finalidad de presentar los lineamientos necesarios para que las empresas puedan implantar un sistema de gestión de la seguridad de la información (SGSI).

Un Sistema de Gestión de la seguridad de la información se implanta mediante un proceso ordenado que consiste en establecer los mecanismos necesarios de seguridad de manera documentada y conocida por todos los miembros de la empresa. Sin embargo es importante que se tenga claro que la implantación de un SGSI no garantiza

la protección en su totalidad ya que su propósito como lo anuncia claramente la ISO en su portal ISO27000.es, “garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías”.⁽¹⁸⁾

2.2.10.2. Origen de las normativas de seguridad

El Instituto británico de estándares (British Standard Institute), fue la primera organización que vio la necesidad de la creación de normativas, con el objetivo de ayudar a las empresas a mejorar sus diferentes actividades de negocio. Fue la precursora de muchas normativas que se han aplicado en otros países e inclusive es un organismo colaborador de ISO. La evolución obtenida a lo largo de los años se muestra a continuación en la siguiente tabla N° 02.⁽¹⁹⁾

Tabla N° 02

Evolución de la organización British Standard Institute (BSI)

Fecha	Alcance
1901	Nacimiento de la British Standard Institute (BSI)
1910	Creación del primer estándar
1926	Inicio del proceso de certificación de productos
1946	Creación de la ISO (Internacional Standard Organization)
1979	Primer estándar para los sistemas de gerencia (BS 5750)
1992	Elaboración del estándar sobre el medio ambiente

1999	Elaboración del estándar sobre seguridad de la información (BS 7799)
------	--

Elaborado por: Castillo. R.; 2016

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

Un SGSI es para una organización el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información. La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. La siguiente figura ilustra este modelo basado en los procedimientos esenciales para un SGSI. (20)

Ilustración N° 03

Procesos de un Sistema de Gestión de Seguridad de Información



Fuente: iso27001.es

Ciclo PDCA (Edward Deming)

Para la implantación de un sistema de Gestión de la seguridad de la información, se requiere del desarrollo de actividades que marquen un orden lógico para llevar

organizado todo el proceso. El modelo PDCA (Plan, do, check, act), en su equivalencia en español es Planificar, hacer, verificar y actuar (PHVA), es una estrategia de mejora continua de calidad en cuatro pasos. Este modelo es muy utilizado para implantación de sistemas de gestión, como los sistemas de gestión de la calidad que muchas empresas de hoy lo implantan para la calidad administrativa y de servicios con el objetivo de perfeccionarlos y continuar en un proceso de mejora continua.

Para el caso de la implantación de Sistemas de Gestión de la Seguridad informática, el ciclo PDCA es una estrategia efectiva para la organización y documentación que se requiere en este proceso. La siguiente figura ilustra este modelo basado en los procedimientos esenciales para un SGSI. ⁽²⁰⁾

Es una estrategia de mejora continua de la calidad en cuatro pasos (PDCA).

Ilustración N° 04

Ciclo PDCA para la implementación de SGSI



Fuente: <http://www.bulsuk.com/2009/02/taking-first-step-with-pdca.html>

PLAN: Establecer con planificación

- a.** Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- b.** Definir una política de seguridad que:
- Incluya el marco general y los objetivos de seguridad de la información de la organización
 - Considere requerimientos legales o contractuales relativos a la seguridad de la información
 - Esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI □ Establezca los criterios con los que se va a evaluar el riesgo
 - Esté aprobada por la dirección.
- c.** Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación del riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles (existen numerosas metodologías estandarizadas para la evaluación de riesgos, aunque es perfectamente aceptable definir una propia).
- d.** Identificar los riesgos:
- Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios
 - Identificar las amenazas en relación a los activos
 - Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas

- Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.
- e.** Analizar y evaluar los riesgos:
- Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información
 - Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados
 - Estimar los niveles de riesgo
 - Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- f.** Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
- Aplicar controles adecuados
 - Aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos
 - Evitar el riesgo, mediante el cese de las actividades que lo originan
 - Transferir el riesgo a terceros, en compañías aseguradoras o proveedores de outsourcing.
- g.** Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- h.** Aprobar por parte de la dirección tanto los riesgos residuales como la implantación y uso del SGSI.
- i.** Definir una declaración de aplicabilidad que incluya:

- Los objetivos de control y controles seleccionados y los motivos para su elección
- Los objetivos de control y controles que actualmente ya están implantados
- Los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además, detectar posibles omisiones involuntarias.

En relación a los controles de seguridad, el estándar ISO 27002 (antigua ISO 17799) proporciona una completa guía de implantación que contiene 133 controles, según 39 objetivos de control agrupados en 11 dominios. Esta norma es referenciada en ISO 27001, en su segunda cláusula, en términos de “documento indispensable para la aplicación de este documento” y deja abierta la posibilidad de incluir controles adicionales en el caso de que la guía no contemplase todas las necesidades

particulares.

DO: Implementar y utilizar el SGSI

- a. Definir un plan de tratamiento de riesgos que identifique las acciones, recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- b. Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.
- c. Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- d. Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.

- e. Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- f. Gestionar las operaciones del SGSI.
- g. Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- h. Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.
- i. Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

CHECK: Monitorizar y revisar el SGSI

La organización deberá:

- a. Ejecutar procedimientos de monitorización y revisión para:
 - Detectar a tiempo los errores en los resultados generados por el procesamiento de la información
 - Identificar brechas e incidentes de seguridad
 - Ayudar a la dirección a determinar si las actividades desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información se desarrollan en relación a lo previsto
 - Detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores
 - Determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.

- b. Revisar regularmente la efectividad del SGSI, atendiendo al cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- c. Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- d. Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio, las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior-requerimiento legal, obligaciones contractuales, etc.
- e. Realizar periódicamente de auditorías internas del SGSI en intervalos planificados.
- f. Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en el proceso del SGSI son evidentes.
- g. Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- h. Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

ACT: Mantener y mejorar el SGSI La

organización deberá regularmente:

- a. Implantar en el SGSI las mejoras identificadas.

- b. Realizar las acciones preventivas y correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones.
- c. Comunicar las acciones y mejoras a todas las partes interesadas con el nivel de detalle adecuado y acordar, si es pertinente, la forma de proceder.
- d. Asegurarse que las mejoras introducidas alcanzan los objetivos previstos.

2.2.12. Estándar De Gestión De La Seguridad De La Información

2.2.12.1. La organización ISO

International Standardization Organization, es la Organización Internacional para la Estandarización que se encarga de la normalización a nivel mundial, las cuales desarrollan bajo diferentes grupos o comités especializados las normativas, modelos o patrones a seguir con el objetivo de definir ciertas características que debe poseer un objeto o producto. ⁽²⁰⁾

La finalidad principal de las normas ISO es:

- Orientar
- Coordinar
- Simplificar
- Unificar los usos, Para conseguir menores costes y efectividad.

Familia de las normas ISO/IEC 27000

La serie ISO/IEC 27000, es un conjunto de normas de gestión de la seguridad de la información con la IEC (International Electrotechnical Commission), comisión internacional de electrotecnia. Cada una de las normas de la familia 27000, define y centra todos los aspectos importantes en el contexto de la gestión de la seguridad de la

información en cualquier empresa pequeña, mediana o grande, así como públicas y privadas. ⁽²⁰⁾

A continuación se relacionan en la siguiente tabla N° 03, la temática que define cada norma.

Tabla N° 03

Relación de serie de las normas ISO/IEC 27000

Normas	Temática
ISO 27000	Gestión de la seguridad de la información
ISO 27001	Especificaciones para un SGSI
ISO 27002	Código de buenas prácticas
ISO 27003	Guía de implantación de un SGSI
ISO 27004	Sistema de métricas e indicadores
ISO 27005	Guía de análisis y gestión de riesgos
ISO 27006	Especificaciones para Organismos Certificadores de SGSI.
ISO 27007	Guía para auditar un SGSI.

Elaborado por: Castillo. R.; 2016

A continuación se presenta un breve resumen de cada una de las normas relacionadas anteriormente para una mayor ilustración.

- **ISO 27000: Gestión de la seguridad de la información (Fundamentos y vocabulario)**

Esta norma fue publicada el 1 de mayo de 2009 y contemplan en forma introductoria todos los aspectos fundamentales que enfoca un sistema de gestión de seguridad de la información (SGSI), una descripción del ciclo PDCA, al igual que las definiciones de los términos que se emplean en toda la serie 27000.

- **ISO 27001 Especificaciones para un SGSI**

Esta norma fue publicada el 15 de Octubre de 2005, la cual enmarca los requisitos y/o especificaciones del sistema de Gestión de la seguridad de la información. Fue originaria de la BS 7799-2:2002, siendo identificada actualmente como norma ISO 27001:2013. Esta es la norma certificable en la actualidad por los auditores externos de los SGSI de las diferentes empresas. En esta norma se enumera en forma resumida, los objetivos de control y controles, para que sean seleccionadas por las empresas que desean implantar el SGS. Si bien es cierto que no es de carácter obligatorio que se implementen todos los controles de esta norma, la empresa debe justificar ante los auditores la no aplicabilidad de los controles cuando estén en el proceso de evaluación para una certificación.

Ilustración N° 05

Evolución estructural del ISO 27001



Fuente: Presentación Collazos. M.

- **ISO 27002: código de buenas prácticas**

Publicado el 1 de julio de 2007. Esta norma no certificable, es una guía de buenas prácticas que detalla los objetivos de control y controles recomendables en los aspectos de seguridad de la información.
- **ISO 27003: Guía de implantación de un SGSI**

Publicado el 1 de Febrero de 2010. Esta norma no es certificable y proporciona una guía que contempla todos los aspectos necesarios para el diseño e implementación de un SGSI de acuerdo a la norma certificable ISO/IEC 27001:2013. El objetivo de esta norma es describir las especificaciones y diseño en el proceso de la implementación del SGSI.
- **ISO 27004: Sistema de métricas e indicadores**

Publicada el 15 de Diciembre de 2009. No certificable. Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
- **ISO/IEC 27005**

Publicada en segunda edición el 1 de Junio de 2011 (primera edición del 15 de Junio de 2008). No certificable. Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
- **ISO/IEC 27006: Especificaciones para Organismos Certificadores de SGSI.**

Esta norma fue publicada en su primera edición el 1 de marzo de 2007 y su segunda edición el 1 de diciembre de 2011. Esta norma especifica los requisitos para la acreditación de entidades de auditoría y certificación de SGSI.

- **ISO 27007: Guía para auditar un SGSI.**

Esta norma fue publicada el 14 de Noviembre de 2011. Es una guía para la aplicación de auditorías a un SGSI como complemento especificado en ISO

19011, no es una norma certificable.

2.2.13. La Normativa ISO/IEC 27001:2013

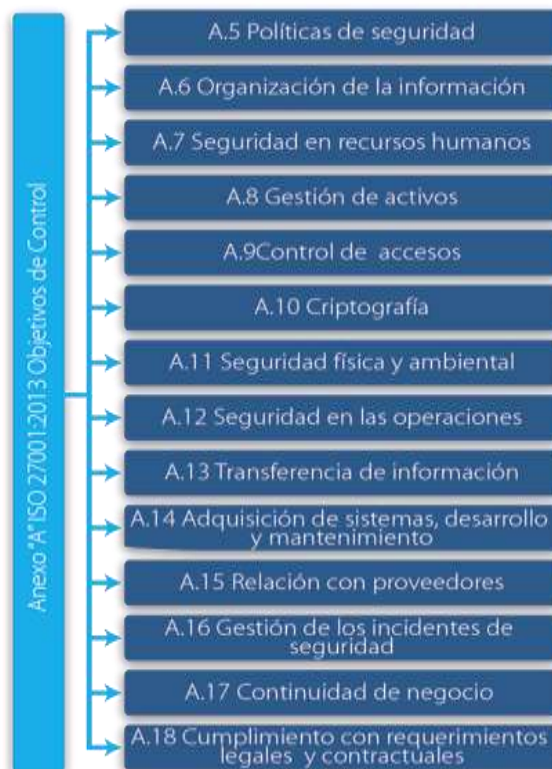
Estructura ISO/IEC 27001:2013

El estándar El ISO/IEC 27001: 2013, para los Sistemas Gestión de la Seguridad de la Información es un modelo de gestión de seguridad de la información, que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

Se define como un conjunto de lineamientos el cual especifica los requisitos para establecer, implementar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información. Estos requisitos describen cual es el comportamiento esperado del sistema de Gestión una vez que esté en funcionamiento. ⁽²⁰⁾

Ilustración N° 06:

Dominios de seguridad normativa ISO/ 27001:2013



Fuente: http://www.magazcitur.com.mx/?p=2397#.VpHuf_nhDIU

Cada dominio estipula unos objetivos en el Sistema de Gestión de Seguridad de Información, los controles de seguridad y la función.

A.5. Políticas de seguridad

En este dominio se especifica la forma de creación de un documento de política de seguridad, el cual debe ser elaborado por el equipo de trabajo que la dirección designa para la implementación del SGSI. Dicho documento debe ser revisado y aprobado por la dirección. En el documento de política de seguridad, se debe especificar toda la normativa interna de la institución con el objetivo de que los funcionarios conozcan y cumplan las medidas de seguridad implantadas a través del (SGSI). Así mismo contempla todos los aspectos orientados al acceso a la información, utilización de los activos físicos y lógicos de la organización y el comportamiento que deben tener en caso de que ocurra un incidente de seguridad. La elaboración del documento debe ser con un lenguaje claro y sencillo con el objetivo de que cualquier funcionario de la

empresa u organización lo pueda interpretar. La subdivisión de este control es la siguiente:

A.5.1.1 Documento de política de seguridad de la información

A.5.1.2 Revisión de la política de seguridad de la información.

A.6 Organización de la Información

Aquí se establece los parámetros internos y externos de la organización. Los internos, hacen referencia al compromiso que la dirección asume para la implantación del SGSI, la designación del equipo de personal que incluye el coordinador de seguridad y la asignación de responsabilidades entre otros. Los parámetros externos hacen referencia a los Riesgos relacionados con el acceso a terceros, seguridad con respecto a los clientes y contratación con terceros. Los subdominios o controles se relacionan a continuación.

A.6.1 Interna

A.6.1.1 Compromiso de la Dirección con la seguridad de la información

A.6.1.2 Coordinación de la seguridad de la información

A.6.1.3 Asignación de responsabilidades relativas a la seguridad de la información

A.6.1.4 Proceso de autorización de recursos para el procesado de la información

A.6.1.5 Acuerdos de confidencialidad

A.6.1.6 Contacto con las autoridades

A.6.1.7 Contacto con grupos de especial interés

A.6.1.8 Revisión independiente de la seguridad de la información

A.6.2 Externa (Terceros)

A.6.2.1 Identificación de los riesgos derivados del acceso de terceros

A.6.2.2 Tratamiento de la seguridad en la relación con los clientes

A.6.2.3 Tratamiento de la seguridad en contratos con terceros

A.7 Seguridad ligada a los recursos humanos:

Este dominio hace énfasis en todo el talento humano de la organización y demás personal contratado de manera externa, los cuales deben conocer las responsabilidades que adquieren para proteger la información, garantizar la seguridad y buen uso, así como mantener confidencialidad a la información que tienen acceso con este carácter. Es tarea de la organización hacer todo tipo de verificación jurídica al personal antes de ser contratado y establecer las debidas cláusulas contractuales para el cumplimiento de sus funciones, responsabilidades que tiene sobre los activos que utilizará entre otros. También deberá definir los procedimientos que se deben realizar cuando un trabajador tenga cambio de funciones o cambio de cargo o haya salido de la empresa por diferentes motivos.

A.7.1 Antes de la contratación

Las responsabilidades de la seguridad se deberían definir antes de la contratación laboral mediante la descripción adecuada del trabajo y los términos y condiciones del empleo.

Todos los candidatos para el empleo, los contratistas y los usuarios de terceras partes se deberían seleccionar adecuadamente, especialmente para los trabajos sensibles. Los trabajadores, contratistas y usuarios de terceras partes de los servicios de procesamiento de la información deberían firmar un acuerdo sobre sus funciones y responsabilidades con relación a la seguridad.

Conjuntamente con RRHH, de debería asegurar que se emplea un proceso de verificación de antecedentes proporcional a la clasificación de seguridad de aquella información a la que va a acceder el trabajador a contratar. Dicho simplemente, el

proceso de contratación de un administrador de sistemas TI debería ser muy diferente del de un administrativo. Haga comprobaciones de procedencia, formación, conocimientos, etc.

A.7.2 Durante la contratación

Se debería definir las responsabilidades de la Dirección para garantizar que la seguridad se aplica en todos los puestos de trabajo de las personas de la organización. A todos los usuarios trabajadores, contratistas y terceras personas se les debería proporcionar un adecuado nivel de concienciación, educación y capacitación en procedimientos de seguridad y en el uso correcto de los medios disponibles para el procesamiento de la información con objeto de minimizar los posibles riesgos de seguridad. Se debería establecer un proceso disciplinario normal para gestionar las brechas en seguridad.

La responsabilidad con respecto a la protección de la información no finaliza cuando un trabajador se va a casa o abandona la organización. Asegure que esto se documenta claramente en materiales de concienciación, contratos de empleo, etc. Contemple la posibilidad de una revisión anual por RRHH de los contratos junto con los trabajadores para refrescar las expectativas expuestas en los términos y condiciones de empleo, incluyendo su compromiso con la seguridad de la información.

A.7.3 Cese o cambio de puesto de trabajo

Se deberían establecer las responsabilidades para asegurar que el abandono de la organización por parte de los trabajadores, contratistas o terceras personas se controla, que se devuelve todo el equipamiento y se eliminan completamente todos los derechos de acceso. Los cambios en las responsabilidades y empleos en la organización se deberían manejar, en el caso de su finalización en línea con esta sección, La devolución de los activos de la organización cuando un trabajador se marcha sería mucho más

sencilla de verificar si el inventario de activos ha sido actualizado y verificado regularmente. Examine qué accesos necesita revocar en primer lugar cuando un trabajador presenta su carta de dimisión: ¿cuáles son los sistemas más críticos o vulnerables?

Haga un seguimiento del uso del e-mail por estas personas antes de salir definitivamente de la empresa, por si comienzan a sacar información confidencial (sujeto a las políticas aplicables y a consideraciones legales sobre privacidad).

A.8 Gestión de Activos

El objetivo del presente dominio es que la organización tenga conocimiento preciso sobre los activos que posee como parte importante de la administración de los riesgos.

Algunos ejemplos de activos son:

- **Recursos de información:** bases de datos y archivos, documentación de sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de continuidad y contingencia, información archivada, etc.
- **Recursos de software:** software de aplicaciones, sistemas operativos, herramientas de desarrollo y publicación de contenidos, utilitarios, etc.
- **Activos físicos:** equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, máquinas de fax, contestadores automáticos, switches de datos, etc.), medios magnéticos (cintas, discos, dispositivos móviles de almacenamiento de datos – pen drives, discos externos, etc.), otros equipos técnicos (relacionados con el

suministro eléctrico, unidades de aire acondicionado, controles automatizados de acceso, etc.), mobiliario, lugares de emplazamiento, etc.

- **Servicios:** servicios informáticos y de comunicaciones, utilitarios generales (calefacción, iluminación, energía eléctrica, etc.).

A.8.1 Responsabilidad sobre los activos

Todos los activos deberían ser justificados y tener asignado un propietario y se deberían identificar a los propietarios para todos los activos y asignarles la responsabilidad del mantenimiento de los controles adecuados. La implantación de controles específicos podría ser delegada por el propietario convenientemente. No obstante, el propietario permanece como responsable de la adecuada protección de los activos. El término “propietario” identifica a un individuo o entidad responsable, que cuenta con la aprobación del órgano de dirección, para el control de la producción, desarrollo, mantenimiento, uso y seguridad de los activos. El término “propietario” no significa que la persona disponga de los derechos de propiedad reales del activo.

Use códigos de barras para facilitar las tareas de realización de inventario y para vincular equipos de Tecnología de Información que entran y salen de las instalaciones.

A.8.2 Clasificación de la información

Se debería clasificar la información para indicar la necesidad, prioridades y nivel de protección previsto para su tratamiento.

La información tiene diversos grados de sensibilidad y criticidad. Algunos ítems podrían requerir niveles de protección adicionales o de un tratamiento especial. Debería utilizarse un esquema de clasificación de la información para definir el

conjunto adecuado de niveles de protección y comunicar la necesidad de medidas especiales para el tratamiento.

A.8.3 Manejo de los soportes de almacenamiento

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

A.9 Control de Accesos

El objetivo del presente dominio es controlar el acceso por medio de un sistema de restricciones y excepciones a la información como base de todo sistema de seguridad informática.

Para impedir el acceso no autorizado a los sistemas de información se deberían implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas de información, bases de datos y servicios de información, y estos deben estar claramente documentados, comunicados y controlados en cuanto a su cumplimiento.

Los procedimientos comprenden todas las etapas del ciclo de vida de los accesos de los usuarios de todos los niveles, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieren el acceso.

La cooperación de los usuarios es esencial para la eficacia de la seguridad, por lo tanto es necesario concientizar a los mismos acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento.

A.9.1 Requisitos de negocio para el control de accesos

Se deberían controlar los accesos a la información, los recursos de tratamiento de la información y los procesos de negocio en base a las necesidades de seguridad y de negocio de la Organización.

Las regulaciones para el control de los accesos deberían considerar las políticas de distribución de la información y de autorizaciones.

A.9.2 Gestión de acceso de usuario

Se deberían establecer procedimientos formales para controlar la asignación de los permisos de acceso a los sistemas y servicios de información.

Los procedimientos deberían cubrir todas la etapas del ciclo de vida del acceso de los usuarios, desde del registro inicial de los nuevos usuarios hasta su baja cuando ya no sea necesario su acceso a los sistemas y servicios de información.

A.9.3 Responsabilidades del usuario

La cooperación de los usuarios autorizados es esencial para una seguridad efectiva.

Los usuarios deberían ser conscientes de sus responsabilidades en el mantenimiento de controles de acceso eficaces, en particular respecto al uso de contraseñas y seguridad en los equipos puestos a su disposición.

Se debería implantar una política para mantener mesas de escritorio y monitores libres de cualquier información con objeto de reducir el riesgo de accesos no autorizados o el deterioro de documentos, medios y recursos para el tratamiento de la información.

A.9.4 Control de acceso a sistemas y aplicaciones

Los medios deberían ser controlados y físicamente protegidos.

Se deberían establecer los procedimientos operativos adecuados para proteger los documentos, medios informáticos (discos, cintas, etc.), datos de entrada o salida y

documentación del sistema contra la divulgación, modificación, retirada o destrucción de activos no autorizadas.

A.10 Criptografía

El objetivo del presente dominio es el uso de sistemas y técnicas criptográficas para la protección de la información en base al análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

La aplicación de medidas de cifrado se debería desarrollar en base a una política sobre el uso de controles criptográficos y al establecimiento de una gestión de las claves que sustenta la aplicación de las técnicas criptográficas.

A.10.1 Controles criptográficos

Controles con el objetivo de proteger la confidencialidad, autenticidad o integridad de la información mediante la ayuda de técnicas criptográficas.

Las organizaciones deberían utilizarán controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios, para la transmisión de información clasificada y/o para el resguardo de aquella información relevante en atención a los resultados de la evaluación de riesgos realizada por la organización.

A.11 Seguridad Física y Ambiental

El objetivo es minimizar los riesgos de daños e interferencias a la información y a las operaciones de la organización.

El establecimiento de perímetros de seguridad y áreas protegidas facilita la implementación de controles de protección de las instalaciones de procesamiento de información crítica o sensible de la organización, contra accesos físicos no autorizados. El control de los factores ambientales de origen interno y/o externo permite garantizar el correcto funcionamiento de los equipos de procesamiento y minimizar las interrupciones de servicio.

A.11.1 Áreas seguras

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

Los medios de procesamiento de información crítica o confidencial deberían ubicarse en áreas seguras, protegidas por los perímetros de seguridad definidos, con las barreras de seguridad y controles de entrada apropiados.

Los medios de procesamiento deberían estar físicamente protegidos del acceso no autorizado, daño e interferencia.

A.11.2 Seguridad de los equipos

Deberían protegerse los equipos contra las amenazas físicas y ambientales. La protección del equipo es necesaria para reducir el riesgo de acceso no autorizado a la información y su protección contra pérdida o robo.

Así mismo, se debería considerar la ubicación y eliminación de los equipos. Se podrían requerir controles especiales para la protección contra amenazas físicas y Para salvaguardar servicios de apoyo como energía eléctrica e infraestructura del cableado.

A.12 Seguridad en las Operaciones

El objetivo es controlar la existencia de los procedimientos de operaciones y el desarrollo y mantenimiento de documentación actualizada relacionada.

Adicionalmente, se debería evaluar el posible impacto operativo de los cambios previstos a sistemas y equipamiento y verificar su correcta implementación, asignando las responsabilidades correspondientes y administrando los medios técnicos necesarios para permitir la segregación de los ambientes y responsabilidades en el procesamiento. Con el fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario, sería necesario monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.

A.12.1 Responsabilidades y procedimientos de operación

Asegurar la operación correcta y segura de los medios de procesamiento de la información mediante el desarrollo de los procedimientos de operación apropiados. Se deberían establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

Se debería implantar la segregación de tareas, cuando sea adecuado, para reducir el riesgo de un mal uso del sistema deliberado o por negligencia.

A.12.2 Protección contra código malicioso

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos y se requiere tomar precauciones para evitar y detectar la introducción de códigos de programación maliciosos y códigos con capacidad de reproducción y distribución automática no autorizados para la protección de la integridad del software y de la información que sustentan. El código malicioso es código informático que provoca infracciones de seguridad para dañar un sistema informático. El malware se refiere específicamente a software malicioso, pero el código malicioso incluye además scripts de sitios web (applets de Java, controles de ActiveX, contenido insertado, plug-ins, lenguajes de scripts u otros lenguajes de

programación en páginas web y correo electrónico) que pueden aprovechar vulnerabilidades con el fin de descargar un malware.

A.12.3 Copias de seguridad

Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación.

Se deberían establecer procedimientos rutinarios para conseguir la estrategia aceptada de respaldo para realizar copias de seguridad y probar su puntual recuperación.

Implante procedimientos de backup y recuperación que satisfagan no sólo requisitos contractuales sino también requisitos de negocio "internos" de la organización.

A.12.4 Registro de actividad y supervisión

Los sistemas deberían ser monitoreados y los eventos de la seguridad de información registrados.

El registro de los operadores y el registro de fallas deberían ser usados para garantizar la identificación de los problemas del sistema de información.

La organización debería cumplir con todos los requerimientos legales aplicables para el monitoreo y el registro de actividades. El monitoreo del sistema debería ser utilizado para verificar la efectividad de los controles adoptados y para verificar la conformidad del modelo de política de acceso.

A.12.5 Control del software en explotación

Se trata de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

Verificar que los cambios sean gestionados por personal autorizado y en atención a los términos y condiciones que surjan de la licencia de uso.

Efectuar un análisis de riesgos previo a los cambios en atención al posible impacto por situaciones adversas.

Aplicar los cambios en sistemas de prueba y/o de manera escalonada empezando por los sistemas menos críticos además de aplicar medidas de backups y puntos de restauración junto a actividades adicionales que permitan retornar los sistemas al estado de estabilidad inicial con ciertas garantías.

Actualizar la documentación para cada cambio implementado, tanto de los manuales de usuario como de la documentación operativa.

Informar a las áreas usuarias antes de la implementación de un cambio que pueda afectar sus operaciones y involucrar a usuarios finales en pruebas de aceptación del nuevo estado.

A.12.6 Gestión de la vulnerabilidad técnica

Se trata de minimizar los riesgos de alteración de los sistemas de información mediante controles de implementación de cambios imponiendo el cumplimiento de procedimientos formales que garanticen que se cumplan los procedimientos de seguridad y control, respetando la división de funciones.

A.12.7 Consideraciones de las auditorías de los sistemas de información

Maximizar la efectividad del proceso de auditoría de los sistemas de información y minimizar las intromisiones a/desde éste proceso.

Durante las auditorías de los sistemas de información debieran existir controles para salvaguardar los sistemas operacionales y herramientas de auditoría.

A.13 Transferencia de información (Telecomunicaciones)

El objetivo es asegurar la protección de la información que se comunica por redes telemáticas y la protección de la infraestructura de soporte.

La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicaciones legales, monitoreo y protección.

La información confidencial que pasa a través de redes públicas suele requerir de controles adicionales de protección.

A.13.1 Gestión de la seguridad en las redes

Se deberían controlar los accesos a servicios internos y externos conectados en red. El acceso de los usuarios a redes y servicios en red no debería comprometer la seguridad de los servicios en red si se garantizan:

- a) que existen interfaces adecuadas entre la red de la Organización y las redes públicas o privadas de otras organizaciones
- b) que los mecanismos de autenticación adecuados se aplican a los usuarios y equipos
- c) el cumplimiento del control de los accesos de los usuarios a los servicios de información

A.13.2 Intercambio de información con partes externas

Se deberían realizar los intercambios sobre la base de una política formal de intercambio, según los acuerdos de intercambio y cumplir con la legislación correspondiente. Se deberían establecer procedimientos y normas para proteger la información y los medios físicos que contienen información en tránsito.

A.14 Adquisición de sistemas, desarrollo y mantenimiento de los sistemas de información

El objetivo es asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.

Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.

Definir los métodos de protección de la información crítica o sensible.

A.14.1 Requisitos de seguridad de los sistemas de información

El diseño e implantación de los sistemas de información que sustentan los procesos de negocio pueden ser cruciales para la seguridad. Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información. Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

A.14.2 Seguridad en los procesos de desarrollo y soporte

Se deberían controlar estrictamente los entornos de desarrollo de proyectos y de soporte.

Los directivos responsables de los sistemas de aplicaciones deberían ser también responsables de la seguridad del proyecto o del entorno de soporte. Ellos deberían garantizar que todas las propuestas de cambio en los sistemas son revisadas para verificar que no comprometen la seguridad del sistema o del entorno operativo.

A.14.3 Datos de prueba

Se debería evitar la exposición de datos sensibles en entornos de prueba. Para proteger los datos de prueba se deberían establecer normas y procedimientos que contemplen prohibir el uso de bases de datos operativas.

A.15 Relaciones con Suministradores (Proveedores)

El objetivo es implementar y mantener el nivel apropiado de seguridad de la información y la entrega de los servicios contratados en línea con los acuerdos de entrega de servicios de terceros.

A.15.1 Seguridad de la información en las relaciones con suministradores

La seguridad de la información de la organización y las instalaciones de procesamiento de la información no debería ser reducida por la introducción de un servicio o producto externo.

Debería controlarse el acceso de terceros a los dispositivos de tratamiento de información de la organización.

A.15.2 Gestión de la prestación del servicio por suministradores

La organización debería verificar la implementación de acuerdos, el monitoreo de su cumplimiento y gestión de los cambios con el fin de asegurar que los servicios que se prestan cumplen con todos los requerimientos acordados con los terceros.

A.16 Gestión de los incidentes de Seguridad

El objetivo es garantizar que los eventos de seguridad de la información y las debilidades asociados a los sistemas de información sean comunicados de forma tal que se apliquen las acciones correctivas en el tiempo oportuno.

Las organizaciones cuentan con innumerables activos de información, cada uno expuesto a sufrir incidentes de seguridad. Resulta necesario contar con una capacidad de gestión de dichos incidentes que permita comenzar por su detección, llevar a cabo su tratamiento y colaborar en la prevención de futuros incidentes similares.

A.16.1 Gestión de incidentes de seguridad de la información y mejoras Deberían establecerse las responsabilidades y procedimientos para manejar los eventos y debilidades en la seguridad de información de una manera efectiva y una vez que hayan sido comunicados.

A.17 Continuidad de Negocio

El objetivo es preservar la seguridad de la información durante las fases de activación, de desarrollo de procesos, procedimientos y planes para la continuidad de negocio y de vuelta a la normalidad.

Se deberían analizar las consecuencias de los desastres, fallas de seguridad, pérdidas de servicio y la disponibilidad del servicio y desarrollar e implantar planes de contingencia para asegurar que los procesos del negocio se pueden restaurar en los plazos requeridos las operaciones esenciales, manteniendo las consideraciones en seguridad de la información utilizada en los planes de continuidad y función de los resultados del análisis de riesgos.

A.17.1 Continuidad de la seguridad de la información

Se deberían determinar los requisitos de seguridad de la información al planificar la continuidad de los procesos de negocio y la recuperación ante desastres.

La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y cambios de implementación para mantener los controles de seguridad de la información existentes durante una situación adversa.

Si los controles de seguridad no pueden continuar resguardando la información ante situaciones adversas, se deberían establecer, implementar y mantener otros controles para mantener un nivel aceptable de seguridad de la información.

A.17.2 Redundancias

Se deberían considerar los componentes o arquitecturas redundantes cuando no se pueda garantizar el nivel de disponibilidad requerido por las actividades de la organización a través de arquitecturas sencillas típicas o los sistemas existentes se demuestren insuficientes.

A.18 Cumplimiento con Requerimientos Legales y Contractuales

El diseño, operación, uso y administración de los sistemas de información están regulados por disposiciones legales y contractuales.

Los requisitos normativos y contractuales pertinentes a cada sistema de información deberían estar debidamente definidos y documentados.

El objetivo es cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la organización y/o a los trabajadores que incurran en responsabilidad civil o penal como resultado de incumplimientos.

A.18.1 Cumplimiento de los requisitos legales y contractuales

El diseño, operación, uso y gestión de los sistemas de información pueden ser objeto de requisitos estatutarios, reguladores y de seguridad contractuales.

Los requisitos legales específicos deberían ser advertidos por los asesores legales de la organización o por profesionales adecuadamente cualificados.

Los requisitos que marca la legislación cambian de un país a otro y pueden variar para la información que se genera en un país y se transmite a otro país distinto (por ej., flujos de datos entre fronteras).

Obtenga asesoramiento legal competente, especialmente si la organización opera o tiene clientes en múltiples jurisdicciones.

A.18.2 Revisiones de la seguridad de la información

Se deberían realizar revisiones regulares de la seguridad de los sistemas de información.

Las revisiones se deberían realizar según las políticas de seguridad apropiadas y las plataformas técnicas y sistemas de información deberían ser auditados para el cumplimiento de los estándares adecuados de implantación de la seguridad y controles de seguridad documentados.

2.2.14. El modelo de madurez de la seguridad de la información

La Gestión de la Seguridad de la Información debe pasar por varios niveles o escalones, cada uno con su coste asociado y contexto de aplicabilidad. Se comienza a perfilar una escala de progresión en lo que ahora conocemos como Sistemas de Gestión de Seguridad de la Información basados en la norma ISO 27001. Considerando los avances y las preocupaciones actuales, esta escala se compondría de los siguientes niveles:

- **Nivel 0 (Sistema Inexistente):** el “sentido común”. Procesos Inexistentes
- **Nivel 1 (Sistema Intermitente):** el cumplimiento de la legislación obligatoria. Procesos desorganizados.
- **Nivel 2 (Sistema Intuitivo):** evaluación del proceso de Gestión de Seguridad. Procesos Inconsistentes.
- **Nivel 3 (Sistema Definido):** analizar el riesgo y la gestión de su resolución. Procesos Documentados y comunicados
- **Nivel 4 (Sistema Administrado):** adquisición de productos para integrarlos en los Sistemas de Gestión. Procesos medidos y monitoreados.
- **Nivel 5 (Sistema Optimizado):** integración de los componentes certificados en sistemas compuestos y su certificación. Mejores Prácticas.

2.2.15. Gestión de Riesgos

Es un método para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. ⁽²¹⁾

Contiene cuatro fases:

2.2.15.1. Análisis De Riesgos

El análisis de riesgos es uno de los procesos más relevantes y prioritarios para la implantación de SGSI, por ser el procedimiento que permite analizar en forma metódica cada uno de los procesos, actividades y demás labores de la empresa que pueden estar en riesgo, así como determinar las necesidades de seguridad, las posibles vulnerabilidades y las amenazas a las que se encuentra expuesta. En tal sentido, el resultado que se obtiene de todo un proceso de análisis de riesgo es la información sobre el estado actual de la empresa en cuanto a sus niveles, controles de seguridad y los riesgos. ⁽²¹⁾

Existen dos aspectos principales que determinarán el análisis de riesgo:

- **Probabilidad:** posibilidad de ocurrencia del riesgo, la cual se puede medir con criterios de frecuencia.
- **Impacto:** consecuencias que pueden ocasionar la materialización del riesgo en la organización.

2.2.15.2. Evaluación del riesgo

La evaluación involucra comparar niveles de riesgo con criterios definidos en el contexto. El objetivo de esta evaluación es la de identificar y evaluar los riesgos, los cuales son calculados por una combinación de valores de activos y niveles de requerimiento de seguridad. Con base en esta comparación, se puede considerar la necesidad de tratamiento; además las decisiones se deben tomar de acuerdo con los

requisitos legales, reglamentarios y otros. ⁽²¹⁾

Las decisiones para tratar el riesgo pueden incluir las siguientes opciones:

a) Evitar el riesgo: La opción de evitar el riesgo, describe cualquier acción donde las actividades del negocio, o las maneras de conducir la gestión comercial del negocio, se modifican, para así poder evitar la ocurrencia del riesgo.

Las maneras tradicionales para implementar esta opción son:

- Dejar de conducir ciertas actividades.
- Desplazar activos de información de un área riesgosa a otra.
- Decidir no procesar cierto tipo de información y no se consigue la protección adecuada.
- La decisión por la opción de “evitar el riesgo” debe ser balanceada contra las necesidades financieras y comerciales de la empresa.
- Aceptar el riesgo cuando no es posible mitigarlo y se debe continuar la actividad que lo originó.

2.2.15.3. Reducir el riesgo

Para los riesgos donde la opción de reducirlos ha sido escogida, se deben implementar los apropiados controles para disminuirlos a los niveles de aceptación previamente indefinidos por la empresa. ⁽²¹⁾

- Reduciendo la posibilidad que la vulnerabilidad sea explotada por las amenazas.
- Reduciendo la posibilidad de impacto si el riesgo ocurre detectando eventos no deseados, reaccionado y recuperándose de ellos.
- Transferir el riesgo fuera del apetito de riesgo, el riesgo se comparte con una o varias partes, pueden ser agentes externos.

2.2.15.4. Controles

Son las políticas, procedimientos, prácticas y estructuras organizacionales para reducir riesgos y que además proveen cierto grado de certeza de que se alcanzarán los objetivos del negocio. ⁽²¹⁾

Existen varias formas de establecer controles sobre riesgos organizacionales. La siguiente es:

- a. **Disuasivos:** su presencia disuade de la comisión de acciones en contra de alguna política o procedimiento establecido y considerado correcto.

Ejemplo:

Cámaras de vigilancia.

- b. **Preventivos:** detectan problemas antes que ocurran por medio de monitoreo constante.

Ejemplo:

Políticas de contratación.

Firewall: previene a la empresa contra posibles intrusos, reduciendo el riesgo de que la amenaza llegue a suceder

- c. **Detectivos:** detectan y reportan los problemas suscitados por errores u omisiones, en el momento en que éstos ocurren.

Ejemplo:

Uso de antivirus

Sistema de detección de intrusiones (IDS): Aporta información para avisar si llega a ocurrir un incidente de intrusos para actuar lo más rápido posible y poder reducir el daño que podría causar.

- d. **Represivos:** Reduce el daño que el incidente está provocando a la Organización o empresa.

Ejemplo:

Sistema de extinción de incendios: esta medida reduce el daño que provocará el incidente.

- e. **Correctivos:** minimizan el impacto de una amenaza ya consumada.

Ejemplo:

Copias de seguridad: permite recuperar a la organización del incidente y volver al estado normal antes del incidente

- f. **Evaluativos:** Se aplican para identificar evidencias para que sean analizadas y determinar las causas que lo provocaron, además de las acciones que se realizaron para la recuperación de la situación ocurrida.

Ejemplo:

Sistemas de gestión de registros (logs): la medida permite analizar todo lo que hace en un determinado sistema. Las causas que lo provocó, así como los pasos que se realizaron para dar solución.

Los activos pueden tener vulnerabilidades que son aprovechadas por las amenazas, las cuales conlleva al riesgo inminente en la empresa. En este orden se describe de manera sucinta cada elemento. ⁽²¹⁾

Activos

Los activos son todos los elementos que requiere una empresa u organización para el desarrollo de sus actividades misionales y las que serán tratadas durante el proceso de análisis de riesgos. Los activos pueden ser físicos como servidores, equipos, cableados, entre otros y lógicos como aplicaciones, bases de datos, sitios web, entre otros.

Amenazas

Son todos aquellos hechos que pueden ocurrir en una empresa, perjudicando directamente los activos ya sea en el funcionamiento incorrecto o eliminación del mismo.

Vulnerabilidades

Son todas las debilidades de seguridad en la cual se encuentran los activos que se han identificado en el análisis y son susceptibles de amenazas para su daño o destrucción.

Las vulnerabilidades pueden clasificarse en las siguientes categorías:

Falta de entrenamiento en seguridad, carencia de toma de conciencia en seguridad, falta de mecanismos de monitoreo, falta de políticas para el uso correcto de las telecomunicaciones, no eliminar los accesos al término del contrato de trabajo, carencia de procedimiento que asegure la entrega de activos al término del contrato de trabajo, trabajadores desmotivados.

2.2.16. Metodologías

Entre las metodologías más utilizadas para realizar el análisis de riesgo a una organización se tienen MAGERIT, OCTAVE y MEHARI entre otras, todas cumplen con el mismo objetivo, su diferencia se determina en la forma de presentación de los resultados. Para el caso de estudio de esta investigación, seleccionaremos la metodología MAGERIT ya que los resultados del análisis de riesgo se pueden expresar en valores cualitativos y cuantitativos (valores económicos), lo cual facilita la toma de decisiones en materia de seguridad por parte del alcalde, al conocer el impacto económico que se podría presentar si la empresa no invierte en la implantación de un sistema de seguridad de la información y comunicaciones. ⁽²²⁾

2.2.16.1. MAGERIT V.03

Es la metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España. Actualizada en 2012 en su versión 3. Esta metodología contempla diferentes actividades enmarcadas a los activos que una organización posee para el tratamiento de la información. A continuación se relacionan cada uno de los pasos que se deben contemplar en un proceso de análisis de riesgos, teniendo en cuenta un orden sistémico que permita concluir el riesgo actual en que se encuentra la empresa. ⁽²³⁾

Capítulo 3: Método de análisis de riesgo

Análisis de Riesgo

El análisis de los riesgos de seguridad de la información presentes en los procesos de negocio pertenecientes al alcance escogido para el análisis es una etapa fundamental en el desarrollo del SGSI. Este proceso establece la metodología que se utilizará para definir los criterios de aceptación y valoración de los riesgos de seguridad de la información, además de la identificación, análisis y evaluación de los mismos sirviendo como entrada directa para el proceso de determinación de los controles aplicables al escenario presentado.

La gestión de riesgos en la Municipalidad es requerida para el cumplimiento de la implementación de un SGSI que sea efectivo en el control de la información que se transmite a través de los procesos de la organización, siendo responsabilidad de la entidad institucional creada con la finalidad de mantener la gestión de la seguridad de la información. ⁽²³⁾

Método

Es una aproximación metódica para determinar el riesgo siguiendo unos pasos pautados:

- a) Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- b) Determinar a qué amenazas están expuestos aquellos activos.
- c) Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
- d) Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
- e) Estimar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

La siguiente ilustración recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

Ilustración 07

Elementos del análisis de riesgos potenciales



Fuente: MAGERIT versión 3

Formalización de las actividades

Este conjunto de actividades tiene los siguientes objetivos:

- Levantar un modelo del valor del sistema, identificando y valorando los activos relevantes.
- Levantar un mapa de riesgos del sistema, identificando y valorando las amenazas sobre aquellos activos.

- Levantar un conocimiento de la situación actual de salvaguardas.
- Evaluar el impacto posible sobre el sistema en estudio, tanto el impacto potencial (sin salvaguardas), como el impacto residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Evaluar el riesgo del sistema en estudio, tanto el riesgo potencial (sin salvaguardas), como el riesgo residual (incluyendo el efecto de las salvaguardas desplegadas para proteger el sistema).
- Informar de las áreas del sistema con mayor impacto y/o riesgo a fin de que se puedan tomar las decisiones de tratamiento con motivo justificado.

El análisis de los riesgos se lleva a cabo por medio de las siguientes tareas:

Ilustración 08

MAR – Método de análisis de Riesgo

MAR – Método de Análisis de Riesgos
MAR.1 – Caracterización de los activos
MAR.11 – Identificación de los activos
MAR.12 – Dependencias entre activos
MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
MAR.21 – Identificación de las amenazas
MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
MAR.31 – Identificación de las salvaguardas pertinentes
MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
MAR.41 – Estimación del impacto
MAR.42 – Estimación del riesgo

Fuente: MAGERIT versión 3.0

MAR. 1 – Caracterización de los activos

Esta actividad busca identificar los activos relevantes dentro del sistema a analizar, caracterizándolos por el tipo de activo, identificando las relaciones entre los diferentes activos, determinando en qué dimensiones de seguridad son importantes y valorando esta importancia.

MAR.1.1 – Identificación de los Activos

Una buena identificación es importante desde varios puntos de vista:

- materializa con precisión el alcance del proyecto
- permite la interlocución con los grupos de usuarios: todos hablan el mismo lenguaje permite determinar las dependencias precisas entre activos
- permite valorar los activos con precisión
- permite identificar y valorar las amenazas con precisión
- permite determinar qué salvaguardas serán necesarias para proteger el sistema

MAR.1.2 – Dependencia entre Activos

Como se mencionó anteriormente, los activos son todos los elementos que una organización posee para el tratamiento de la información (hardware, software, recurso humano, etc.). MAGERIT diferencia los activos agrupándolos en varios tipos de

acuerdo a la función que ejercen en el tratamiento de la información. A la hora de realizar el análisis de riesgo el primer paso es identificar los activos que existen en la organización y determinar el tipo. (En la tabla N° 04) se relacionan cada tipo de activos.

Tabla N° 04

Relación de activos de seguridad de la información

Tipos de activos	Descripción
Activo de información	Bases de datos, documentación (manuales de usuario, contratos, normativas, etc.)
Software o aplicación	Sistemas de información, herramientas de desarrollo, aplicativos desarrollados y en desarrollo, sistemas operativos, aplicaciones de servidores etc.
Hardware	Equipos de oficina (PC, portátiles, servidores, dispositivos móviles, etc.)
Red	Dispositivos de conectividad de redes (router, swith, concentradores, etc.)
Equipamiento auxiliar	Sistema de alimentación ininterrumpida (SAI)-(UPS) es un dispositivo que gracias a sus baterías u otros elementos almacenadores de energía, puede proporcionar energía eléctrica por un tiempo limitado y durante un apagón eléctrico a todos los dispositivos que tenga conectados.
Instalación	Cableado estructurado, instalaciones eléctricas.
Servicios	Conectividad a internet, servicios de mantenimiento, etc.

Personal	Personal informático (administradores, webmaster, desarrolladores, etc.), usuarios finales y personal técnico.
----------	--

Elaborado por: Castillo. R.; 2016

El levantamiento de la información de los activos y la respectiva clasificación es la primera actividad que se debe realizar en un análisis de riesgos. Esta identificación se debe hacer en conjunto con las personas directamente responsables de manejar en la organización todo el sistema de información y comunicaciones.

MAR. 1.3 – Valoración de los Activos

Cada activo de información tiene una valoración distinta en la empresa, puesto que cada uno cumple una función diferente en la generación, almacenaje o procesamiento de la información. Pero a la hora de valorarlos no sólo debemos tener en cuenta cuanto le costó a la empresa adquirirlo o desarrollarlo, sino que además debemos contemplar el costo por la función que ella desempeña y el costo que genera ponerlo nuevamente en marcha en caso de que éste llegase a dañarse o deteriorarse. Es por ello que se hace necesario tener en cuenta diferentes variables a la hora de darle valor a un activo. En libro I en la metodología MAGERIT que es la que actualmente estamos estudiando, expone que los activos se deben valorar de acuerdo 5 dimensiones de seguridad (confiabilidad, integridad, disponibilidad, autenticidad y trazabilidad). Durante la investigación se implementó las 4 primeras dimensiones como pilares de la seguridad, pero no se contempló trazabilidad que la metodología incluye. Por tal razón, define que a efectos técnicos se traducen en mantener la integridad y la confidencialidad de ciertos activos del sistema que pueden ser los servicios de directorio, las claves de firma digital, los registros de actividad, etc.

La metodología MAGERIT contempla dos tipos de valoraciones, cualitativa y cuantitativa. La primera hace referencia al de calcular un valor a través de una escala cualitativa donde se valora el activo de acuerdo al impacto que puede causar en la empresa su daño o pérdida, en consecuencia la escala se refleja en:

- Muy Alto (MA)
- Alto (A)
- Medio (M)
- Bajo (b)
- Muy bajo (MB)

En el libro III, “guía técnica”, en la página 6, se encuentra en detalle esta valoración.

En cuanto a la valoración cuantitativa es necesario también que se realice una escala de valores que permita a la empresa estimar su costo que no sólo es el costo que tuvo inicialmente el activo sino teniendo en cuenta variables de valor inicial, costo de reposición, costo de configuración, costo de uso del activo y valor de pérdida de oportunidad. En la guía técnica se explica esta valoración cuantitativa pero no en profundidad, por lo tanto se detalla los términos en que se podría valorar un activo.

- Valor de reposición
- Valor de configuración o puesta a punto
- Valor de uso del activo

De acuerdo a dicha valoración es preciso que se estime 5 escalas que podríamos asignar a cada activo de acuerdo a la valoración cualitativa dada. Se relaciona con la escala cuantitativa.

Dimensiones de Seguridad

Como se mencionó anteriormente, las dimensiones de seguridad que contempla la metodología MAGERIT son: Confiabilidad, integridad, autenticidad, disponibilidad y

trazabilidad, el cual se puede profundizar cada una, en el Libro II: Catálogo de Elementos, en el capítulo 3 pagina 15. Para contemplar en la valoración de activos cada una de estas dimensiones, es necesario definir unos criterios de valoración que nos permitan ubicar la posición en que se encuentra cada activo frente a cada dimensión. A continuación se relacionan los criterios que se podrían tener en cuenta para valorar los activos con respecto a cada dimensión de seguridad, ver tabla N°. 05.

Tabla N° 05

Criterios de valoración de los activos

VALOR	CRITERIO
10	Daño muy grave a la organización
7-9	Daño grave a la organización
4-6	Daño importante a la organización
1-3	Daño menor a la organización
0	Irrelevante para la organización

Elaborado por: Castillo. R.; 2016

MAR.2 – Caracterización de las Amenazas

Esta actividad busca identificar las amenazas relevantes sobre el sistema a analizar, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

MAR.2.1 Identificación de las Amenazas

Una Amenaza es todo aquello, ya sea físico o lógico que puede causar un incidente no deseado, generando daños materiales o inmateriales a la organización y a sus activos, como la pérdida de información o de su privacidad, o bien un fallo en los equipos físicos.

En las organizaciones, los activos de información están sujetos a distintas formas de amenazas.

MAGERIT, en el libro II, catálogo de elementos, presenta el catálogo de amenazas posibles que puede tener un activo de información. Las amenazas se clasifican en cuatro grandes grupos: Desastres naturales(N), de origen industrial (I), errores y fallos no intencionados (E), ataques deliberados o intencionados(A). Cada grupo de amenaza se representa por una letra, así mismo cada grupo presenta en forma específica los tipos de amenazas que se pueden presentar. A continuación se presenta el listado codificado de las posibles amenazas que se pueden presentar en cada uno de los grupos mencionados.

[N] Desastres naturales

[N.1] Fuego

[N.2] Daños por agua

[N.*] Desastres naturales

[I] De origen industrial

[I.1] Fuego

[I.2] Daños por agua

[I*] Desastres industriales

[I.3] Contaminación mecánica

[I.4] Contaminación electromagnética

[I.5] Avería de origen físico o lógico

[I.6] Corte del suministro eléctrico

[I.7] Condiciones inadecuadas de temperatura o humedad

[I.8] Fallo de servicios de comunicaciones

[I.9] Interrupción de otros servicios o suministros esenciales

[I.10] Degradación de los soportes de almacenamiento de la información

[I.11] Emanaciones electromagnéticas

[E] Errores y fallos no intencionados

[E.1] Errores de los usuarios

[E.2] Errores del administrador

[E.3] Errores de monitorización (log)

[E.4] Errores de configuración

[E.7] Deficiencias en la organización

[E.8] Difusión de software dañino

[E.9] Errores de [re-]encaminamiento

[E.10] Errores de secuencia

[E.14] Fugas de información

[E.15] Alteración de la información

[E.16] Introducción de falsa información

[E.17] Degradación de la información

[E.18] Destrucción de la información

[E.19] Divulgación de información

[E.20] Vulnerabilidades de los programas (software)

[E.21] Errores de mantenimiento / actualización de programas (software)

[E.23] Errores de mantenimiento / actualización de equipos (hardware)

[E.24] Caída del sistema por agotamiento de recursos

[E.25] Pérdida de equipos

[E.28] Indisponibilidad del personal

[A] Ataques deliberados

[A.4] Manipulación de la configuración

- [A.5] Suplantación de la identidad del usuario
- [A.6] Abuso de privilegios de acceso
- [A.7] Uso no previsto
- [A.8] Difusión de software dañino
- [A.9] Encaminamiento de mensajes
- [A.10] Alteración de secuencia
- [A.11] Acceso no autorizado
- [A.12] Análisis de tráfico
- [A.13] Repudio
- [A.14] Interceptación de información (escucha)
- [A.15] Modificación de información
- [A.16] Introducción de falsa información
- [A.17] Corrupción de la información
- [A.18] Destrucción de la información
- [A.19] Divulgación de información
- [A.22] Manipulación de programas
- [A.24] Denegación de servicio
- [A.25] Robo de equipos
- [A.26] Ataque destructivo
- [A.27] Ocupación enemiga
- [A.28] Indisponibilidad del personal
- [A.29] Extorsión
- [A.30] Ingeniería social (picaresca)

MAR.2.2 – Valoración de Amenazas

MAGERIT, Toma como base el listado de amenazas propuesto la cual se procede a realizar la valoración de amenazas a cada uno de los activos, es decir, determinar que amenazas los puede afectar, con qué frecuencia se puede presentar la amenaza y que dimensión de seguridad puede ser afectada.

la valoración se puede realizar de manera porcentual; Así mismo se podría estimar en qué grado el activo es afectado sobre algunas de las dimensiones de seguridad que la metodología MAGERIT ha considerado como la Autenticidad (A), confiabilidad (C), integridad (I), disponibilidad (D).

La segunda para representar el nivel de frecuencia en que se puede presentar la amenaza, la cual se representa denotándose como: Alta (A), media (M), muy alta (MA), baja (B), muy baja (MB) que en nuestro caso, se estima de manera numérica en el cuadro que se presentara.

MAR.3 Caracterización de las Salvaguardas

Esta actividad busca identificar las salvaguardas desplegadas en el sistema a analizar, calificándolas por su eficacia frente a las amenazas que pretenden mitigar.

MAR.3.1 – Identificación de las salvaguardas pertinentes

Las amenazas estimadas en cada uno de los activos, el riesgo e impacto presentado son contempladas en caso de que no existan salvaguardias, la cual define MAGERIT, como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Es así como dentro del proceso de análisis de riesgos se contemplan las salvaguardias de los activos.

Impacto residual

El impacto residual supera el impacto potencial, por cuanto esta vez ya se ha aplicado en cada activo los salvaguardias de seguridad, lo cual minimizaría en cada activo el

impacto en caso de que materialicen las amenazas. Por tanto, este impacto deberá estar muy por debajo del impacto potencial.

Riesgo residual

El nivel de riesgo residual, es el riesgo que la institución puede asumir después de aplicar medidas o salvaguardias de seguridad. El nivel de riesgo residual obtenido supera el riesgo potencial, por tanto todo lo que éste por debajo de éste nivel no se considera una amenaza importante para la empresa.

MAR.3.2 Valoración de las salvaguardas

Así como se estimaron las amenazas para cada activo de información en el ítem de amenazas, también se debe estimar las salvaguardias para cada uno. En el libro II, catálogo de elementos se encuentra dieciséis tipos de salvaguardias, sin embargo, para seleccionarnos se debe tener en cuenta aspectos importantes que el libro I contempla, las cuales resumo a continuación:

- Tipo de activos a proteger, pues cada tipo se protege de una forma específica
- Dimensión o dimensiones de seguridad que requieren protección
- Amenazas de las que necesitamos protegernos
- Si existen salvaguardas alternativas

MAR.4 – Estimación del Estado de Riesgo

Esta actividad procesa todos los datos recopilados en las actividades anteriores para:

- Realizar un informe del estado de riesgo: estimación de impacto y riesgo
- Realizar un informe de insuficiencias: deficiencias o debilidades en el sistema de salvaguardas

MAR.4.1 – Estimación del Impacto

Teniendo como resultado la tabla resumen que se detalla, se puede determinar el impacto potencial que se puede estimar en la empresa en caso de que llegue a materializarse las amenazas consideradas en cada activo.

La definición del impacto que se puede producir en la empresa se resume sobre los activos esenciales, es decir, donde se centra la información que se maneja y los servicios prestados.

En el libro I (método) de la metodología MAGERIT, se habla sobre impacto acumulado y el impacto repercutido, el cual pueden mirar en detalle. Sin embargo considero suficiente hacer el análisis del impacto potencial a nivel general para de alguna manera mirar en forma general el estado de la empresa.

MAR.4.2 Estimación del Riesgo

Al determinar el impacto potencial, se debe determinar el riesgo que asume la empresa al no tener implementados controles de seguridad. En tal sentido, se tiene en cuenta también, que se debe estimar el riesgo por cada activo y en cada dimensión. Para MAGERIT, se denomina riesgo a la medida del daño probable sobre un sistema, al igual que la tabla resumen, así se debe determinar la probabilidad de la ocurrencia de la amenaza para detectar el riesgo.

Resultados del análisis de riesgos

Al desarrollar las fases consideradas en el análisis de riesgos se debe presentar a manera de resumen los resultados obtenidos. Dichos resultados pueden ser:

- Un análisis detallado de los activos relevantes a nivel de seguridad para la empresa.
- Un estudio de las posibles amenazas sobre los sistemas de información, así como cuál sería su impacto en la misma.

- Una evaluación del impacto potencial que tendría la materialización de las diferentes amenazas a que están expuestos nuestros activos.

Documentación

a. Documentación intermedia

MAGERIT V 3.0, especifica que según el análisis de riesgos genera un informe que proyecta el análisis de impacto y el riesgo potencial, que será presentado a los directivos de la empresa para que entren en conciencia del estado en que se encuentra la organización y los riesgos que ésta tendría que asumir como riesgo residual, después de haber implantado los salvaguardias.

Las utilidades de herramientas para análisis de riesgos permiten que se pueda presentar un resumen de cada uno de los pasos realizados en el análisis de riesgos incluyendo gráficas representativas que muestre la situación actual, el plan de remedios urgentes, el plan de seguridad y los objetivos a cumplir en largo plazo. En libro II, catálogo de elementos, en el apéndice 4, se estima que se deben realizar informes ejecutivos donde se excluyan los detalles, para dar una visión general del análisis de riesgo realizado. Los informes que proyecta este catálogo en la metodología MAGERIT y que a la vez, identifica numerándolos son:

- **Modelo de valor**

Informe que detalla los activos, sus dependencias, las dimensiones en las que son valiosos y la estimación de su valor en cada dimensión.

- **Mapa de riesgos:**

Informe que detalla las amenazas significativas sobre cada activo, caracterizándolas por su frecuencia de ocurrencia y por la degradación que causaría su materialización sobre el activo.

- **Evaluación de salvaguardas:**

Informe que detalla las salvaguardas existentes calificándolas en su eficacia para reducir el riesgo que afrontan.

- **Informe de insuficiencias o vulnerabilidades:**

Informe que detalla las salvaguardas necesarias pero ausentes o insuficientemente eficaces.

- **Declaración de aplicabilidad:**

Informe que recoge las contramedidas que se consideran apropiadas para defender el sistema de información bajo estudio.

- **Estado de riesgo:**

Informe que detalla para cada activo el impacto y el riesgo, potenciales y residuales, frente a cada amenaza.

Esta documentación es un fiel reflejo del estado de riesgo y de las razones por la que este riesgo no es aceptable. Es fundamental entender las razones que llevan a una valoración determinada de riesgo para que el proceso de gestión de riesgos esté bien fundamentado. El proceso de gestión de riesgos partirá de estas valoraciones para atajar el riesgo o reducirlo a niveles aceptables.

TASACIÓN DE ACTIVOS

LISTA DE ACTIVOS DE INFORMACIÓN												PLAN DE TRATAMIENTO DEL RIESGO				
Activos	Amenazas	Vulnerabilidades	Probabilidad de ocurrencia	Confidencialidad	Integridad	Disponibilidad	Posibilidad de ser las vulnerabilidades explotadas	Valores de activos en riesgo	Posibilidad de ocurrencia de amenazas	TOTAL	Actividades de mitigación de riesgo	Objetivo de control	Control	Responsable		
			Alto=3, Medio=2, Bajo=1													
Bienes de información (documentos)	Libro de Actas	Degradación soportes almacenamiento Datos	No se tiene un deposito adecuado	3			5				9.78	Almacenar los datos en una zona segura en buenas condiciones	11.1	11.1.4	Municipalidad	
		Introducción de falsa información	No se tiene un deposito adecuado	2	4	3	4	5	3.67			Revisión de la introducción de datos manualmente	12.2	12.2.1		
	Lista de Expedientes	Ferromentos naturales	No existe un sistema de respaldo de información	2				5					11.1	11.1.4	Municipalidad	
		Fuga de Información	Los equipos móviles no tienen restricciones de copiado de información	3				5					12.5	12.5.4		
		Divulgación de información	Los equipos móviles no tienen restricciones de copiado de información	3	5	4	3	5	4.00		10.67	Crear políticas en restricciones de copiado	11.2	11.2.2		
		Degradación soportes almacenamiento Datos	No se tiene un deposito adecuado	3			5					11.1	11.1.4			
Bienes físicos	Equipos informáticos	Corte del suministro eléctrico	UPS solo tiene autonomia de 15 minutos	1			2					11.1	11.1.4	Municipalidad		
		Avería de origen físico o lógico	No se tiene equipos redundantes	2	5	5	5	3	5.00	1.33	6.67	Aplicar equipos redundantes	17.1		17.1.1	
		Condiciones inadecuadas de T/Humed.	Aire acondicionado no es de precisión	1				1					11.2		11.2.4	
Bienes de Software	Sistema operativo	Corte del suministro eléctrico	No hay UPS para usuarios	2			1					11.1	11.1.4	Municipalidad		
		Avería de origen físico o lógico	Equipos tienen antigüedad mayor a 2 años	2	5	5	5	1	5.00	1.33	6.67	Mantenimiento mensual de equipos	11.2		11.2.4	
	Aplicaciones	Errores de los usuarios	Falta de entrenamiento	1				3				7.2	7.2.2	Municipalidad		
		Corte del suministro eléctrico	UPS solo tiene autonomia de 15 minutos	1				1				11.1	11.1.4			
		Avería de origen físico o lógico	No se tiene equipos redundantes	1	5	5	5	1	5.00	6.67	Aplicar equipos redundantes	17.1	17.1.1			
		Fallo de servicios de comunicaciones	No se tiene contratación de servicio de alta disponibilidad	1			3					17.1	17.1.1			
Personal	Municipalidad	Errores de los usuarios	Falta de entrenamiento	2			3					7.2	7.2.2	Municipalidad		
		Deficiencias en la organización	Alta rotación de personal del área	1			3					7.2	7.2.1			
		Fuga de Información	Los equipos móviles no tienen restricciones de copiado de información	2	1	2	4	5	2.33	1.40	3.27	5.1	5.1.1			
		Errores de configuración	Falta de entrenamiento	1				2				7.2	7.2.2			
		Difusión de softwares dañinos	Vencimiento de la licencia del antivirus	1				5				12.2	12.2.1			
Servicios	Telecomunicaciones	Falla de servicio	No se tiene un plan de contingencia	2			1					11.1	11.1.4	Alcaldía		
		Avería de origen físico o lógico	No se tiene equipos redundantes	2	5	3	2	1	3.33	1.50	5.00	Mantenimiento mensual de equipos	11.2		11.2.4	
		Errores de la instalación	Falta de entrenamiento	2				4				7.2	7.2.2			
	Internet	Corte del suministro eléctrico	UPS solo tiene autonomia de 15 minutos	1				1				11.1	11.1.4	Alcaldía		
		Avería de origen físico o lógico	No se tiene equipos redundantes	1	2	2	5	1	3.00	4.50	Mantenimiento mensual de equipos	11.2	11.2.4			
		Fallo de servicios de comunicaciones	No se tiene contratación de servicio de alta disponibilidad	1				2				17.1	17.1.1			

TASACIÓN DE LOS ACTIVOS DE INFORMACIÓN DE LA MUNICIPALIDAD DISTRITAL DE PIRA

Lista de activos de información

Flas de transmisión del riesgo

TIPO	CODIGO	Activos	Amenazas	Vulnerabilidades	Probabilidad de ocurrencia				TOTAL (Rango)	Actividades de mitigación de riesgo	Objetivo (si aplica)	Criterio	Responsable
					Muy Alta=5, Alta=4, Medio=3, Bajo=2, MuyBajo=1	Confidencial	Integridad	Disponibilidad					

Bienes de Software	ES-01	SIAF - Web	Corte del suministro eléctrico	No existe UPS	3				4	6	Grupo eléctrico	11.1	11.14	Alcaldía	
			Avená de origen físico o lógico	No tiene equipos redundantes	5	4	1	2	3	2	6	Mantenimiento mensual de equipos	11.2		11.24
			Erorres de los usuarios	Falta de entrenamiento	3						3	Capacitación continua	7.2		7.22
	ES-02	OPI - Web	Corte del suministro eléctrico	No existe UPS	3					4	6	Grupo eléctrico	11.1	11.14	Alcaldía
			Avená de origen físico o lógico	No tiene equipos redundantes	3	4	1	2	3	2	6	Aplicar equipos redundantes	17.1	17.11	
			Fallo de servicios de comunicaciones	Falta de entrenamiento	3						3	Contratar un servicio de alta disponibilidad	17.1	17.11	
	ES-03	SISFO - Web	Corte del suministro eléctrico	No existe UPS	3					4	6	Grupo eléctrico	11.1	11.14	Alcaldía
			Avená de origen físico o lógico	No tiene equipos redundantes	3	4	1	2	3	2	6	Mantenimiento mensual de equipos	11.2	11.24	
			Fallo de servicios de comunicaciones	Falta de entrenamiento	3						3	Capacitación continua	7.2	7.22	
	ES-04	Sistema Agente Nacion	Corte del suministro eléctrico	No existe UPS	3					4	6	Grupo eléctrico	11.1	11.14	Alcaldía
			Avená de origen físico o lógico	No tiene equipos redundantes	3	4	1	2	3	2	6	Aplicar equipos redundantes	17.1	17.11	
			Fallo de servicios de comunicaciones	Falta de entrenamiento	3						3	Capacitación continua	7.2	7.22	
ES-05	Microsoft Office	Corte del suministro eléctrico	No existe UPS	3					4	12	Grupo eléctrico	11.1	11.14	General	
		Avená de origen físico o lógico	No tiene equipos redundantes	3	5	5	5	3	5	12	Aplicar equipos redundantes	11.2	11.24		
		Fallo de servicios de comunicaciones	Falta de entrenamiento	3						3	Capacitación continua	7.2	7.22		
ES-06	Sistema operativo	Corte del suministro eléctrico	No existe UPS	3					4	12	Grupo eléctrico	11.1	11.14	General	
		Avená de origen físico o lógico	No tiene equipos redundantes	3	5	5	5	2	5	12	Aplicar equipos redundantes	17.1	17.11		
		Fallo de servicios de comunicaciones	Falta de entrenamiento	3						3	Capacitación continua	7.2	7.22		
Personal	P-01	Alcalde	Erorres de los usuarios	Falta de entrenamiento	3					9	Capacitación continua	7.2	7.22	Alcaldía	
			Deficiencias en la organización	Falta de capacitación del personal	3	3	3	3	3	3	9	Mantener clave personal	7.2		7.21
	P-02	Secretaria General	Paga de Información	Los equipos móviles no tienen restricciones de copiado de informados	2					1	9	Crear políticas en restricciones de copiado	17.1	17.13	Alcaldía
			Erorres de los usuarios	Falta de entrenamiento	3						3	Capacitación continua	7.2	7.22	
	P-03	Regidores	Erorres de configuración	Falta de entrenamiento	2	2	3	4	3	3	9	Capacitación continua	7.2	7.22	Concejo Municipal
			Difusión de software dañino	La licencia del antivirus vencida	3						4	Extensión de licencias de software de protección	14.2	14.21	
	P-04	Jefe Recursos Humanos	Erorres de configuración	Falta de entrenamiento	3					3	9	Capacitación continua	7.2	7.22	Unidad Recursos Humanos
			Erorres de configuración	Falta de capacitación	3	4	4	4	3	4	12	Capacitación continua	7.2	7.22	
	P-05	Jefe Abastecimiento y Control Patrimonial	Difusión de software dañino	Licencias vencidas	3					3	12	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad de Abastecimiento y Control Patrimonial
			Erorres de configuración	Falta de entrenamiento	3	4	3	4	3	4	12	Capacitación continua	7.2	7.22	
	P-06	Encargada Tesorería	Erorres de configuración	Falta de entrenamiento	3					3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad de Tesorería
			Difusión de software dañino	La licencia del antivirus vencida	3	4	3	3	4	3	9	Capacitación continua	7.2	7.22	
	P-07	Encargada Contabilidad	Erorres de configuración	Falta de entrenamiento	3	4	3	3	4	3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad de Contabilidad
			Difusión de software dañino	La licencia del antivirus vencida	3						4	Capacitación continua	7.2	7.22	
P-08	Jefe Infraestructura y Catastro	Erorres de configuración	Falta de entrenamiento	3	4	3	3	4	3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad de Infraestructura y Catastro	
		Difusión de software dañino	La licencia del antivirus vencida	3						4	Capacitación continua	7.2	7.22		
P-09	Jefe Administración Tributaria y Renta	Erorres de configuración	Falta de entrenamiento	3					3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad de Administración Tributaria y Renta	
		Difusión de software dañino	La licencia del antivirus vencida	3	4	3	3	4	3	9	Capacitación continua	7.2	7.22		
P-10	Encargado Servicios Públicos	Erorres de configuración	Falta de entrenamiento	3					3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad Servicios Públicos	
		Difusión de software dañino	La licencia del antivirus vencida	3	4	3	3	4	3	9	Capacitación continua	7.2	7.22		
P-11	Jefe Desarrollo Económico y Social	Erorres de configuración	Falta de entrenamiento	3					3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad de Desarrollo Económico y Social	
		Difusión de software dañino	La licencia del antivirus vencida	3	4	3	3	4	3	9	Capacitación continua	7.2	7.22		
P-12	Secretaria01	Erorres de configuración	Falta de entrenamiento	3					3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad de Recursos Humanos	
		Difusión de software dañino	La licencia del antivirus vencida	3	4	3	3	4	3	9	Capacitación continua	7.2	7.22		
P-13	Secretaria02	Erorres de configuración	Falta de entrenamiento	3					3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Concejo Municipal	
		Difusión de software dañino	La licencia del antivirus vencida	3	4	3	3	3	3	9	Capacitación continua	7.2	7.22		
P-14	Secretaria03	Erorres de configuración	Falta de entrenamiento	3					3	9	Contra con un software antivirus y concienciación al personal	14.2	14.21	Unidad de Abastecimiento y Control Patrimonial	
		Difusión de software dañino	La licencia del antivirus vencida	3	4	3	3	3	3	9	Capacitación continua	7.2	7.22		

Servicio	3-01	Internet satelital	Corte del suministro eléctrico	No hay UPS	3				1				9	Grupo electrogéneo	11.1	11.1.4	
			Avería de origen físico o lógico	No se tiene equipos redundantes	3	2	2	4	1	3	3			Mantenimiento mensual de equipos	11.2	11.2.4	Alcalde
			Fallo de servicios de comunicación	No se tiene contratación de servicio de alta disponibilidad	3				2					Contratar un servicio de alta disponibilidad	17.1	17.1.1	

Análisis de Riesgo

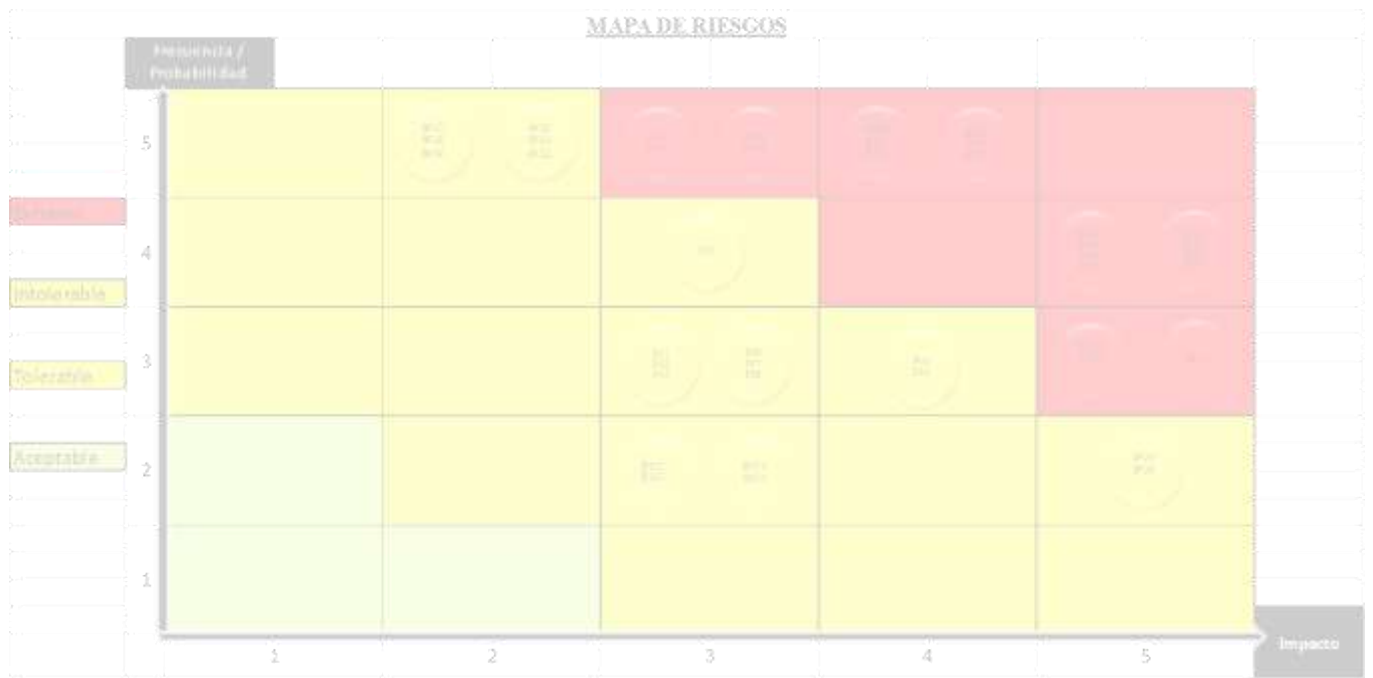
Riesgo = Probabilidad de Amenaza * Magnitud Daño (Impacto)

Desastrozo Mayor Moderado Menor Insignificante	Impacto	5	5	10	15	20	25	<table border="1"> <tr><th colspan="4">Riesgo</th></tr> <tr><td>1</td><td>2</td><td>1</td><td>Aceptable</td></tr> <tr><td>3</td><td>7</td><td>2</td><td>Tolerable</td></tr> <tr><td>8</td><td>14</td><td>3</td><td>Intolerable</td></tr> <tr><td>15</td><td>25</td><td>4</td><td>Extremo</td></tr> </table>	Riesgo				1	2	1	Aceptable	3	7	2	Tolerable	8	14	3	Intolerable	15	25	4	Extremo
		Riesgo																										
		1	2	1	Aceptable																							
		3	7	2	Tolerable																							
		8	14	3	Intolerable																							
15	25	4	Extremo																									
4	4	8	12	16	20																							
3	3	6	9	12	15																							
2	2	4	6	8	10																							
1	1	2	3	4	5																							
Riesgos		Probabilidad de Amenaza																										
		1	2	3	4	5																						
		Raro	M. Bajo	Bajo	Medio	Alto																						

Impacto = Valor * Degradación

Muy Alto Alto Medio Bajo Muy Bajo	Valor	5	0.05	0.5	5	<table border="1"> <tr><th colspan="2">Impacto</th></tr> <tr><td>1</td><td>Muy bajo</td></tr> <tr><td>2</td><td>Bajo</td></tr> <tr><td>3</td><td>Medio</td></tr> <tr><td>4</td><td>Alto</td></tr> <tr><td>5</td><td>Muy Alto</td></tr> </table>	Impacto		1	Muy bajo	2	Bajo	3	Medio	4	Alto	5	Muy Alto
		Impacto																
		1	Muy bajo															
		2	Bajo															
		3	Medio															
4	Alto																	
5	Muy Alto																	
4	0.04	0.4	4															
3	0.03	0.3	3															
2	0.02	0.2	2															
1	0.01	0.1	1															
Impacto		Degradación																
		1%	10%	100%														
		Media	Alta	Muy alta														

MAPA DE RIESGOS



b. Documentación final

- Resultados de las encuestas.

- Documentación de otras fuentes: estadísticas, observaciones de expertos y observaciones de los analistas.
- Información existente utilizable por el proyecto (por ejemplo inventario de activos)
- Documentación auxiliar: planos, organigramas, requisitos, especificaciones, análisis funcionales, cuadernos de carga, manuales de usuario, manuales de explotación, diagramas de flujo de información y de procesos, modelos de datos, etc.
- Informes y evaluaciones de defectos de los productos, procedentes de fabricantes o de centros de respuesta a incidentes de seguridad.

2.3. Hipótesis

La investigación tiene un alcance de carácter descriptivo, no es posible plantear una hipótesis debido a que no se intenta correlacionar o explicar casualidades de variables y el objetivo a alcanzar está claro. Por tal razón se considera una hipótesis implícita.

III. METODOLOGÍA

3.1. Diseño de la Investigación

Esta investigación por el grado de cuantificación reúne las condiciones de una investigación cuantitativa.

Es cuantitativa, porque permite examinar los datos de manera científica, o de manera más específica en forma numérica, generalmente con ayudas de herramientas de campo de la estadística, en este caso mediante la estadística descriptiva. Un estudio cuantitativo o encuesta permite conocer las opiniones, actitudes o comportamientos que se desean investigar expresados en forma de porcentajes que son aplicables al conjunto de la población estudiada. Para obtenerlos se elabora un cuestionario que se debe responder para una muestra representativa de dicha población.

Un aspecto fundamental es la investigación cuantitativa consiste en garantizar la responsabilidad de la muestra seleccionada para que los resultados sean extrapolables al conjunto de la población. Para ello es importante definir correctamente el universo, seleccionar adecuadamente la muestra, definir las variables sobre las que es necesario fijar cuotas, etc.

De acuerdo a la naturaleza del estudio de la investigación, reúne por su nivel las características de un estudio descriptivo, no experimental y de acuerdo a orientación es aplicada.

Se trata de un estilo descriptivo, porque el objetivo de la investigación es llegar a conocer la situación, costumbres y actitudes predominantes a través de la descripción exacta de las actividades, objetos, procesos y personas, y que no se limita a la recolección de datos. En esta investigación se examinan y describen las variables de estudio.

Es no experimental, ya que en ella no es posible la manipulación de las variables que interfieren en el estudio, es utilizada cuando el investigador no dispone de la información necesaria para la solución del problema planteado, no tiene la

posibilidad de crear el fenómeno, como en los casos de la investigación experimental y casi experimental y cuando el fenómeno ya se ha producido, se adecua más a los estudios naturales, cuando se quieren estudiar los fenómenos tal cual ocurren y se relacionan sin intervención.

De acuerdo a la orientación se tipifica como una investigación aplicada, ya que contribuye a la aplicación del conocimiento de modelos para construcción de sistemas de gestión de la seguridad, busca nuevos conocimientos en vista de posibles aplicaciones prácticas la que incluye cualquier esfuerzo sistemático y socializado por resolver problemas o intervenir situaciones.

Esta investigación es de corte transversal de una sola casilla porque se intenta analizar el fenómeno en un periodo determinado, pues se recopilan datos en un solo momento, es un tiempo único, su propósito es describir variables y analizar e interrelación en un momento dado.

3.2. Población y muestra

Población

Para la presente investigación, se tomó como población a todo el personal administrativo que consta de 16 trabajadores que labora en la oficina matriz de la Municipalidad Distrital de Pira, que son aquellos involucrados directamente en los procesos, para cada una de las variables en estudio sobre sistemas de gestión de seguridad de la información.

Muestra

Dado que el número de elementos que comprenden la población es reducido no es necesario obtener una muestra por lo que en la presente investigación se trabajó con toda la población.

3.3. Definición y operacionalización de variables e indicadores

A continuación se expone la declaración y operacionalización de las variables.

VARIABLE	DIMENSIONES	INDICADORES
<p style="text-align: center;">VARIABLE I Sistema De Gestión De La Seguridad De La Información</p>	<p style="text-align: center;">Software Hardware</p>	<input type="checkbox"/> Políticas de seguridad <input type="checkbox"/> Organización de la información
	<p style="text-align: center;">Gestión administrativa</p>	<input type="checkbox"/> Seguridad en recursos humanos <input type="checkbox"/> Gestión de activos <input type="checkbox"/> Control de accesos <input type="checkbox"/> Criptografía <input type="checkbox"/> Seguridad física y ambiental <input type="checkbox"/> Seguridad en la operaciones <input type="checkbox"/> Transferencia de información <input type="checkbox"/> Adquisición de sistemas, desarrollo y mantenimiento <input type="checkbox"/> Relación con proveedores <input type="checkbox"/> Gestión de los incidentes de seguridad <input type="checkbox"/> Continuidad de negocio <input type="checkbox"/> Cumplimiento con requerimientos legales y contractuales <input type="checkbox"/>

<p>VARIABLE II Activos de Información</p>	<p>Determinar Control</p>	<ul style="list-style-type: none"><input type="checkbox"/> Documentos<input type="checkbox"/> Metodología<input type="checkbox"/> Riesgos
--	-------------------------------	---

3.4. Técnicas e instrumentos de recolección de datos

Las técnicas e instrumentos empleados para el presente informe de investigación fueron:

Definición de los sujetos

En la presente investigación, los sujetos que participaron en la investigación fueron al teniente alcalde y el personal administrativo de la Municipalidad Distrital Pira. Así como cada una de las computadoras que les han sido asignadas para realizar sus labores diarias.

Técnicas

Para la obtención de la información se utilizó las técnicas de:

- **Entrevista:** dirigida al teniente alcalde para conocer el estado de seguridad en la que se encuentra la municipalidad.
- **Encuesta:** dirigida al personal de la municipalidad, la cual permitió conocer las expectativas que tienen respecto al conocimiento de las consideraciones en seguridad de la información.
- **Observación Directa:** en lo que se refirió a la revisión de los Sistemas Informáticos que utiliza cada usuario que forma parte de la población detallada anteriormente.

Instrumentos

En virtud de la información que se deseaba recabar, los instrumentos a que se utilizaron son:

- **Cuestionario de preguntas:** de tipo cerradas, elección única, tanto dicotómica y politómica para la entrevista y encuestas.

- **Fichas (lista de cotejo):** para lo que corresponde a la observación.

106

Se tomó solo las encuestas realizadas a las personas seleccionadas y se absolvió las dudas referidas a las interrogantes planteadas.

Elección de un software

Se elaboró un archivo en Microsoft Excel 2013 para la tabulación de las respuestas de cada encuesta para cada variable en estudio y se obtuvo rápidamente los resultados que se detallaran más adelante.

3.5. Plan de análisis

El presente estudio de investigación se realizará a través de la recopilación de datos haciendo uso de la técnica de la encuesta, la cual se aplicó a todos los trabajadores.

El cuestionario fue prediseñado, y no modifica el entorno ni controla el proceso que está en observación. Los datos se obtienen a partir de realizar un conjunto de preguntas normalizadas dirigidas a una muestra representativa, con el fin de conocer estados de opinión, características o hechos específicos.

Luego de la obtención de datos se procedió a codificarlos, para mantener el orden y posteriormente elaborar los cuadros estadísticos, haciendo uso del programa Microsoft Office Excel 2013; de los cuales se realizó el análisis e interpretación de los datos, la elaboración de las conclusiones y recomendaciones.

3.6. Matriz de consistencia

Problema	Objetivos	Hipótesis	Variables	Metodología
-----------------	------------------	------------------	------------------	--------------------

<p>¿Cómo el desarrollo de un sistema de gestión de seguridad de la información basada en la norma ISO/IEC 27001:2013, permitirá una adecuada administración en la seguridad de los activos de información en la Municipalidad Distrital de Pira?</p>	<p>Objetivo General Evaluar el sistema de gestión de seguridad de la información en la Municipalidad Distrital de Pira basado en la norma ISO/IEC 27001:2013; la cual permitirá una mejor administración en los activos de información.</p> <p>Objetivos Específicos</p> <p>a) Identificar la existencia de los riesgos considerando la seguridad de la información.</p> <p>b) Evaluar los mecanismos de seguridad, localizando los problemas.</p> <p>c) Desarrollar el informe final en base a la Norma ISO 27001/2013, apoyado de metodología MAGERIT V.03.</p>	<p>La investigación tiene un alcance de carácter descriptivo, no es posible plantear una hipótesis debido a que no se intenta correlacionar o explicar casualidades de variables y el objetivo a alcanzar está claro. Por tal razón se considera una hipótesis implícita.</p>	<p>Variable I Sistema de Gestión de Seguridad de la Información</p> <p>Variable II Activos de información</p>	<p>Diseño de investigación Investigación cuantitativa, de estudio descriptivo, no experimental y de acuerdo a la orientación es aplicada y de corte transversal.</p> <p>Población y Muestra Se tomó como población a todo el personal administrativo que consta de 16 trabajadores, Dado que el número de elementos que comprenden la población es reducido no es necesario obtener una muestra.</p> <p>Técnicas de recolección de datos Entrevista, Encuestas, Observación directa.</p> <p>Técnicas de análisis de resultados Medida de tendencia central; Medida de dispersión Gráfico de barras, tablas de frecuencia; Software Microsoft Office 2013</p>
--	--	---	---	---

3.7. Principios éticos

La investigación casi nunca ocurre de forma independiente. Muchas investigaciones requieren interactuar con personas, grupos o instituciones. Estas interacciones enfrentan al investigador con situaciones éticas. Por lo tanto, un código de ética es importante para asegurar el bienestar del investigador y de las personas que se estudien.

En esta investigación se ha tomado en cuenta los siguientes principios éticos:

- Transparencia en la recolección de datos de la población en estudio
- Énfasis en la autenticidad de los resultados obtenidos
- Confidencialidad en las respuestas a las encuestas aplicadas
- Honestidad al momento de realizar el análisis
- Veracidad de los resultados

IV. RESULTADOS

4.1. Resultados

Los resultados de la encuesta aplicada a los trabajadores de la Municipalidad Distrital de Pira, se basan en aspectos generales, las cuales fueron tabuladas permitiendo así realizar el respectivo análisis e interpretación de cada pregunta.

Tabla N° 06

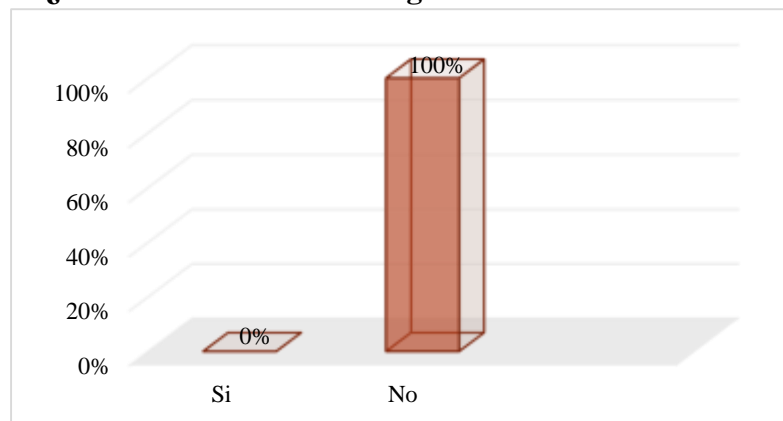
¿Conoce las Políticas de seguridad de la Información?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	0	0.00%
NO	16	100.00%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 09

¿Conoce las Políticas de seguridad de la Información?



Fuente: Tabla N° 06 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) trabajadores encuestados, se refleja el escaso conocimiento de las políticas de Seguridad de la Información considerando que el 100% (16) trabajadores encuestados afirma no conocerlas.

Tabla N° 07

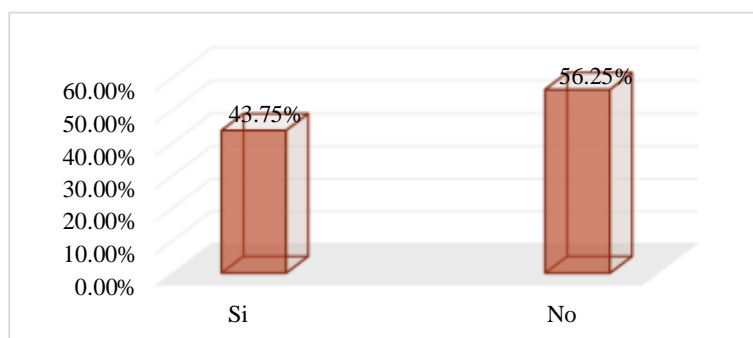
¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la Municipalidad

Distrital de Pira?		
OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	7	43.75%
NO	9	56.25%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:** Castillo, R.; 2016.

Ilustración N° 10

¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la Municipalidad
Distrital de Pira?



Fuente: Tabla N° 07
Elaborado por: Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el grafico que del 100% (16) de los trabajadores encuestados el 43.75% (7) de los trabajadores se sienten responsables de los equipos que utilizan dentro de las instalaciones en tanto que el restante 56.25% (9) de los trabajadores no se sienten responsables del equipo que utiliza por lo que podríamos decir que falta responsabilidad con las cosas que utilizan.

Tabla N° 08

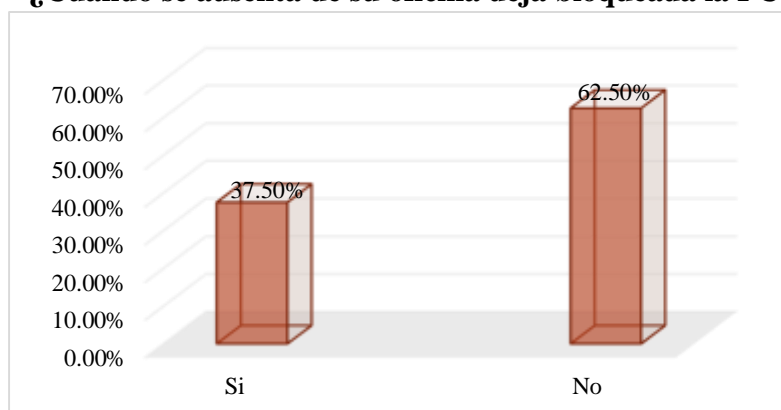
¿Cuándo se ausenta de su oficina deja bloqueada la PC?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	6	37.50%
NO	10	62.50%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 11

¿Cuándo se ausenta de su oficina deja bloqueada la PC?



Fuente: Tabla N° 08

Análisis e interpretación:

Elaborado por: Castillo, R.; 2016.

37.50% (6) siempre deja bloqueada su PC cuando no la está utilizando mientras que el 62.50% (10) restante no.

Lo anterior deja al descubierto que cualquier persona; sea o no trabajador de la empresa, con solo hacer un clic puede desbloquear la mayoría de los equipos y tener acceso total a la información que en éstos se encuentra almacenada.

Tabla N° 09

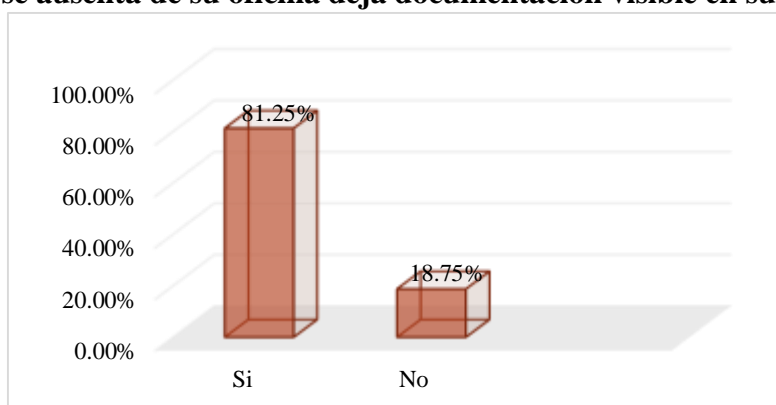
¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	13	81.25%
NO	3	18.75%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 12

¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?



Fuente: Tabla N° 09
Elaborado por: Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) de los trabajadores encuestados el 81.25% (13) de los trabajadores deja documentos visibles sobre el escritorio, y lo restante 18.75% (3) no deja visible.

Queda en evidencia el alto nivel de vulnerabilidad de los documentos que dejan a la vista de los demás.

Tabla N° 10

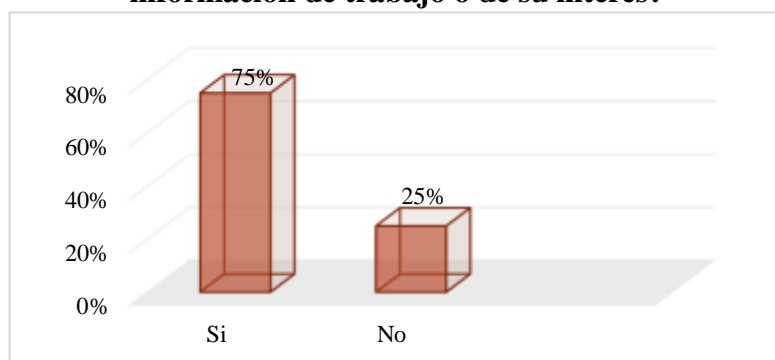
¿Has utilizado algún dispositivo externo para extraer algún tipo de información de trabajo o de su interés?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	12	75.00%
NO	4	25.00%
TOTAL	16	100%

Fuente: Encuesta
Elaborado por: Castillo, R.; 2016.

Ilustración N° 13

¿Has utilizado algún dispositivo externo para extraer algún tipo de información de trabajo o de su interés?



Fuente: Tabla N° 10

Análisis e interpretación:

Elaborado por: Castillo, R.; 2016.

75.00% (12) de los trabajadores utiliza algún tipo de dispositivo para extraer información. El 25 % (4) no utilizo ningún dispositivo para extraer información.

Tabla N° 11

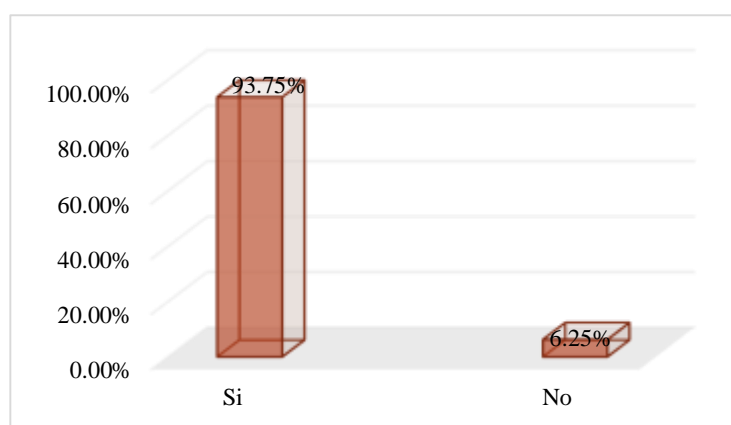
¿La clave de acceso es la misma para todos los sistemas con los que cuenta la Municipalidad Distrital de Pira?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	15	93.75%
NO	1	6.25%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 14

¿La clave de acceso es la misma para todos los sistemas con los que cuenta la Municipalidad Distrital de Pira?



Fuente: Tabla N° 11 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) de los trabajadores encuestados el 93.75% (15) de los trabajadores cuentan con una misma clave de acceso para todos los sistemas con los que cuenta. El 6.25% (01) vemos que tiene una clave diferente para cada sistema. Casi la totalidad de los trabajadores de la Municipalidad desconoce de la inseguridad que puede ocurrir al no tener claves de acceso distinto para cada sistema que utilizan.

Tabla N° 12

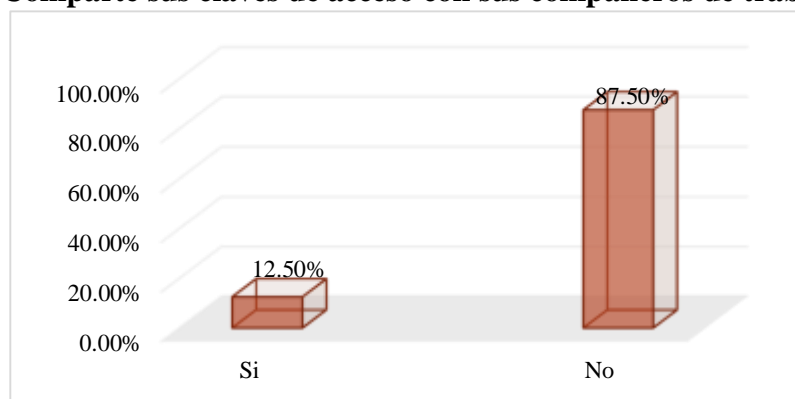
¿Comparte sus claves de acceso con sus compañeros de trabajo?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	2	12.50%
NO	14	87.50%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 15

¿Comparte sus claves de acceso con sus compañeros de trabajo?



Fuente: Tabla N° 12
Elaborado por: Castillo, R.; 2016.

Análisis e interpretación:

12.50% (02) de ellos, demuestran la escasa responsabilidad que tienen al compartir sus claves de acceso. El 87.50% (14) restante no comparten dichas informaciones. El 12.50% (02) de los encuestados desconoce o minimiza el riesgo y las vulnerabilidades a las que se encuentra expuesta la información al compartir sus claves de acceso.

Tabla N° 13

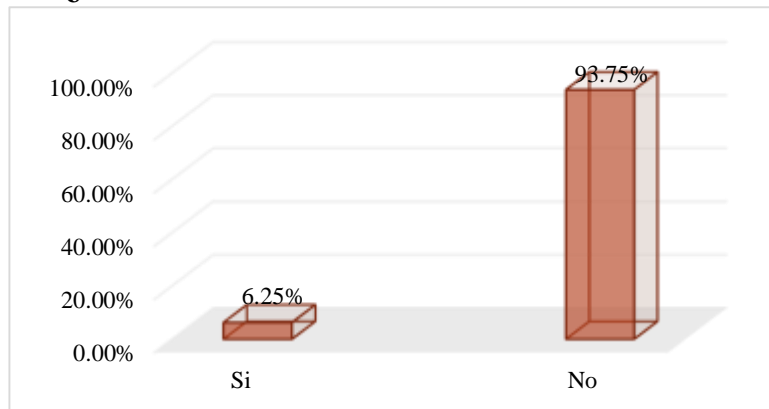
¿Ud. cambia con frecuencia sus Claves de acceso?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	1	6.25%
NO	15	93.75%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:** Castillo, R.; 2016.

Ilustración N° 16

¿Ud. cambia con frecuencia sus Claves de acceso?



Fuente: Tabla N° 13

Elaborado por: Castillo, R.; 2016.

Se puede apreciar en el grafico que del 100% (16) de los trabajadores encuestados el 6.25% (01) de los encuestados afirma que cambia con frecuencia sus claves de acceso

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) de los trabajadores encuestados el 93.75% (15) afirmó nunca cambiar sus claves de acceso.

La mayoría de los trabajadores coincide en que el cambiar sus claves de acceso constantemente podría llegar a olvidar, por lo que pueda representar un gran riesgo para su información.

Tabla N° 14

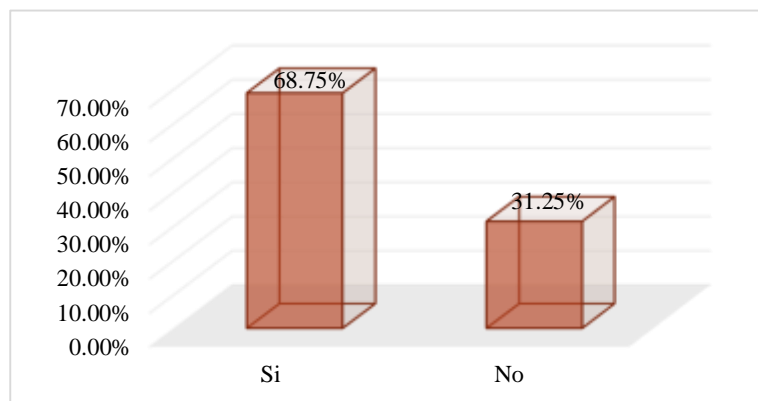
¿Ud. Ha observado que algún compañero ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en cualquiera de las computadoras de la Municipalidad Distrital de Pira?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	11	68.75%
NO	5	31.25%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 17

¿Ud. Ha observado que algún compañero ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en cualquiera de las computadoras de la Municipalidad Distrital de Pira?



Fuente: Tabla N° 14 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) de los trabajadores encuestados el 68.75% (11) de los trabajadores han observado que se ingiere alimentos y bebidas líquidos durante sus labores y el 31.25% (05) no ven lo que realizan sus compañeros de trabajo durante horas de trabajo.

La mayoría de los trabajadores de la Municipalidad han observado que se ingiere alimentos y bebidas líquidos durante sus labores. Esto eleva notablemente la posible pérdida de información.

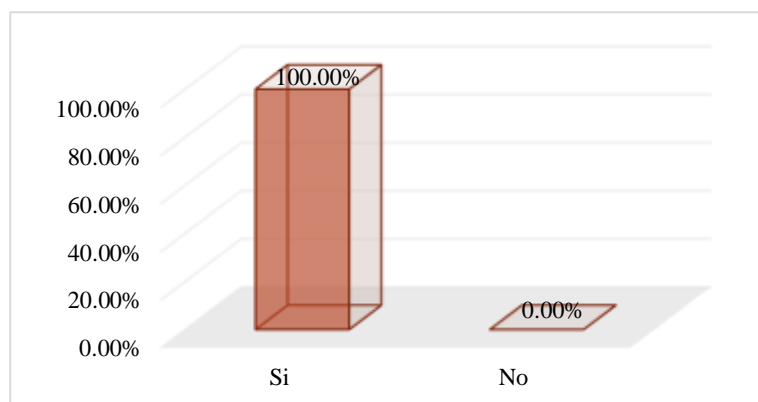
Tabla N° 15

¿Cuenta con correo electrónico?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	16	100.00%
NO	0	0.00%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:** Castillo, R.; 2016.

Ilustración N° 18
¿Cuenta con correo electrónico?



Fuente: Tabla N° 15
Elaborado por: Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) trabajadores encuestados afirman que hace uso del correo electrónico personal.

Este medio permite a muchos de los usuarios el ingreso y salida de información confidencial de la Municipalidad.

Tabla N° 16

¿Reconoce Ud. Cuáles son los activos importantes de la Municipalidad

Distrital de Pira?

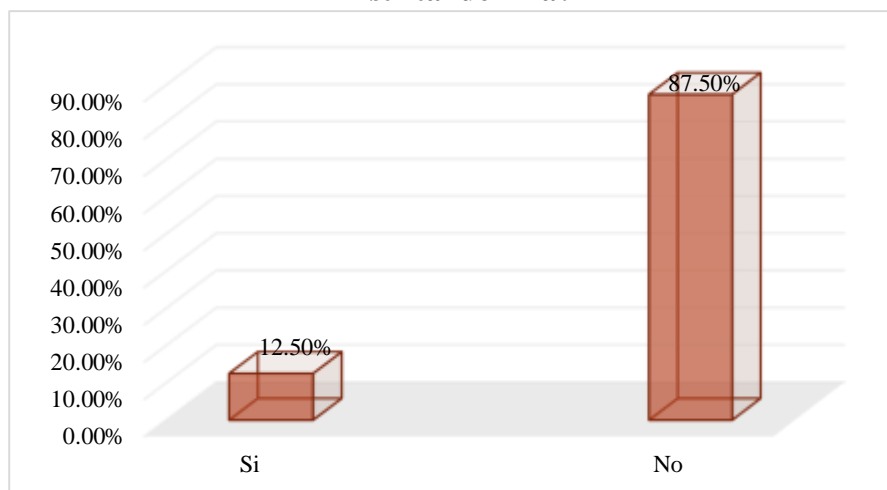
OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	2	12.50%
NO	14	87.50%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
 Castillo, R.; 2016.

Ilustración N° 19

¿Reconoce Ud. Cuáles son los activos importantes de la Municipalidad

Distrital de Pira?



Fuente: Tabla N° 16 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) de los trabajadores encuestados el 12.50% (02) si logra identificarse con los activos de información del área.

El restante 87.50% (14) de los encuestados afirma el escaso conocimiento de la identificación de los activos de información del área.

Un gran porcentaje de trabajadores no tiene identificación con los activos de información que a diario utiliza para realizar sus actividades de trabajo. Estos constituyen una gran vulnerabilidad a la información.

Tabla N° 17

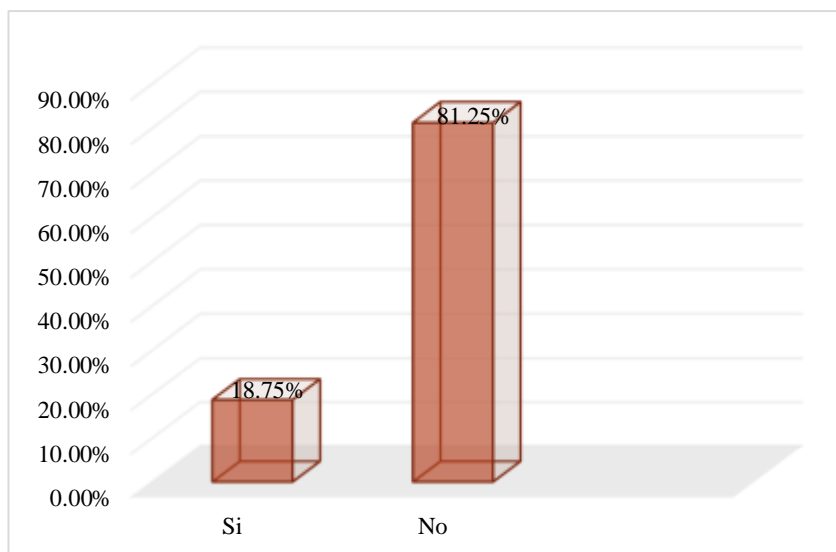
¿Usted ha detectado que el antivirus de la Municipalidad Distrital de Pira funciona adecuadamente y que se encuentra actualizado?

OPCIONES	CANTIDAD	FRECUENCIA (%)
SI	3	18.75%
NO	13	81.25%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 20

¿Usted ha detectado que el antivirus de la Municipalidad Distrital de Pira funciona adecuadamente y que se encuentra actualizado?



Fuente: Tabla N° 17 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) de los trabajadores encuestados el 18.75% (03) de los trabajadores si detectan que el antivirus funciona adecuadamente mientras que el 81.25% (13) no toman en cuenta que el antivirus funciona correctamente.

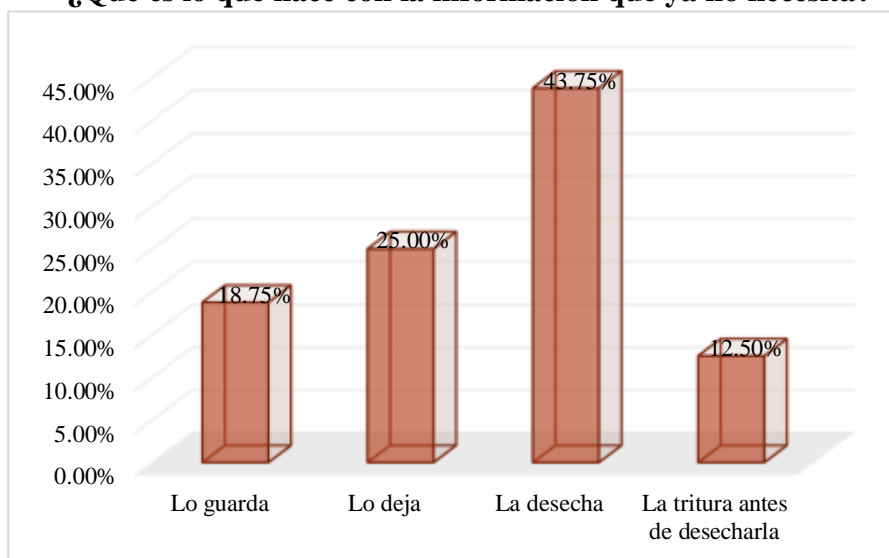
Queda en evidencia el alto nivel de vulnerabilidad de los equipos que utilizan los trabajadores ya que sus antivirus podrían estar desactualizados, y al no tomar importancia de ello la información estaría en riesgo por los virus que podrían ingresar.

Tabla N° 18

¿Qué es lo que hace con la información que ya no necesita?		
OPCIONES	CANTIDAD	FRECUENCIA (%)
Lo Guarda	3	18.75%
Lo Deja	4	25.00%
Lo Desecha	7	43.75%
La Tritura Antes de Desecharla	2	12.50%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

¿Qué es lo que hace con la información que ya no necesita?



Fuente: Tabla N° 18 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el gráfico que del 100% (16) de los trabajadores encuestados el 43.75% (7) de los trabajadores desecha la información aun así ese no es el procedimiento para deshacerse de cierta información. El 12.50% (02) trabajadores procede a cumplir con el procedimiento, sin embargo 18.75% (03) personas sigue guardando y el restante que es el 25.00% (04) de los trabajadores lo deja en cualquier lugar no procede a darle el tratamiento adecuado. La mayoría de los trabajadores de la Municipalidad no cumple con el procedimiento por lo que la información eleva notablemente su vulnerabilidad.

Tabla N° 19

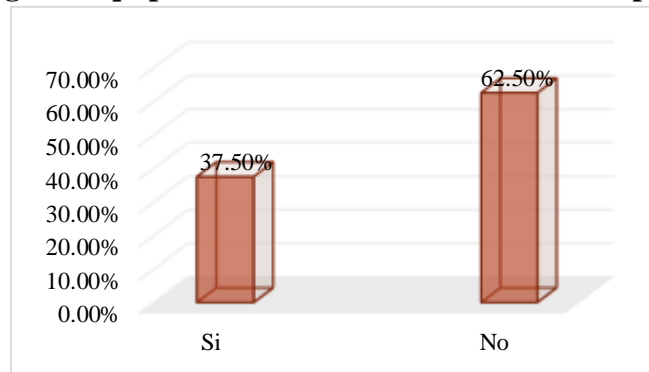
¿Usted apaga los equipos informáticos correctamente después de utilizarlos?

OPCIONES	CANTIDAD	FRECUENCIA (%)
Si	6	37.50%
No	10	62.50%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 22

¿Usted apaga los equipos informáticos correctamente después de utilizarlos?



Fuente: Tabla N° 19 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

Se puede apreciar en el grafico que del 100% (16) de los trabajadores encuestados el 37.50% (6) de los encuestadores de la Municipalidad siempre apagan adecuadamente el computador mientras que el 62.50% (10) de los trabajadores no siguen los pasos adecuadamente de como apagar un computador.

Esto nos indica que la probabilidad de dañar, quemarse los circuitos u otros de un computador tendría un riesgo fatal de perder información.

Tabla N° 20

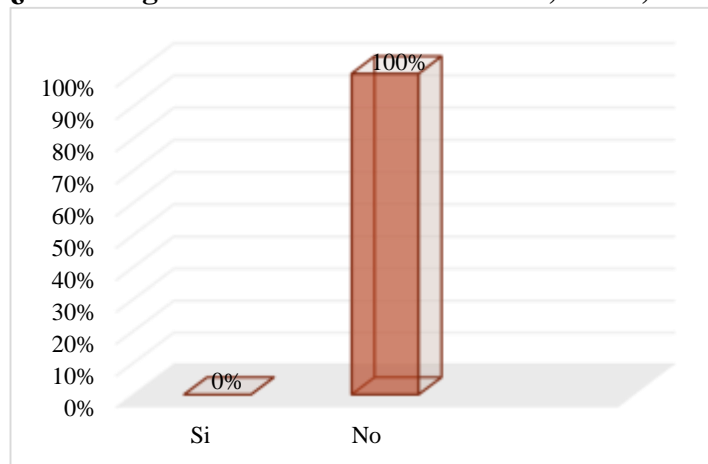
¿Existe alguna alarma contra incendios, robos, otros?

OPCIONES	CANTIDAD	FRECUENCIA (%)
Si	0	0.00%
No	16	100.00%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.

Ilustración N° 23

¿Existe alguna alarma contra incendios, robos, otros?



Fuente: Tabla N° 20 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

El 100% (16) de los encuestados afirma que dentro de las instalaciones de la municipalidad no cuentan con alarmas de cualquier índole para incidente que pueda suceder.

Cabe indicar que sin alarmas de cualquier índole las informaciones podrían sufrir graves consecuencias.

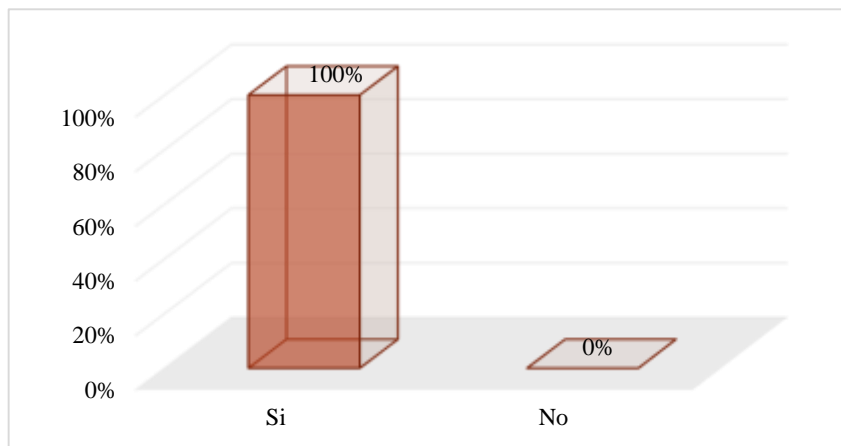
Tabla N° 21

¿Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información?

OPCIONES	CANTIDAD	FRECUENCIA (%)
Si	16	100.00%
No	0	0.00%
TOTAL	16	100%

Fuente: Encuesta **Elaborado por:**
Castillo, R.; 2016.
Ilustración N°
24

¿Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información?



Fuente: Tabla N° 21 **Elaborado por:** Castillo, R.; 2016.

Análisis e interpretación:

El 100% (16) de los trabajadores están interesados en tener mayor información sobre Seguridad de la Información.

Se puede apreciar que absolutamente todos los trabajadores de la Municipalidad necesitan saber sobre seguridad en la Información.

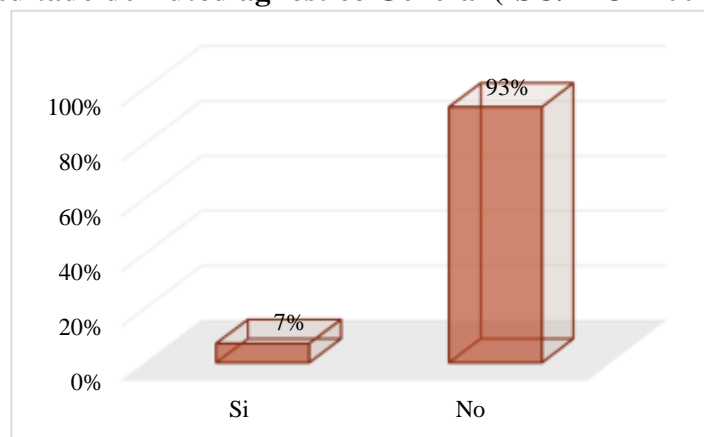
4.2. Análisis de resultados

Según los resultados de la encuesta aplicada a los trabajadores se determinó que no cuentan con el conocimiento y las medidas adecuadas para salvaguardar los activos de información.

Con el Autodiagnóstico General para la evaluación de madurez, el 93% consideran por conocimiento que en la Municipalidad, este proceso está en el nivel Inexistente, según los niveles de madurez de la ISO/IEC 27001:2013, lo que significa que se reconoce la necesidad de recolectar y evaluar información sobre los procesos de monitoreo. No se han identificado procesos estándar de recolección y evaluación. El control se implanta y las métricas se seleccionan de acuerdo a las necesidades de los Sistemas de Información. El control se implanta como respuesta a algún incidente que ha ocasionado alguna pérdida a la organización. La autoridad municipal solo cuenta con una indicación aproximada de cómo el SGSI contribuye al desempeño de la organización, sin embargo la autoridad municipal solo responde en respuesta a los incidentes que hayan causado pérdidas a la institución.

Ilustración N° 25

Resultado de Autodiagnóstico General (ISO/IEC 27001:2013)



Fuente: Formulario Autodiagnóstico General **Elaborado por:** Castillo, R.; 2016.

V. CONCLUSIONES

Al finalizar el proceso de evaluación, se llegó a determinar que ciertos procesos no cuentan con una buena administración para su operación tales como: manuales, planes y más recursos necesarios.

Al efectuar la evaluación se pudo determinar el alto nivel de riesgos que existe en el manejo de los activos de información dentro de la municipalidad, ello debido al poco control.

Esta evaluación permite a la empresa tomar medidas preventivas y correctivas en los procesos que necesitan ser atendidos con mayor brevedad a nivel de seguridad para el mejor funcionamiento de los mismos.

Por ello se desarrolló el presente informe en base a la norma ISO/IEC 27001:2013, apoyado de la metodología MAGERIT versión 3.0 el estándar que permitió evaluar los riesgos de la seguridad de información, con el objetivo de determinar en qué condiciones se encuentran y si están alineadas con los objetivos del negocio garantizando la integridad de su información para el beneficio de la municipalidad. Para la ejecución del presente trabajo fue necesario realizar varias tareas y actividades de revisión en la municipalidad que sustenten las observaciones identificadas y el análisis del presente trabajo.

VI. RECOMENDACIONES

Es responsabilidad del área encargada, desarrollar, someter a revisión y divulgar en adición a los demás medios de difusión (intranet, email, sitio web oficial) de los

Procedimientos de Seguridad. Asimismo, es responsabilidad del supervisor inmediato capacitar a sus trabajadores en lo relacionado con los Procedimientos de Seguridad.

Tener un conjunto mínimo de medidas de seguridad informática que garantice la integridad de la información.

La información y los equipos que conforman la plataforma tecnológica sobre la que se procesan los procedimientos administrativos y operativos que la rigen

Establecer el adecuado comportamiento que debe tener cada uno de los usuarios, sin excepción, en el manejo de los componentes tecnológicos y la información soportada dentro de la municipalidad.

Asimismo establecer políticas de seguridad dentro de la empresa para tener un mejor control en salvaguardar la información.

REFERENCIAS BIBLIOGRÁFICAS

1. Guachi Aucapiña V, Guevara Aulestia O. Repositorio Digital Universidad Tecnica de Ambato. [Tesis para obtener el título de Ingeniero de sistemas].; 2012
[Consulta 2016 Diciembre 01. Disponible desde:
<http://repositorio.uta.edu.ec/jspui/handle/123456789/2361>.

2. Barragán Paguay I, Góngora Zambrano I, Martínez Cárdenas E. Repositorio De ESPOL. [Tesis para obtener el título de Ingeniero de sistemas].; 2013 [Consulta 2016 Diciembre 01. Disponible desde: <http://www.dspace.espol.edu.ec/handle/123456789/21546>.
3. Aguirre Cardona, J.; Aristizabal Bentancourt, C. Repositorio de UTP. [Tesis para obtener el título de Ingeniero de sistemas].; 2013 [Consulta 2016 Diciembre 01] Disponible desde: <http://repositorio.utp.edu.co/dspace/bitstream/11059/4117/1/0058A284.pdf>.
4. Yagual Del Valle, C.; Chilán, L. Repositorio Digital Universidad Politécnica Salesiana. [Tesis para obtener el título de Ingeniero de sistemas].; 2014 [Consulta 2016 Diciembre 01]. Disponible desde: <http://www.dspace.ups.edu.ec/bitstream/123456789/7401/1/UPS-GT000773.pdf>.
5. Montoya Pachas, K. Repositorio Digital de Tesis PUCP. [Tesis para obtener el título de Ingeniero de sistemas].; 2013 [Consulta 2016 Diciembre 01]. Disponible desde: <http://tesis.pucp.edu.pe/repositorio/handle/123456789/5005>.
6. Espinoza Aguinaga, R. Repositorio Digital de Tesis PUCP. [Tesis para obtener el título de Ingeniero de sistemas].; 2013 [Consulta 2016 Diciembre 01]. Disponible desde: <http://tesis.pucp.edu.pe/repositorio/handle/123456789/4957>.

7. Aguirre Mollehuanca, A. Repositorio Digital de Tesis PUCP. [Tesis para obtener el título de Ingeniero de sistemas].; 2014 [Consulta 2016 Diciembre 01].

Disponible desde: <http://tesis.pucp.edu.pe/repositorio/handle/123456789/5677>.

8. Talavera Álvarez, R. Repositorio Digital de Tesis PUCP. [Tesis para obtener el título de Ingeniero de sistemas].; 2016 [Consulta 2016 diciembre 01].

Disponible desde:

<http://tesis.pucp.edu.pe/repositorio/handle/123456789/6092>.

9. WIKIPEDIA La Inciclopedia Libre. [Monografía en Internet].; Ayuntamiento; 2016 [Consulta 2016 Diciembre 17]. Disponible desde:

<https://es.wikipedia.org/wiki/Ayuntamiento>.

10. Pastor i Collado, A. Concepto de Información en las organizaciones. Primera ed. Pastor i Collado A, editor. Barcelona: UOC papers; 2002.

11. Activos de información. RealISO. [Documento Sitio Web]; 2012 [Consulta 2016 Diciembre 29]. Disponible desde:

<https://sites.google.com/a/realiso.com/realisms-spa/gestao-de-risco/-3-3-ativos-deinformacao>.

12. Laudon, K.; Laudon, J. Sistemas de Información Gerencial. Octava ed. Hall P, editor. Mexico: Pearson; 2004.

- 13.** Senn, J. Sistemas de Información para la Administración. Segunda ed. México: Iberoamérica; 1992.
- 14.** Zamora, S. IZAMORAR. [Documento Sitio Web]; 2014 [Consulta 2016 Enero 05]. Disponible desde:
<http://izamorar.com/actividades-basicas-de-un-sistema-de-informacion/>.
- 15.** Ormella Meyer, C. ISO27000 Seguridad Informática. [Documento Sitio Web]; 2012 [Consulta 2016 Enero 08]. Disponible desde:
<http://www.iso27000.es/download/seguridad%20informaticavsinformacion.pdf>.
- 16.** Recio, J. De la seguridad informática a la Seguridad de la Información. [Sitio Web]; 2012 [Consulta 2016 Enero 29]. Disponible desde:
http://www.aec.es/c/document_library/get_file?uuid=e25028ca-cb3b-4ffd-ada0-4ce2efa86f80&groupId=10128.
- 17.** Markus, E. Wordpress. [Sitio Web]; 2012 [consulta 2016 Enero 29].
Disponible desde:
https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/
- 18.** Mifsud, E. Recursostic. [Sitio Web]; 2012 [consulta 2016 Enero 29].
Disponible desde:
<http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040introduccion-a-la-seguridad-informatica?start=1>.

19. British Standards Institution (BSI). [Sitio Web]. 1998 [Consulta 2016 Enero 30]. Disponible desde: <http://www.bsigroup.com/es-ES/Sobre-BSI/Nuestra-historia/>.
20. López Neira, A; Ruiz Spohr, J. El Portal de ISO 27000 en español (ISO27000.es). [Sitio Web]. 2005 [Consulta 2016 Enero 30]. Disponible desde:
<http://www.iso27000.es/>.
21. Markus, E. Wordpress. Gestión Riesgos [Sitio Web].; 2012 [Consulta 2016 Enero 30]. Disponible desde: https://protejete.wordpress.com/gdr_principal/
22. Ferrer, J. Metodología de la Investigación. [Sitio Web].; 2010 [Consulta 2016 Diciembre 29]. Disponible desde:
http://metodologia02.blogspot.com/p/operacionalizacion-de-variable_03.html.
23. PAe Portal Administración Electrónica. [Sitio Web].; 2010 [consulta 2016 Diciembre 28]. Disponible desde:
https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WG8xMFXhDIU
24. Hernández Sampieri, R.; Fernández Collado, C. Baptista Lucio MdP. Metodología de la investigación. 5th ed. Chacón JM, editor. México: McGRAW-HILL / INTERAMERICANA EDITORES, S.A. DE C.V; 2010.

25. Toro Jaramillo, I.; Parra Ramírez, R. Método y Conocimiento - Metodología de la Investigación. Primera ed. Medellín: Fondo Editorial Universidad EAFIT; 2006.

ANEXOS

ANEXO 01


Cuestionario dirigido al alcalde de la Municipalidad Distrital de Pira.

ITEM	PREGUNTAS	SI	NO
01	¿En la Municipalidad Distrital de Pira cuentan con políticas de seguridad de la información?		
02	¿La Municipalidad Distrital de Pira cuenta con un comité de seguridad de la información?		

03	¿Existe algún tipo de manual o documento donde se especifique los controles para la seguridad de la información?		
04	¿Se registran los accesos de personas a las áreas donde se encuentran los equipos servidores?		
05	¿Existe un documento donde se especifique las políticas de seguridad de la información?		
06	Frente a cualquier desastre natural, provocado o humano ¿Su personal conoce cuales son los activos más importantes que debe proteger en relación a la información?		
07	¿Los equipos de cómputo en el área tienen fuente de poder interrumpible (UPS), Generadores de energía, baterías ante cortes de energía eléctrica?		
08	¿A Usted se le brinda capacitación por parte de la Municipalidad Distrital de Pira acerca de seguridad de la información?		
09	¿Ud. sabe distinguir la información que es estrictamente confidencial, de uso interno o público?		
10	¿Ud. Contrataría a un especialista para una capacitación a todo el personal de la Municipalidad Distrital de Pira para un buen manejo de seguridad de la información?		

ANEXO 02

Cuestionario dirigido al personal de la Municipalidad Distrital de Pira.


 UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE				
ENCUESTA SOBRE SEGURIDAD DE LA INFORMACIÓN				
El presente cuestionario va dirigido a todo el personal, con la finalidad de recoger información con respecto a la seguridad de la información.				
ITEM	PREGUNTAS	SI	NO	OTROS
01	¿Conoce las Políticas de seguridad de la Información?			

02	¿Usted cree que debe sentirse responsable e identificarse con el equipo informático que usa o utilizará en algún momento dentro de la Municipalidad Distrital de Pira?			
03	¿Cuándo se ausenta de su oficina deja bloqueada la PC?			
04	¿Cuándo se ausenta de su oficina deja documentación visible en su escritorio?			
05	¿Has utilizado algún dispositivo externo para extraer algún tipo de información de trabajo o de su interés?			
06	¿La clave de acceso es la misma para todos los sistemas con los que cuenta la Municipalidad Distrital de Pira?			
07	¿Comparte sus claves de acceso con sus compañeros de trabajo?			
08	¿Ud. cambia con frecuencia sus Claves de acceso?			
09	¿Ud. Ha observado que algún compañero ha bebido líquidos o ingerido algún alimento cuando realiza algún trabajo en cualquiera de las computadoras de la Municipalidad Distrital de Pira?			
10	¿Cuenta con correo electrónico?			
11	¿Reconoce Ud. Cuáles son los activos importantes de la Municipalidad Distrital de Pira?			

12	¿Usted ha detectado que el antivirus de la Municipalidad Distrital de Pira funciona adecuadamente y que se encuentra actualizado?			
13	¿Qué es lo que hace con la información que ya no necesita?			Lo guarda () Lo deja () Lo desecha () La tritura antes de desecharla ()
14	¿Usted apaga los equipos informáticos correctamente después de utilizarlos?			
15	¿Existe alguna alarma contra incendios, robos, otros?			
16	¿Le interesaría conocer o tener un mayor conocimiento de lo que refiere a Seguridad de la Información?			

ANEXO 03

Formulario para el autodiagnóstico general

FORMULARIO PARA GENERAL	 <small>UNIVERSIDAD CATÓLICA LOS ÁNGELES CHIMBOTE</small>	AUTODIAGNÓSTICO
<p>El presente formulario es para evaluar el nivel de madurez que se encuentra la seguridad de la información, según los controles definidos en la ISO/IEC 27001:2013</p>		

CONTROL	PREGUNTAS	SI	NO
POLÍTICAS DE SEGURIDAD	Existen documento(s) de políticas de seguridad de Sistema de Información		
	Existe normativa relativa a la seguridad de los Sistemas de Información		
	Existen procedimientos relativos a la seguridad de Sistema de Información		
	Existe un responsable de las políticas, normas y procedimientos		
	Existen mecanismos para la comunicación a los usuarios de las normas		
	Existen controles regulares para verificar la efectividad de las políticas		
ORGANIZACIÓN DE LA INFORMACIÓN	Existen roles y responsabilidades definidos para las personas implicadas en la seguridad		
	Existe un responsable encargado de evaluar la adquisición y cambios de Sistema de Información		
	La Dirección y las áreas de la Organización participa en temas de seguridad		
	Existen condiciones contractuales de seguridad con terceros y outsourcing		
	Existen criterios de seguridad en el manejo de terceras partes		
	Existen programas de formación en seguridad para los empleados		
	Existe un acuerdo de confidencialidad de la información de acceso.		
Se revisa la organización de la seguridad periódicamente por una empresa externa			

SEGURIDAD EN RECURSOS HUMANOS	Se tienen definidas responsabilidades y roles de seguridad		
	Se tiene en cuenta la seguridad en la selección y baja del personal		
	Se plasman las condiciones de confidencialidad y responsabilidades en los contratos		
	Se imparte la formación adecuada de seguridad y tratamiento de activos		
	Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad		

	Se recogen los datos de los incidentes de forma detallada		
	Informan los usuarios de las vulnerabilidades observadas o sospechadas		
	Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades		
	Existe un proceso disciplinario de la seguridad de la información		
GESTIÓN DE ACTIVOS	Existen un inventario de activos actualizado		
	El Inventario contiene activos de datos, software, equipos y servicios		
	Se dispone de una clasificación de la información según la criticidad de la misma		
	Existe un responsable de los activos		
	Existen procedimientos para clasificar la información		
	Existen procedimientos de etiquetado de la información		
CONTROL DE ACCESOS	Existe una política de control de accesos		
	Existe un procedimiento formal de registro y baja de accesos		
	Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario		
	Existe una gestión de los password de usuarios		
	Existe una revisión de los derechos de acceso de los usuarios		
	Existe el uso del password		
	Se protege el acceso de los equipos desatendidos		
	Existen políticas de limpieza en el puesto de trabajo		
	Existe una política de uso de los servicios de		
		red	
	Se asegura la ruta desde el terminal al servicio		
	Existe una autenticación de usuarios en conexiones externas		
	Existe un control de la conexión de redes		
	Existe un control del routing de las redes		

	Existe una identificación única de usuario y una automática de terminales		
	Existen procedimientos de login al terminal		
	Se ha incorporado medidas de seguridad a la computación móvil		
	Está controlado el teletrabajo por la organización		
CRIPTOGRAFÍA	Existe protección en la integridad de transferencias electrónicas		
	Existe autenticación en la identidad de usuarios		
	Existen controles criptográficos		
	Existe codificación en la información de archivos o de un correo electrónico para que no pueda ser descifrado en caso de ser interceptado por alguien mientras esta información viaja por la red		
SEGURIDAD FÍSICA Y AMBIENTAL	Existe perímetro de seguridad física (una pared, puerta con llave).		
	Existen controles de entrada para protegerse frente al acceso de personal no autorizado		
	Un área segura ha de estar cerrada, aislada y protegida de eventos naturales		
	En las áreas seguras existen controles adicionales al personal propio y ajeno		
	Las áreas de carga y expedición están aisladas de las áreas de Sistema de Información		
	La ubicación de los equipos está de tal manera para minimizar accesos innecesarios		
	Existen protecciones frente a fallos en la alimentación eléctrica		
	Existe seguridad en el cableado frente a daños e intercepciones		
	Se asegura la disponibilidad e integridad de todos los equipos		
	Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente		
Se incluye la seguridad en equipos móviles			
	Todos los procedimientos operativos		
	identificados en la política de seguridad han de estar documentados		

SEGURIDAD EN LAS OPERACIONES

Están establecidas responsabilidades para controlar los cambios en equipos		
Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad		
Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas		
Existe una separación de los entornos de desarrollo y producción		
Existen contratistas externos para la gestión de los Sistemas de Información		
Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento		
Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones		
Controles contra software maligno		
Realizar copias de backup de la información esencial para el negocio		
Existen logs para las actividades realizadas por los operadores y administradores		
Existen logs de los fallos detectados		
Existe algún control en las redes		
Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)		
Eliminación de los medios informáticos. Pueden disponer de información sensible		
Existe seguridad de la documentación de los Sistemas		
Existen acuerdos para intercambio de información y software		
Existen medidas de seguridad de los medios en el tránsito		
Existen medidas de seguridad en el comercio electrónico.		
Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada		
Existen medidas de seguridad en las transacciones en línea		
Se monitorean las actividades relacionadas a la seguridad		

TRANSFERENCIA DE INFORMACIÓN	Existe herramientas de seguridad avanzadas que permiten la privacidad y el resguardo de la información		
	Existe políticas de seguridad para transferencias de información		
ADQUISICIÓN DE SISTEMAS, DESARROLLO Y MANTENIMIENTO	Se asegura que la seguridad está implantada en los Sistemas de Información		
	Existe seguridad en las aplicaciones		
	Existe seguridad en los procesos de desarrollo, testing y soporte		
	Existen controles de seguridad para los resultados de los sistemas		
	Existe la gestión de los cambios en los SO.		
	Se controlan las vulnerabilidades de los equipos		
RELACIÓN CON PROVEEDORES	Existen programas de formación en seguridad para los clientes y terceros		
GESTIÓN DE LOS INCIDENTES DE SEGURIDAD	Se comunican los eventos de seguridad		
	Se comunican las debilidades de seguridad		
	Existe definidas las responsabilidades antes un incidente.		
	Existe un procedimiento formal de respuesta		
	Existe la gestión de incidentes		
CONTINUIDAD DE NEGOCIO	Existen procesos para la gestión de la continuidad.		
	Existe un plan de continuidad del negocio y análisis de impacto		
	Existe un diseño, redacción e implantación de planes de continuidad		
	Existe un marco de planificación para la continuidad del negocio		
	Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.		
CUMPLIMIENTO CON REQUERIMIENTOS LEGALES Y CONTRACTUALES	Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas		
	Existe el resguardo de la propiedad intelectual		
	Existe el resguardo de los registros de la organización		
	Existe una revisión de la política de seguridad y de la conformidad técnica		
	Existen consideraciones sobre las auditorías de los sistemas		

