UNIVERSIDAD PARTICULAR DE CHICLAYO

FACULTAD DE AQUITECTURA, URBANISMO E INGENIERÍAS

ESCUELA PROFESIONAL DE INGENIERÍA INFORMÁTICA Y DE SISTEMAS

TESIS

“APLICACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA MUNICIPALIDAD PROVINCIAL DE CHICLAYO”

PARA OPTAR EL TÍTULO PROFESIONAL DE:

INGENIERO INFORMÁTICO Y SISTEMAS

AUTOR:

BACH. JUAN FRANCISCO OTERO MORE

ASESOR:

ING. CHRISTIAN QUEZADA MACHADO

CHICLAYO – PERU

2016

T E S I S

TÍTULO:

“APLICACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA MUNICIPALIDAD PROVINCIAL DE CHICLAYO”

Presentada como requisito para optar el **Título de INGENIERO INFORMÁTICO Y DE SISTEMAS**, y sustentada por:

_____

JUAN FRANCISCO OTERO MORE
Bachiller en Ingeniería Informática y de Sistemas

_____

Ing. Christian Quezada Machado
ASESOR

Aprobada por los siguientes Miembros de Jurado:

_____

Mag. Luis Campos Contreras
PRESIDENTE DEL JURADO

_____

Ing. Eduardo Arrascue Becerra
SECRETARIO DEL JURADO

_____

Ing. Ricardo Guanilo Gonzales
VOCAL DEL JURADO

Fecha de Sustentación: Chiclayo, Jueves 18 de febrero de 2016

AGRADECIMIENTOS

A ti mamá, por ser mi ejemplo a seguir, por darme fuerzas cuando flaqueaba y por guiarme con tu luz siempre por el camino correcto. Nunca estaré lo suficiente agradecido con Dios por haberme regalado una madre como tú.

A mi padre, estuviste físicamente lejos pero gracias a tus bendiciones soy la persona que soy ahora.

A mi hermana Florencia, por darme otra visión de las cosas y por apoyarme a que yo cumpla exitosamente este reto de la vida.

A mi esposa Mimi, por su apoyo y ánimo que me brinda día con día para alcanzar nuevas metas, tanto profesionales como personales.

PRESENTACION

Señores miembros del Jurado

Cumpliendo con los requerimientos estipulados en el Reglamento de Grados y Títulos de la Universidad de Chiclayo, para obtener el Título Profesional de Ingeniero Informático y de Sistemas, se pone a la disposición nuestro proyecto denominado: “APLICACIÓN DE UN SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA LA MUNICIPALIDAD PROVINCIAL DE CHICLAYO”

.

En este presente proyecto pretendemos lograr palpar todos los conocimientos adquiridos en los diferentes cursos de los diez ciclos de estudio académico de la Universidad de Chiclayo, sin dejar de lado que somos conscientes de algunas limitaciones y dificultades en el mismo, que probablemente haya incurrido en algunos errores, por tanto, pedimos a ustedes Miembros del Jurado dispensar dichos errores y omisiones que adolece el presente estudio.

Gracias.

Chiclayo, Febrero del 2016

_____

Bach. Juan Francisco Otero More

RESUMEN

En la actualidad, las inversiones en seguridad de la información que realizan las instituciones, públicas como privadas, se destinan cada vez menos a la compra de productos, destinando más bien parte de su presupuesto a la gestión de seguridad de la información. El concepto de seguridad ha variado, acuñándose uno nuevo, el de seguridad gestionada, que va desplazando poco a poco al de "seguridad informática". Éste tiene tres vertientes: técnica, legal y organizativa, es decir, un planteamiento coherente de directivas, procedimientos y criterios que permiten desde la administración de las empresas asegurar la evolución eficiente de la seguridad de los sistemas de información, la organización afín y sus infraestructuras.

Para gestionar la seguridad de la información de una entidad se debe partir de una premisa fundamental y es que la seguridad absoluta no existe. Tomando lo anterior como punto de partida, una entidad puede adoptar algunas de las normas existentes en el mercado que establecen determinadas reglas o estándares que sirven de guía para gestionar la seguridad de la información.

La presente tesis ha realizado una investigación de las normas y estándares que van difundiéndose con mayor énfasis en el mercado Peruano, en especial en el sector gubernamental. Se rescataron los aspectos más saltantes de cada norma y estándar, a partir de los cuales se plantea un esquema de gestión de seguridad de información que puede ser empleado por una entidad pública en el Perú. Esto permitiría que se cumpla con las normas de regulación vigentes en lo relacionado a la Seguridad de Información.

Palabras clave: sistema de gestión de seguridad de la información, análisis y evaluación de riesgos, gestión del riesgo, activo de información.

ABSTRACT

Currently, investments in information security made by institutions, public and private, are used less and less for purchasing products and are allocating more of their budget to managing information security. The concept of security has changed, a new term has been coined, the “managed security”, which is shifting gradually to that of "information security". The measures that companies have begun taking go around to the new concept of information security management. This has three aspects: technical, legal and organizational, that is, a coherent approach to policy, procedures and criteria, which allow the enterprises management to ensure the efficient development of information systems security, the organization itself and its infrastructure.

To manage the information security of an entity, it should start from a fundamental premise since an absolute security does not exist. Taking this as a starting point, an entity may adopt some existing market regulations that establish specific rules or standards providing guidance for managing information security.

This thesis has conducted an investigation of the rules and standards that are spreading with greater emphasis on the Peruvian market, especially in the government sector. The most prominent aspects of each rule and standard were retrieved from which a scheme of information security management can be used by any Peruvian public institution. This will allow compliance with current regulatory standards related to information security.

Keywords: information security management system, analysis and risk assessment, risk management, information assets.

INTRODUCCION

En el presente proyecto, se diseña y desarrolla el modelo para implementar un sistema de gestión de seguridad de información para cualquier tipo de organización y se aplicará en la Municipalidad Provincial de Chiclayo

La seguridad de información, en términos generales es entendida como todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistemas tecnológicos que permitan resguardar y proteger la información, buscando de esta manera mantener la confidencialidad, la disponibilidad e integridad de la misma. Un activo de información es un activo que tiene un determinado valor para la organización, sus operaciones comerciales y su continuidad.

La característica principal de un sistema de gestión de seguridad de información es resguardar la integridad, confidencialidad e integridad de los activos de información en una empresa; lo cual se logra a través de un minucioso análisis de los riesgos a los que están expuestos los activos de información para luego implantar los controles necesarios que ayudarán a proteger estos activos.

La problemática principal actual de las empresas es la falta de seguridad y la poca previsión respecto a los riesgos con la que cuentan sus activos de información. El resultado de no tener las medidas necesarias para mitigar estos riesgos puede llevar a la empresa a pérdidas no solo de información, sino también económica.

Es por ello, que La Municipalidad Provincial de Chiclayo se ve en la necesidad de implementar un conjunto de herramientas, procedimientos, controles y políticas que aseguren la confidencialidad, disponibilidad e integridad de la información; con ellos garantizar a que se acceda a la información solo por quienes estén designados para su uso, que esté disponible cuando requieran los que estén autorizados y permanezca tal y como fue creada por sus propietarios, y asegurar así también la actualización de la misma.

El presente estudio ha sido desarrollado en cinco capítulos; en el primero se presentan los aspectos metodológicos de la investigación, desarrollándose dentro de ella el planteamiento del problema, los objetivos de la investigación, las hipótesis general y específicas, y sus pertinentes variables independientes y dependientes.

En la segunda parte se desarrolla el marco teórico que sustenta la investigación. En esta se estudia el origen de la información y los atributos principales de la seguridad como son la confidencialidad, la integridad y la disponibilidad. Se estudia la teoría de los sistemas de información y los controles de seguridad. También se resalta las normativas de seguridad tanto nacional como internacional.

En el tercer capítulo se realiza el análisis e interpretación de los resultados obtenidos, para ello fue necesario el uso de programas informáticos y se pudo comprobar las hipótesis planteadas.

En el cuarto capítulo se presenta una propuesta piloto de un plan de seguridad de la información para la Municipalidad Provincial de Chiclayo, y que servirá de guía y puedan tomarla como referencia para la implantación de sus planes de seguridad.

En el último capítulo se precisan las conclusiones arribadas con la presente investigación y las recomendaciones que de ellas se generan, como una forma de contribuir con la gestión de seguridad de la información en las instituciones públicas.

De esta forma, teniendo en cuenta los lineamientos establecidos por la Facultad de Ciencias Empresariales, Informática y Sistemas, con esta investigación espero contribuir con los postulados de la MPCH y el desarrollo de las organizaciones de nuestro medio.

INDICE

INDICE DE ILUSTRACIONES

INDICE DE TABLAS

INDICE DE GRAFICOS

CAPITULO I: GENERALIDADES DEL PROYECTO

1.1 PLANTEAMIENTO DEL PROBLEMA

La gestión de la seguridad de una organización puede ser muy compleja, no tanto desde el punto de vista puramente técnico sino más bien desde un punto de vista organizativo. Pensar que en una gran MPCH con un número elevado de departamentos, alguien que pertenece a uno de ellos abandona la organización, eliminar su acceso a un cierto sistema no implica ningún problema técnico ya que el administrador sólo ha de borrar o bloquear al usuario de forma inmediata, pero sí va existir graves problemas organizativos.

Un ejemplo para empezar sería de ¿cómo se entera un administrador de sistemas que un cierto usuario, que no trabaja directamente junto a él, abandona la empresa?, ¿quién decide si al usuario se le elimina directamente o se le permite el acceso a su correo durante un mes?, ¿puede el personal del área de seguridad decidir bloquear el acceso a alguien de cierto "rango" en la organización, como un director de departamento, nada más que este abandone la misma?, ¿y si resulta que es amigo del rector, y luego este se enfada? Como vemos, desde un punto de vista técnico no existe ningún escollo insalvable, pero sí que existen desde un punto de vista de la gestión de la seguridad.

Hoy en día, una entidad que trabaje con cualquier tipo de entorno informático, desde pequeñas empresas con negocios no relacionados directamente con las nuevas tecnologías hasta grandes de ámbito internacional, está o debería estar preocupada por su seguridad. Y no es para menos pues el número de amenazas a los entornos informáticos y de comunicaciones crece casi exponencialmente año tras año alcanzando cotas inimaginables hace apenas una década.

Por otra parte la mayoría de redes informáticas en la Municipalidad Provincial de Chiclayo no fueron diseñadas originalmente pensando en la seguridad. A diferencia de las redes corporativas y otras redes comerciales, que son más cerradas y segmentadas con énfasis en la protección de los recursos valiosos de la información, las redes de la MPCH están diseñadas para funcionar como proveedores del servicio de Internet, facilitar el acceso a los usuarios y facilitar el flujo de la información.

Históricamente, los trabajadores de la Municipalidad Provincial de Chiclayo han esperado, y en algunos casos solicitado, acceso gratuito y abierto a los sistemas informáticos de la entidad. Sin embargo a la luz de las recientes amenazas y riesgos de la información tales como sabotaje, fraude, extorsión, violación de la privacidad, intrusos, hackers, interrupción de servicios, y de las expectativas de más amenazas a la seguridad en el futuro, no puede continuar este acceso abierto e ilimitado.

La preocupación de las organizaciones por la seguridad de la información no debe estar centrada sólo en los aspectos más técnicos de la seguridad, sino es necesario proponer a la Municipalidad Provincial de Chiclayo estrategias de gestión de seguridad de la información que abarque el desarrollo, revisión y cumplimiento de las políticas de seguridad y abordar temas claves de seguridad como la identificación de riesgos críticos, sensibilización, capacitación y privacidad.

Finalmente, para gestionar eficientemente la seguridad de la información se requiere que todos los miembros de la MPCH como autoridades, trabajadores y terceros tomen conciencia de la importancia de la seguridad de la información y su papel que juega en generar aportes de calidad y eficacia en los servicios críticos de la Municipalidad Provincial de Chiclayo.

1.2 FORMULACION DEL PROBLEMA

1.2.1 Problema principal

¿Qué efectos produce el Sistema de Gestión de Seguridad de la Información (SGSI) en los servicios críticos de la Sede Central Administrativa de la Municipalidad Provincial de Chiclayo? (Anexo N° 4)

1.2.2 Problemas específicos

1. ¿Tienen la Municipalidad Provincial de Chiclayo estrategias preventivas y planes de contingencia para minimizar los riesgos en el manejo de la información ante incidentes?
2. ¿Cuáles son los beneficios SGSI en los sistemas de información como son tesorería y trámites documentarios en la Municipalidad Provincial de Chiclayo?
3. ¿Cómo generar conciencia de seguridad en los trabajadores sobre la información que manejan en la Municipalidad Provincial de Chiclayo?
4. ¿Cómo optimizar el soporte, gestión y seguridad de las redes informáticas de la Municipalidad Provincial de Chiclayo?

1.3 OBJETIVOS DE LA INVESTIGACIÓN

1.3.1 Objetivo General

Proponer estrategias de Gestión de Seguridad de la Información y sus implicancias en la calidad y eficacia en los servicios críticos de la Sede central Administrativa de la Municipalidad Provincial de Chiclayo.

1.3.2 Objetivos Específicos

1. Analizar los riesgos en el manejo de la información, para minimizar los mismos como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios con la implementación de políticas de seguridad de la información.

2. Diseñar un nuevo esquema de red informática municipal que permita un tráfico de la información más seguro y un servicio eficaz a los trabajadores y terceros.

3. Elaborar un plano cooperativo con la finalidad de contribuir a la calidad en el servicio y en la protección más segura de los sistemas de información de la Municipalidad Provincial de Chiclayo

4. Capacitación con programas de charlas y/o talleres, para generar conciencia de seguridad en los trabajadores de la MPCH sobre un buen uso de la información.

1.4 JUSTIFICACIÓN DE LA INVESTIGACIÓN

a) Justificación Teórica

La investigación propuesta mediante la aplicación de conceptos y teorías de información dentro del ámbito de seguridad de la información como son los sistemas de información, análisis y gestión de riesgos y cultura de seguridad, busca encontrar explicaciones para contribuir con calidad y eficacia en los servicios críticos de la Municipalidad Provincial de Chiclayo.

Para ello se hace necesario desarrollar un marco teórico y conceptual revisando el material bibliográfico existente, contrastando las diversas corriente y posiciones, y a partir de ella comprobar su validez en la Municipalidad Provincial de Chiclayo.

b) Justificación Práctica

En la actualidad el tema SGSI y su papel en los servicios críticos de la Municipalidad Provincial de Chiclayo es un tema muy importante. Los recursos de información (sistemas de información, redes, etc.) que sirven como apoyo tanto los trabajadores y terceros deben emplearlos para su

trabajo y estudio, y que no debe estar permitida la utilización de estos recursos con fines comerciales o recreativos. Por ello, los alcances de la investigación tiene repercusión práctica porque aporta información valiosa que servirá como fuente de reflexión y acción para que las autoridades y directivos analicen los resultados sobre calidad y eficacia en los servicios críticos de la Municipalidad Provincial de Chiclayo y a la vez se propone un plan de seguridad de información para la entidad que sirva como modelo para otras instituciones y éstas la puedan aplicar.

c) Metodológica

El tema de la seguridad de la información es reciente y en la Municipalidad Provincial de Chiclayo se torna más preocupante por las amenazas a los recursos de su información, por tanto la metodología ha sido la consulta a expertos del área de Tecnología de Información y Comunicaciones de la Municipalidad Provincial de Chiclayo.

Para lograr el cumplimiento de los objetivos de la investigación, se acude al empleo de técnicas de investigación. En el trabajo de campo, procesamiento y análisis de los resultados obtenidos fue necesario el uso de las herramientas de aplicación como Microsoft Office, de la misma forma para la preparación y presentación del informe definitivo.

1.5 DELIMITACIÓN DE LA INVESTIGACIÓN

La presente investigación se circunscribe a la consulta de expertos en Tecnología de Información y Comunicaciones que laboran en la Municipalidad Provincial de Chiclayo, la información recolectada corresponde a los meses comprendidos entre marzo y mayo de 2015.

1.6 HIPOTESIS DE LA INVESTIGACION

1.6.1 Hipótesis General

La aplicación de estrategias de Gestión de Seguridad de la Información contribuye con calidad y eficacia en los servicios críticos de la Municipalidad Provincial de Chiclayo.

1.6.2 Hipótesis Auxiliares

1. Al implementar políticas de seguridad de la información, se minimizarán los riesgos en el manejo de la información como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios.

2. El rediseño la red informática municipal permitirá un tráfico de la información más seguro y un servicio eficaz a los trabajadores y terceros.

3. La gestión de seguridad de la información va a contribuir a la calidad en el servicio y en la protección más segura de los sistemas de información de la Municipalidad Provincial de Chiclayo

4. Los programas y talleres de capacitación de seguridad de la información crearán conciencia de seguridad en los trabajadores y terceros para un buen uso de la información.

1.7 VARIABLES DE LA INVESTIGACION

Variable Independiente
Sistema de Gestión de Seguridad de la Información

Variable Dependiente
Servicios Críticos de la Sede central Administrativa de la Municipalidad Provincial de Chiclayo

1.8 OPERACIONALIZACION DE VARIABLES

Las variables obtenidas de nuestras hipótesis las podemos medir con uno o varios indicadores, que se muestran a continuación:

Hipótesis Auxiliar N° 1

HIPOTESIS	VARIABLES	INDICADORES
Las áreas que implementen políticas de seguridad de la información en sus servicios críticos, minimizan los riesgos en el manejo de la información como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios.	**VARIABLE INDEPENDIENTE** Políticas de seguridad de la información.	a. Frecuencia de cumplir con las políticas de seguridad. b. Beneficios de usar políticas de seguridad.
	VARIABLE DEPENDIENTE Riesgos en el manejo de la información.	a. Frecuencia de riesgos a los recursos de información. b. Incidencias de seguridad por los usuarios.

Tabla 1: Hipótesis Auxiliar N° 1

Hipótesis Auxiliar N° 2

HIPOTESIS	VARIABLES	INDICADORES
El rediseño la red informática de la Sede Central Administrativa de la MPCH permite un tráfico más seguro	**VARIABLE INDEPENDIENTE** Rediseño de la red informática de la Sede Central	a. Nivel de conocimiento sobre el diseño de redes informáticas institucionales.

de la información y un servicio eficaz a los trabajadores y terceros.	Administrativa de la MPCH.	
	VARIABLE DEPENDIENTE Servicio eficaz y tráfico de información más seguro de los sistemas de información.	a. Nivel de Gestión de seguridad en los servicios administrativos.

Tabla 2: Hipótesis Auxiliar N° 2

Hipótesis Auxiliar N° 3

HIPOTESIS	VARIABLES	INDICADORES
La gestión de seguridad de la información contribuye a la calidad en el servicio y en la protección más segura de los sistemas de información de la Sede Central Administrativa de la MPCH.	**VARIABLE INDEPENDIENTE** Gestión de seguridad de la información.	a. Frecuencia de la importancia de las medidas de seguridad de la información.
	VARIABLE DEPENDIENTE Servicio eficaz y tráfico de información más seguro de los sistemas de información.	a. Nivel de gestión de seguridad de la información en los servicios.

Tabla 3: Hipótesis Auxiliar N° 3

Hipótesis Auxiliar N° 4

HIPOTESIS	VARIABLES	INDICADORES
Los programas y talleres de capacitación de seguridad de la información crean conciencia de seguridad en los trabajadores y terceros para un buen uso de la información.	**VARIABLE INDEPENDIENTE** Programas y talleres de capacitación.	a. Frecuencia de asistencia a programas de capacitación. b. Grado de interés del personal por capacitación.
	VARIABLE DEPENDIENTE Conciencia de seguridad a trabajadores y terceros.	a. Grado de interés del personal por capacitación.

Tabla 4: Hipótesis Auxiliar N° 4

1.9 BASE LEGAL

1.9.1. Resolución Ministerial Nº 129-2012-PCM

Que aprueba el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/ IEC 27001:2008 EDI Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de seguridad de la Información. Requisitos" en todas las entidades integrantes del Sistema Nacional de Informática.

1.9.2. Resolución Ministerial Nº 246-2007-PCM

Que aprueba la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 EDI. Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información.

1.9.3. Puntos de la documentación de la política

A. Cumplimiento de requisitos legales

A.1. Identificación de la legislación aplicable

Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

A.2. Derechos de Propiedad Intelectual

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual. Los empleados únicamente podrán utilizar material autorizado por el Organismo.

El Organismo solo podrá autorizar el uso de material producido por el mismo, o material autorizado o suministrado al mismo por su titular, conforme los términos y condiciones acordadas y lo dispuesto por la normativa vigente.

La infracción a estos derechos puede tener como resultado acciones legales que podrían derivar en demandas penales.

Se deberán tener presentes las siguientes normas:

- *Ley Sobre el Derecho de Autor Decreto legislativo No. 822*: Protege los derechos de autor de las obras científicas, literarias y artísticas,

incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

- *Decreto Legislativo Nº 1075*: Protege la propiedad de una marca y la exclusividad de su uso. Protege el derecho del titular de la patente de invención a impedir que terceros utilicen su producto o procedimiento.

A.2.1. Derecho de Propiedad Intelectual del Software

El software es considerado una obra intelectual que goza de la protección de Ley Sobre el Derecho de Autor Decreto legislativo No. 822. Esta Ley establece que la explotación de la propiedad intelectual sobre los programas de computación incluirá, entre otras formas, los contratos de licencia para su uso o reproducción. Los productos de software se suministran normalmente bajo acuerdos de licencia que suelen limitar el uso de los productos al equipamiento específico y su copia a la creación de copias de resguardo solamente.

El Responsable de Seguridad Informática, con la asistencia del Área Legal, analizará los términos y condiciones de la licencia, e implementará los siguientes controles:

a) Definir normas y procedimientos para el cumplimiento del derecho de propiedad intelectual de software que defina el uso legal de productos de información y de software.
b) Divulgar las políticas de adquisición de software y las disposiciones de la Ley de

   Propiedad Intelectual, y notificar la determinación de tomar acciones disciplinarias contra el personal que las infrinja.
c) Mantener un adecuado registro de activos.
d) Conservar pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc.
e) Implementar controles para evitar el exceso del número máximo permitido de usuarios.
f) Verificar que sólo se instalen productos con licencia y software autorizado.
g) Elaborar y divulgar un procedimiento para el mantenimiento de condiciones adecuadas con respecto a las licencias.
h) Elaborar y divulgar un procedimiento relativo a la eliminación o transferencia de software a terceros.

i) Utilizar herramientas de auditoría adecuadas.
j) Cumplir con los términos y condiciones establecidos para obtener software e información en redes públicas.

A.3. Protección de los Registros del Organismo

Los registros críticos del Organismo se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales del Organismo. Los registros se clasificarán en diferentes tipos, por ejemplo registros contables, registros de base de datos, registros de auditoría y procedimientos operativos, cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento, por ejemplo papel, microfichas, medios magnéticos u ópticos.

Tipo de Registro	Sistema de Información	Período de Retención	Medio de Almacenamiento	Responsable

Las claves criptográficas asociadas con archivos cifrados se mantendrán en forma segura y estarán disponibles para su uso por parte de personas autorizadas cuando resulte necesario. Se debe considerar la posibilidad de degradación de los medios utilizados para el almacenamiento de los registros. Los procedimientos de almacenamiento y manipulación se implementarán de acuerdo con las recomendaciones del fabricante. Si se seleccionan medios de almacenamiento electrónicos, se incluirán los procedimientos para garantizar la capacidad de acceso a los datos (tanto legibilidad de formato como medios) durante todo el período de retención, a fin de salvaguardar los mismos contra eventuales pérdidas ocasionadas por futuros cambios tecnológicos.

Los sistemas de almacenamiento de datos serán seleccionados de modo tal que los datos requeridos puedan recuperarse de una manera que resulte aceptable para un tribunal de justicia, por ejemplo que todos los registros requeridos puedan recuperarse en un plazo y un formato aceptable.

El sistema de almacenamiento y manipulación garantizará una clara identificación de los registros y de su período de retención legal o normativa.

Asimismo, se permitirá una adecuada destrucción de los registros una vez transcurrido dicho período, si ya no resultan necesarios para el Organismo.

A fin de cumplir con estas obligaciones, se tomarán las siguientes medidas:

a) Elaborar y divulgar los lineamientos para la retención, almacenamiento, manipulación y eliminación de registros e información.
b) Preparar un cronograma de retención identificando los tipos esenciales de registros y el período durante el cual deben ser retenidos.
c) Mantener un inventario de programas fuentes de información clave.
d) Implementar adecuados controles para proteger la información y los registros esenciales contra pérdida, destrucción y falsificación.

En particular, se deberán tener presente las siguientes normas:

LEY Nº 27815, "LEY DEL CÓDIGO DE ÉTICA DE LA FUNCIÓN PÚBLICA"
EMITIDA POR LA COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA.
CAPÍTULO II PRINCIPIOS Y DEBERES ÉTICOS DEL SERVIDOR PÚBLICO.
ARTÍCULO 7º.- DEBERES DE LA FUNCIÓN PÚBLICA.
NRO. 5. USO ADECUADO DE LOS BIENES DEL ESTADO.
Dispone que el funcionario público Debe proteger y conservar los bienes del Estado, debiendo utilizar los que le fueran asignados para el desempeño de sus funciones de manera racional, evitando su abuso, derroche o desaprovechamiento, sin emplear o permitir que otros empleen los bienes del Estado para fines particulares o propósitos que no sean aquellos para los cuales hubieran sido específicamente destinados.

LEY Nº 27309
LEY QUE INCORPORA LOS DELITOS INFORMÁTICOS AL CÓDIGO PENAL
EMITIDA POR EL CONGRESO DE LA REPÚBLICA
CAPÍTULO X
DELITOS INFORMÁTICOS
Artículo 207º-A.- El que utiliza o ingresa indebidamente a una base de datos, sistema o red de computadoras o cualquier parte de la misma, para diseñar, ejecutar o alterar un esquema u otro similar, o para interferir, interceptar, acceder o copiar información en tránsito o contenida en una base de datos, será reprimido

con pena privativa de libertad no mayor de dos años o con prestación de servicios comunitarios de cincuenta y dos a ciento cuatro jornadas.

Si el agente actuó con el fin de obtener un beneficio económico, será reprimido con pena privativa de libertad no mayor de tres años o con prestación de servicios comunitarios no menor de ciento cuatro jornadas.

Artículo 207º-B.- El que utiliza, ingresa o interfiere indebidamente una base de datos, sistema, red o programa de computadoras o cualquier parte de la misma con el fin de alterarlos, dañarlos o destruirlos, será reprimido con pena privativa de libertad no menor de tres ni mayor de cinco años y con setenta a noventa días multa.

Artículo 207º-C.- En los casos de los Artículos 207º-A y 207º-B, la pena será privativa de libertad no menor de cinco ni mayor de siete años, cuando:

1. El agente accede a una base de datos, sistema o red de computadora, haciendo uso de

Información privilegiada, obtenida en función a su cargo.

2. El agente pone en peligro la seguridad nacional.

NORMAS DE CONTROL INTERNO PARA EL SECTOR PÚBLICO - RELACIONADO CON LA PARTE INFORMÁTICA.

EMITIDAS POR LA CONTRALORÍA GENERAL DE LA REPÚBLICA

500-05 SEGURIDAD DE PROGRAMAS, DE DATOS Y EQUIPOS DE CÓMPUTO

Deben establecerse mecanismos de seguridad en los programas y datos del sistema para proteger la información procesa da por la entidad, garantizando su integridad y exactitud, así como respecto de los equipos de computación.

COMPENDIO DE NORMAS TÉCNCAS INFORMÁTICAS.

EMITIDO POR INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA (INEI)

RESOLUCION JEFATURAL Nº O76-95-INEI

"RECOMENDACIONES TECNICAS PARA LA SEGURIDAD E INTEGRIDAD DE LA INFORMACION QUE SE PROCESA EN LA ADMINISTRACION PUBLICA"

V. CONSIDERACIONES GENERALES

DEL ACCESO A LA INFORMACION

5.1 En los procedimientos administrativos es recomendable la identificación previa del personal que va a ingresar a las áreas de cómputo, verificando si cuenta con la autorización correspondiente y registrándose el ingreso y salida al área

5.2 En los Sistemas Informáticos es preferible utilizar programas de cómputo, que cuenten con rutinas de control para el acceso de los usuarios.

5.3 Las rutinas de control, permiten que los usuarios ingresen al Sistema, previa identificación, mediante una palabra clave (password), la cual será única para cada uno de ellos; negando el acceso a las personas que no han sido definidos como usuarios del Sistema.

5.4 Las rutinas de control de acceso identificarán a los usuarios autorizados a usar determinados sistemas con su correspondiente nivel de acceso, el cual incluye la lectura o modificación en sus diferentes formas.

5.5 Es recomendable existan 4 niveles de acceso a la información:

a) Nivel de consulta de la información no restringida o reservada.

b) Nivel de mantenimiento de la información no restringida o reservada

c) Nivel de consulta de la información incluyendo la restringida o reservada.

d) Nivel de mantenimiento de la información incluyendo la restringida o reservada

Para garantizar estos niveles cada palabra clave tendrá asignada uno de estos niveles de acceso.

5.6 Consecuentemente la información que se considere restringida o reservada estará debidamente identificada, así como a los usuarios que accesen a ella.

5.7 Cada Unidad Orgánica de Informática, maneja los 4 niveles de acceso a la información, contando para ello con un Administrador de la Información, quien es responsable de la asignación de las palabras claves, de los niveles de acceso y las fechas de expiración.

5.8 La unidad Orgánica dispondrá de un procedimiento que posibilite que las palabras claves tengan o se generen bajo un período a tiempo prudencial de vigencia

5.9 El Jefe de cada Unidad Orgánica es responsable del acceso a la información y será quien alcance las directivas adecuadas al Administrador de la Información.

5.10 Los operadores de la información restringida o reservada realizarán estrictamente lo indicado en cada procedimiento establecido de procesamiento de la información, para lo cual éstos deberán estar claramente documentados.

DECRETO LEGISLATIVO 822 - LEY SOBRE EL DERECHO DE AUTOR
EMITIDA POR EL CONGRESO DE LA REPÚBLICA.
Protege los derechos de autor de las obras científicas, literarias y artísticas, incluyendo los programas de computación fuente y objeto; las compilaciones de datos o de otros materiales.

A.4. Protección de Datos y Privacidad de la Información Personal
Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones.
El Organismo redactará un “Compromiso de Confidencialidad”, el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por el Organismo. Mediante este instrumento el empleado se comprometerá a utilizar la información solamente para el uso específico al que se ha destinado y a no comunicar, diseminar o de alguna otra forma hacer pública la información a ninguna persona, firma, compañía o tercera persona, salvo autorización previa y escrita del Responsable del Activo de que se trate. A través del “Compromiso de Confidencialidad” se deberá advertir al empleado que determinadas actividades pueden ser objeto de control y monitoreo. Estas actividades deben ser detalladas a fin de no violar el derecho a la privacidad del empleado. En particular, se deberán tener presente las siguientes normas:

COMPENDIO DE NORMAS TÉCNCAS INFORMÁTICAS.
EMITIDO POR INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMÁTICA (INEI)
RESOLUCION JEFATURAL Nº O76-95-INEI
"RECOMENDACIONES TECNICAS PARA LA SEGURIDAD E INTEGRIDAD DE LA INFORMACION QUE SE PROCESA EN LA ADMINISTRACION PUBLICA"
V. CONSIDERACIONES GENERALES

DE LA PROTECCION ESPECIAL DE LA INFORMACION

5.11 Cuando se desee proteger especialmente una base de datos se preverá en su desarrollo, que esté garantizado un límite máximo de instalaciones (licencias autorizadas), para uso.

5.12 Cuando se considere necesario proteger la información clasificada como restringida o reservada, es conveniente encriptarla, es decir, utilizar un software que elabore un algoritmo que permita encontrar un equivalente por cada letra o bloque de información, de tal manera que ese equivalente pueda

5.13 El software de encriptación deberá cumplir las siguientes condiciones:

a) Ser portable, es decir que funciones en todos los ambientes: computadoras grandes, mini y microcomputadoras.

b) Podrá utilizarse en cualquier lenguaje de programación.

c) Ser de fácil entendimiento por el usuario, de tal manera que permita su uso sin necesidad que éste conozca las técnicas de encriptación. d) Estar debidamente documentado, para ser entendible por cualquier usuario.

5.14 La protección especial de la información incluye establecer procedimientos adecuados para el control y distribución de la información impresa, así como para la grabación de los medios magnéticos u ópticos y su respectivo almacenamiento.

LEY Nº 27815, "LEY DEL CÓDIGO DE ÉTICA DE LA FUNCIÓN PÚBLICA"

EMITIDA POR LA COMISIÓN PERMANENTE DEL CONGRESO DE LA REPÚBLICA.

CAPÍTULO III

PROHIBICIONES ÉTICAS DEL SERVIDOR PÚBLICO

ARTÍCULO 8.- PROHIBICIONES ÉTICAS DE LA FUNCIÓN PÚBLICA

NRO. 1. MANTENER INTERESES DE CONFLICTO

Mantener relaciones o de aceptar situaciones en cuyo contexto sus intereses personales, laborales, económicos o financieros pudieran estar en conflicto con el cumplimento de los deberes y funciones a su cargo.

NRO. 2. OBTENER VENTAJAS INDEBIDAS

Obtener o procurar beneficios o ventajas indebidas, para sí o para otros, mediante el uso de su cargo, autoridad, influencia o apariencia de influencia.

NRO. 4. HACER MAL USO DE INFORMACIÓN PRIVILEGIADA

Participar en transacciones u operaciones financieras utilizando información privilegiada de la entidad a la que pertenece o que pudiera tener acceso a ella por su condición o ejercicio del cargo que desempeña, ni debe permitir el uso impropio de dicha información para el beneficio de algún interés.

LEY N° 30096
EMITIDA POR EL CONGRESO DE LA REPÚBLICA
LEY DE DELITOS INFORMATICOS
Atentado contra la integridad de sistemas informáticos El que, a través de las tecnologías de la información o de la comunicación, Inutiliza, total o parcialmente, un sistema Informático, Impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días multa

A.5. Prevención del Uso Inadecuado de los Recursos de Procesamiento de Información

Los recursos de procesamiento de información del Organismo se suministran con un propósito determinado. Toda utilización de estos recursos con propósitos no autorizados o ajenos al destino por el cual fueron provistos debe ser considerada como uso indebido.
Todos los empleados deben conocer el alcance preciso del uso adecuado de los recursos informáticos y deben respetarlo.

A.6. Regulación de Controles para el Uso de Criptografía

Los dispositivos criptográficos a utilizarse para la firma digital dentro de la IOFE, según los alcances de lo que señala la Ley de Firmas y Certificados Digitales y su Reglamento, se guiarán además de por estas normas, por lo referido en las Guías de Acreditación emitidas por la Autoridad Administrativa Competente:
LEY DE FIRMAS Y CERTIFICADOS DIGITALES LEY Nº 27269.
ARTÍCULO 1º.- Objeto de la ley La presente ley tiene por objeto regular la utilización de la firma electrónica otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita u otra análoga que conlleve manifestación

de voluntad.

RESOLUCIÓN MINISTERIAL Nº 381-2008-PCM CAPITULO II. ESTÁNDARES Y ESPECIFICACIONES DE INTEROPERABILIDAD DEL ESTADO PERUANO
8. SEGURIDAD
8.1. Políticas técnicas
NRO. 11. El uso de criptografía y certificación digital, para la protección del tráfico, almacenamiento de datos, control de acceso, firma digital y firma de código, debe estar en conformidad con las Guías de Acreditación respectivas aprobadas por la Autoridad Administrativa Competente INDECOPI.

A.7. Recolección de Evidencia

Es necesario contar con adecuada evidencia para respaldar una acción contra una persona u organización. Siempre que esta acción responda a una medida disciplinaria interna, la evidencia necesaria estará descrita en los procedimientos internos.

Cuando la acción implique la aplicación de una ley, tanto civil como penal, la evidencia presentada debe cumplir con lo establecido por las normas procesales. Para lograr la validez de la evidencia, el Organismo garantizará que sus sistemas de información cumplen con la normativa y los estándares o códigos de práctica relativos a la producción de evidencia válida.

Para lograr la calidad y totalidad de la evidencia es necesaria una sólida pista de la misma. Esta pista se establecerá cumpliendo las siguientes condiciones:

a) Almacenar los documentos en papel originales en forma segura y mantener registros acerca de quién lo halló, dónde se halló, cuándo se halló y quién presenció el hallazgo.
b) Cualquier investigación debe garantizar que los originales no sean alterados.
c) Copiar la información para garantizar su disponibilidad. Se mantendrá un registro de todas las acciones realizadas durante el proceso de copia. Se almacenará en forma segura una copia de los medios y del registro. Cuando se detecta un incidente, puede no resultar obvio si éste derivará en una demanda legal por lo tanto se deben tomar todos los recaudos establecidos para la obtención y preservación de la evidencia.

Se deberá tener presente lo dispuesto por el Reglamento de Investigaciones Administrativas, procedimiento administrativo especial, de naturaleza correctiva interna que constituye garantía suficiente para la protección de los derechos y correcto ejercicio de las responsabilidades impuestas a los agentes públicos. Este Decreto debe ser complementado por lo dispuesto en la Ley del Procedimiento Administrativo General. Ley Nº 27444 y por toda otra normativa aplicable, incluido el Código Penal, Capitulo II Delitos Contra Datos y Sistemas Informáticos Artículo 3. Atentado contra la integridad de datos informáticos.

1.10 ASPECTOS METODOLOGICOS

1.10.1 Tipo de Nivel de Investigación

La presente investigación es de carácter descriptivo, debido a que su propósito es la formulación de un problema, y proponer estrategias en la gestión de la seguridad de los servicios críticos de la Municipalidad Provincial de Chiclayo y así posibilitar una investigación más precisa o el desarrollo de una hipótesis.

Además, cabe resaltar que a través de fuentes de información de otros autores como monografías e investigaciones bibliográficas, nos ha ayudado a reunir y sintetizar experiencias, y a la vez que se aclaren conceptos sobre el nivel de conocimiento científico desarrollado previamente por estos trabajos y poder catalogar este tipo de estudio.

1.10.2 Población y Muestra

1.10.2.1. Población
La población-objeto.

Encargados y trabajadores de la Gerencia de Tecnología y Comunicaciones de las áreas de Desarrollo de Sistemas y Soporte Técnico es de 10.

1.10.2.2. Muestra

Para la determinación de la muestra he creído conveniente utilizar la técnica de muestreo aleatorio simple, para cada uno de los sectores a encuestar:

- Encargados y personal que labora en las áreas de Desarrollo de Sistemas y de Soporte Técnico de la Gerencia de Tecnología y Comunicaciones.
  Debido a que la muestra del sector de jefes y personal que labora en las áreas de Desarrollo de Sistemas y de Soporte Técnico, es muy pequeña se vio por conveniente aplicar la técnica de muestreo aleatorio simple, la que permitirá trabajar con toda la muestra obtenida en dicho sector.

  n = 10 personas a trabajar, ya sea, con entrevistas u otros instrumentos de recolección de información.

1.10.3 Diseño de la Investigación

Se realizó encuesta. En el Anexo Nº 1 se muestra el diseño de la encuesta.

1.10.3.1. Indicadores

Para determinar la contrastación de nuestra investigación entre las operaciones antes del diseño del Sistema de Gestión de la Seguridad de la Información y después del mismo, se han determinado los siguientes indicadores:

- ✓ Porcentaje de evaluación de riesgos de seguridad identificados y evaluados con niveles de importancia alta, media o baja
- ✓ Grado de aplicación de políticas de seguridad en la organización
- ✓ Porcentaje de empleados que han recibido y aceptado formalmente, roles y responsabilidades con respecto a seguridad de la información
- ✓ Número de informes de inspecciones periódicas de seguridad física de instalaciones, incluyendo actualización
- ✓ Número y costes acumulados de incidentes por software malicioso como virus, gusanos, troyanos o spam detectados y bloqueados
- ✓ Porcentaje de backups y archivos con datos sensibles o valiosos que se encuentran protegidos dentro y fuera de la empresa
- ✓ Número de incidentes de seguridad de red identificados en los meses anteriores, dividido por categorías de leve importante y grave importancia
- ✓ Número de peticiones de cambios de acceso por parte del personal que labora en la empresa
- ✓ Estado de la seguridad en entorno portátil, es decir, un informe sobre el estado actual de la seguridad de equipos informáticos portátiles (laptops, tablets, teléfonos móviles, etc.)
- ✓ Porcentaje de sistemas para los cuales los controles de validación de datos se han definido e implementado y demostrado eficaces mediante pruebas
- ✓ Porcentaje de sistemas evaluados de forma independiente conforme a estándares de seguridad básica
- ✓ Numero de informes sobre el estado actual de la seguridad en los procesos de desarrollo de software, con comentarios sobre incidentes recientes/actuales, vulnerabilidades actuales de seguridad conocidas y pronósticos sobre cualquier riesgo

- ✓ Número de chequeos (a personas a la salida) realizados en el último mes y porcentaje de chequeos que evidenciaron movimientos no autorizados de equipos o soportes informáticos u otras cuestiones de seguridad
- ✓ Porcentaje de nuevos empleados relacionados con las tecnologías de información y comunicaciones (contratistas, consultores, temporales, etc.) que hayan sido totalmente verificados y aprobados de acuerdo con las políticas de la empresa antes de comenzar a trabajar.

1.10.4 Técnicas e instrumentos de Recolección de Datos

El cuestionario se aplicó al personal experto de TIC que se seleccionó en la muestra, la cual estableció las consecuencias lógicas de los objetivos e hipótesis planteados.

Para la obtención de información haremos uso de herramientas como son: entrevista, encuestas y observación.

TÉCNICA / MÉTODO	JUSTIFICACIÓN	HERRAMIENTAS	APLICACIÓN
Entrevista	Nos va a permitir conocer más acerca de los procesos de la institución, sus problemas, objetivos y requerimientos.	Cuestionarios. Aplicación grabador de voz de smartphone.	Trabajadores de las áreas en estudio.
Observación	Es el método en la cual enfocamos la perspectiva de los problemas que existen en las áreas a trabajar.	Fichas o guías de observaciones	Trabajadores de las áreas en estudio.
Encuestas	Permite conocer las expectativas que tienen los usuarios respecto al nuevo sistema y necesidades de Información de los usuarios.	Encuesta de Preguntas Abiertas y Cerradas y Checklist	Trabajadores de las áreas en estudio.

Tabla 5: Técnicas, Instrumentos, Fuentes e Informantes

Fuente: Elaboración propia

1.10.5 Tratamiento y procesamiento de los datos

Se procedió a la codificación y tabulación de la información para el recuento, clasificación y ordenación de la información en tablas.

Una vez que se obtuvo la información tabulada se procedió a procesarla mediante las herramientas de Microsoft Office.

1.10.5.1. Análisis de la información

Mediante la observación y los datos obtenidos en las investigaciones a través del personal de las áreas involucradas, se hará el análisis respectivo con la finalidad de mejorar la seguridad de la información. Esto dará origen a que se sugiera algunos controles de seguridad para mejorar el control de la información.

1.10.5.2. Recurso disponible

A.- Personal

Recurso: Otero More, Juan Francisco

B.- Equipo

Partida	Descripción	Cantidad	Costo S/.	Costo Total S/.
01	Bienes			**430.50**
01.01	Materiales de escritorio			
	Hojas A4 75gr.	2 millar	19.00	38.00
	USB 16 Gb	2 unidades	35.00	70.00
	PC Intel Core i3	1 unidad	-	-
	Laptop Lenovo Core i5	1 unidad	-	-
01.02	Materiales de impresión, fotográfico y fonotécnico			
	DVD-ROM	5 unidades	1.50	7.50
	Tinta de impresora	4 unidades	35.00	140.00
	Fotocopias	½ millar	0.05	25.00
01.03	Otros	-	150.00	150.00
02	Servicios			**3040.00**
02.01	Servicios básicos			
	Luz	12 meses	100.00	1200.00
02.02	Teléfono + Internet	12 meses	120.00	1440.00
02.03	Pasajes	-	250.00	250.00
02.04	Otros	-	150.00	150.00
TOTAL				**3470.50**

Tabla 6: Recurso disponible Equipo

C.- Consolidado

El costo total de este proyecto es un aproximado de S/. 3470.50

D.- Financiación

Costo Total del Proyecto: S/. 3470.50

Financiamiento: Autofinanciamiento

CAPITULO II: MARCO TEORICO

2.1 ANTECEDENTES DE LA INVESTIGACION

La Presidencia del Consejo de Ministros a través de la Oficina Nacional de Gobierno Electrónico e Informático (ONGEI) consciente de la modernización de las organizaciones públicas en el Gobierno Electrónico que requieren un enfoque más agudo en seguridad de la información, emitió la primera encuesta nacional sobre seguridad de la información con RM- 310-2004 (Anexo Nº 2).

Posteriormente se modificó la Encuesta de Seguridad de la Información en la Administración Pública, y es aplicada a las entidades públicas como poderes del Estado, organismos autónomos y gobiernos locales[1].

Dentro de los puntos más relevantes de la encuesta se ha observado que:

- El 63% no posee un responsable en temas de seguridad de la información.
- El 86% no cuenta con asesoramiento en temas de seguridad de la información.
- El 59% de instituciones no prepara a sus usuarios para reportar incidentes de seguridad.
- El 82% no recibe capacitación en temas de seguridad.
- El 70% no tiene preparados procedimientos de respuesta a incidentes o anomalías que pudieran suceder.

Con fecha 23 de Julio de 2004 la Presidencia del Consejo de Ministro a través de la Oficina Nacional de Gobierno Electrónico e Informático, dispone de uso obligatorio de la Norma Técnica Peruana: “NTP – ISO 17999:2004 EDI. Tecnología de la Información: Código de Buenas Prácticas para la Gestión de la Seguridad de la Información” en las entidades del Sistema Nacional de Informática[2].

1 OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA. Encuesta de Seguridad de la Información en la Administración Pública. [En línea] http://www2.pcm.gob.pe/Transparencia/Resol_ministeriales/2010/RM-187-2010-PCM.pdf. [Consulta: 10 de Octubre de 2015]

2 OFICINA NACIONAL DE GOBIERNO ELECTRÓNICO E INFORMÁTICA. Norma Técnica Peruana. [En línea]. http://www.pecert.gob.pe/_normas/ISO27000/RM-004-2016-PCM.pdf. [Consulta: 10 de Octubre de 2015]

Dicha norma se basa en el estándar internacional ISO 17799 que es una compilación de recomendaciones para las prácticas exitosas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector.

2.1.1. Casos en Europa

Tema:

Proyecto CAMERSEC - Implantación de Sistemas de Gestión de Seguridad de la Información en PyMEs

Autor:

Andrés García Martínez.

Lugar de investigación:

España, Cámara de Comercio, Industria y Navegación de Málaga

Año de investigación:

26 de octubre de 2006

Resumen:

El Proyecto CAMERSEC promueve actuaciones de consultoría para Sistemas de Gestión de Seguridad de la Información realizadas por Grupo Nexus Consultores y Auditores y Tecnotur 3000, siendo decisión de la empresa adherida certificar o no dicho sistema. La iniciativa se está tramitando para que cuente con el apoyo a modo de incentivos por parte de la Agencia IDEA (Consejería de Innovación, Ciencia y Empresa) de cara a la financiación del mismo, así como la obtención de precios en condiciones ventajosas para la consultoría y certificación.

Análisis:

Este proyecto es altamente recomendado para empresas cuyos activos de información tengan un alto valor para la actividad organizacional, la implantación de un sistema de esta naturaleza ayuda a la gestión de la seguridad de sus activos de información ya que afecta a políticas y estrategias de la empresa y constituye un aporte de valor indiscutible para cualquier tipo de actividad empresarial.

Tema:

Proyecto Sanitas - Sistema de Gestión de Seguridad de la Información y certificación UNE 71502 e ISO 27001

Autor:

Enrique Martín Méndez

Miguel Ángel Aguilar

Lugar de investigación:

España, El Grupo Sanitas

Año de investigación:

Noviembre 2006

Resumen:

Sanitas, empresa puntera en el sector de asistencia sanitaria, ha culminado con éxito la implantación de un Sistema de Gestión de Seguridad de la Información y la consiguiente obtención de los certificados UNE 71502 e ISO 27001 bajo el sello de Aenor. El proyecto se ha llevado a cabo con el apoyo de la consultora especializada en seguridad de la información ESA Security, que ha aportado su experiencia en la implantación de estos sistemas. El Departamento de Seguridad de Sanitas, perteneciente a la Dirección General de Sistemas de Información, ha sido el impulsor de este proyecto con el objetivo de mejorar continuamente en su gestión.

Análisis:

El desarrollo del proyecto en Sanitas le permitió ser certificable, esto debido a la confianza y colaboración de querer salir adelante; también al reconocer que los activos de información de su empresa son muy importantes en el desarrollo de sí misma, por ello busco métodos para salvaguardar y proteger su información

2.1.2. Casos en Latinoamérica

Tema:

Trabajo final: Plan de Seguridad Informática.

Autores:

María Dolores Cerini.

Pablo Ignacio Prá.

Lugar de investigación:

Córdoba – Argentina, EMPRESA ARGENTINA nacional.

Año de investigación:

Universidad Católica de Córdoba - 2002

Resumen:

Esta es una empresa concesionaria automotriz que a través del proyecto se quiere desarrollar documentos y directrices que orienten el uso adecuado de las tecnologías de información para obtener el mayor provecho de las ventajas que brindan. De esta manera se va a implementar políticas de seguridad de la información en la compañía para que pueda desarrollarse y mantenerse en su sector de negocios. Las políticas de seguridad de la información van a fijar los mecanismos y procedimientos que deben adoptar las empresas para salvaguardar sus sistemas y la información que estos contienen.

Análisis:

Este trabajo es muy importante ya que su aplicación está basada en un entorno diferente al de nosotros, el cual nos permitirá tener un mejor enfoque al proyecto de investigación que tratamos de llevar a cabo.

Tema:

Tesis de licenciatura: Seguridad Informática – sus Implicancias e Implementación

Autor:

Borghello Cristian Fabian.

Lugar de investigación:

Argentina, Universidad Tecnológica Nacional.

Año de investigación:

2001

Resumen:

Esto es un proyecto general sobre la seguridad informática en el entorno de las empresas. El estudio se avala en la forma como utilizar las herramientas adecuadas para la seguridad informática desde su implantación hasta su resultado e implicancias que tiene dentro de las organizaciones.

Análisis:

Este proyecto es muy interesante en cuanto al grado de conocimientos descriptos para la implementación y sus posteriores implicancias resultantes del proyecto.

A grandes rasgos se podrá ver la forma técnica en la que se va desarrollando el trabajo.

2.1.3. Casos en Perú

Tema:

Tesis: "Factores inhibidores en la implementación de Sistemas de Gestión de la Seguridad de la Información basado en la NTP-ISO/IEC 17799 en la Administración Pública."

Autor:

Alipio Mariño Obregón

Lugar de investigación:

Lima – Perú, Universidad Nacional Mayor de San Marcos.

Año de investigación:

2010.

Resumen:

Es un estudio cuantitativo, transversal, hipotético – deductivo sobre el proceso de implantación de la Norma Técnica NTP – ISO/IEC 17799. Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática del Perú.

Esta investigación, se introduce dentro del marco del desarrollo de la Sociedad de la Información, la Agenda Digital Peruana y el Proyecto de Gobierno Electrónico en el Perú y responde a la siguiente pregunta ¿Cuáles son los factores inhibidores que influyen en el bajo nivel de implementación de la Norma Técnica NTP – ISO/IEC 17799 Código de buenas prácticas para la gestión de la seguridad de la información en las Entidades del Sistema Nacional de Informática?

Para este propósito, se recopiló información a través de una encuesta semi estructurada en 16 Organismos Públicos Descentralizados adscritas a la Presidencia del Consejo de Ministros (PCM) del Gobierno Nacional,

que tienen su Sede en la ciudad de Lima. La información recopilada en la encuesta, fue procesada y analizada, que permitió luego identificar factores de orden estratégico y operativo causantes del bajo nivel de implantación de la norma. Finalmente, hemos planteado las recomendaciones orientadas a superar las dificultades que enfrentan dichas entidades, cumpliéndose de esta manera con el propósito de la investigación.

Análisis:

Este tema de investigación nos permite tener un conocimiento más amplio de la seguridad, que se regirá bajo normas para el adecuado uso de la información dentro y fuera de la organización siendo muy importante dentro de la misma.

2.2 MARCO TEÓRICO

2.2.1. ISO 27000

2.2.1.1. Origen

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution, la organización británica equivalente a AENOR en España) es responsable de la publicación de importantes normas como:

1979 Publicación BS 5750 - ahora ISO 9001

1992 Publicación BS 7750 - ahora ISO 14001

1996 Publicación BS 8800 - ahora OHSAS 18001

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica o no un conjunto de buenas prácticas para la gestión de la seguridad de su información. La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. Es la segunda parte (BS 7799-2), publicada por primera vez en 1998, la que establece los requisitos de un sistema de gestión de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.

En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, con más de 1700 empresas certificadas en BS7799-2, este esquema se publicó por ISO como estándar ISO 27001, al tiempo que se revisó y actualizó ISO17799. Esta última norma se renombra como ISO 27002:2005 el 1 de Julio de 2007, manteniendo el contenido así como el año de publicación formal de la revisión.

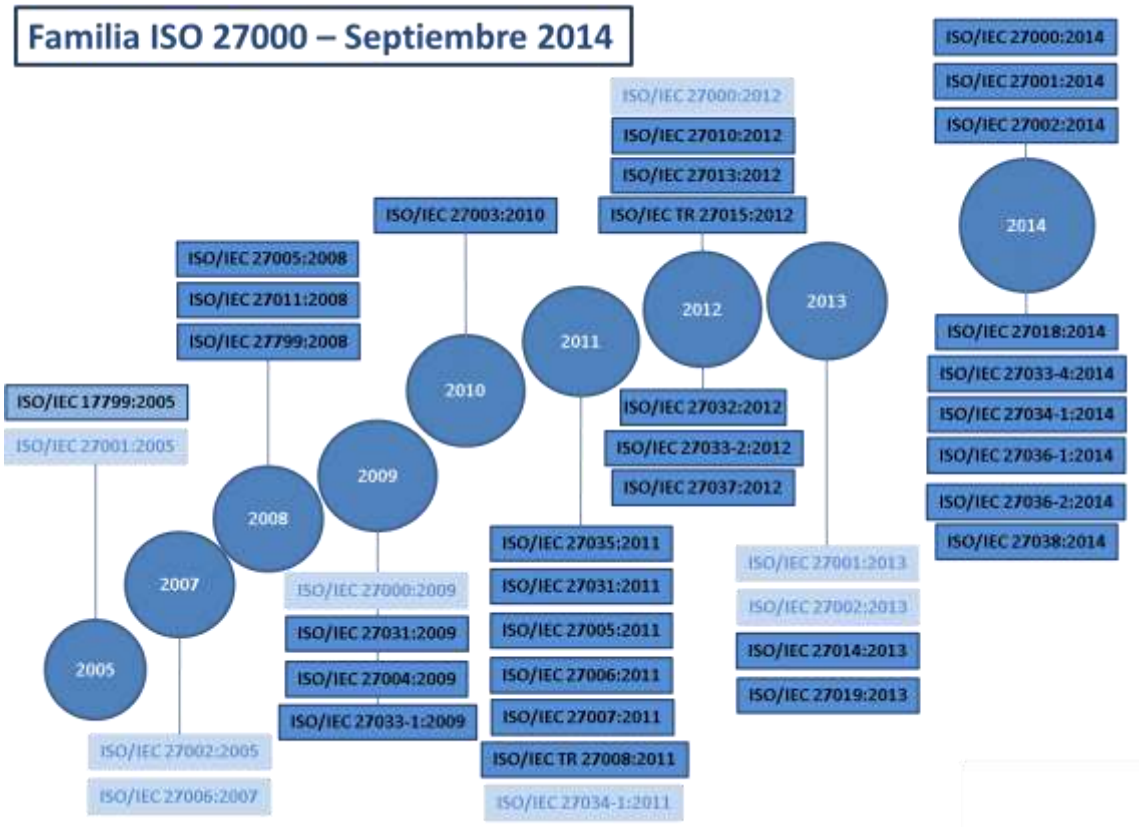

Ilustración 1: Historia de ISO 27000

Fuente: http://es.slideshare.net/RicardoUrbinaM/iso-40313086

En Marzo de 2006, posteriormente a la publicación de la ISO27001:2005, BSI publicó la BS7799-3:2006, centrada en la gestión del riesgo de los sistemas de información.

Únicamente considerar la reciente publicación de la revisión de las normas ISO/IEC 27001:2013, ISO/IEC 27002:2013 ambas aprobadas en la misma fecha: 25 de Septiembre de 2013.

Para aquellas normas aún no publicadas o en fase de revisión puede consultarse el estado de aprobación en ISO y consultar su estado de avance por el comité según la tabla de referencia. Toda la información disponible públicamente sobre el desarrollo de las normas de la serie 27000 puede consultarse en las páginas web del subcomité JTC1/SC27:

http://www.jtc1sc27.din.de/

http://www.iso.org/iso/

2.2.1.2. La serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Los rangos de numeración reservados por ISO van de 27000 a 27019 y de 27030 a 27044.

- ISO 27000: Publicada el 1 de Mayo de 2009, revisada con una segunda edición de 01 de Diciembre de 2012 y una tercera edición de 14 de Enero de 2014. Esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua). Exiten versiones traducidas al español aunque hay que prestar atención a la versión descargada. El original en inglés y su traducción al francés en su versión de 2014 puede descargarse gratuitamente de www.standards.iso.org

- ISO 27001: Publicada el 15 de Octubre de 2005, revisada el 25 de Septiembre de 2013. Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 (que ya quedó anulada) y es la norma con arreglo a la cual se certifican por auditores externos los SGSI de las organizaciones. En su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002:2005, para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI; a pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados. El original en inglés y la traducción al francés pueden adquirirse en www.iso.org

Actualmente, la última edición de 2013 este estándar se encuentra en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013.

- ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios. Como se ha mencionado en su apartado correspondiente, la norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005. Publicada en Perú como ISO 17799 (descarga gratuita). El original en inglés y su traducción al francés pueden adquirirse en www.iso.org

  Actualmente, la última edición de 2013 este estándar ha sido actualizada a un total de 14 Dominios, 35 Objetivos de Control y 114 Controles publicándose inicialmente en inglés y en francés tras su acuerdo de publicación el 25 de Septiembre de 2013.

2.2.1.3. Contenido

A. ISO 27001:2005:

Generalidades

Esta Norma Internacional ha sido preparada para proporcionar un modelo que permita establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para la organización. Se espera que la escala de implementación de un SGSI se establezca de acuerdo a las necesidades de la organización, es decir, una situación sencilla requiere una solución de SGSI sencilla.

¿Qué aporta la certificación ISO 27001?

La certificación ISO 27001 avala la adecuada implantación, gestión y operación de todo lo relacionado con la implantación de un SGSI, siendo la norma más completa que existe en lo relativo a la implantación de controles, métricas e

indicadores que permiten establecer un marco adecuado de gestión de la seguridad de la información para las organizaciones.

Entre las ventajas que ofrece, al ser un estándar ISO, se encuentran las facilidades que ofrece de integración con otros sistemas de gestión vigentes en la empresa, por ejemplo ISO 9001 e ISO 14001.

- **Introducción:** generalidades e introducción al método PDCA.
- **Objeto y campo de aplicación:** se especifica el objetivo, la aplicación y el tratamiento de exclusiones.
- **Normas para consulta:** otras normas que sirven de referencia.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- **Sistema de gestión de la seguridad de la información:** cómo crear, implementar, operar, supervisar, revisar, mantener y mejorar el SGSI; requisitos de documentación y control de la misma.
- **Responsabilidad de la dirección:** en cuanto a compromiso con el SGSI, gestión y provisión de recursos y concienciación, formación y capacitación del personal.
- **Auditorías internas del SGSI:** cómo realizar las auditorías internas de control y cumplimiento.
- **Revisión del SGSI por la dirección:** cómo gestionar el proceso periódico de revisión del SGSI por parte de la dirección.
- **Mejora del SGSI:** mejora continua, acciones correctivas y acciones preventivas.
- **Objetivos de control y controles:** anexo normativo que enumera los objetivos de control y controles que se encuentran detallados en la norma ISO 27002:2005.
- **Relación con los Principios de la OCDE:** anexo informativo con la correspondencia entre los apartados de la ISO 27001 y los principios de buen gobierno de la OCDE.
- **Correspondencia con otras normas:** anexo informativo con una tabla de correspondencia de cláusulas con ISO 9001 e ISO 14001.
- **Bibliografía:** normas y publicaciones de referencia.

B.- ISO 27002:2005 (anterior ISO 17799:2005):

- **Introducción:** conceptos generales de seguridad de la información y SGSI.
- **Campo de aplicación:** se especifica el objetivo de la norma.
- Términos y definiciones: breve descripción de los términos más usados en la norma.
- **Estructura del estándar:** descripción de la estructura de la norma.
- **Evaluación y tratamiento del riesgo:** indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- **Política de seguridad:** documento de política de seguridad y su gestión.
- **Aspectos organizativos de la seguridad de la información:** organización interna; terceros.
- **Gestión de activos:** responsabilidad sobre los activos; clasificación de la información.
- **Seguridad ligada a los recursos humanos:** antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.
- **Seguridad física y ambiental:** áreas seguras; seguridad de los equipos.
- **Gestión de comunicaciones y operaciones:** responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- **Control de acceso:** requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.

- **Gestión de incidentes de seguridad de la información:** notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- **Gestión de la continuidad del negocio:** aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- **Cumplimiento:** cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorias de los sistemas de información.
- **Bibliografía:** normas y publicaciones de referencia.

2.2.1.4. Beneficios

- ✓ Establecimiento de una metodología de gestión de la seguridad clara y estructurada.
- ✓ Reducción del riesgo de pérdida, robo o corrupción de información.
- ✓ Los clientes tienen acceso a la información a través medidas de seguridad.
- ✓ Los riesgos y sus controles son continuamente revisados.
- ✓ Confianza de clientes y socios estratégicos por la garantía de calidad y confidencialidad comercial.
- ✓ Las auditorías externas ayudan cíclicamente a identificar las debilidades del sistema y las áreas a mejorar.
- ✓ Posibilidad de integrarse con otros sistemas de gestión (ISO 9001, ISO 14001, OHSAS 1800).
- ✓ Continuidad de las operaciones necesarias de negocio tras incidentes de gravedad.
- ✓ Conformidad con la legislación vigente sobre información personal, propiedad intelectual y otras.
- ✓ Imagen de empresa a nivel internacional y elemento diferenciador de la competencia.
- ✓ Confianza y reglas claras para las personas de la organización.
- ✓ Reducción de costes y mejora de los procesos y servicio.
- ✓ Aumento de la motivación y satisfacción del personal.
- ✓ Aumento de la seguridad en base a la gestión de procesos en vez de en la compra sistemática de productos y tecnologías.

2.2.2. Sistema de Gestión de la Seguridad de la Información

El SGSI (Sistema de Gestión de Seguridad de la Información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. 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.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

- Confidencialidad: La información no se pone a disposición ni se revela a individuos, entidades o procesos; está protegida de personas no autorizadas.
- Integridad: La información se muestra como se pretende sin modificaciones inapropiadas.
- Disponibilidad: Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que constituye un SGSI.

2.2.2.1. ¿Para qué sirve un SGSI?

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

Ilustración 2: Riesgos - SGSI

Fuente: www.ISO27000.es

2.2.2.2. ¿Qué incluye un SGSI?

En el ámbito de la gestión de la calidad según ISO 9001, siempre se ha mostrado gráficamente la documentación del sistema como una pirámide de cuatro niveles. Es posible trasladar ese modelo a un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001 de la siguiente forma:

Ilustración 3: Documentación del Sistema de Seguridad

Fuente: www.ISO27000.es

- **Documentos de Nivel 1**

  Manual de seguridad: Documentación que inspira y dirige todo el sistema, el que expone y determina las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales, etc., del SGSI.

- **Documentos de Nivel 2**

  Procedimientos: Documentación en el nivel operativo, que aseguran que se realicen de forma eficaz la planificación, operación y control de los procesos de seguridad de la información.

- **Documentos de Nivel 3**

  Instrucciones, checklists y formularios: Documentación que describen cómo se realizan las tareas y las actividades específicas relacionadas con la seguridad de la información.

- **Documentos de Nivel 4**

  Registros: Documentación que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados a documentos de los otros tres niveles como output que demuestra que se ha cumplido lo indicado en los mismos.

  De manera específica, ISO 27001 indica que un SGSI debe estar formado por los siguientes documentos (en cualquier formato o tipo de medio):

  - **Alcance del SGSI:** Ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la

organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- **Política y objetivos de seguridad**: Documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.
- **Procedimientos y mecanismos de control que soportan al SGSI:** Aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- **Enfoque de evaluación de riesgos:** Descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.
- **Informe de evaluación de riesgos:** Estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- **Plan de tratamiento de riesgos:** Documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.
- **Procedimientos documentados:** Todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- **Registros:** Documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- **Declaración de aplicabilidad:** (SOA -Statement of Applicability-, en sus siglas inglesas); documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los

resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

2.2.2.3. ¿Qué aspectos de seguridad cubre un SGSI?

Niveles de seguridad:

- Lógica: Confidencialidad, integridad y disponibilidad del software y datos de un SGI.
- Organizativa: Relativa a la prevención, detección y corrección de riesgos.
- Física: Protección de elementos físicos de las instalaciones: servidores, PCs, etc.
- Legal: Cumplimiento de la legislación vigente.

Ilustración 4: Aspectos que cubre el SGSI

2.2.2.4 ¿Cómo se implementa un SGSI?

Se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

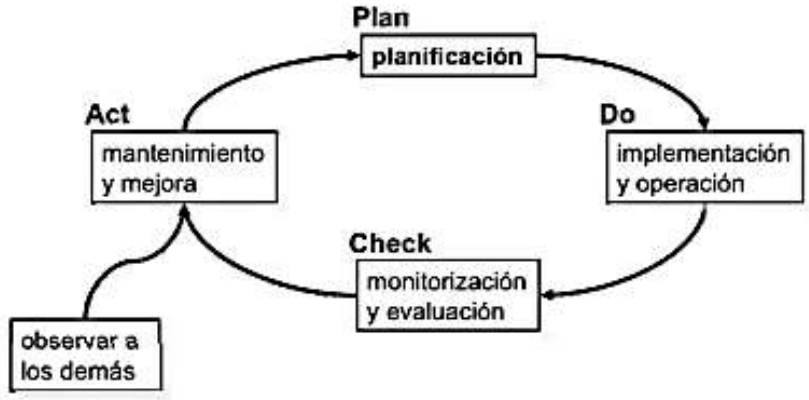

Ilustración 5: Modelo de Desarrollo del SGSI

Fuente: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/index.html

2.2.2.5. Revisión del SGSI

A la dirección de la organización se le asigna también la tarea de, al menos una vez al año, revisar el SGSI, para asegurar que continúe siendo adecuado y eficaz. Para ello, debe recibir una serie de informaciones, que le ayuden a tomar decisiones, entre las que se pueden enumerar:

1. Resultados de auditorías y revisiones del SGSI.
2. Observaciones de todas las partes interesadas.
3. Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
4. Información sobre el estado de acciones preventivas y correctivas.
5. Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
6. Resultados de las mediciones de eficacia.
7. Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
8. Cualquier cambio que pueda afectar al SGSI.
9. Recomendaciones de mejora.
10. Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:
11. Mejora de la eficacia del SGSI.
12. Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.

13. Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
14. Necesidades de recursos.
15. Mejora de la forma de medir la efectividad de los controles.

2.2.3. Análisis y Evaluación del Riesgo

Es un conjunto de pasos metodológicos que debe desarrollar la empresa, que abarca desde que se identifican los activos de información hasta que se establece la importancia de las amenazas por su impacto en el riesgo de los activos. En esencia el análisis del riesgo busca estimar la magnitud del riesgo que afecta a los activos de información. A continuación mostramos la secuencia de pasos metodológicos que sigue el "análisis del riesgo".

Una vez concluido el "análisis del riesgo" es deber realizar la "evaluación del riesgo". La empresa "debe comparar los niveles calculados de riesgo con una escala de riesgo establecida especialmente para dicho efecto." (BS 7799-3:2006). Los criterios para efectuar la evaluación, que usualmente se utilizan, son: "impacto económico del riesgo" y "posibilidad de interrumpir actividades de la empresa." El propósito fundamental de realizar la evaluación del riesgo, es la de identificar el nivel de significado que el riesgo de los activos tienen en la organización y poder jerarquizarlos por su importancia.

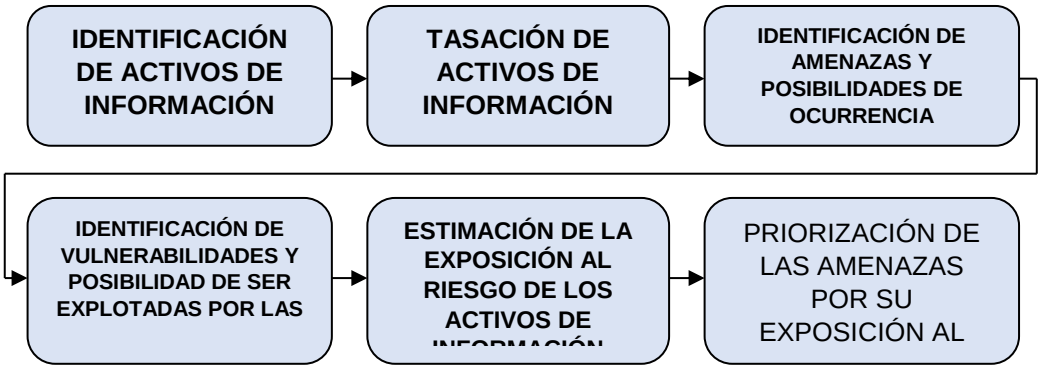

Ilustración 6: Pasos para la Metodología de Análisis de Riesgos

2.2.3.1. Tratamiento del Riesgo y la Toma de Decisiones Gerenciales

Una vez que el riesgo ha sido evaluado y la empresa ha determinado cuales son aquellos activos de información sujetos a riesgo con significado para la firma, debe tomar la decisión de elegir la estrategia adecuada para tratar al riesgo.

Los riesgos pueden ser gestionados a través de una serie de combinaciones de prevención y controles de detección, tácticas de aceptación o realizando la transferencia a otra empresa.

La gerencia para tomar la decisión sobre cómo tratar el riesgo, siempre estará influenciada por dos factores, los cuales deben ser siempre bien analizados:

- ✓ El posible impacto si el riesgo se cristalizara.
- ✓ La posibilidad de su ocurrencia.

Al margen de considerar el impacto financiero del riesgo en la empresa, la firma debe considerar el costo de actuar sobre alguna de las opciones del tratamiento del riesgo. La organización debe asegurarse que existe un buen balance entre poder alcanzar seguridad y los beneficios de protección, sin perjudicar la rentabilidad ni la competitividad de la empresa.

A.- Opciones para el Tratamiento del Riesgo

Para el tratamiento del riesgo existen cuatro estrategias, que son las más difundidas a nivel internacional.

A continuación se hará una breve descripción de cada una de ella:

A.1.- Reducción del Riesgo

Para los riegos 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. Los controles deben obtenerse del anexo “A” del ISO 270001:2005. Al identificar el nivel de los controles es importante considerar los requerimientos de seguridad relacionados con el riesgo, así como la vulnerabilidad y las amenazas previamente identificadas.

Los controles pueden reducir los riesgos valorados en varias maneras:

- 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.

Cualquiera de estas maneras que la empresa escoja para controlar los riesgos, es una decisión que dependerá de una serie de factores, tales como: requerimientos comerciales de la organización, el ambiente, y las circunstancias en que la firma requiere operar.

A.2.- Aceptación del Riesgo

En muchas ocasiones a la empresa se le presentan circunstancias donde no se pueden encontrar controles ni tampoco es factible diseñarlos o el costo de implantar el control es mayor que las consecuencias del riesgo. En estas circunstancias una decisión razonable pudiera ser la de inclinarse por la aceptación del riesgo, y vivir con las consecuencias si el riesgo ocurriese.

Cuando la situación se presenta donde es muy costoso para la empresa mitigar el riesgo a través de los controles o las consecuencias del riesgo son devastadoras para la organización, se deben visualizar las opciones de "transferencia de riesgo" o la de "evitar el riesgo".

A.3.- Transferencia del Riesgo

La transferencia del riesgo, es una opción para la empresa, cuando es muy difícil, tanto técnica como económicamente para la organización llevar al riesgo a un nivel aceptable. En estas circunstancias podría ser económicamente viable, transferir el riesgo a una aseguradora.

Se debe estar pendiente al escoger esta opción de tratamiento de riesgo, que con las empresas aseguradoras, siempre existe un elemento de riesgo residual. Siempre existen condiciones con las aseguradoras de exclusiones, las cuales se aplicaran dependiendo del tipo de ocurrencia, bajo la cual no se provee una indemnización. La transferencia, del riesgo por lo tanto, debe ser muy bien analizada para así poder identificar con precisión, cuando el riesgo actual está siendo transferido.

Otra posibilidad es la de utilizar a terceras partes para el manejo de activos o procesos considerados críticos. Claro está, en la medida que exista la preparación para dicho efecto, por parte de la empresa que ofrece los servicios de tercerización. Lo que debe estar claro, es que al tercerizar servicios, el riesgo residual, no se delega, es responsabilidad de la empresa.

A.4.- 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 si 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.

Ilustración 7: Gestión de Riesgos

Fuente: www.ISO27001.es

2.2.4. Controles de seguridad

Los controles de seguridad son políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos. El objetivo de control en tecnologías de información se define como una sentencia del resultado o propósito que se desea alcanzar

implementando procedimientos de control en una actividad de tecnología de información particular.

El gobierno de las tecnologías de información se define como una estructura de relaciones y procesos para dirigir y controlar la empresa con el fin de lograr sus objetivos al añadir valor mientras se equilibran los riesgos contra el retorno sobre las tecnologías de información y sus procesos.

Lo que es necesario recalcar aquí es que los controles serán seleccionados e implementados de acuerdo a los requerimientos identificados por la valoración del riesgo y los procesos de tratamiento del riesgo. Es decir, que de esta actividad surgirá la primera decisión acerca de los controles que se deberán abordar.

La preparación y planificación de SGSI, son pasos importantes, pero en definitiva, lo importante de todo este proceso es que desencadena en una serie de controles (o mediciones) a considerar y documentar, que se puede afirmar, son uno de los aspectos fundamentales del SGSI (junto con la Valoración de riesgo). Cada uno de ellos se encuentra en estrecha relación a todo lo que especifica la norma ISO/IEC 17799:2005 en los puntos 5 al 15, y tal vez estos sean el máximo detalle de afinidad entre ambos estándares. La evaluación de cada uno de ellos debe quedar claramente documentada, y muy especialmente la de los controles que se consideren excluidos de la misma. El estándar especifica en su “Anexo A” el listado completo de cada uno de ellos, agrupándolos en once dominios. Para cada uno de ellos define el objetivo y lo describe brevemente.

Cabe aclarar que el anexo A proporciona una buena base de referencia, no siendo exhaustivo, por lo tanto se pueden seleccionar más aún. Es decir, estos 133 controles (hoy) son los mínimos que se deberán aplicar, o justificar su no aplicación, pero esto no da por completa la aplicación de la norma si dentro del proceso de análisis de riesgos aparecen aspectos que quedan sin cubrir por algún tipo de control. Por lo tanto, si a través de la evaluación de riesgos se determina que es necesaria la creación de nuevos controles, la implantación del SGSI impondrá la inclusión de los mismos, sino seguramente el ciclo no estará cerrado y presentará huecos claramente identificables.

Los controles que el anexo A de esta norma propone quedan agrupados y numerados de la siguiente forma:

A.5 Política de seguridad

A5.1 Política de seguridad de la información

A.6 Organización de la información de seguridad

A.6.1 Organización interna

A.6.2 Terceros

A.7 Administración de recursos

A.7.1 Responsabilidad por los activos

A.7.2 Clasificación de la información

A.8 Seguridad de los recursos humanos

A.8.1 Antes del empleo

A.8.2 Durante el empleo

A.8.3 Terminación o cambio de empleo

A.9 Seguridad física y del entorno

A.9.1 Áreas aseguradas

A.9.2 Seguridad del equipo

A.10 Administración de las comunicaciones y operaciones

A.10.1 Procedimientos y responsabilidades operativas

A.10.2 Gestión de servicios de terceros

A.10.3 Planeamiento y aceptación de sistemas

A.10.4 Protección contra código malicioso y código móvil

A.10.5 Respaldo

A.10.6 Gestión de seguridad de redes

A.10.7 Manipulación de medios

A.10.8 Intercambio de información

A.10.9 Sistemas de información de negocios

A.10.10 Monitoreo

A.11 Control de accesos

A.11.1 Requisito de negocios para el control de acceso

A.11.2 Gestión del acceso de usuarios

A.11.3 Responsabilidades de los usuarios

A.11.4 Control del acceso a redes

A.11.5 Control de acceso al sistema operativo

A.11.6 Control del acceso a aplicación e información

A.11.7 Computación móvil y teletrabajo

A.12 Adquisición de sistemas de información, desarrollo y mantenimiento

A.12.1 Requisitos de seguridad para sistemas de información

A.12.2 Procesamiento correcto en aplicaciones

A.12.3 Controles criptográficos

A.12.4 Seguridad de archivos del sistema

A.12.5 Seguridad en los procesos de desarrollo y soporte

A.12.6 Gestión de vulnerabilidades técnicas

A.13 Administración de los incidentes de seguridad

A.13.1 Reportes de eventos y debilidades de seguridad de la información

A.13.2 Gestión de incidentes y mejoras de seguridad de la información

A.14 Administración de la continuidad de negocio

A.14.1 Aspectos de seguridad de la información en la gestión de la continuidad de negocios

A.15 Cumplimiento (legales, de estándares, técnicas y auditorias)

A.15.1 Cumplimiento de requisitos legales

A.15.2 Cumplimiento de las políticas y normas de seguridad, y cumplimiento técnico

A.15.3 Consideraciones de auditoría de sistemas de información

(Anexo N° 3)

2.3. Marco Conceptual

C.1. ISO 27000: Se desarrolló por ISO/IEC JTC/SC27 una familia de estándares internacionales para sistemas de gestión de la seguridad de la información (SGSI), la que incluye requerimientos de sistemas de gestión de seguridad de la información, gestión de riesgo, métricas y medidas, guías de implantación, vocabulario y mejora continua.

C.2. ISO (Organización Internacional de Normalización) es el mayor desarrollador y editor de Normas Internacionales: ISO is a network of the national standards institutes of 157 countries , one member per country, with a Central Secretariat in Geneva, Switzerland, that coordinates the system. “ISO” deriva del griego isos que significa “igual”. Whatever the country, whatever the language, the short form of the organization’s name is always ISO. Sea cual sea el país, cualquiera que sea el idioma, la forma corta del nombre de la organización es siempre la ISO. La ISO es una organización no gubernamental que forma un puente entre los sectores público y privado. On the one hand, many of its member institutes are part of the governmental structure of their countries, or are mandated by their government. ISO es una red de los organismos nacionales de normalización de 157 países, un miembro por país, con una Secretaría Central en Ginebra, Suiza, que coordina el sistema .ISO is a non-governmental organization that forms a bridge between the public and private sectors. Therefore, ISO enables a consensus to be reached on solutions that meet both the requirements of business and the broader needs of society.

C.3. AENOR (Asociación Española de Normalización y Certificación. Organismo certificador Español): Es una entidad dedicada al desarrollo de la normalización y la certificación en todos los sectores industriales y de servicios. Tiene como propósito contribuir a mejorar la calidad y la competitividad de las empresas, así como proteger el medio ambiente. Fue designada para llevar a cabo estas actividades por la Orden del Ministerio de Industria y Energía, de 26 de febrero de 1986, de acuerdo con el Real Decreto 1614/1985 y reconocida como organismo de normalización y para actuar como entidad de certificación por el Real Decreto 2200/1995, en desarrollo de la Ley 21/1992, de Industria.

C.4. La Seguridad de la información: es el conjunto de estándares, procesos, procedimientos, estrategias, recursos informáticos y recurso humano integrado para proveer toda la protección debida y requerida a la información y a los recursos informáticos de una empresa, institución o agencia gubernamental.

C.5. La información: es un recurso o activo que, como otros recursos importantes del negocio, es esencial a una organización y a su operación y por consiguiente necesita ser protegido adecuadamente.

C.6. Concienciación de la seguridad de información: Se debe ser consciente de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad. Deben tener el conocimiento de los riesgos y de los mecanismos disponibles de salvaguardia, que son el primer paso en la defensa de la seguridad de los sistemas y redes de información. Estos sistemas y redes de información pueden verse afectados tanto por riesgos internos como externos. Los participantes deben comprender que los fallos en la seguridad pueden dañar significativamente los sistemas y redes que están bajo su control.

C.7. Daños potenciales: La interceptación ilegal puede causar daños tanto por intrusión en la vida privada de las personas como por la explotación de los datos interceptados, como palabras clave o datos de las tarjetas de crédito, para usos comerciales o sabotaje. Este es uno de los principales frenos del desarrollo del comercio electrónico en Europa.

C.8. Soluciones potenciales: La defensa contra la interceptación podrá realizarse a través de los operadores que deben velar por la seguridad de la red con arreglo a lo dispuesto en la Directiva 97/66 CE1 y de los usuarios que pueden encriptar los datos transmitidos por la red.

C.9. La seguridad de las redes es un problema dinámico: La velocidad en el cambio de la tecnología plantea nuevos desafíos de forma permanente. Los problemas que ayer se planteaban desaparecen y las soluciones actuales de

dichos problemas dejan de tener sentido. Casi cada día aparecen en el mercado aplicaciones, servicios y productos nuevos.

C.10. Conformidad con la legislación: Evitar el incumplimiento de cualquier ley, estatuto, regulación u obligación contractual y de cualquier requerimiento de seguridad. Garantizar la alineación de los sistemas con la política de seguridad de la organización y con la normativa derivada de la misma. Maximizar la efectividad y minimizar la interferencia de o desde el proceso de auditoría de sistemas.

2.4. Marco Metodológico del desarrollo de la investigación

2.4.1. Modelo del Sistema de Gestión de Seguridad de la Información PDCA (Plan, Do, Check, Act)

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información en base a ISO 27001, se utiliza el ciclo continuo PDCA, tradicional en los sistemas de gestión de la calidad.

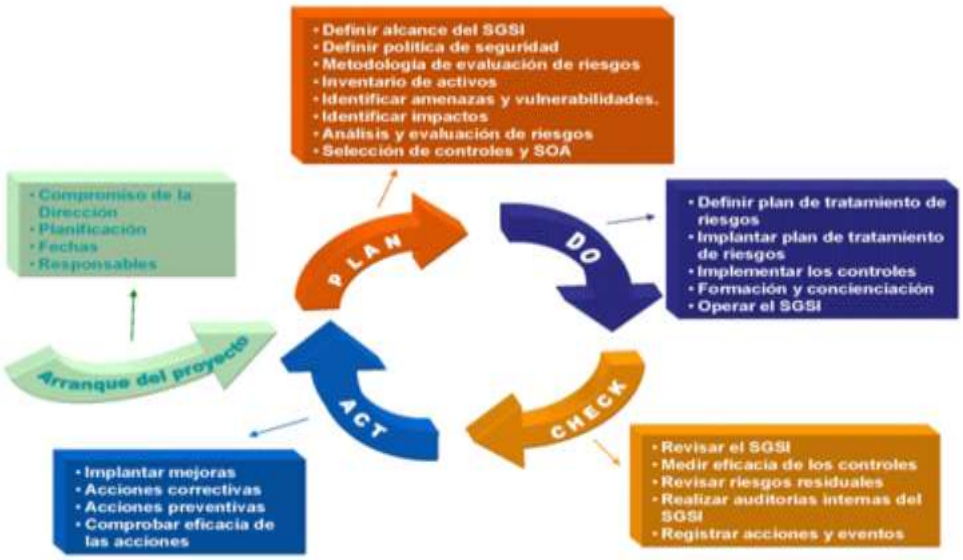

Ilustración 8: Modelo de Desarrollo del SGSI
Fuente: www.ISO27001.es

- *Plan (planificar): establecer el SGSI.*
- *Do (hacer): implementar y utilizar el SGSI.*
- *Check (verificar): monitorizar y revisar el SGSI.*
- *Act (actuar): mantener y mejorar el SGSI.*

2.4.1.1. Arranque del proyecto

- Compromiso de la Dirección: una de las bases fundamentales sobre las que iniciar un proyecto de este tipo es el apoyo claro y decidido de la Dirección de la Institución. No sólo por ser un punto contemplado de forma especial por la norma sino porque el cambio de cultura y concienciación que lleva consigo el proceso hacen necesario el impulso constante de la Dirección.
- Planificación, fechas, responsables: como en todo proyecto de envergadura, el tiempo y el esfuerzo invertidos en esta fase multiplican sus efectos positivos sobre el resto de fases.

2.4.1.2. Plan: Establecer el SGSI

- Definir el alcance del SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión. Definir el alcance y los límites del SGSI (el SGSI no tiene por qué abarcar toda la organización; de hecho, es recomendable empezar por un alcance limitado).
- 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.

La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección, por lo que no pasará de dos o tres páginas.

- Definir una metodología de evaluación del riesgo apropiada para para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO 27001 no impone ninguna ni da indicaciones adicionales sobre cómo definirla (en el futuro, ISO 27005 proporcionará ayuda en este sentido). El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.

Metodología

M.01. COBIT

M.01.1. La necesidad de control en tecnologías de la información:

Las organizaciones exitosas requieren una apreciación y un entendimiento básico de los riesgos y limitaciones de TI a todos los niveles dentro de la empresa con el fin de obtener una efectiva dirección y controles adecuados. La administración (management) debe decidir cuál es la inversión razonable en seguridad y en control en TI y cómo lograr un balance entre riesgos e inversiones en control, en un ambiente de TI frecuentemente impredecible. Mientras la seguridad y los controles en los sistemas de información ayudan a administrar los riesgos, no los eliminan. Adicionalmente, el exacto nivel de riesgo nunca puede ser conocido ya que siempre existe un grado de incertidumbre. Finalmente, la administración debe decidir el nivel de riesgo que está dispuesta a aceptar. Juzgar cual puede ser el nivel tolerable, particularmente cuando se tiene en cuenta el costo, puede ser una decisión difícil para la administración. Por esta razón, la Administración necesita un marco de referencia de las

prácticas generalmente aceptadas de control y seguridad de TI para compararlos contra el ambiente de TI existente y planeado.

Ilustración 9: Gobierno de Tecnología de Información

Fuente: www.itgi.org

www.isaca.org

Para asegurar que la Gerencia alcance los objetivos de negocios, ésta debe dirigir y administrar las actividades de TI para alcanzar un balance efectivo entre el manejo de riesgos y los beneficios encontrados. Para cumplir esto, la Gerencia necesita identificar las actividades más importantes que deben ser desarrolladas, midiendo el progreso hacia el cumplimiento de las metas y determinando que tan bien se están desarrollando los procesos de TI. Aún más, necesita tener la habilidad de evaluar el nivel de madurez de la organización contra las mejores prácticas industriales y los modelos internacionales. Para soportar estas necesidades la Gerencia necesita las Directrices Gerenciales de COBIT en las cuales se han identificado Factores Críticos de Éxito específicos, Indicadores Claves por Objetivo e Indicadores Clave de Desempeño y un Modelo de Madurez asociado al Gobierno de TI.

M.01.2. Orientación a objetivos de negocio:

El COBIT está alineado con los Objetivos del Negocio. Los Objetivos de Control muestran una relación clara y distintiva con los objetivos del negocio con el fin de apoyar su uso en forma significativa fuera de las fronteras de la comunidad de auditoría. Los Objetivos de Control están definidos con una orientación a los procesos, siguiendo el principio de reingeniería de negocios. En

dominios y procesos identificados, se identifica también un objetivo de control de alto nivel para documentar el enlace con los objetivos del negocio. Adicionalmente, se establecen consideraciones y guías para definir e implementar el Objetivo de Control de TI. El Marco de Referencia de COBIT consta de Objetivos de Control de TI de alto nivel y de una estructura general para su clasificación y presentación. La teoría subyacente para la clasificación seleccionada se refiere a que existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos.

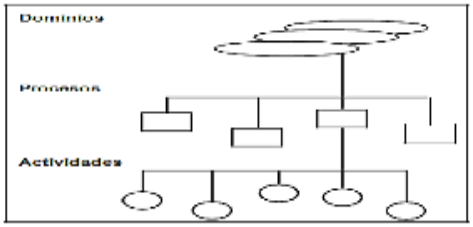

Ilustración 10: Niveles de Actividades de Tecnología de Información

Fuente: www.itgi.org

www.isaca.org

Por lo tanto, el Marco de Referencia conceptual puede ser enfocado desde tres puntos estratégicos: (1) Criterios de información, (2) recursos de TI y (3) procesos de TI. Estos tres puntos estratégicos son descritos en el Cubo COBIT que se muestra a continuación:

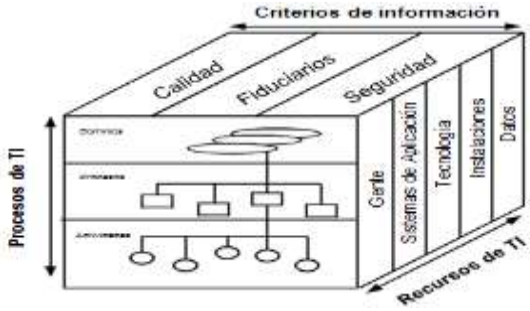

Ilustración 11: Niveles de Actividades de Tecnología de Información

Fuente: www.itgi.org

www.isaca.org

Con lo anterior como marco de referencia, los dominios son identificados utilizando las palabras que la gerencia utilizaría en las actividades cotidianas de la organización y no la jerga o terminología del auditor. Por lo tanto, cuatro

grandes dominios son identificados: planeación y organización, adquisición e implementación; entrega y soporte y monitoreo. Las definiciones para los dominios mencionados son las siguientes:

- **Planeación y organización**

  Este dominio cubre las estrategias y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas.

- **Adquisición e implementación**

  Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes, para asegurar que el ciclo de vida es continuo para esos sistemas

- **Entrega y soporte**

  En este dominio se hace referencia a la entrega o distribución de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por la seguridad en los sistemas y la continuidad de las operaciones así como aspectos sobre entrenamiento. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos el cual es ejecutado por los sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

- **Monitoreo**

  Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control

  El Gobierno de TI debe ser entrenado por la organización para asegurar que los recursos de TI serán administrados por una colección de procesos de TI agrupados naturalmente. El siguiente diagrama ilustra este concepto.

PROCESOS DE TI DE COBIT DEFINIDOS EN LOS CUATRO DOMINIOS

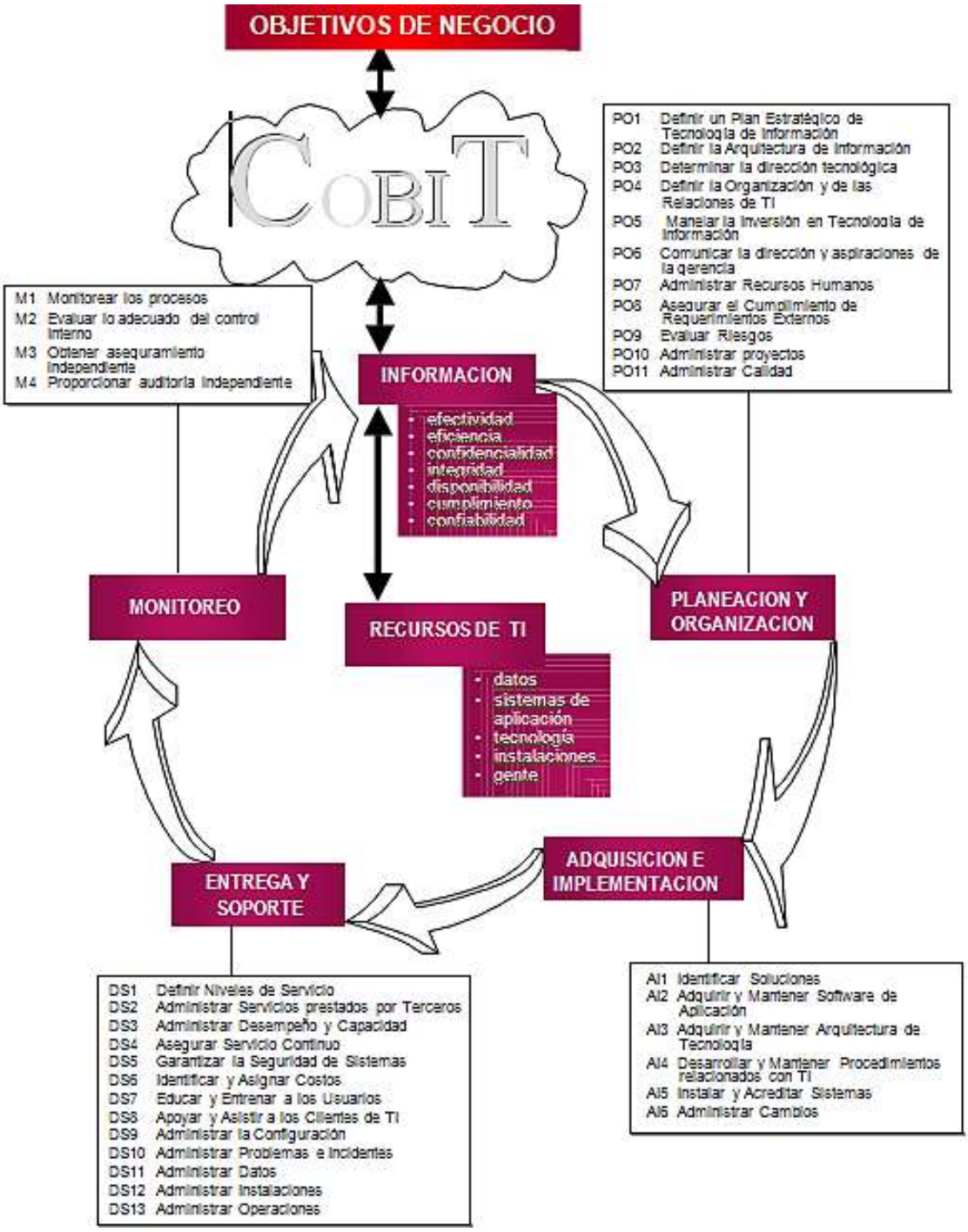

Ilustración 12: Procesos de Tecnología de Información COBIT – Definición en sus cuatro dominios

Fuente: www.itgi.org

www.isaca.org

M.01.3. Objetivos de control de la tabla resumen:

La siguiente tabla proporciona una indicación, por proceso y dominio de TI, de cuáles criterios de información son impactados por los objetivos de alto nivel, así como una indicación de cuáles recursos de TI son aplicables.

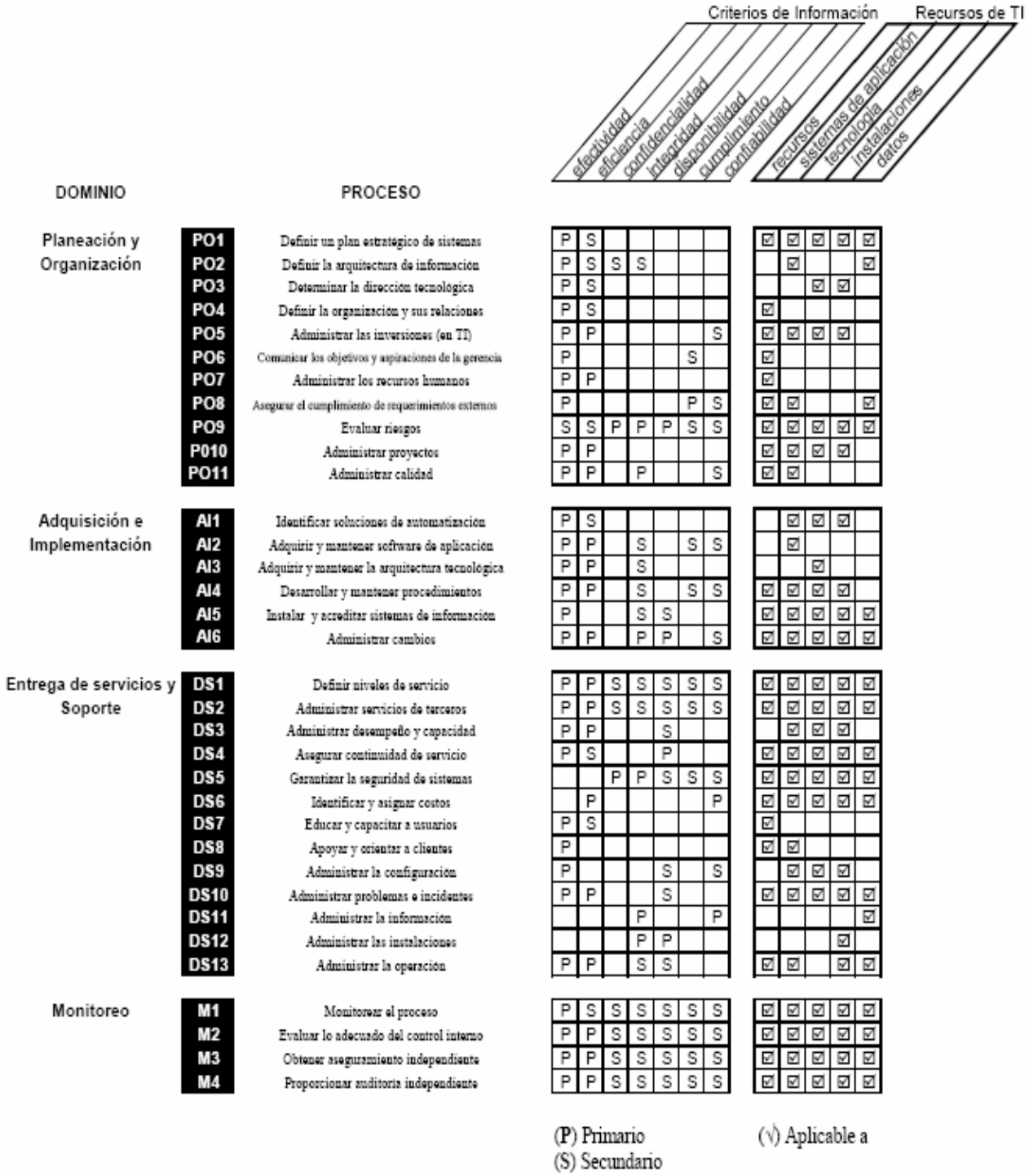

Ilustración 13: Objetivos de Control

Fuente: www.itgi.org

www.isaca.org

M.02. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - MAGERIT – versión 3

M.02.1. Introducción a Magerit

La razón de ser de Magerit está directamente relacionada con la generalización del uso de los medios electrónicos, informáticos y telemáticos, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en el uso de tales medios. Esta metodología interesa a todos aquellos que trabajan con información mecanizada y los sistemas informáticos que la tratan.

M.02.2. Objetivos de Magerit

Magerit persigue los siguientes objetivos:

Directos:

- Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.

Indirectos:

- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

M.02.3. Organización de las guías

Esta versión 3 de Magerit se ha estructurado en tres libros: éste, que describe “El Método”, un “Catálogo de Elementos” y una “Guía de Técnicas”. Esta guía describe la metodología desde tres ángulos:

- El capítulo 2 describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual.
- El capítulo 3 describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente pautar roles, actividades, hitos

y documentación para que la realización del proyecto de análisis y gestión de riesgos esté bajo control en todo momento.

- El capítulo 4 aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema.
- Como complemento, el capítulo 5 desgrana una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo para la realización de un análisis y una gestión realmente efectivos.
- Los apéndices recogen material de consulta: un glosario, referencias bibliográficas, referencias al marco legal, marco normativo de evaluación y certificación, las características que se requieren de las herramientas, presentes o futuras, para soportar el proceso de análisis y gestión de riesgos, una guía comparativa de cómo Magerit versión 1 ha evolucionado en esta versión 3, por último, se desarrolla un caso práctico como ejemplo

M.02.4. Evaluación, certificación, auditoria y acreditación

El análisis de riesgos es una piedra angular de los procesos de evaluación, certificación, auditoria y acreditación que formalizan la confianza que merece un sistema de información. Dado que no hay dos sistemas de información iguales, la evaluación de cada sistema concreto requiere amoldarse a los componentes que lo constituyen. En análisis de riesgos proporciona una visión singular de cómo es cada sistema, qué valor posee, a qué amenazas está expuesto y de qué salvaguardas se ha dotado. Es pues el análisis de riesgos, paso obligado para poder llevar a cabo todas las tareas mencionadas, que se relacionan según el siguiente esquema:

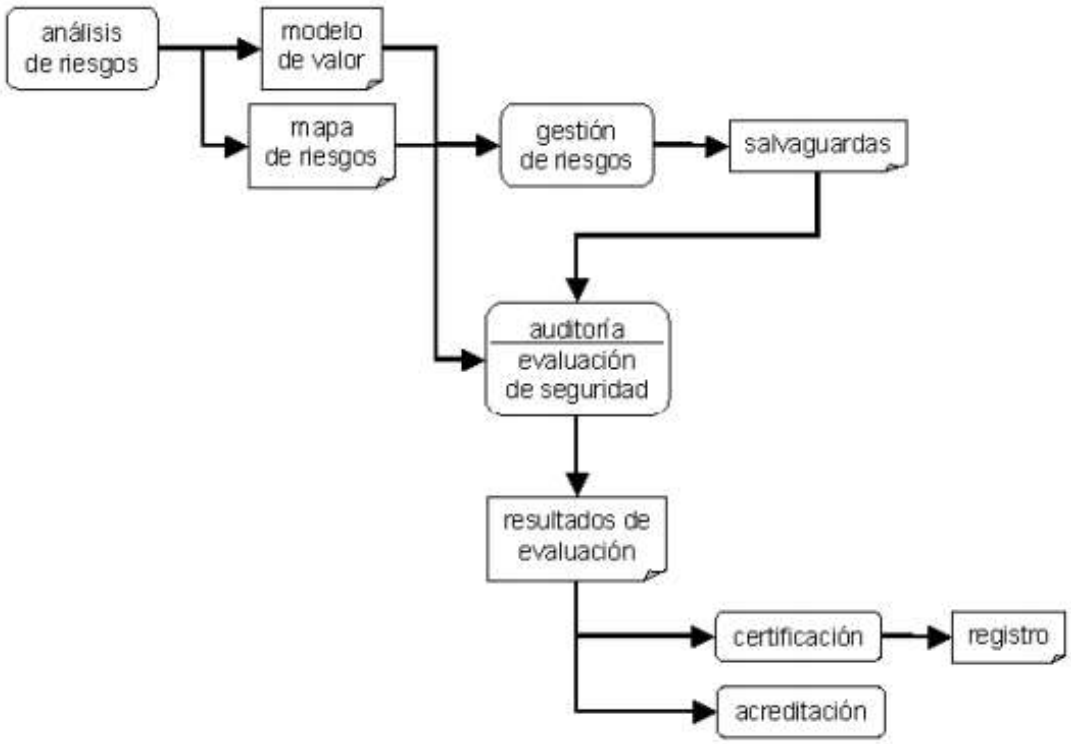

Ilustración 14: Marcos normativos relativos a sistemas de gestión y productos de seguridad

Fuente: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/index.html

M.02.5. Realización del análisis y de la gestión

Este capítulo expone de forma conceptual en qué consiste esto del análisis de riesgos y aquello de su gestión, qué se busca en cada momento y qué conclusiones se derivan. Hay dos grandes tareas a realizar:

I. Análisis de Riesgos, que permite determinar qué tiene la Organización y estimar lo que podría pasar.

- Elementos: Activos, amenazas, salvaguardas.
- Con estos elementos se puede estimar: el impacto, el riesgo

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento. La siguiente figura recoge este primer recorrido, cuyos pasos se detallan en las siguientes secciones:

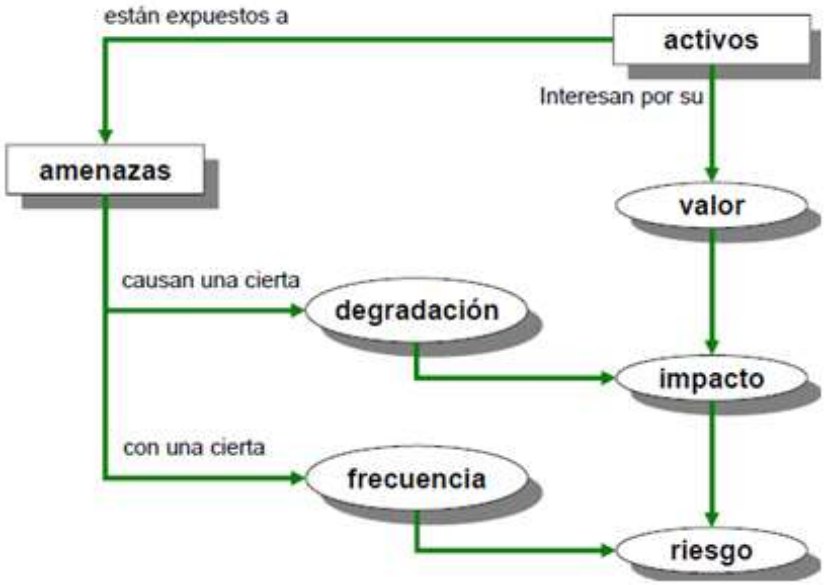

Ilustración 15: Pasos pautados para la realización de Análisis de Riesgo

Fuente: https://www.ccn-cert.cni.es/publico/herramientas/pilar5/magerit/index.html

II. Gestión de Riesgos, que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la dirección asume. Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

M.02.6. Estructuración del proyecto

Si en el capítulo anterior se ha marcado de forma conceptual cómo llevar a cabo un análisis y una gestión de riesgos, en este capítulo se plasman aquellos conceptos en componentes de un proyecto de análisis y gestión de riesgos. Los pasos se organizan en tres grandes procesos (preparación, análisis y gestión). Cada proceso se organiza en actividades que, finalmente, se estructuran en tareas a realizar. En cada tarea se indica lo que hay que hacer así como las posibles dificultades para conseguirlo y la forma de afrontarla con éxito.

Las tareas se detallan a continuación y hay que adaptarlas:

1. Horizontalmente al alcance que se requiere.
2. Verticalmente a la profundidad oportuna.

A. Participantes:

Durante el desarrollo del proyecto Análisis y Gestión de Riesgos (AGR), desde su inicio a su terminación, se identifican los siguientes órganos colegiados:

- Comité de Dirección
- Comité de Seguimiento
- Equipo de proyecto
- Grupos de Interlocutores

Además de dichos órganos colegiados, hay que identificar algunos roles singulares:

- Promotor
- Director del Proyecto
- Enlace operacional

B. Desarrollo del proyecto

En esta sección se ordenan y formalizan las acciones a realizar a lo largo de un proyecto AGR, estableciendo un marco normalizado de desarrollo. Este marco de trabajo define: El proyecto se divide en tres grandes procesos, desglosándose cada uno en una serie de actividades y estas, a su vez, en tareas con el grado de detalle oportuno. Un proyecto AGR conlleva tres procesos:

Proceso P1: Planificación
• Se establecen las consideraciones necesarias para arrancar el proyecto AGR. • Se investiga la oportunidad de realizarlo. • Se definen los objetivos que ha de cumplir y el dominio (ámbito) que abracará. • Se planifican los medios materiales y humanos para su realización. • Se procede al lanzamiento del proyecto.
Proceso P2: Análisis de Riesgos
• Se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen. • Se identifican las amenazas significativas sobre aquellos activos y se valoran en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado. • Se identifican las salvaguardas existentes y se valora la eficacia de su implementación. • Se estima el impacto y el riesgo al que están expuestos los activos del sistema. • Se interpreta el significado del impacto y el riesgo.
Proceso P3: Gestión de Riesgos
• Se elige una estrategia para mitigar impacto y riesgo.

- Se determinan las salvaguardas oportunas para el objetivo anterior.
- Se determina la calidad necesaria para dichas salvaguardas.
- Se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables.
- Se lleva a cabo el plan de seguridad.

Tabla 7: Procesos de un Proyecto AGR

Fuente: http://publicaciones.administracion.es

Estos tres procesos no son necesariamente secuenciales. El proceso P1 es claramente el iniciador del proyecto. El proceso P2 funciona como soporte del proceso P3 en el sentido de que la gestión de riesgos (P3) es una tarea continua soportada por las técnicas de análisis (P2). La gestión de riesgos supone siempre la alteración del conjunto de salvaguardas, bien porque aparecen nuevas salvaguardas, bien porque se reemplazan unas por otras, bien porque se mejoran las existentes. En definitiva, a lo largo del proceso P3 se recurrirá a tareas del proceso P2.

Ilustración 16: Procesos de un Proyecto AGR

Fuente: http://publicaciones.administracion.es

C. Visión global

Sin perjuicio de una exposición detallada más adelante, se relaciona a continuación el árbol completo de procesos, actividades y tareas que vertebran un proyecto AGR.

Procesos, Actividades y Tareas
Proceso P1: Planificación
Actividad A1.1: Estudio de oportunidad
Tarea T1.1.1: Determinar la oportunidad
Actividad A1.2: Determinación del alcance del proyecto
Tarea T1.2.1: Objetivos y restricciones generales
Tarea T1.2.2: Determinación del dominio y límites
Tarea T1.2.3: Identificación del entorno
Tarea T1.2.4: Estimación de dimensiones coste
Actividad A1.3: Planificación del proyecto
Tarea T1.3.1: Evaluar cargas y planificar entrevistas
Tarea T1.3.2: Organizar a los participantes
Tarea T1.3.3: Planificar el trabajo
Actividad A1.4: Lanzamiento del proyecto
Tarea T1.4.1: Adaptar los cuestionarios
Tarea T1.4.2: Criterios de evaluación
Tarea T1.4.3: Recursos necesarios
Tarea T1.4.4: Sensibilización
Proceso P2: Análisis de riesgos
Actividad A2.1: Caracterización de los activos
Tarea T2.1.1: Identificación de los activos
Tarea T2.1.2: Dependencias entre activos
Tarea T2.1.3: Valoración de los activos
Actividad A2.2: Caracterización de las amenazas
Tarea T2.2.1: Identificación de las amenazas
Tarea T2.2.2: Valoración de las amenazas
Actividad A2.3: Caracterización de las salvaguardas
Tarea T2.3.1: Identificación de las salvaguardas existentes
Tarea T2.3.2: Valoración de las salvaguardas existentes
Actividad A2.4: Caracterización de las salvaguardas
Tarea T2.4.1: Estimación del impacto
Tarea T2.4.2: Estimación del riesgo
Tarea T2.4.3: Interpretación de los resultados
Proceso P3: Gestión de riesgos
Actividad A3.1: Toma de decisiones
Tarea T3.1.1: Calificación de los riesgos
Actividad A3.2: Plan de seguridad
Tarea T3.2.1: Programas de seguridad
Tarea T3.2.2: Plan de ejecución
Actividad A3.3: Ejecución del plan
Tarea T3.3.*: Ejecución de cada programa de seguridad

Tabla 8: Visión Global de un Proyecto AGR

Fuente: http://publicaciones.administracion.es

M.02.7. Desarrollo de sistemas de información

Las aplicaciones (software) constituyen un tipo de activos frecuente y nuclear para el tratamiento de la información en general y para la prestación de servicios basados en aquella información. La presencia de aplicaciones en un sistema de información es siempre una fuente de riesgo en el sentido de que constituyen un punto donde se pueden materializar amenazas. A veces, además, las aplicaciones son parte de la solución en el sentido de que constituyen una salvaguarda frente a riesgos potenciales. En cualquier caso es necesario que el riesgo derivado de la presencia de aplicaciones esté bajo control.

El análisis de los riesgos constituye una pieza fundamental en el diseño y desarrollo de sistemas de información seguros. Es posible, e imperativo, incorporar durante la fase de desarrollo las funciones y mecanismos que refuerzan la seguridad del nuevo sistema y del propio proceso de desarrollo, asegurando su consistencia y seguridad, completando el plan de seguridad vigente en la Organización. Es un hecho reconocido que tomar en consideración la seguridad del sistema antes y durante su desarrollo es más efectivo y económico que tomarla en consideración a posteriori. La seguridad debe estar embebida en el sistema desde su primera concepción.

Se pueden identificar dos tipos de actividades diferenciadas:

- SSI: actividades relacionadas con la propia seguridad del sistema de información.
- SPD: actividades que velan por la seguridad del proceso de desarrollo del sistema de información.

Tras una primera exposición sobre el desarrollo de aplicaciones en general, la sección 4.5 profundiza en su aplicación a Métrica versión 3. Métrica ha sido desarrollada por el CSAE como la “Metodología de Planificación, Desarrollo y Mantenimiento de sistemas de información”.

A. Ciclo de vida de las aplicaciones:

Típicamente, una aplicación sigue un ciclo de vida a través de varias fases:

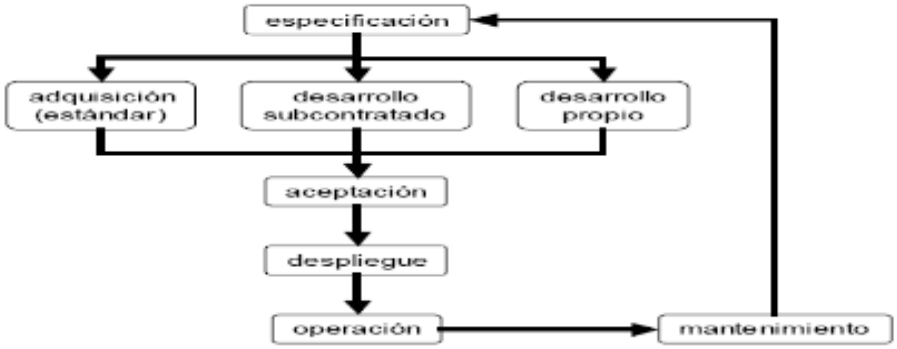

Ilustración 17: Ciclo de Vida de las Aplicaciones
Fuente: http://publicaciones.administracion.es

B. Análisis de riesgos:

El método permite identificar y valorar amenazas y salvaguardas, derivando información de impacto y riesgo sobre la propia aplicación y los activos relacionados con ella.

C. Gestión de riesgos:

El proceso P3 de gestión de riesgos recomienda salvaguardas y evalúa el efecto de las salvaguardas desplegadas sobre el impacto y el riesgo.

D.MÉTRICA versión 3:

La metodología MÉTRICA Versión 3 ofrece a las Organizaciones un instrumento útil para la sistematización de las actividades que dan soporte al ciclo de vida del software dentro del marco que desea alcanzar.

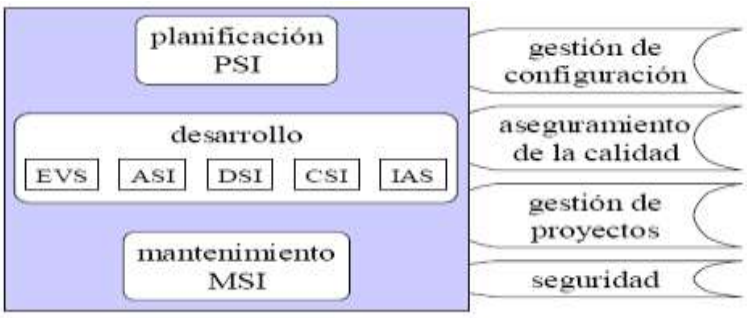

Ilustración 18: MÉTRICA versión 3 identifica 3 procesos, 5 subprocesos y 4 interfaces
Fuente: http://publicaciones.administracion.es

PSI – Planificación del sistema de información
EVS – Estudio de viabilidad del sistema
ASI – Análisis del sistema de información
DSI – Diseño del sistema de información.
CSI – Construcción del sistema de información
IAS – Implantación y aceptación del sistema
MSI – Mantenimiento del sistema de información

- 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.
- 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.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
    - Aplicar controles para el tratamiento el riesgo en función de la evaluación anterior. Utilizar para ello los controles del Anexo A de ISO 27001 (teniendo en cuenta que las exclusiones habrán de ser justificadas) y otros controles adicionales si se consideran necesarios.

- Aprobación por parte de la Dirección del riesgo residual y autorización de implantar el SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el que queda, aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).
- Confeccionar una Declaración de Aplicabilidad: la llamada SOA (Statement of Applicability) es una lista de todos los controles seleccionados y la razón de su selección, los controles actualmente implementados y la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

2.4.1.3. Do: Implementar y utilizar el SGSI

- 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.
- 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.
- Implementar los controles anteriormente seleccionados que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.

- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

2.4.1.4. Check: Monitorizar y revisar el SGSI

La organización deberá:

- 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.
- 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.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de seguridad.
- 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 -requerimientos legales, obligaciones contractuales, etc.-.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- 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.

- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

2.3.1.5. ACT (Actuar):

La organización deberá regularmente:

- Implantar en el SGSI las mejoras identificadas.
- Realizar acciones preventivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones para solucionar no conformidades detectadas.
- Realizar acciones correctivas adecuadas en relación a la cláusula 8 de ISO 27001 y a las lecciones aprendidas de las experiencias propias y de otras organizaciones para prevenir potenciales no conformidades.
- 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.
- Asegurarse de que las mejoras introducidas alcanzan los objetivos previstos a través de la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

PDCA es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de Plan para iniciar un nuevo ciclo de las cuatro fases. Téngase en cuenta que no tiene que haber una secuencia estricta de las fases, sino que, p. ej., puede haber actividades de implantación que ya se lleven a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

2.5. Tipo de Investigación

El proyecto propuesto está referido a una investigación descriptiva y aplicada.

- De acuerdo al fin que persigue:
    - Descriptiva; porque se intenta determinar los problemas actuales, mediante una descripción y comprender de forma íntegra el presente.
- De acuerdo a la técnica de contrastación:
    - Aplicada; porque se busca la aplicación o utilización de los conocimientos adquiridos durante el desarrollo del proyecto.

CAPITULO III: LA ENCUESTA Y ANALISIS DE RESULTADOS

3.1 ANALISIS E INTERPRETACION DE RESULTADOS

Cuadro Nº 01

¿En la entidad donde labora tienen políticas de seguridad de la información?

Opción	Frecuencia
Si	**9**
No	**1**

Gráfico 1: ¿En la entidad donde labora tienen políticas de seguridad de la información?

Análisis Interpretativo

El 90% de los encuestados respondió que la entidad cuenta con políticas de seguridad de la información, un 10% opina lo contrario.

Cuadro Nº 02

¿Si en la Pregunta 1 respondió si, se cumplen o se llevan a la práctica estas políticas?

Se cumplen las políticas de Seguridad	Frecuencia	%
A cabalidad	3	33
Medianamente	6	67
No se cumple	0	0
Total	**9**	**100**

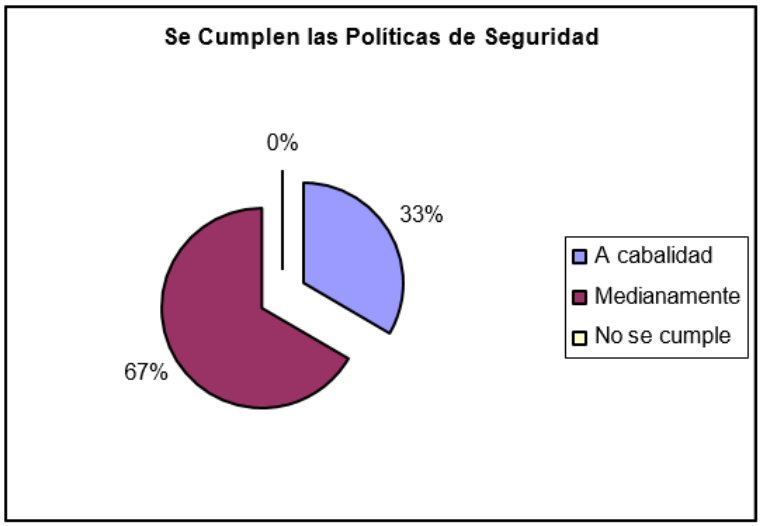

Gráfico 2: ¿Si en la Pregunta 1 respondió si, se cumplen o se llevan a la práctica estas políticas?

Análisis Interpretativo

Del total de personas que respondió que en la entidad tienen políticas de seguridad, un 33% opina que si se cumplen a cabalidad y que un 67% lo hace medianamente, es decir no siempre se toma en cuenta estas políticas como mejores prácticas de seguridad. Por los resultados obtenidos, podemos concluir que la MPCH no cuenta con un área que desarrolle políticas de seguridad de la información y muchos que respondieron que sí lo hicieron para dar la apariencia de cumplir con estos requisitos.

Cuadro Nº 03

¿Elija que beneficios se presentan cuando la MPCH cuenta con Políticas de Seguridad la información? Marcar una o más opciones.

Opciones	Frecuencia	%
Mayor seguridad en los medios de almacenamiento de información	8	50
Aumenta la productividad a través de consultas confiables	4	25
Calidad en el servicio para los trabajadores y terceros	4	25
Otros	0	0
Total	**16**	**100**

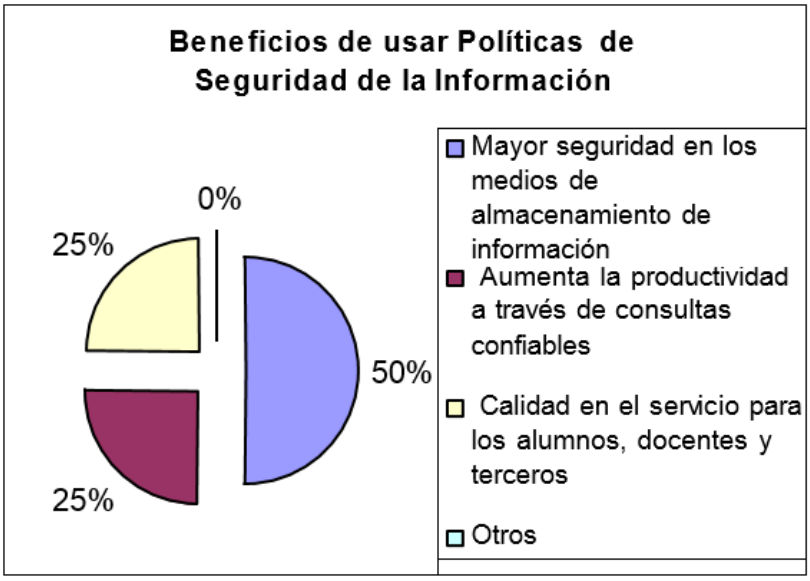

Gráfico 3: ¿Elija que beneficios se presentan cuando la MPCH cuenta con Políticas de Seguridad la información? Marcar una o más opciones.

Análisis Interpretativo

Del total de respuestas marcadas el 50% considera que la mayor seguridad de los medios de almacenamiento de información es uno de los beneficios de usar políticas de seguridad de la información, un 25% apuesta por la calidad en el servicio a los trabajadores y el otro 25% consideran que aumenta la productividad a través de consultas confiables.

Cuadro Nº 04

¿Cuáles de estas medidas son las más prioritarias en la Gestión de seguridad de la información? Marcar una o más opciones.

Medidas en la Gestión de seguridad de la información	Frecuencia	%
Desarrollo de políticas de seguridad	10	37
Clasificación del acceso de la información	4	15
Capacitación de usuarios	4	15
Monitoreo y reportes de la actividades en la red	4	15
La continuidad del negocio después de incidentes	5	18
Otros	0	0
Total	**27**	**100**

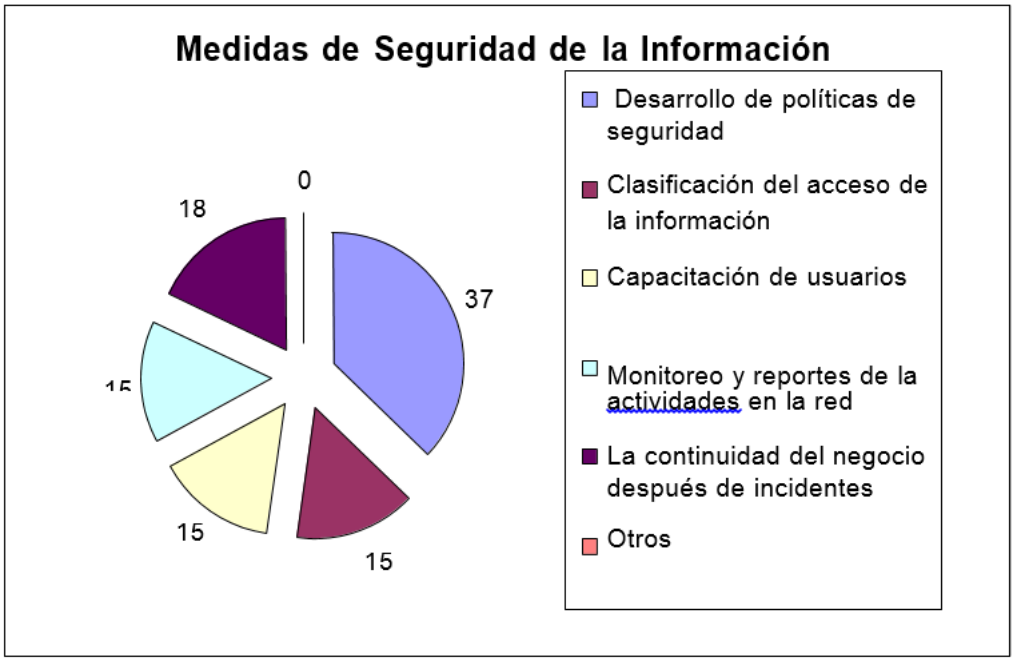

Gráfico 4:¿Cuáles de estas medidas son las más prioritarias en la Gestión de seguridad de la información? Marcar una o más opciones.

Análisis Interpretativo

Sobre qué medidas de seguridad de la información son las más prioritarias, un 37% considera el desarrollo de políticas de seguridad, un 18% opina que la continuidad del negocio es muy importante y en un 15% consideran a la capacitación de usuarios, clasificación y acceso a la información y monitoreo de las actividades de la red informática de la MPCH.

Cuadro Nº 05

¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico? Marcar una o más opciones.

Errores más comunes cuando se usa Internet y el correo electrónico	Frecuencia	%
Omitir la seguridad como un aspecto fundamental de configuración del Servidor	4	25
Transmisión en pleno texto de contraseñas	4	25
Uso inadecuado de herramientas de seguridad, o no uso alguno	3	19
Obtener y mantener programas y aplicaciones (software) que son vulnerables	5	31
Otros	0	0
Total	**16**	**100**

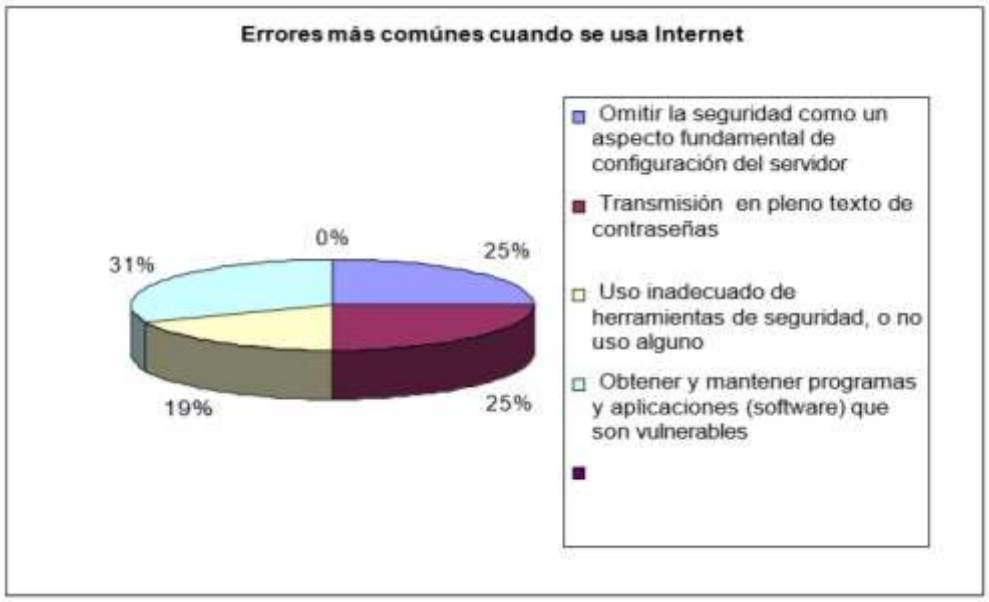

Gráfico 5: ¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico? Marcar una o más opciones.

Análisis Interpretativo

Podemos apreciar que todos los errores mencionados son muy comunes cuando se usa Internet, pero sobresale con un 31% el obtener y mantener programas que son vulnerables. Le siguen como errores más frecuentes el omitir la seguridad al momento de configurar el servidor y la transmisión en pleno texto de contraseñas con un 25% y finalmente otro error común es el uso inadecuado de herramientas de seguridad.

Cuadro Nº 06

¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?

MF = Muy Frecuentes RF = Regularmente frecuentes PF = Poco frecuentes

Riesgos	MF	%	RF	%	PF	%
Fenómenos Naturales (Terremotos, Inundaciones)	0	0	0	0	10	38
Fallas mecánicas (Cortes de fluido eléctrico, incendios)	1	11	5	20	4	15
Divulgación ilícita de la información por el personal	0	0	7	28	3	12
Destrucción o modificación de la información	1	11	2	8	7	27
Intrusos al sistema de la red	2	22	6	24	2	8
Virus informáticos, gusanos, spam	5	56	5	20	0	0
Otros (Especifique)	0	0	0	0	0	0
Total	**9**	**100**	**25**	**100**	**26**	**100**

Gráfico 6: ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información?

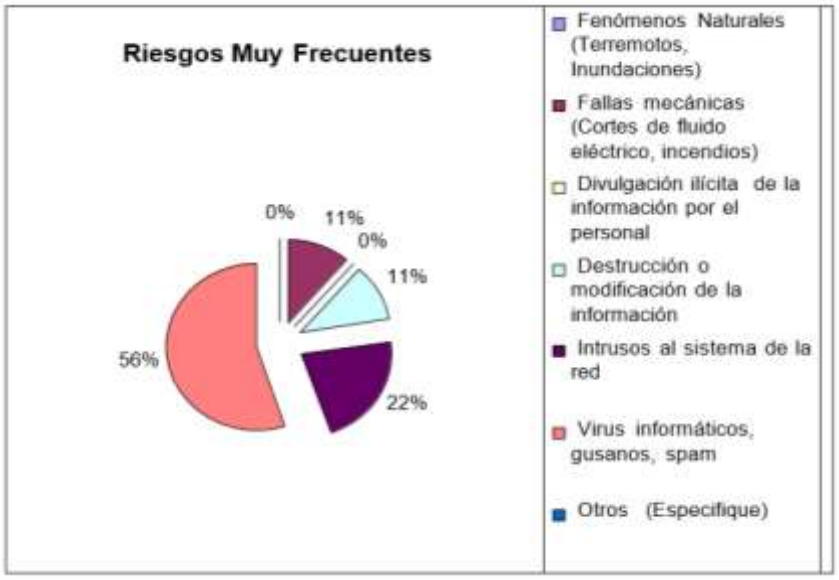

Grafico 6. 1: Riesgos Muy Frecuentes

Análisis Interpretativo

Según el gráfico, los riesgos más frecuentes que se presentan en la MPCH son “los virus informáticos, gusanos y spam” con un 56%, en segundo lugar están “los intrusos al sistema de la red” con un 22% y el tercer lugar lo comparten “las fallas mecánicas” como los cortes de fluido eléctrico y “la destrucción y/o modificación de la información” con un 11%.

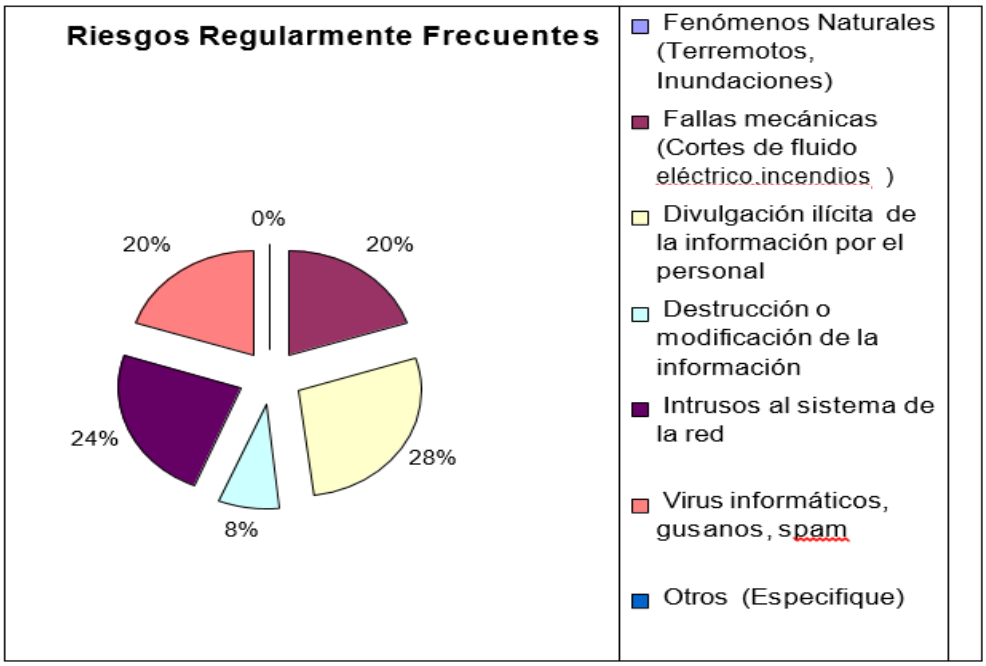

Grafico 6. 2: Riesgos Regularmente Frecuentes

Análisis Interpretativo

Los riesgos regularmente frecuentes se presentan en su mayoría por: divulgación ilícita de la información (28%), por los intrusos al sistema de la red (24%), por los cortes de fluido eléctrico (20%), por los virus informáticos (20%) y una minoría considera como riesgo regularmente frecuente la destrucción o modificación de la información por parte del personal (8%).

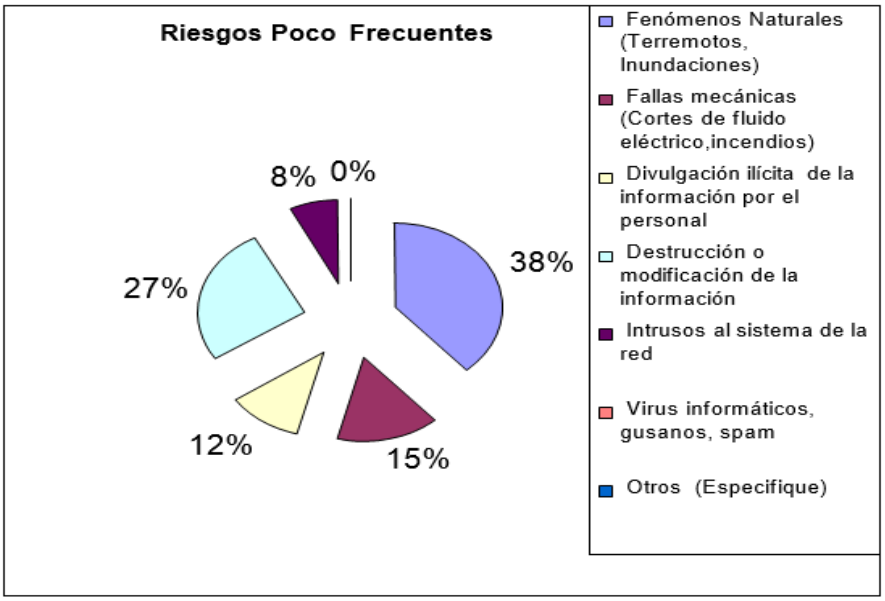

Grafico 6. 3: Riesgos Poco Frecuentes

Análisis Interpretativo

Los riesgos poco frecuentes se presentan ocasionalmente por fenómenos naturales como terremotos o inundaciones (38%), por la destrucción de la información por parte del personal (27%) y en algunos casos por los cortes de fluido eléctrico (15%).

Cuadro Nº 07

¿Sus equipos de cómputo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?

Protección de equipos cómputo	Frecuencia	%
Si	6	60
No	4	40
Total	**10**	**100**

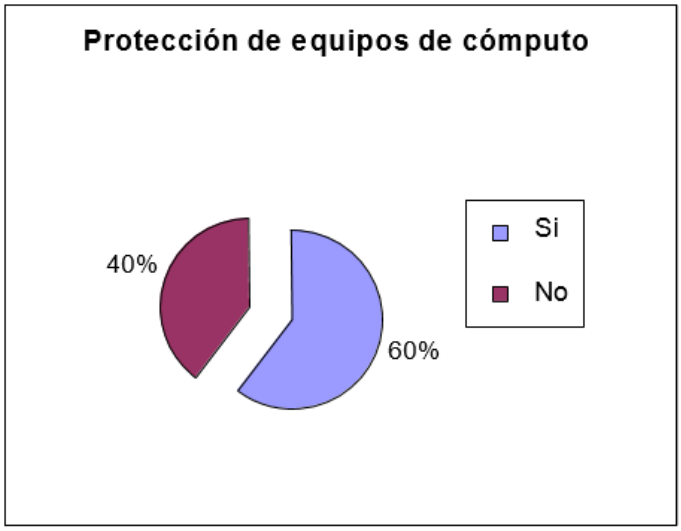

Gráfico 7: ¿Sus equipos de cómputo en su oficina tienen fuente de poder ininterrumpible (UPS), baterías o generador de energía ante cortes de fluido eléctrico?

Análisis Interpretativo

Según el gráfico del total de encuestados un 60% cuenta con equipos en sus oficinas para protegerse ante cortes de energía eléctrica y hay un considerable 40% que no tienen estos equipos de protección.

Cuadro Nº 08

¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

Incidencias que se dan con más frecuencia	Frecuencia	%
Saturación de la red por programas indebidos (música,	5	29
Uso del correo electrónico de la MPCH para otros fines	6	35
Olvido de contraseña	2	12
No realizar copias de respaldo	3	18
Otros: No organizar la información para mayor seguridad	1	6
Total	**17**	**100**

Gráfico 8: ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

Análisis Interpretativo

Del total de respuestas recogidas las incidencias más frecuentes son: el uso del correo electrónico de la MPCH para fines personales con 35% , la saturación de la red e Internet por programas indebidos (29%); y menos frecuentes pero que tampoco dejan de ser preocupantes son: los usuarios que no realizan copias de seguridad (18%) y el olvido de sus contraseñas (12%) y en la opción otros un 6% de respuestas coincidieron que existen usuarios que no organizan sus archivos, lo que genera también problemas de seguridad.

Cuadro Nº 09

¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

Ultima vez que participó a eventos	Frecuencia	%
Aproximadamente 3 meses	1	10
Aproximadamente 6 meses	3	30
Aproximadamente 1 año	4	40
Nunca	2	20
Total	**10**	**100**

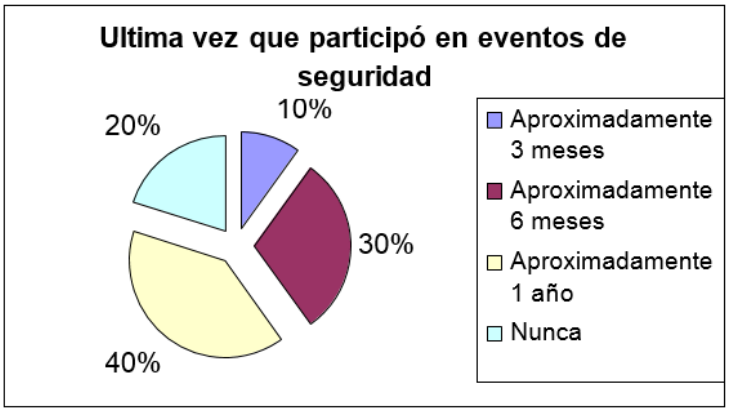

Gráfico 9: ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

Análisis Interpretativo

El 20% del personal de TIC de la MPCH nunca ha asistido a eventos o talleres de seguridad de la información pero también hay personas que consciente del problema de seguridad han asistido de alguna manera a talleres o seminarios de seguridad de información, así un 40% ha asistido aproximadamente hace 1 año, un 30% ha participado aproximadamente hace 6 meses y un 10% ha asistido aproximadamente hace 3 meses.

Cuadro Nº 10

¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

Disposición a talleres de Capacitación	Frecuencia	%
Muy interesado	8	80
Poco interesado	2	20
Nada interesado	0	0
Total	**10**	**100**

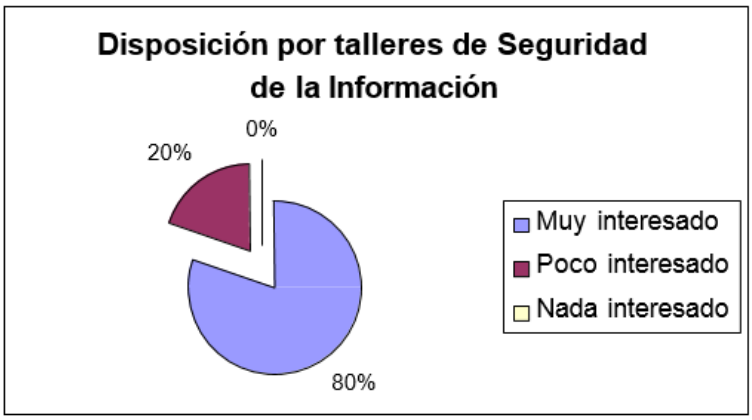

Gráfico 10: ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

Análisis Interpretativo

Del personal encuestado un 80% está muy interesado si se realizan programas y talleres de capacitación de seguridad de la información, existe un 20% que está poco interesado debido a que no consideran a la seguridad como una prioridad dentro de la MPCH. Lo positivo es que no hay ningún personal que esté ajeno a la capacitación de seguridad.

Cuadro Nº 11

¿Considera que la red informática de la MPCH fue diseñada sin pensar originalmente en la seguridad? ¿Por qué?

	Frecuencia	%
Si	7	70
No	3	30
Total	**100**	**100**

	Razones
Si	• No había Internet y por ende no había riesgos a la información • La MPCH como institución pública no debe tener restricciones en el acceso a la información
No	• Se diseñó pensando en la seguridad de acuerdo a la tecnología de ese tiempo

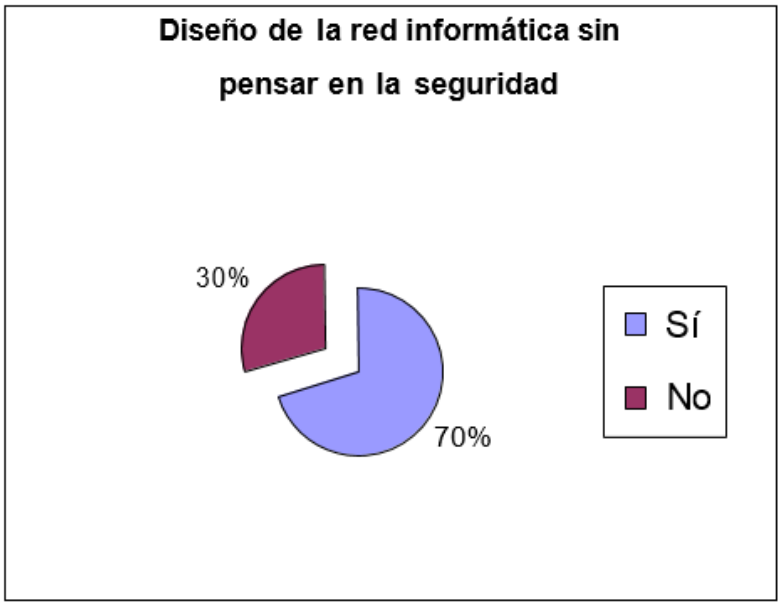

Gráfico 11: ¿Considera que la red informática de la MPCH fue diseñada sin pensar originalmente en la seguridad. Porqué?

Análisis Interpretativo

Sobre si la red informática de la MPCH fue diseñada sin pensar originalmente en la seguridad un 70% considera que sí, y las razones se han consolidado en el cuadro anterior. Por otra parte un 30% opina lo contrario.

Cuadro Nº 12

¿Cómo considera la gestión de seguridad de la información en la gestión administrativa de la MPCH sobre los sistemas de información como son: admisión y registros, tesorería y trámite documentario?

Gestión de la Seguridad en la Gestión Administrativa	Frecuencia	%
Buena	9	90
Regular	1	10
Mala	0	0
Total	**10**	**100**

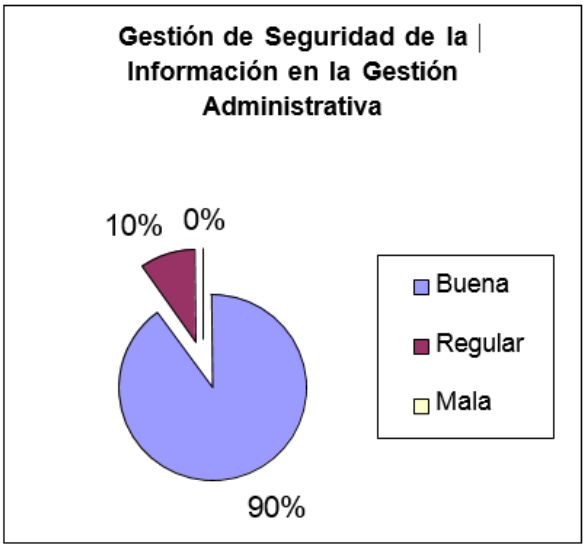

Gráfico 12: ¿Cómo considera la gestión de seguridad de la información en la gestión administrativa de la MPCH sobre los sistemas de información como son: admisión y registros, tesorería y trámite documentario?

Análisis Interpretativo

Del total del personal de TIC un 90% considera que la gestión de seguridad de la información en la gestión administrativa es buena, sólo un 10% opina que la gestión es regular pues han sido partícipes de diferentes problemas de seguridad y nadie considera que la gestión es mala.

Cuadro Nº 13

¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la MPCH?

Impacto económico	Frecuencia	%
Muy beneficioso	6	60
Poco beneficioso	0	0
Nada beneficioso	4	40
Total	**10**	**100**

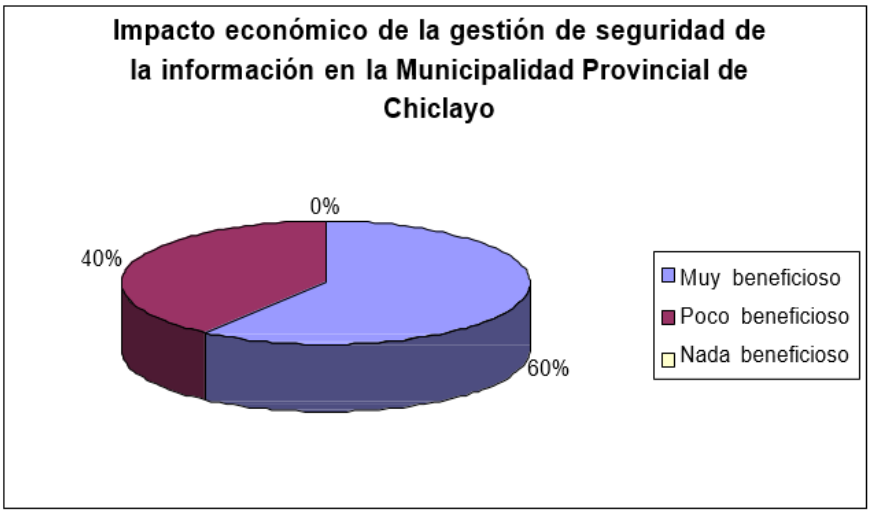

Gráfico 13: ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la MPCH?

Análisis Interpretativo

Con respecto al impacto económico de implementar un plan de gestión de seguridad de la información en la gestión integral de la MPCH las apreciaciones se encuentran divididas pues si bien hay un 60% que lo considera muy beneficioso existe un 40% que piensa que es poco beneficioso. Por otro lado no hay ningún personal que opina que el impacto económico no es beneficioso.

3.2 PRUEBA DE HIPOTESIS

Hipótesis Auxiliar Nº 1

Al implementar políticas de seguridad de la información, se minimizan los riesgos en el manejo de la información como divulgación ilícita, destrucción, sabotaje, fraude, violación de la privacidad, intrusos, interrupción de servicios.

Entidad	Estrategia de Gestión de seguridad de la información	Riesgos muy frecuentes		
	Desarrollo de políticas de seguridad (%)	Divulgación Ilícita de Información (%)	Intrusos en la red (%)	Virus infor-máticos (%)
MPCH	37	0	22	56

Tabla 9: Hipótesis Auxiliar Nº 1

Fuente: Elaboración propia

Análisis

En la MPCH el desarrollo de políticas de seguridad (37%) y el cumplimiento de las normativas y procedimientos va reducir el número de programa infectados con virus informáticos pues alcanza un 56%.

Este análisis permite comprobar que al implementar políticas de seguridad de la información se minimizarán los riesgos de la información como son la divulgación ilícita de la información por parte de los trabajadores y la presencia de los virus informáticos que son muy frecuentes en la MPCH, según las personas encuestadas.

Por otra parte, los resultados que se obtuvo de la Primera Encuesta Nacional de Seguridad de la Información-2004 de la Presidencia del Consejo de Ministros – ONGEI también han servido para validar esta hipótesis.

Sobre los tipos de incidentes o riesgos más frecuentes que ha tenido las instituciones se obtuvieron los siguientes resultados:

- El 86% de las instituciones ha tenido incidentes de virus informático.
- El 19% de las instituciones ha tenido incidentes de Acceso no autorizado por personal interno

- EL 10% de las instituciones ha tenido incidentes de Robo de información confidencial.

Hipótesis Auxiliar Nº 2

El rediseño la red informática permite un tráfico de la información más seguro y un servicio eficaz a los trabajadores y terceros.

Entidad	Se diseñó la red informática sin pensar en la seguridad (%)
MPCH	70

Tabla 10: Hipótesis Auxiliar Nº 2

Fuente: Elaboración propia

Análisis

Los expertos consultados de las TICS estuvieron de acuerdo que la red informática municipal fue diseñada sin pensar originalmente en la seguridad. Las razones fueron las siguientes: Antes no había Internet por tanto no había riesgos, no se previó el crecimiento exponencial de la tecnología y comunicaciones y todavía existe la idea de que la MPCH como entidad de administración pública no debe tener restricciones. El rediseño de la red informática permite segmentar las áreas de tal forma que por ejemplo los trabajadores y/o terceros con conocimientos de tecnología no puedan accesar a información confidencial de la institución. Asimismo, va permitir un tráfico más seguro y una mejor calidad en el servicio a los trabajadores y terceros.

Comprobamos esta hipótesis con la encuesta nacional de la ONGEI donde se obtuvieron los siguientes resultados:

- El 82% de las instituciones planea usar Firewalls
- El 71% de las instituciones planea usar Sistemas de detección de intrusos
- El 58% de las instituciones planea usar Redes Privadas Virtuales

Hipótesis Auxiliar Nº 3

La gestión de seguridad de la información contribuye a la calidad en el servicio y en la protección de los sistemas de información como son admisión y registros, cobranzas y trámites documentarios en la Municipalidad Provincial de Chiclayo

Entidad	Beneficios de la gestión de la seguridad de la información			Impacto en la gestión administrativa		
	Mejor protección de la información (%)	Calidad en el servicio a los trabajadores	Aumenta la productividad a través de consultas directas y confiables (%)	Muy buena (%)	Regular (%)	Mala (%)
MPCH	50	25	25	90	10	0

Tabla 11: Hipótesis Auxiliar Nº 3

Fuente: Elaboración propia

Análisis

En la MPCH al igual que las otras instituciones públicas, la mejor protección de la información es uno de los beneficios más importantes (50%) seguido de la calidad en el servicio a los terceros (25%) esto da como consecuencia un impacto positivo a la gestión administrativa con los sistemas de información.

Este análisis permite comprobar que con la gestión de seguridad de la información se obtienen beneficios como una mejor protección de los recursos de información (sistemas de información, redes, etc), una mejor calidad en el servicio a los trabajadores y va tener un impacto muy positivo cuando hagan uso de los servicios municipales reflejados en los sistemas de información que brinda la Municipalidad Provincial de Chiclayo.

Comprobamos esta hipótesis con la encuesta nacional de la ONGEI donde se obtuvieron los siguientes resultados:

- En el 78% de las instituciones los sistemas informáticos críticos si están aislados de personal no autorizado.
- El 54% de las instituciones si tienen mecanismos de monitoreo del uso de los Sistemas informáticos.
- El 65% de las instituciones si tienen políticas y mecanismos de protección de datos y privacidad de la información del personal de la institución.

Hipótesis Auxiliar Nº 4

Los programas y talleres de capacitación de seguridad de la información crean conciencia de seguridad en los trabajadores y terceros para un buen uso de la información.

Entidad	Incidencias de seguridad de los usuarios			Asistencia a talleres de capacitación	Interés en capacitación de seguridad
	Saturación de la red (%)	No hacer copias de seguridad (%)	Divulgación de la Informa-ción (%)	Nunca (%)	Muy interesado (%)
MPCH	29	18	6	20	80

Tabla 12: Hipótesis Auxiliar Nº 4

Fuente: Elaboración propia

Análisis

Podemos apreciar en el cuadro, que las incidencias de seguridad por parte de los usuarios de la Municipalidad Provincial de Chiclayo que resalta la saturación de la red por programa indebidos con un 29%. En cuanto a la asistencia de eventos seguridad de la información para la capacitación, están muy interesados y demuestran un interés el 80%.

Este análisis nos permite comprobar que los programas de capacitación, talleres, eventos y lecturas con respecto a la seguridad de la información va crear conciencia en los trabajadores y terceros para que se sientan identificados con la información que manejan y se reduzca el número de incidencias de seguridad como saturación de la red por programas indebidos (música, video, etc.), divulgación de la información, etc.

Comprobamos esta hipótesis con la encuesta nacional de la ONGEI donde se obtuvieron los siguientes resultados:

- En el 80% de las instituciones, los usuarios no reciben capacitación en temas de seguridad de la información
- El 85% de las instituciones no tienen asesoramiento especializado en materia de seguridad de la información
- En el 68% de las Instituciones, los usuarios no están preparados para reportar los incidentes de la seguridad de los Sistemas de información.

CAPITULO IV: PROPUESTA DE UN SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION (SGSI) PARA LA MUNICIPALIDAD PROVINCIAL DE CHICLAYO

4.1 SITUACION ACTUAL

Efectuado el diagnóstico se observa que la Municipalidad Provincial de Chiclayo carece en general de una metodología, guía o marco de trabajo que ayude a la identificación de riesgos y vulnerabilidades. A continuación se mencionas los siguientes aspectos críticos:

• Políticas de seguridad. Dentro de los diferentes aspectos a considerar en la gestión de seguridad de la información que brinda la Municipalidad Provincial de Chiclayo se ha podido observar que en su mayoría los trabajadores no saben si tienen políticas de seguridad de la información, y si tienen conocimiento de las mismas no las cumplen en la práctica. Muchas veces no cumplen con las políticas de seguridad porque simplemente desconocen de estas buenas prácticas de seguridad y no toman conciencia del rol que cumplen cuando manejan información confidencial.

Entidad	Tienen políticas		Se cumplen las políticas de Seguridad de la Información		
	Si (%)	No (%)	A cabalidad (%)	Mediana mente (%)	No se cumple (%)
MPCH	90	10	33	67	0

Tabla 13: Sit Políticas de seguridad

Fuente: Elaboración propia

• Protección de los equipos de cómputo. No todas las áreas de la Municipalidad Provincial de Chiclayo están preparadas para mantener el correcto funcionamiento del suministro eléctrico pues en sus áreas no cuentan con un sistema de alimentación ininterrumpida de energía (UPS) o generadores de energía según la tabla Nº 14. Es importante un sistema de UPS para apoyar un cierre ordenado o el funcionamiento de los equipos que soporten operaciones críticas dentro de las actividades de la institución.

Entidad	Protección a los equipos de cómputo	
	Si (%)	No (%)
MPCH	60	40

Tabla 14: Protección de los equipos de cómputo

Fuente: Elaboración propia

• Capacitación. La mayoría del personal de TIC de la Municipalidad Provincial de Chiclayo no está capacitado en temas actuales de seguridad de la información y lo más preocupante es que nunca han asistido a eventos o talleres de seguridad como se puede apreciar en la tabla Nº 15. En muchas áreas de la MPCH no existe una cultura de seguridad debidamente arraigada en todos los niveles incluyendo los directivos, quiénes no toman conciencia que la capacitación en seguridad de la información debe estar alineada con las estrategias de la institución.

Entidad	Asistencia a eventos de seguridad de la información		
	Hace 6 Meses (%)	Hace 1 año (%)	Nunca (%)
MPCH	40	40	20

Tabla 15: Capacitación

Fuente: Elaboración propia

• Incidencias de seguridad. La tabla Nº 16 nos muestra las incidencias de seguridad por los usuarios que manejan la información, y que ocurren muchas veces por descuido, desconocimientos técnicos o porque simplemente no cumplen con las normas internas de seguridad de la institución. Los incidentes de seguridad más devastadores tienden a ser más internos que externos. La gestión de la seguridad de la información necesita como mínimo la participación de todos los empleados de la MPCH.

Entidad	Incidencias de seguridad que ocasionan los usuarios			
	Olvido de Contraseñas (%)	Saturación de la red por programas prohibidos (%)	No hacer copias de seguridad (%)	Divulgación de la Información (%)
MPCH	12	29	18	6

Tabla 16: Incidencias de seguridad

Fuente: Elaboración propia

• Riesgos más frecuentes. También hemos observado que la Municipalidad Provincial de Chiclayo carece en general de una metodología, que ayude a la identificación de riesgos y vulnerabilidades y cuenten con mecanismos de control para mitigar los mismos. La tabla Nº 17 presenta los riesgos más frecuentes que se presentan en la MPCH:

Entidad	Riesgos más frecuentes				
	Cortes de energía eléctrica (%)	Destrucción o modificación de la información (%)	Divulgación Ilícita de Información (%)	Intrusos en la red (%)	Virus infor-máticos (%)
MPCH	11	11	0	22	56

Tabla 17: Riesgos más frecuentes

Fuente: Elaboración propia

• Red informática. La Municipalidad Provincial de Chiclayo corre mayor riesgo que la mayoría de las grandes corporaciones porque utilizan redes informáticas abiertas, comunicativas y descentralizadas, generalmente con diversos niveles de seguridad. La consulta a expertos de TIC sobre: ¿La red informática fue diseñada pensando originalmente en la seguridad? ¿Por qué?. Las razones se describen en la tabla Nº 18.

	Razones
Si	• No había Internet y por tanto no había riesgos de seguridad de la información • No se previó el vasto y rápido desarrollo tecnológico y de comunicaciones • La MPCH como institución pública no debe tener restricciones de acceso a los recursos de la información
No	• Se diseñó pensando en la seguridad de acuerdo a la tecnología de ese tiempo

Tabla 18: Red informática

Fuente: Elaboración propia

4.2 OBJETIVOS

- Lograr el compromiso de la Dirección con la Seguridad de la Información
- Asignar roles y responsabilidades a personal de la Institución para la Seguridad de la Información
- Determinar los requerimientos de seguridad y evaluar los riesgos y la administración de los mismos.
- Establecer la necesidad de educar e informar a toda la comunidad municipal sobre materias de seguridad de la información.
- Controlar y prevenir los accesos no autorizados de la información.
- Garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información.

4.3 EVALUACION DE RIESGOS Y VULNERABILIDADES Y ESTRATEGIAS DE SEGURIDAD

En este cuadro se muestran los riesgos y vulnerabilidades identificadas y las estrategias o medidas de seguridad necesarias para mitigar dichos riesgos.

Riesgos / Vulnerabilidades	Estrategias o medidas de seguridad a Aplicar
• Interés en obtener información estratégica de la MPCH por parte de otras instituciones. • Personal que trabaja la MPCH que se puede prestar para estas actividades desleales.	• Estándares de seguridad para servidores con sistemas operativos Windows y Linux. • Restricciones en el manejo de la información enviada por correo electrónico hacia redes externas. • Revisiones periódicas de los registros de los sistemas y operaciones realizadas por los usuarios
Pérdida de información ocasionada por la infección de virus informático.	• Adecuada arquitectura e implementación del sistema antivirus • Verificación periódica de la actualización del antivirus de computadoras personales y servidores. • Generación periódica de reporte de virus detectados.
Ausencia o exceso de contraseñas manejadas por los usuarios	• Uniformizar dentro de lo posible la estructura de las contraseñas empleadas y sus fechas de renovación • Implementar un sistema de Servicio de Directorio, el cual permita al usuario identificarse en él, y mediante un proceso automático, éste lo identifique en los sistemas en los cuales posee acceso.

Falta de conciencia en seguridad de la información por parte del personal de la MPCH.	• Programa de capacitación de la MPCH en temas relacionados a la seguridad de la información.
Arquitectura de red inapropiada para controlar accesos desde redes externas. Posibilidad de acceso no autorizado a sistemas por parte de personal externo a la MPCH.	• Diseño de arquitectura de seguridad de red. • Adecuada configuración de elementos de control de conexiones (Firewalls) • Implementación y administración de herramientas de seguridad
No existen controles con respecto a las copias de seguridad. Se realizan copias de seguridad pero muchas veces no se ha probado que se puede recuperar la información .	• Establecimiento de un procedimiento formal que contemple la generación de una copia de respaldo para los usuarios.. • Asegurar que la información del usuario se almacene en el servidor y estén protegidas por una contraseña. • Enviar fuera de la oficina una copia de seguridad completa una vez por semana.
No existe un control de protección sobre los correos electrónicos no solicitados por los usuarios	• Implementación y administración de herramientas para la inspección del contenido de los correos electrónicos recibidos
Acceso abierto a redes inalámbricas por parte de intrusos	• Separación del segmento de red Inalámbrico mediante un firewall. • Configuración la red inalámbrica para permitir el tráfico sólo de los equipos de escritorio y portátiles de la oficina.

4.4 POLITICAS DE SEGURIDAD DE LA INFORMACION

Se elaborarán las políticas de seguridad con el propósito de proteger la información de la MPCH, éstas servirán de guía para la implementación de un plan de seguridad que contribuirá a mejorar la disponibilidad, la integridad y la confiabilidad de la información dentro de los sistemas de aplicación, redes, instalaciones de cómputo y procedimientos manuales de la MPCH.

Alcance

Estas políticas están dirigidas a los empleados incluyendo el personal externo que presta servicios a la MPCH y que usa tecnología de información. Estas políticas aplican a los equipos propios o arrendados que tiene la MPCH y a los equipos propiedad de personas que sean conectados a las redes de la MPCH. La garantía del cumplimiento de estas políticas será responsabilidad de cada miembro de la comunidad municipal pues su contravención afecta a toda la MPCH.

A continuación definimos las siguientes políticas de seguridad de la información:

4.4.1 Organización de la seguridad

Se tiene como objetivo gestionar la seguridad dentro de la institución. Sugiere diseñar una estructura de administración que establezca la responsabilidad de los grupos en ciertas áreas de la seguridad y un proceso para el manejo de respuesta a incidentes.

En esta política se definen los roles y responsabilidades a lo largo de la institución con respecto a la protección de los recursos de información. Los miembros de la entidad deben tener el criterio para decidir cuándo pueden hacer uso personal de los recursos de información y serán responsables de dicha decisión. De igual manera, el área de seguridad de la información es responsable de crear unas normas internas de uso personal de los servicios de Internet y de la red de la MPCH. Los empleados y terceros deben guiarse por las políticas de la MPCH sobre uso personal, y si hay incertidumbre, los deben consultar de inmediato con los directivos de la institución.

4.4.2 Inventario de activos

Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos de información. El proceso de constituir un inventario de activos es un aspecto importante de la gestión de riesgos. La MPCH debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, la organización puede entonces, asignar niveles de protección proporcionales al valor e importancia de los activos. Se debe elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información. Cada activo debe ser claramente identificado y su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo. Ejemplos de activos asociados a los recursos de información son los siguientes:

- 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, disposiciones relativas a sistemas de emergencia para la reposición de información perdida, información archivada.
- Recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios;
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (Routers, Pbs., contestadores automáticos), medios magnéticos (cintas, discos), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado), mobiliario, lugares de emplazamiento.

4.4.3 Clasificación de la información

El objetivo es asegurar un nivel de protección adecuado a los activos de la información. La información debería clasificarse para indicar la necesidad, prioridades y grado de protección. La información y los resultados de los sistemas que manejan datos clasificados deberían catalogarse en relación con su valor e importancia para la organización. También puede ser adecuado catalogar la información en términos de criticidad por ejemplo de su integridad y disponibilidad para la institución.

La clasificación de la información debe ser documentada por el propietario de la información, aprobada por la dirección responsable y distribuida al personal del área de sistemas de información durante el proceso de desarrollo de sistemas o antes de la distribución de los documentos o datos. La clasificación asignada a un tipo de información, solo puede ser cambiada por el propietario de la información, luego de justificar formalmente el cambio en dicha clasificación.

La información que existe en más de un medio (por ejemplo, documento fuente, registro electrónico, reporte o red) debe tener la misma clasificación sin importar el formato. Frecuentemente, la información deja de ser sensible o crítica después de un cierto período de tiempo, cuando la información se ha hecho pública.

La información debe ser examinada para determinar el impacto en la MPCH si fuera divulgada o alterada por medios no autorizados. A continuación detallamos algunos ejemplos de información sensible:

- Registros del personal administrativo
- Cuenta Corriente de empleados
- Lista de rubros de pagos a la MPCH (tarifas)
- Datos financieros de la MPCH

4.4.4 Seguridad del Personal

- Seguridad en la definición de los puestos de trabajo y recursos. El departamento de Recursos Humanos debe notificar al área de Seguridad de la Información, la renuncia o despido de los empleados así como el inicio y fin de los períodos de vacaciones de los mismos. Cuando se notifique el despido o transferencia, el personal del área debe de asegurarse que la cuenta de usuario sea revocado. Cualquier ítem entregado al empleado o al proveedor como computadoras portátiles, llaves, software, datos, documentación, manuales, etc. Deben ser entregados a su gerente o al área de Recursos Humanos.
- Capacitación de Usuarios. Los empleados de la MPCH deben recibir la formación adecuada y actualizaciones regulares de las políticas y procedimientos de la institución, donde se incluya los requisitos de seguridad, responsabilidades legales, así como prácticas en el uso

correcto de los recursos de tratamiento de la información (Procedimientos de conexión, uso de paquetes de software, etc.) antes de obtener acceso a la información o los servicios.

- Procedimientos de respuestas ante incidentes de seguridad. Si un empleado de la MPCH detecta o sospecha la ocurrencia de un incidente de seguridad, tiene la obligación de notificarlo al personal de seguridad de la información o directamente al proveedor de servicio. Bajo ninguna circunstancia los usuarios deben de probar las sospechas de vulnerabilidad o fallas del sistema. El área de seguridad de la información debe documentar todos los reportes de incidentes de seguridad.

4.4.5 Control de Acceso a los datos

a) La interfaz de usuario para acceder a la información disponible en los sistemas debe ser clasificada como confidencial o no. Las personas que estén involucradas con este tipo de información deben seguir procedimientos adecuados para evitar el acceso sin autorización a esta información.
b) Tenga claves seguras y no comparta su cuenta. Los usuarios autorizados son los responsables por la seguridad de su cuenta y de su clave. Las claves de los usuarios con privilegios deben cambiarse mínimo cada mes y las claves de los usuarios sin privilegios deben cambiarse mínimo cada tres meses.
c) En medios electrónicos debe tener controles de acceso individuales (clave personal) y se recomienda que los archivos se almacenen encriptados. La seguridad física es muy importante para este tipo de información, así que el equipo donde sea almacenada debe estar asegurado físicamente y debe conectarse a las redes de la MPCH sólo cuando las necesite (idealmente, el equipo donde se almacena la información debe sólo ser utilizado por las personas autorizadas a tener acceso a dicha información). Entre los métodos que se pueden utilizar para garantizar esto está el uso de llaves que aseguran el hardware del equipo para poder ser encendido. Si es un equipo portátil nunca debe dejarlo solo y siempre debe utilizar el cable de aseguramiento (lockdown cable) y cuando salga de la oficina asegúrese que el equipo y cualquier material crítico queden

bajo llave. En caso de que la información sea muy importante no se debe dudar en guardar los medios y los equipos en una caja fuerte.

d) Si después de utilizar este tipo de información no se hará pública y no se necesita para procesos posteriores, destrúyala (una picadora de papel para estos fines puede ser utilizada o puede incinerarla) o depositarla en los tachos de basura de la MPCH rompiendo antes el documento (aquí se supone que las personas encargadas de retirar el contenido de los tachos labora con la MPCH y realiza un manejo correcto de los desechos); los datos en medio electrónico deben ser borrados de manera confiable (no basta con emitir el comando de borrado, es aconsejable hacer dos cosas adicionales: desocupar la papelera de reciclaje y reescribir el disco con otro archivo que tenga el mismo nombre del que fue borrado, en el mismo directorio donde estaba ubicado).
e) Todas las conexiones de red internas y externas deben cumplir con las políticas de la MPCH sobre servicios de red y control de acceso. Es responsabilidad del área de sistemas y del área de seguridad de la información determinar: los elementos de red que pueden ser accedidos, el procedimiento de autorización para la obtención de acceso y controles para la protección de la red.

Las siguientes actividades están prohibidas:

- Copia no autorizada de material protegido por derechos de autor que incluye, pero no está limitado a, digitalización y distribución de imágenes o fotografías de cualquier origen (revistas, libros, páginas web, etcétera), digitalización y distribución de música, audio o video, distribución e instalación de software de los cuales ni la MPCH ni el usuario tienen la licencia debida.
- Exportar software, información técnica, software y tecnologías para criptografía en contra de leyes de control regionales o internacionales. Las dependencias apropiadas (área de sistemas de información y asesoría legal) deben ser consultadas antes de exportar cualquier material de este tipo.
- Revelar la clave o código de su cuenta a otros (por ejemplo, su cuenta de correo electrónico, su usuario de bases de datos, su código para realizar

llamadas de larga distancia) o permitir su uso a terceros para actividades ajenas a la misión de la MPCH. La prohibición incluye familiares y cualquier otra persona que habite en la residencia del funcionario cuando la actividad se realiza desde el hogar (por ejemplo, computadores portátiles, teléfonos celulares o agendas electrónicas propiedad de la MPCH).

- Utilizar la infraestructura de tecnología de información de la MPCH para conseguir o transmitir material con ánimo de lucro. Igualmente se prohíbe el uso del sistema de comunicaciones de la MPCH con el fin de realizar algún tipo de acoso, difamación, calumnia o cualquier forma de actividad hostil.
- Hacer ofrecimientos fraudulentos de productos o servicios cuyo origen sean los recursos o servicios propios de la MPCH.
- Realizar actividades que contravengan la seguridad de los sistemas o que generen interrupciones de la red o de los servicios. Entre las acciones que contravienen la seguridad de la red se encuentran, aunque no están limitadas, acceder a datos cuyo destinatario no es usted, ingresar a una cuenta de un servidor o de una aplicación para la cual no está autorizado.
- Está prohibido explícitamente el monitoreo de puertos o análisis de tráfico de red con el propósito de evaluar vulnerabilidades de seguridad. Las personas responsables de la seguridad de la información pueden realizar estas actividades cuando se realicen en coordinación con el personal responsable de los servidores, los servicios, las aplicaciones y de la red.
- Burlar los mecanismos de seguridad, autenticación, autorización o de auditoria de cualquier servicio de red, aplicación, servidor, o cuenta de usuario.
- Interferir o negar el servicio a usuarios autorizados con el propósito de lesionar la prestación del servicio o la imagen de la MPCH.
- Uso de comandos o programas o el envío de mensajes de cualquier tipo con el propósito de interferir o deshabilitar una sesión de usuario a través de cualquier medio, local o remoto (Internet o Intranet).
- Proporcionar información sobre empleados administrativos a personas o entidades externas que no tengan ningún tipo de relación contractual,

relación jurídico-administrativa o convenio con la MPCH donde se especifique que ellos pueden disponer de dicha información.

4.4.6 Gestión de Comunicaciones y Operaciones

La gestión de las comunicaciones y operaciones de la MPCH son esenciales para mantener un adecuado nivel de servicio a los trabajadores. Los procedimientos operacionales y las responsabilidades para mantener accesos adecuados a los sistemas, así como el control y la disponibilidad de los mismos, deben ser incluidos en las funciones operativas de la MPCH.

a) Procedimientos y responsabilidades de operación

- Se deben documentar y mantener los procedimientos de operación identificados por la política de seguridad. Estos procedimientos, se deben tratar como documentos formales y sus cambios han de autorizarse por la dirección.
- Se deben controlar los cambios en los sistemas y recursos de tratamiento de información. Un control inadecuado de dichos cambios es una causa habitual de fallos de seguridad o del sistema. Se deben implantar responsabilidades y procedimientos formales de gestión para asegurar un control satisfactorio de todos los cambios en los equipos, el software o los procedimientos.
- La separación de los recursos para desarrollo, prueba y producción es importante para conseguir la segregación de las responsabilidades implicadas. Se deberían definir y documentar las reglas para transferir el software del entorno de desarrollo al de producción y así evitar problemas operacionales.
- La contratación de un proveedor externo para gestionar los recursos de tratamiento de información puede introducir posibles vulnerabilidades, como la posibilidad de daño, pérdida o comprometer los datos en las instalaciones de la MPCH. Se deberían identificar estos riesgos de antemano e incorporarse al contrato las medidas de seguridad apropiadas de acuerdo con la MPCH.

b) Gestión de respaldo y recuperación

- Almacenar un nivel mínimo de información de respaldo, junto a los registros exactos y completos de las copias de seguridad y a

procedimientos documentados de recuperación, a una distancia suficiente para evitar todo daño por un desastre en el local principal. Se retendrán como mínimo tres generaciones o ciclos de información de respaldo para las aplicaciones importantes del negocio.

- Dar a la información de respaldo un nivel adecuado de protección física y del entorno, un nivel consistente con las normas aplicadas en el local principal. Se deberían extender los controles y medidas aplicados a los medios en el local principal para cubrir el local de respaldo.
- Los medios de respaldo se deben probar regularmente, donde sea factible, para asegurar que son fiables cuando sea preciso su uso en caso de emergencia. Comprobar y probar regularmente los procedimientos de recuperación para asegurar que son eficaces y que pueden cumplirse en el tiempo establecido por los procedimientos operativos de recuperación.

c) Protección de software malicioso

- Política formal que requiera el cumplimiento de las licencias de software y la prohibición del uso de software no autorizado para los empleados.
- Verificación de todo archivo adjunto al correo electrónico o de toda descarga para buscar software malicioso antes de usarlo.
- Está prohibido para el personal, el uso de discos compactos, memorias USB provenientes de otras fuentes que no sea de la MPCH, a excepción de los provenientes de organismos reguladores, proveedores, los cuales deben pasar por un procedimiento de verificación y control en el área respectiva.
- Procedimientos y responsabilidades de administración para la utilización de la protección de antivirus, la formación para su uso, la información de los ataques de los virus y la recuperación de éstos
- Se debe evitar compartir archivos o carpetas con otros usuarios; en caso de ser necesario coordinar con el área respectiva y habilitar el acceso sólo a nivel de lectura informando a personal de Soporte Técnico.
- Todos los PCs, laptops y estaciones de trabajo deben tener configurados un protector de pantalla con clave y con un tiempo de espera máximo de 10 minutos o con logging-off automático cuando el equipo esté desatendido.

d) Intercambio de información y software

- Los mensajes enviados a listas de correo o grupos de discusión por los miembros de la institución y que utilicen las direcciones de correo de la MPCH deben contener un párrafo donde diga "las opiniones expresadas en este mensaje son estrictamente personales y no es una posición oficial de la MPCH". Se recomienda que los mensajes de correo electrónico y las cubiertas (cover) de fax con información confidencial incluyan la siguiente nota:

  ✉ CONFIDENCIAL. MPCH

- La información contenida en este mensaje es confidencial y sólo puede ser utilizada por la persona o la organización a la cual está dirigido. Si usted no es el receptor autorizado, cualquier retención, difusión, distribución o copia de este mensaje está prohibida y será sancionada por la ley. Si por error recibe este mensaje, favor reenvíelo y borre el mensaje recibido inmediatamente.
- Los miembros de la comunidad municipal deben ser cuidadosos cuando abran los anexos (attachments) colocados en los mensajes de correo electrónico que sean recibidos de remitentes desconocidos o sospechosos ya que pueden contener virus.
- Está totalmente prohibido lo siguiente :
  - ✓ Enviar mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que nunca han solicitado ese tipo de material (email spam, mensajes electrónicos masivos, no solicitados y no autorizados en el correo electrónico).
  - ✓ Generar o enviar correos electrónicos a nombre de otra persona sin autorización o suplantándola.
  - ✓ Envío de mensajes de correo electrónico con una dirección de correo diferente al verdadero remitente con el fin de realizar algún tipo de acoso, difamación u obtener información.
  - ✓ Crear o reenviar cartas cadena o cualquier otro tipo esquema de “pirámide” de mensajes.

- ✓ Colocar mensajes de correo iguales o similares no relacionados con las actividades de la MPCH a un gran número de grupo de noticias (mensajes electrónicos masivos no solicitados y no autorizados en grupos de noticias).

4.4.7 Desarrollo y Mantenimiento de los Sistemas

El diseño de la infraestructura de la MPCH, las aplicaciones de negocio y las aplicaciones del usuario final deben soportar los requerimientos generales de seguridad documentados en la política de seguridad de la MPCH. Estos requerimientos deben ser incorporados en cada paso del ciclo de desarrollo de los sistemas, incluyendo todas las fases de diseño, desarrollo, mantenimiento y producción.

Todos los requisitos de seguridad, incluyendo las disposiciones para contingencias, deberían ser identificados y justificados en la fase de requisitos de un proyecto, consensuados y documentados como parte del proceso de negocio global para un sistema de información.

4.4.8 Cumplimiento Normativo

Se deben cumplir los siguientes objetivos:

- Evitar infringir cualquier norma civil o penal. Ley, reglamento, obligación contractual o cualquier requerimiento de seguridad.
- Asegurar la compatibilidad de los sistemas con las políticas y estándares de seguridad.
- Maximizar la efectividad y minimizar las interferencias hacia y del sistema de auditoría del proceso.
- Buscar el asesoramiento sobre requisitos legales específicos de los asesores legales de la organización, o de profesionales de derecho calificados.

4.4.9 Gestión de Continuidad del Negocio

El objetivo es reaccionar a la interrupción de las actividades de la MPCH y proteger sus procesos críticos frente a grandes fallos o desastres. Se debe implantar un proceso de gestión de continuidad del negocio para reducir, a niveles aceptables, la interrupción causada por los desastres y fallas de

seguridad como por ejemplo desastres naturales, accidentes, fallas de equipos o acciones deliberadas mediante una combinación de controles preventivos y de recuperación. Se debe desarrollar e implantar planes de contingencia para asegurar que los procesos de negocio se pueden restaurar en los plazos requeridos, dichos planes se deben mantener y probar para que se integren con todos los demás procesos de gestión.

Proceso de Gestión de la continuidad del negocio

- Comprender los riesgos que la MPCH corre desde el punto de vista de su vulnerabilidad e impacto, incluyendo la identificación y priorización de los procesos críticos del negocio.
- Comprender el impacto que tendrían las interrupciones en las actividades de la MPCH. Es importante encontrar soluciones que manejen las pequeñas incidencias así como los grandes accidentes que puedan amenazar la viabilidad de la organización.
- Tiempo de respuesta lo mínimo posible cuando la MPCH haya sufrido una infracción de seguridad como por ejemplo la infección de virus informáticos en los servidores. Supervisar que los servidores y los firewall marchen bien.
- Probar y actualizar regularmente los planes y procesos que describen las acciones a realizar tras una contingencia que amenace las actividades de la MPCH. Por ejemplo que los procedimientos de las copias de seguridad de la información funcionen adecuadamente.
- Considerar la adquisición de los seguros adecuados que formarán parte de los proceso de continuidad del negocio.
- Formular y documentar planes de continuidad del negocio en línea con la estrategia acordada por la MPCH.

4.5 IMPLEMENTACION

Con la identificación de riesgos, amenazas y vulnerabilidades se pudo determinar el conjunto de actividades más importantes a ser realizadas por la MPCH, las cuales permiten alinear las estrategias o medidas de seguridad existentes con las exigidas por las políticas de seguridad elaboradas.

Estas actividades han sido agrupadas en un plan de implementación, el cual contiene las metas de cada actividad, y las etapas a ser cubiertas en cada actividad identificada.

4.5.1 Clasificación de la Información

Metas	Clasificar los activos de información de manera adecuada con el objetivo de priorizar la utilización de recursos para aquella información que requiere de mayores niveles de protección.
Etapas	• Elaboración de un inventario de activos de información incluyendo información almacenada en medios digitales e información impresa. • Definición de responsables por activos identificados • Clasificación de la información por parte de los responsables definidos. • Consolidación de los activos de información clasificados. • Determinación de las medidas de seguridad a ser aplicados para cada activo clasificado. • Implementación de las medidas de seguridad determinadas previamente.

4.5.2 Campaña de concientización de usuarios

Metas	Lograr un compromiso y concienciación de los miembros de la comunidad municipal en temas referentes a la seguridad de la información. Se debe realizar una campaña de concienciación que esté orientada a todos los usuarios y relacionada con conceptos básicos de seguridad y a grupos específicos con temas correspondientes a sus responsabilidades en la institución.
Etapas	• Definición del mensaje a transmitir y material a ser empleado para los distintos grupos de usuarios, entre ellos : **Comunidad en general:** Información general sobre seguridad, Políticas de seguridad y estándares incluyendo protección de virus, contraseñas, seguridad física, sanciones, correo electrónico y uso de Internet. **Personal de TIC:** Políticas de seguridad, estándares y controles específicos para la tecnología y aplicaciones utilizadas. **Dirección y Jefaturas:** Monitoreo de seguridad, responsabilidades de supervisión, políticas de sanción. • Capacitación mediante charlas, videos, presentaciones, afiches, etc., los cuales recuerden permanentemente al usuario la importancia de la seguridad de la información.

4.5.3 Seguridad de red y comunicaciones

Metas	Para evitar manipulación de los equipos de comunicaciones por personal no autorizado y garantizar que la configuración que poseen, brinden mayor seguridad y eficiencia a las comunicaciones, se requiere que los equipos que soportan dicho servicio se encuentren adecuadamente configurados.

Etapas	• Adaptación de los equipos y sistemas de comunicaciones a políticas de seguridad. • Elaboración de un inventario de equipos de comunicaciones (routers, switches, firewalls, etc.) • Adaptación de los equipos a la política de seguridad • La arquitectura de red propuesta debe considerar la segmentación de las áreas administrativas tanto a nivel hardware como software. • Controlar mediante un firewall la comunicación entre la red de la MPCH y redes externas para evitar actividades no autorizadas desde dichas redes hacia los equipos de red de la entidad. • Implementar una estructura de la red para evitar el ingreso de conexiones desde Internet hacia la red interna de datos. • Implementar un sistema de Antivirus para servicios de Internet. • Implementar un sistema de monitoreo de Intrusos para detectar los intentos de intrusión o ataque desde redes externas hacia la red de datos de la entidad. • Implementar un servidor de gestión de seguridad de la red que monitoree todos los demás servidores como antivirus, web, firewall, correo electrónico, etc.

4.5.4 Inventario de accesos a los sistemas

Metas	Con el propósito de obtener un control adecuado sobre el acceso de los usuarios a los sistemas de la MPCH, se debe realizar un inventario de todos los accesos que poseen ellos sobre cada uno de los sistemas. Este inventario debe ser actualizado al modificar el perfil de acceso de algún usuario y será utilizado para realizar revisiones periódicas de los accesos otorgados en los sistemas.

Etapas	• Elaboración de un inventario de las aplicaciones y sistemas de la MPCH. • Elaboración de un inventario de los perfiles de acceso de cada sistema. • Verificación de los perfiles definidos en los sistemas para cada usuario. • Revisión y aprobación de los accesos por parte de las direcciones respectivas. • Depurar los perfiles de accesos de los usuarios a los sistemas. • Mantenimiento periódico del inventario.

4.5.5 Adaptación de contratos con proveedores

Metas	Asegurar el cumplimiento de las políticas de seguridad de la MPCH en el servicio brindado por los proveedores, necesario para realizar una revisión de los mismos y su grado de cumplimiento respecto a las políticas de seguridad definidas. Si es necesario dichos contratos deben ser modificados para el cumplimiento de la política de seguridad.
Etapas	• Elaboración de cláusulas estándar referidas a la seguridad de la Información, para ser incluidas en los contratos con proveedores. • Elaboración de un inventario de los contratos existentes con proveedores • Revisión de los contratos y analizar el grado de cumplimiento de la política de seguridad • Negociar con los proveedores para la inclusión de las cláusulas en los contratos.

4.5.6 Verificación y Adaptación de los sistemas de la MPCH

Metas	Para asegurar el cumplimiento de la política de seguridad en los controles existentes, se debe verificar el grado de cumplimiento de las políticas de seguridad en los sistemas de la MPCH y adaptarlos en caso de verificar su incumplimiento.

Etapas	• Elaboración de un inventario de las aplicaciones existentes. • Elaboración de un resumen de los requisitos que deben cumplir las aplicaciones según las políticas y estándares de seguridad • Evaluación del grado de cumplimiento de la política de seguridad para cada una de las aplicaciones existentes y la viabilidad de su modificación para cumplir con las políticas de seguridad, elaborando la relación de cambios que deben ser realizados en cada aplicación. • Estandarización de controles para contraseñas de los sistemas.

4.5.7 Revisión y adaptación de procedimientos complementarios

Metas	Adaptar los procedimientos y controles complementarios de la MPCH de acuerdo a lo estipulado en las políticas de seguridad
Etapas	• Revisión y adaptación de los controles y estándares para desarrollo de sistemas. • Elaboración de procedimientos de monitoreo, incluyendo procedimientos para verificación periódica de carpetas compartidas, generación de copias de respaldo de información de usuarios, aplicación de controles de seguridad para información en computadoras portátiles, etc. • Elaboración de procedimientos de monitoreo y reporte sobre la administración de los sistemas y herramientas de seguridad, entre ellas: antivirus, servidores de seguridad del contenido, servidor Proxy, servidor Firewall, sistema de detección de intrusos. • Revisión y establecimiento de controles para el almacenamiento físico de la información. • Revisión y establecimiento de controles para personal externo que realiza labores utilizando activos de información de la MPCH para la misma. (Soporte técnico, proveedores de comunicación: Claro, Telefónica, etc.)

4.6 CRONOGRAMA

ACTIVIDAD	MES 01	MES 02	MES 03	MES 04	MES 05	MES 06	MES 07	MES 08	MES 09	MES 10
Clasificación de Información										
Campaña de concienciación de usuarios										
Seguridad de red y comunicaciones										
Inventario de accesos a los sistemas										
Adaptación de contratos con proveedores										
Verificación y adaptación de los sistemas de la MPCH										
Revisión y adaptación de procedimientos complementarios										

Diagrama de GANTT

Fuente: Elaboración Propia

4.7 EVALUACION DE LAS ESTRATEGIAS DE SEGURIDAD

Estrategias o medidas de seguridad	Indicadores de Gestión
• Estándares de seguridad para servidores con sistemas operativos Windows y Linux • Revisiones periódicas de los registros de los sistemas y operaciones realizadas por los usuarios • Restricciones en el manejo de la información enviada por correo electrónico hacia redes externas	• Incremento de los niveles de seguridad de la información a los servidores de base de datos y servidores de aplicaciones. • Reducción de abusos de Internet por parte de los usuarios • Tasa de incidencias de seguridad ocasionada por intrusos internos como externos.
• Adecuada arquitectura e implementación del sistema antivirus • Verificación periódica de la actualización del antivirus de computadoras personales y servidores. • Generación periódica de reporte de virus detectados y actualización de Antivirus.	• Reducción de archivos infectados por virus informáticos • Incremento de la productividad en la institución
• Uniformizar dentro de lo posible la estructura de las contraseñas empleadas y sus fechas de renovación • Implementar un sistema de Servicio de Directorio, el cual permita al usuario identificarse en él, y mediante un proceso automático, éste lo identifique en los sistemas en los cuales posee acceso.	• Incremento de los niveles de seguridad de la información. • Reducción general del tiempo de ciclo de reestablecer contraseñas cada vez que el usuario se olvida.

• Programa de capacitación de la MPCH en temas relacionados a la seguridad de la información.	• Grado de compromiso y responsabilidad con el manejo de la información • Comparar el número de incidencias de seguridad por parte de los usuarios en períodos diferentes.
• Diseño de arquitectura de seguridad de red • Adecuada configuración de elementos de control de conexiones (Firewalls) • Implementación y administración de herramientas de seguridad • Separación del segmento de red inalámbrico mediante un firewall.	• Tasa de incidencias de seguridad ocasionada por intrusos internos como externos. • Reducción de los riesgos de la información
• Establecimiento de un procedimiento formal que contemple la generación de copia de respaldo de información importante de los usuarios. • Asegurar que la información del usuario que se almacene en el servidor esté protegida por una contraseña.	• Incremento de confiabilidad y productividad de por parte de los usuarios • Adecuado respaldo de la información.
• Implementación y administración de herramientas para la inspección del contenido de los correos electrónicos	• Reducción de abusos de mensaje de correo electrónico no solicitado ni autorizado dentro de la institución.

CAPITULO V: CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

1. Los resultados de la investigación con respecto a los riesgos de la información en la Municipalidad Provincial de Chiclayo como son: la divulgación ilícita de la información por los trabajadores, no realizar copias de seguridad, virus informáticos, corroboran con lo que está pasando a nivel mundial, donde el 70% de los robos o accidentes que se producen en los sistemas informáticos de las organizaciones los causan los propios trabajadores, muchas veces son resultados de errores, descuidos en sus conocimientos sobre la seguridad de la organización o actos delictivos propiamente dichos.

2. A diferencia de las redes informáticas corporativas y otras redes comerciales, que son más cerradas y segmentadas con énfasis en la protección de los recursos valiosos de la información. En la presente investigación, los resultados revelan que la de las red informática municipal fue diseñada sin pensar originalmente en la seguridad (70%). Las razones principales sobre estos resultados fueron que en la MPCH como entidad pública no debe haber restricciones al acceso de la información. Otra razón fue que cuando fue diseñada las red municipal no había Internet o recién estaba apareciendo, y por tanto no había demasiados riesgos a la información desde el exterior de la institución.

3. En una organización existen recursos humanos, recursos técnicos e infraestructura que están expuestos a diferentes tipos de riesgos e inseguridades procedentes de una amplia variedad de fuentes, incluyendo fraudes basados en informática, virus informáticos, espionajes, sabotaje, vandalismo y otros. La dependencia de los sistemas y servicios de información implica que las organizaciones son más vulnerables a las amenazas de seguridad, y se han vuelto más vulnerables al compartir sus recursos de información e interconectar las redes públicas (Internet) con las privadas. Los hackers pueden penetrar a las redes informáticas de una institución y causar graves interrupciones en el sistema. La seguridad de la información ha sido siempre considerada como un problema de ingeniería,

donde la responsabilidad debe recaer en el personal de Tecnología de Información y Comunicaciones, de tal forma que las organizaciones han tratado de resolverlo utilizando tecnología como controles de acceso pero este enfoque es incorrecto porque la gestión de la seguridad de la información requiere la participación de todos los empleados de una organización. Los resultados de la investigación demuestran que la estrategia de desarrollar políticas de seguridad de la información es de prioridad en la Municipalidad Provincial de Chiclayo.

4. Las autoridades no consideran a la seguridad como una prioridad alineada con la estrategia municipal. Ello se refleja en las encuestas realizadas al personal de TIC donde se les formuló la pregunta si habían asistido a eventos o programas de capacitación de seguridad de la información, la cual reportó que la mayoría nunca asistió a programas de capacitación (20%). La seguridad de la información está siendo un tema crítico dentro de las organizaciones, y por tanto deben establecerse requisitos de seguridad en la parte legal como normativas, estatutos, regulaciones y contratos que deberían satisfacer las organizaciones, los contratistas y los proveedores de servicios, de tal forma que se garantice la seguridad de los activos, la exactitud y confiabilidad de sus registros y la aceptación de las normas administrativas.

5.2 RECOMENDACIONES

1. Muchos sistemas de información no han sido diseñados para ser seguros, y la seguridad que puede lograrse a través de los medios técnicos es limitada, y debería apoyarse en una gestión y unos procedimientos adecuados. La Municipalidad Provincial de Chiclayo deben implementar políticas de seguridad de la información o hacerlas cumplir si las tienen, pues son la base para la gestión de seguridad. La implementación de las estrategias o medidas de seguridad, para que sea eficaz, debe basarse en un plan organizado que tenga en cuenta todos los aspectos de las necesidades de seguridad de la organización. Muchas organizaciones tienen políticas de seguridad, pero muy pocas implantan una cultura de conciencia de seguridad que fomente la identificación del trabajador con la información que manejan. Para que tenga éxito un plan de gestión de seguridad en la Municipalidad Provincial de Chiclayo es necesario un marketing efectivo de seguridad de la información a las autoridades, trabajadores y terceros. Debe haber normas y guías que controlen la forma en la que se lleva a cabo el plan, y que se distribuya en forma de políticas.

2. A la luz de las recientes brechas de seguridad y de las expectativas de más amenazas a la seguridad en el futuro, la Municipalidad Provincial de Chiclayo no pueden continuar con un acceso abierto e ilimitado de la información. Se deben rediseñar la red informática de la Municipalidad Provincial de Chiclayo separando las áreas de la Sede Central Administrativa pues tienen sistemas administrativos críticos. Es necesario consolidar sus redes informáticas aplicando tecnología de prevención y detección de intrusos, que es una buena solución para observar el tráfico de la red, permitir el ingreso del tráfico legítimo y detectar comportamientos maliciosos como los ataques de negación de servicios para evitar interrupciones en la red.

3. Existen estándares internacionales sobre seguridad de la información. Las más conocidas son la ISO 17799 que es una compilación de recomendaciones para las buenas prácticas de seguridad que toda organización puede aplicar independientemente de su tamaño o sector, y la ISO 27001 que es un sistema de gestión de seguridad de la información que

comprende los procedimientos adecuados y la planificación e implantación de controles de seguridad basadas en una evaluación de riesgos. En el País, la Presidencia del Consejo de Ministros (PCM) a través de la Oficina Nacional de Gobierno Electrónico, dispone del uso obligatorio de la Norma Técnica Peruana ISO 17799:2004 para ser implementada en Entidades Públicas. Esta norma se ha basado en la norma internacional ISO/IEC 17799:2000.

Para minimizar los efectos de un problema de seguridad se realiza lo que llamamos un análisis de riesgos y responder a tres cuestiones básicas sobre nuestra seguridad:

- ¿Qué queremos proteger?
- ¿Contra quién o qué lo queremos proteger?
- ¿Cómo lo queremos proteger?

Lograr establecer un rol de “Oficial de Seguridad de Información” dentro de la MPCH para el monitoreo y cumplimiento de las políticas y controles establecidos por la alta gerencia. Este rol no implica la contratación de personal, sino que puede ser algún colaborador del departamento de Sistemas de la MPCH. Actualizar periódicamente el SGSI. El plazo recomendado es cada 2 años ya que este periodo implica la posible adquisición de nuevas tecnologías dentro del campus de la MPCH, o la posible modificación de las actividades de los procesos. Esta actualización, la debe realizar la persona que tenga el rol de “Oficial de Seguridad de Información” dentro de la entidad

4. Se deben implementar programas de capacitación de seguridad de la información en la MPCH comenzando por la cima de la escala jerárquica; primero implementar el programa de seguridad para las autoridades, los jefes de departamentos, luego trabajadores y personal externo que brinda servicios.

REFERENCIAS BIBLIOGRAFICAS

[1] *AREITIO BERTOLIN, Javier. Seguridad de la Información. 1ª ed. Madrid, 2008. 592p. Ediciones Paraninfo, S.A. 2013*. ISBN: 8497325028 ISBN-13: 9788497325028

[2] *Alfa- Redi Revista Electrónica de Derecho Informático* | *GenderIT.org*. (2015). *Genderit.org*. Fecha de Consulta: 12 Abril 2015, de: <http://www.genderit.org/es/content/alfa-redi-revista-electr%C3%B3nica-de-derecho-inform%C3%A1tico>

[3] *ArCERT - RedGealc*. (2015). *Redgealc.org*. Fecha de Consulta: 15 Abril 2015, de: <http://redgealc.org/arcert/contenido/4371/es>

[4] *Aviso de Privacidad - Protección de Datos*. (2015). *Protección de Datos Personales*. Fecha de Consulta: 25 Marzo 2015, de: <http://www.protecciondedatospersonales.org>

[5] *Bienvenidos al Portal del OC*. (2015). *Oc.ccn.cni.es*. Fecha de Consulta: 15 Abril 2015, de: <https://oc.ccn.cni.es>

[6] *CNI - Centro Nacional de Inteligencia*. (2015). *Cni.es*. Fecha de Consulta: 1 Junio 2015, de: <http://www.cni.es>

[7] *Decreto Supremo mediante el cual se aprueba la Política Nacional de Gobierno Electrónico 2013-2017*. (2013) (1st ed.). Fecha de Consulta: de: <http://www.ongei.gob.pe/normas/0/NORMA_0_Decreto%20Supremo%20N%C2%B0%20081-2013-PCM.pdf>

[8] *esCERT* | *inLab UPC*. (2015). *Escert.upc.edu*. Fecha de Consulta: 11 Marzo 2015, de: <http://escert.upc.edu>

[9] *Cooperation for Accreditation*. (2015). *European-accreditation.org*. Fecha de Consulta: 30 Marzo 2015, de: <http://www.european-accreditation.org>

[10] *European Corporate Governance Institute*. (2015). *Ecgi.org*. Fecha de Consulta: 15 Abril 2015, de: < http://www.ecgi.org>

[11] *Guide to data protection* | *ICO*. (2015). *Ico.org.uk*. Fecha de Consulta: 12 Marzo 2015, de: <https://ico.org.uk/for-organisations/guide-to-data-protection>

[12] *Information Security Forum*. (2015). *Information Security Forum*. Fecha de Consulta: 30 Marzo 2015, de: <http://www.securityforum.org>

[13] *Information Technology - Information Security – Information Assurance* | *ISACA*. (2015). *Isaca.org*. Fecha de Consulta: 13 Abril 2015, de: <http://www.isaca.org>

[14] *BSI Group*. (2015). *Bsigroup.com*. Fecha de Consulta: 20 Abril 2015, de: <http://www.bsigroup.com/es-MX>

[15] *INTECO*. (2015). *Espacios de Ciberseguridad*. Fecha de Consulta: 10 Abril 2015, de: <https://www.incibe.es>

[16] *ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información*. (2015).*Iso27000.es*. Fecha de Consulta: 18 Marzo 2015, de: <http://www.iso27000.es>

[17] *ISO - International Organization for Standardization*. (2015). *Iso.org*. Fecha de Consulta: 12 Abril 2015, de: <http://www.iso.org>

[18] *IT Certification and Security Experts*. (2015). *Isc2.org*. Fecha de Consulta: 10 Abril 2015, de: <http://www.isc2.org>

[19] Mac, K., & WhatsApp, N. (2015). *CCN-CERT*. *Ccn-cert.cni.es*. Fecha de Consulta: 20 Marzo 2015, de: <http://www.ccn-cert.cni.es>

[20] *Microsoft Malware Protection Center Home Page*. (2015). *Microsoft.com*. Fecha de Consulta: 11 Marzo 2015, de: <http://www.microsoft.com/security/portal/default.aspx>

[21] *Nextel Ingeniería y Consultoría IT*. (2015). *Nextel.es*. Fecha de Consulta: 14 Abril 2015, de: <http://www.nextel.es>

[22] *Nuevas tecnologías aplicadas a Nuevas tecnologías aplicadas a la gestión documental*. (2015) (1st ed.). Fecha de Consulta: 1 Junio 2015, de: <http://www.ongei.gob.pe/eventos/programasdocu/39/programa_273.pdf>

[23] *Oficina Nacional de Gobierno Electronico e Informática - ONGEI*. (2015). *Ongei.gob.pe*. Fecha de Consulta: 1 Junio 2015, de: <http://www.ongei.gob.pe>

[24] *ONGEI*. (2015). http://www.ongei.gob.pe/eventos/Programas_docu/35/MAX%20Presentacion-Seguridad-ONGEI-cajamarca.ppt>

[25] *RedIRIS - Security Service (IRIS-CERT)*. (2015). *Rediris.es*. Fecha de Consulta: 20 Marzo 2015, de: <http://www.rediris.es/cert>

[26] *WG Chair Dashboard*. (2015). *Sec.ietf.org*. Fecha de Consulta: 25 Abril 2015, de: <http://sec.ietf.org>

ANEXOS

Anexo Nº 1: Encuesta de opinión a expertos en Tecnología de Información y Comunicaciones

Sr. /Sra. Estamos realizando encuestas a expertos de TIC en forma anónima, para una Tesis de Maestría. Por ello, mucho agradeceré se sirva absolver tales preguntas. MUCHAS GRACIA

1. ¿En el área donde labora tienen políticas de seguridad de la información?

[ ] Si
[ ] No

2. ¿Si en la Pregunta 1 respondió si, Se cumplen o se llevan a la práctica estas políticas?

[ ] A cabalidad
[ ] Medianamente
[ ] No se cumplen

3. Elija los beneficios que se presentan cuando la entidad cuenta con políticas de seguridad de la información. Marcar uno o más opciones.

[ ] Mayor seguridad de la información mediante el respaldo de medios magnéticos
[ ] Aumenta la productividad a través de consultas directas y confiables
[ ] Calidad en el servicio para los trabajadores y terceros
[ ] Otros
……

4. ¿Cuáles de estas medidas de seguridad de la información son más importantes para Usted?. Marcar uno o más opciones.

[ ] Desarrollo de Políticas de Seguridad
[ ] Clasificación del acceso de la información
[ ] Capacitación de usuarios
[ ] Monitoreo y reportes de las actividades en la red informática
[ ] La continuidad del negocio después de ataques de intrusos
[ ] Otros
……

5. ¿Cuáles son los errores más comunes cuando se usa Internet y el correo electrónico?. Marcar uno o más opciones.

[ ] Omitir la seguridad como un aspecto fundamental de configuración del servidor
[ ] Transmisión en pleno texto de contraseñas
[ ] Uso inadecuado de herramientas de seguridad, o no uso alguno
[ ] Obtener y mantener programas y aplicaciones (software) que son vulnerables
[ ] No tomar medidas preventivas en los aspectos de seguridad relevantes
[ ] Otros
……

6. ¿Cuáles son los riesgos y la frecuencia que se presentan en los recursos de información? Marcar en el cuadro todos los riesgos y frecuencias presentados.
MF: Muy frecuente RF: Regularmente frecuente PF: Poco frecuente

RIESGOS	M	RF	PF
Fenómenos Naturales (Terremotos, Inundaciones)			
Fallas mecánicas (Cortes de fluido eléctrico, incendios)			
Divulgación ilícita de la información por el personal			
Destrucción o modificación de la información por el personal			
Intrusos al sistema de la red			
Virus informáticos, gusanos, spam			
Otros:			

7. ¿Sus equipos de cómputo en su área tienen fuente de poder ininterrumpible (UPS), generadores de energía, baterías ante cortes de energía eléctrica?

[ ] Si
[ ] No

8. ¿Cuáles son las incidencias que se dan con más frecuencia por parte de los usuarios que manejan información?

[ ] Saturación de la red por programas indebidos (música, video)
[ ] Uso del correo electrónico de la entidad para fines personales
[ ] Pérdida de su información
[ ] Olvido de contraseña
[ ] No realizar copias de seguridad
[ ] Accesar a carpetas compartidas de otros usuarios
[ ] Otros
……

9. ¿Cuándo fue la última vez que asistió a un evento o taller sobre seguridad de la información?

[ ] Hace 3 meses
[ ] Hace 6 meses [
] Hace 1 año
[ ] Nunca

10. ¿Estaría dispuesto a asistir a talleres de capacitación de seguridad de la información?

[ ] Muy interesado
[ ] Poco interesado
[ ] Nada interesado

11. ¿Considera que la red informática fuer diseñada sin pensar originalmente en la seguridad?

[ ] Si
[ ] No

¿Porqué?
……
……..

12. ¿Cómo considera la gestión de seguridad de la información en la gestión administrativa de la MPCH sobre los sistemas de información como son: admisión y registros, tesorería, y trámites documentarios?

[ ] Buena
[ ] Regular
[ ] Mala

13. ¿Cuál es el impacto económico de implementar un Plan de Gestión de Seguridad de la Información en la gestión integral de la MPCH?

[ ] Muy beneficioso
[ ] Poco beneficioso
[ ] Nada beneficioso

Anexo Nº 2: Resolución Ministerial N° 310-2004-PCM

RESOLUCION MINISTERIAL N° 310-2004-PCM

Lima, 4 de Octubre de 2004

CONSIDERANDO:

Que, el artículo 2° del Decreto Supremo N° 066-2003-PCM y el numeral del artículo 3° y artículo 22° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 067-2003- PCM, prevén que la Presidencia del Consejo de Ministros se encarga de normar, coordinar, integrar y promover el desarrollo de la actividad informática en la Administración Pública, impulsando y fomentando el uso de las nuevas tecnologías de la información para la modernización y desarrollo del Estado, actúa como ente rector del Sistema Nacional de Informática, dirige y supervisa la política nacional de informática y gobierno electrónico;

Que, de acuerdo con los numerales 25.2 y 25.3 del artículo 25° del Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por el Decreto Supremo N° 067- 2003-PCM, son funciones de la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros, proponer la normatividad y coordinar el desarrollo del gobierno electrónico y de la actividad informática en la Administración Pública, impulsando su modernización, y desarrollar acciones orientadas a la consolidación y desarrollo del Sistema Nacional de Informática;

Que, mediante Resolución Ministerial N° 224-2004-PCM se aprobó el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la Información. Código de Buenas Prácticas para la Gestión de la Seguridad de la Información. 1ª Edición" en las entidades integrantes del Sistema Nacional de Informática;

Que, la Oficina Nacional de Gobierno Electrónico e Informática de la Presidencia del Consejo de Ministros - ONGEI ha propuesto ejecutar la Primera Encuesta de Seguridad de la Información en la Administración Pública - 2004, para obtener y mantener actualizada la información técnica relacionada con la seguridad de la información de las instituciones del Sistema Nacional de Informática;

De conformidad con lo dispuesto por el Decreto Legislativo Nº 560 - Ley del Poder Ejecutivo y el Reglamento de Organización y Funciones de la Presidencia del Consejo de Ministros, aprobado por Decreto Supremo Nº 067-2003- PCM;

SE RESUELVE:

Artículo 1º.- Autorizar la ejecución de la "Primera Encuesta de Seguridad de la Información en la Administración Pública - 2004" en todas las instituciones públicas pertenecientes al Sistema Nacional de Informática.

Artículo 2º.- La ejecución y la actualización de la Encuesta de Seguridad de la Información en la Administración Pública" será efectuada por la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros.

Artículo 3º.- Las instituciones públicas deberán remitir documento de la encuesta a la Oficina Nacional de Gobierno Electrónico e Informática - ONGEI de la Presidencia del Consejo de Ministros hasta el 15 de diciembre del 2004, de acuerdo a las indicaciones y a la información solicitada en el anexo adjunto, que constituye parte integrante de la presente Resolución Ministerial.

Regístrese, comuníquese y publíquese.

CARLOS FERRERO
Presidente del Consejo de Ministros

Fuente: *Publicada en el Diario Oficial El Peruano el 06/10/2004*

Anexo Nº 3: ISO 27001: Sistema de Gestión de la Seguridad de la Información

A.5 Política de seguridad		
A.5.1 Política de seguridad de la información Objetivo: Proveer dirección y soporte de la dirección para la seguridad de la información conforme a los requisitos del negocio, las leyes y reglamentos pertinentes.		
A.5.1.1	Documento de política de seguridad de la Información	Control El documento de política de seguridad de la información deberá ser aprobado por Gerencia General, y publicado y comunicado a todos los empleados y terceros pertinentes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información deberá revisarse a intervalos planeados o si ocurren cambios significativos, para asegurar la continuidad de su propiedad, adecuación y efectividad
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo: Gestionar la seguridad de la información dentro de la organización.		
A.6.1.1	Comité de Gestión de seguridad de la Información.	Control La Gerencia deberá apoyar activamente la seguridad dentro de la organización mediante una dirección clara, compromiso demostrado, delegación explícita, y reconocimiento de las responsabilidades de seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información	Control Las actividades de seguridad de la información deberán coordinarse con los representantes de diferentes partes de la organización que tengan funciones y trabajos pertinentes.
A.6.1.3	Asignación de responsabilidades sobre seguridad de la información	Control Todas las responsabilidades de seguridad de la información deben definirse claramente.
A.6.1.4	Proceso de autorización para las nuevas instalaciones de procesamiento de información.	Control Deberá definirse e implementarse un proceso de autorización de gerencia para nuevas instalaciones de procesamiento de la información.
A.6.1.5	Acuerdos de confidencialidad	Control Los requerimientos de convenios de confidencialidad o de no divulgación que reflejen las necesidades de la organización para protección de la información deberán

		ser identificados y revisados periódicamente.
A.6.1.6	Contacto con autoridades	Control Deberán mantenerse contactos apropiados con las autoridades pertinentes.
A.6.1.7	Contacto con grupos de interés especial	Control Deberán mantenerse contactos apropiados con los grupos de interés especial u otros foros especializados de seguridad y asociaciones profesionales.
A.6.1.8	Revisión independiente de seguridad de la información	Control El enfoque de la organización a la gestión de la seguridad de la información (objetivos de control, controles, políticas, procesos, y procedimientos de seguridad de la información) deberá revisarse independientemente a intervalos planeados, o cuando ocurran cambios significativos en la implementación de la seguridad.
A.6.2 Seguridad del acceso a terceras partes Objetivo: Mantener la seguridad de la información y de las instalaciones de procesamiento de información de la organización, que son accesadas, procesadas, comunicadas a terceros, o administradas por terceros.		
A.6.2.1	Identificación de riesgos por el acceso de terceros	Control Deberán identificarse los riesgos para la información e instalaciones de procesamiento de información de la organización, provenientes de procesos de negocios que involucran a terceros, e implementarse controles adecuados antes de conceder acceso.
A.6.2.2	Requisitos de seguridad cuando se trata con clientes	Control Deberán enfocarse todos los requisitos de seguridad identificados antes de darles a los clientes acceso a la información o activos de la organización.
A.6.2.3	Requisitos de seguridad en contratos con terceros	Control Los convenios con terceros que involucren acceder, procesar, comunicar o administrar la información o instalaciones de procesamiento de información de la organización, o agregar productos o servicios a dichas instalaciones, deberán abarcar todos los requisitos de seguridad pertinentes
A.7 Gestión de activos		
A.7.1 Responsabilidad por los activos		

Objetivo: Alcanzar y mantener una protección adecuada de los activos de la organización.		
A.7.1.1	Inventario de activos	Control Todos los activos deberán identificarse claramente y efectuarse y mantenerse un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y activos relacionados con instalaciones de procesamiento de información deberán tener un “dueño” que sea un miembro designado de la organización.
A.7.1.3	Uso aceptable de los activos	Control Deberán identificarse, documentarse e implementarse reglas para el uso aceptable de la información y de los activos relacionados con las instalaciones de procesamiento de información.
A.7.2 Clasificación de la información Objetivo: Asegurar que la información reciba el nivel de protección adecuado.		
A.7.2.1	Guías de clasificación	Control La información deberá clasificarse en función de su valor, requisitos legales, sensibilidad y criticabilidad para la organización.
A.7.2.2	Etiquetado y tratamiento de la información	Control Deberá prepararse e implementarse un conjunto de procedimientos adecuados para la rotulación y manipulación de la información, de acuerdo al esquema de clasificación adoptado por la organización.
A.8 Seguridad ligada a los recursos humanos		
A.8.1 Previo al empleo Objetivo: Asegurar que los empleados, contratistas y usuarios de terceros entiendan sus responsabilidades y sean adecuados para las funciones en las que se les ha considerado, así como reducir el riesgo de robo, estafa o mal uso de las instalaciones		
A.8.1.1	Roles y responsabilidades	Control Las funciones y responsabilidades de seguridad de los empleados, contratistas y usuarios de terceros deberán definirse y documentarse de acuerdo a la política de seguridad de información de la organización.
A.8.1.2	Investigación	Control Tamizaje: Deberá efectuarse la verificación de antecedentes de todos los candidatos a empleo, contratistas, y usuarios de terceros, conforme a las leyes, reglamentos y ética pertinentes, y en

		proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y a los riesgos percibidos.
A.8.1.3	Términos y condiciones de la relación laboral	Control Como parte de su obligación contractual, los empleados, contratistas y usuarios de terceros deberán aceptar y firmar los términos y condiciones de su contrato de empleo, el cual deberá indicar sus responsabilidades de seguridad de la información así como las de la organización.
A.8.2 Durante el empleo		
Objetivo: Asegurar que todos los empleados, contratistas y usuarios de terceros conozcan las amenazas y problemas de seguridad de la información, así como sus responsabilidades y obligaciones, y estén capacitados para apoyar la política de seguridad de la organización en el curso de su trabajo normal, y reducir el riesgo de error humano.		
A.8.2.1	Gestión de responsabilidades	Control La Gerencia General exigirá que los empleados, contratistas y usuarios de terceros apliquen la seguridad de acuerdo con las políticas y procedimientos establecidos por la organización.
A.8.2.2	Concientización, educación y entrenamiento en la seguridad de información	Control Todo el personal de la organización y, cuando sea pertinente, los contratistas y usuarios de terceros, deberán recibir el entrenamiento de concientización adecuado y actualizaciones periódicas de políticas y procedimientos de la organización, según corresponda a sus funciones de trabajo.
A.8.2.3	Proceso disciplinario	Control Habrá un proceso disciplinario formal para los empleados que hayan cometido una violación de seguridad.
A.8.3 Finalización o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y usuarios de terceros salgan de una organización o cambien de empleo en forma ordenada.		
A.8.3.1	Responsabilidades de finalización	Control Deberán definirse y asignarse claramente las responsabilidades para efectuar la terminación del empleo o cambio de empleo.
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y usuarios de terceros deberán devolver todos los activos de la organización en su

		poder al terminar su empleo, contrato o convenio.
A.8.3.3	Retiro de los derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y usuarios de terceros a la información y a las instalaciones de procesamiento de información deberán retirarse al terminar su empleo, contrato o convenio, o modificarse según el cambio.
A.9 Seguridad física y del entorno		
A.9.1 Áreas seguras Objetivo: Impedir el acceso físico no autorizado, daños e interferencias en los locales y la información de la organización.		
A.9.1.1	Seguridad física perimetral	Control Perímetros de seguridad (barreras tales como muros, puertas controladas por tarjeta o recepcionistas) deberán utilizarse para proteger las áreas que contienen información y las instalaciones de procesamiento de información.
A.9.1.2	Controles físicos de entradas	Control Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado.
A.9.1.3	Seguridad de oficinas, despachos y recursos	Control Deberá diseñarse y aplicarse seguridad física para las oficinas, cuartos e instalaciones.
A.9.1.4	Protección contra amenazas externas y ambientales	Control Deberá diseñarse y aplicarse protección física contra daños por incendio, inundación, terremoto, explosión, desorden civil, y otras formas de desastres naturales o artificiales.
A.9.1.5	El trabajo en las áreas seguras	Control Las áreas seguras deberán protegerse mediante controles de ingreso adecuados para asegurar que sólo se permita el acceso del personal autorizado.
A.9.1.6	Áreas de carga, descarga y de acceso publico	Control Los puntos de acceso tales como las áreas de entrega y carga y otros puntos donde personas no autorizadas pueden ingresar a los locales deberán controlarse y, de ser posible, aislarse de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.9.2 Seguridad de los equipos		

Objetivo: Impedir la pérdida, daño, robo o compromiso de activos así como interrupción de las actividades de la organización.		
A.9.2.1	Ubicación y protección de equipos	Control El equipo deberá ubicarse y protegerse para reducir los riesgos de amenazas y peligros ambientales, y las oportunidades de acceso no autorizado.
A.9.2.2	Suministro eléctrico	Control El equipo deberá estar protegido contra cortes de energía y otros trastornos ocasionados por fallas en los servicios de soporte.
A.9.2.3	Seguridad del cableado	Control El cableado de energía y telecomunicaciones que conduzca datos o soporte los servicios de información deberá estar protegido de intercepción o daño.
A.9.2.4	Mantenimiento de los equipos	Control Los equipos deberán mantenerse correctamente para asegurar su continua disponibilidad e integridad.
A.9.2.5	Seguridad de equipos fuera de los locales de la organización	Control Deberá aplicarse seguridad al equipo fuera de las instalaciones, teniendo en cuenta los diversos riesgos de trabajar fuera de las instalaciones de la organización.
A.9.2.6	Seguridad en el re-uso o eliminación de equipo	Control Todos los artículos de equipo que contengan medios de almacenamiento deberán revisarse para asegurar la remoción o sobre escritura apropiada de cualquier información sensible y “software” autorizado antes de su eliminación.
A.9.2.7	Retiro de propiedad	Control Remoción de propiedad: No se sacará equipo, información o “software” fuera de las instalaciones sin previa autorización.
A.10 Gestión de comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades de operación Objetivo: Asegurar la correcta y segura operación de los recursos de procesamiento de información.		
A.10.1.1	Documentación de procedimientos operativos	Control Los procedimientos operativos deberán documentarse, mantenerse y ponerse a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de los cambios	Control

		Se controlarán los cambios en las instalaciones y sistemas de procesamiento de información.
A.10.1.3	Segregación de tareas	Control Los deberes y áreas de responsabilidad deberán separarse para reducir las oportunidades de modificación no autorizada o inadvertida o mal uso de los activos de la organización.
A.10.1.4	Separación de las instalaciones de desarrollo, prueba y operación	Control Las instalaciones de desarrollo, prueba y operaciones deberán separarse para reducirlos riesgos de acceso o cambios no autorizados al sistema operativo.
A.10.2 Gestión de entrega de servicios externos Objetivo: Implementar y mantener el nivel adecuado de seguridad de información y servicios en línea con los convenios de servicios por terceros.		
A.10.2.1	Entrega de servicios	Control Se deberá asegurar que los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el convenio de servicios por terceros, sean implementados, operados y mantenidos por el tercero.
A.10.2.2	Monitoreo y revisión de los servicios externos	Control Los servicios, informes y registros suministrados por terceros deberán monitorearse y revisarse periódicamente, y efectuarse auditorias regularmente.
A.10.2.3	Gestión de cambios de los servicios externos	Control Deberá gestionarse los cambios en la provisión de servicios, incluyendo el mantenimiento y mejora de las políticas, procedimientos y controles de seguridad de información existentes, tomando en cuenta la criticabilidad de los sistemas y procesos de negocios involucrados y la reevaluación de los riesgos.
A.10.3 Planificación y aceptación del sistema Objetivo: Minimizar el riesgo de fallas de sistemas.		
A.10.3.1	Gestión de la capacidad	Control El uso de los recursos debe monitorearse y refinarse, y deben hacerse proyecciones de las necesidades de capacidad futuras para asegurar el desempeño requerido del sistema.
A.10.3.2	Aceptación del sistema	Control Deberán establecerse criterios de aceptación de nuevos sistemas de información, actualizaciones y nuevas

		versiones, y realizarse pruebas adecuadas de los sistemas durante el desarrollo y antes de la aceptación.
A.10.4 Protección contra software malicioso Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	Control Deberá implementarse controles de detección, prevención y recuperación para protegerse contra código malicioso así como procedimientos adecuados de concientización de usuarios.
A.10.4.2	Controles contra software móvil	Control Cuando el uso de código móvil está autorizado, la configuración deberá asegurar que el código móvil autorizado opere según una política de seguridad claramente definida, y se impedirá la ejecución de código móvil no autorizado.
A.10.5 Gestión interna de respaldo y recuperación Objetivo: Mantener la integridad y disponibilidad de la información y de las instalaciones de procesamiento de información.		
A.10.5.1	Recuperación de la información	Control Deberán hacerse copias de respaldo de la información y el “software”, y probarse periódicamente según la política de respaldo convenida.
A.10.6 Gestión de seguridad de redes Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de redes	Control Las redes deberán manejarse y controlarse debidamente, a fin de protegerse de amenazas, y mantener la seguridad de los sistemas y aplicaciones que usan la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Las características de seguridad, niveles de servicio, y requisitos de gestión de todos los servicios de red deberán identificarse e incluirse en cualquier convenio de servicios de red, ya sea que los servicios se provean internamente o del exterior.
A.10.7 Utilización y seguridad de los medios de información Objetivo: Impedir la divulgación, modificación, remoción o destrucción no autorizadas de activos, y la interrupción de las actividades de negocios.		

A.10.7.1	Gestión de medios removibles	Control Deberá haber procedimientos para el manejo de medios removibles.
A.10.7.2	Eliminación de medios	Control Los medios deberán eliminarse de modo seguro y sin riesgo de accidente cuando no se les necesite más, usando procedimientos formales.
A.10.7.3	Procedimientos de manipulación de la información	Control Deberán establecerse procedimientos para la manipulación y almacenamiento de información, a fin de protegerla de la divulgación no autorizada o del mal uso.
A.10.7.4	Seguridad de la documentación de sistema	Control Deberá protegerse la documentación del sistema contra el acceso no autorizado.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y "software" que se intercambian dentro de una organización y con cualquier organización exterior.		
A.10.8.1	Políticas y procedimientos para el intercambio de información	Control Deberán existir políticas, procedimientos y controles formales de intercambio de información para protegerlo mediante el uso de todo tipo de facilidades de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Deberán establecerse convenios para el intercambio de información y "software" entre la organización y organismos externos.
A.10.8.3	Seguridad de medios físicos en tránsito	Control Los medios que contengan información deberán protegerse contra el acceso no autorizado, el mal uso o corrupción durante su transporte más allá de los límites físicos de una organización.
A.10.8.4	Seguridad de correo electrónico	Control La información contenida en la mensajería electrónica deberá protegerse debidamente.
A.10.8.5	Seguridad en los sistemas de información de negocio	Control Deberán prepararse e implementarse políticas y procedimientos para proteger la información relacionada con la interconexión de los sistemas de información de negocios.
A.10.9 Servicios de comercio electrónico Objetivo: Verificar la seguridad de los servicios de comercio electrónico y su uso seguro.		

A.10.9.1	Seguridad en electrónico	Control La información involucrada en el comercio electrónico que circula por redes públicas, deberá protegerse de la actividad fraudulenta, objeción de contrato y de la divulgación y modificación no autorizadas.
A.10.9.2	Seguridad en las transacciones en línea	Control La información involucrada en las transacciones en línea deberá protegerse para impedir su transmisión incompleta, desviación, alteración no autorizada del mensaje, divulgación no autorizada, y duplicación o reproducción no autorizadas del mensaje.
A.10.9.3	Información disponible públicamente	Control Deberá protegerse la integridad de la información colocada en un sistema de disponibilidad pública para impedir su modificación no autorizada.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas		
A.10.10.1	Registro de Auditoría	Control Los registros de auditoría que graban las actividades, excepciones, y eventos de seguridad de la información de los usuarios deberán existir y mantenerse durante un período convenido para asistir futuras investigaciones y en el monitoreo de control de acceso.
A.10.10.2	Uso del sistema de monitoreo	Control Deberán establecerse procedimientos para monitorear el uso de las instalaciones de procesamiento de información, y los resultados de las actividades de monitoreo deberán revisarse regularmente.
A.10.10.3	Protección de la información de registro	Control Las instalaciones de registro y la información de registro deberán protegerse contra las alteraciones y el acceso no autorizado.
A.10.10.4	Registros de Administrador y operador	Control Se deberán registrar las actividades del administrador del sistema y del operador del sistema.
A.10.10.5	Registro con faltas	Control Las fallas deberán registrarse, analizarse y deberán tomarse las medidas adecuadas.
A.10.10.6	Sincronización de reloj	Control Los relojes de todos los sistemas de procesamiento de información pertinentes

		dentro de una organización o dominio de seguridad, deberán sincronizarse con una fuente de tiempo exacto convenida.
A.11 Control de acceso		
A.11.1 Requisito de negocios para el control de acceso Objetivo: Controlar el acceso a la información		
A.11.1.1	Política de control del accesos	Control Se deberá establecer, documentar, y revisar una política de control del acceso basada en los requisitos de negocios y de seguridad para el acceso.
A.11.2 Gestión del acceso de usuarios Objetivo: Asegurar el acceso de usuarios autorizados e impedir el acceso no autorizado a los sistemas de información.		
A.11.2.1	Inscripción de usuarios	Control Deberá haber un procedimiento formal de inscripción y des-inscripción de usuarios para otorgar y revocar el acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Deberá restringirse y controlarse la asignación y uso de privilegios.
A.11.2.3	Gestión de contraseñas de usuario	Control La asignación de contraseñas deberá controlarse mediante un proceso de manejo formal.
A.11.2.4	Revisión de los derechos de acceso de los usuarios	Control La gerencia deberá revisar los derechos de acceso de usuarios a intervalos regulares utilizando un procedimiento formal.
A.11.3 Responsabilidades de los usuarios Objetivo: Impedir el acceso de usuario no autorizado, así como el compromiso o robo de información o de instalaciones de procesamiento de información.		
A.11.3.1	Uso de contraseñas	Control Se deberá exigir a los usuarios que sigan buenas prácticas de seguridad en la selección y uso de las contraseñas.
A.11.3.2	Equipo informático de usuario desatendido	Control Los usuarios deberán asegurar que el equipo no atendido tenga protección adecuada.
A.11.3.3	Política de pantalla y escritorio limpio	Control Deberá adoptarse una política de escritorio limpio de papeles y medios de almacenamiento removibles, y una política de pantalla limpia para instalaciones de procesamiento de información.
A.11.4 Control de acceso a la redes Objetivo: Prevenir el acceso no autorizado a los servicios de redes.		

A.11.4.1	Política de uso de los servicios de la red	Control A los usuarios sólo deberá dárseles acceso a los servicios que están específicamente autorizados para usar.
A.11.4.2	Autenticación de usuarios para conexiones externas	Control Deberán usarse métodos de autenticación apropiados para controlar el acceso de usuarios remotos.
A.11.4.3	Autenticación de equipos en la red	Control La identificación automática de equipo deberá considerarse como un medio de autenticar las conexiones desde lugares y equipo específicos.
A.11.4.4	Protección para la configuración de puertos y diagnóstico remoto	Control Deberá controlarse el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Segregación en las redes	Control En las redes deberán separarse los grupos de servicios de información, usuarios y sistemas de información.
A.11.4.6	Control de conexión a las redes	Control En redes compartidas, especialmente aquellas que se extienden más allá de los límites de la organización, deberá restringirse la capacidad de los usuarios para conectarse a la red, conforme a la política de control de acceso y a los requisitos de las aplicaciones de negocios (ver 11.1).
A.11.4.7	Control de enrutamiento en la rede	Control Deberá implementarse el control de ruteo de redes para asegurar que las conexiones y los flujos de información de computadores no violen la política de control de acceso de las aplicaciones de negocios.
A.11.5 Control de acceso al sistema operativo Objetivo: Impedir el acceso no autorizado a los sistemas operativos		
A.11.5.1	Procedimientos seguros de conexión	Control El acceso a los sistemas operativos deberá controlarse mediante un procedimiento seguro de inicio de sesión.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios deberán tener un código de id organización único para uso personal solamente, y deberá seleccionarse una técnica de autenticación

		apropiada para fundamentar la id organización reclamada por un usuario.
A.11.5.3	Sistema de gestión de contraseñas	Control Los sistemas de manejo de contraseñas deberán ser interactivos y deberán asegurar contraseñas de calidad.
A.11.5.4	Uso de los programas utilitarios del sistema	Control El uso de programas utilitarios que podrían ser capaces de cancelar los controles de sistema y de aplicación deberá restringirse y controlarse estrictamente.
A.11.5.5	Desconexión de terminales	Control Las sesiones inactivas deberán cerrarse después de un período de inactividad definido.
A.11.5.6	Limitación del tiempo de conexión	Control Deberá usarse restricciones del tiempo de conexión para proveer seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control del acceso a las aplicaciones e información Objetivo: Impedir el acceso no autorizado a la información contenida en los sistemas de aplicaciones		
A.11.6.1	Restricción de acceso a la información	Control El acceso por los usuarios a las funciones del sistema de información y aplicaciones deberá restringirse según la política de control de acceso definida.
A.11.6.2	Aislamiento de sistemas sensibles	Control Los sistemas sensibles deberán tener un ambiente de computación dedicado (aislado).
A.11.7 Informática móvil y teletrabajo Objetivo: Asegura la seguridad de la información cuando se utilice computación móvil y actividades de teletrabajo		
A.11.7.1	Informática y comunicaciones móviles	Control Deberá existir una política formal y adoptarse medidas de seguridad adecuadas para protegerse contra los riesgos de usar facilidades móviles de computación y comunicación.
A.11.7.2	Teletrabajo	Control Deberá prepararse e implementarse una política, planes y procedimientos operativos para las actividades de teletrabajo.
A.12 Adquisición, desarrollo y mantenimiento de sistemas de información		
A.12.1 Requisitos de seguridad de los sistemas de información Objetivo: Exigir que la seguridad sea parte integral de los sistemas de información		

A.12.1.1	Análisis y especificación de los requisitos de seguridad	Control Los enunciados de requisitos de negocios para nuevos sistemas de información, o para mejoras de sistemas de información existentes, deberán especificar los requisitos para controles de seguridad.
A.12.2 Proceso correcto en aplicaciones Objetivo: Prevenir errores, pérdidas, modificación no autorizada o mal uso de la información en aplicaciones		
A.12.2.1	Validación de los datos de entrada	Control Los datos de entrada para aplicaciones deberán validarse para asegurar que estos datos son correctos y adecuados.
A.12.2.2	Control de proceso interno	Control Deberán incorporarse comprobaciones de validación en las aplicaciones, para detectar cualquier corrupción de información debido a errores de proceso o actos deliberados.
A.12.2.3	Integridad de mensajes	Control Deberán identificarse los requerimientos para asegurar la autenticidad y proteger la integridad del mensaje en las aplicaciones, así como identificarse e implementarse los controles apropiados.
A.12.2.4	Validación de datos de salida	Control Los datos de salida de las aplicaciones deberán validarse para asegurar que el procesamiento de la información almacenada es correcto y adecuado a las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información por medios criptográficos.		
A.12.3.1	Política de uso de los controles criptográficos	Control Deberá prepararse e implementarse una política sobre el uso de controles criptográficos para protección de la información.
A.12.3.2	Gestión de claves	Control Deberá efectuarse la administración de claves para apoyar el uso de técnicas criptográficas en la organización.
A.12.4 Seguridad de los archivos del sistema Objetivo: Establecer la seguridad de los archivos del sistema		
A.12.4.1	Control del software en producción	Control Deberán existir procedimientos para controlar la instalación de “software” en los sistemas operativos.

A.12.4.2	Protección de los datos de prueba del sistema	Control Los datos de prueba deberán seleccionarse cuidadosamente, y ser protegidos y controlados.
A.12.4.3	Control del acceso a la librería de programas fuente	Control Deberá restringirse el acceso al código fuente de programas.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo: Mantener la seguridad del "software" e información del sistema de aplicaciones		
A.12.5.1	Procedimientos de control de cambios	Control La implementación de cambios deberá controlarse mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de los cambios en el sistema operativo	Control Cuando se cambien los sistemas operativos, deberán revisarse y probarse las aplicaciones de negocios críticas para asegurar que no existe impacto negativo en las operaciones o seguridad de la organización.
A.12.5.3	Restricciones en los cambios a los paquetes de software	Control Deberá desalentarse las modificaciones a los paquetes de "software", limitarse a los cambios necesarios, y todos los cambios deberán controlarse estrictamente.
A.12.5.4	Fuga de información	Control Deberá evitarse las ocasiones de filtración de información.
A.12.5.5	Desarrollo externo del software	Control La organización deberá supervisar y monitorear el desarrollo de programas por terceros.
A.12.6 Gestión de vulnerabilidades técnicas Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Deberá obtenerse información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso, evaluarse la exposición de la organización a esas vulnerabilidades, y tomarse medidas adecuadas para resolver el riesgo relacionado.
A.13 Gestión de incidentes de seguridad de la información		
A.13.1 Reportando eventos y debilidades en la seguridad de la información		

Objetivo: Asegurar que los eventos y debilidades de la seguridad de la información asociadas con los sistemas de información sean comunicados de tal manera que se tomen las acciones correctivas oportunamente.		
A.13.1.1	Reportando eventos de la seguridad de información	Control Los eventos de seguridad de la información deberán reportarse por medio de los canales de gerencia apropiados tan pronto como sea posible.
A.13.1.2	Reportando debilidades de seguridad	Control Los eventos de seguridad de la información deberán reportarse por medio de los canales de gerencia apropiados tan pronto como sea posible.
A.13.2 Gestión de los incidentes y mejoras en la seguridad de información Objetivo: Verificar que se aplique un enfoque uniforme y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Deberán establecerse responsabilidades y procedimientos de gerencia para asegurar la respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendiendo de los incidentes en la seguridad de información	Control Deberán existir mecanismos en ejecución que permitan cuantificar y monitorear los tipos, volúmenes, y costos de los incidentes de seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona o organización después de un incidente de seguridad de la información involucre medidas legales (ya sea civiles o penales), deberá recolectarse, retenerse y presentarse evidencia de conformidad con las reglas de prueba establecidas en la legislación pertinente.
A.14 Gestión de la continuidad de negocios		
A.14.1 Aspectos de la gestión de continuidad del negocio en la seguridad de información Objetivo: Contrarrestar las interrupciones de las actividades de negocios y proteger los procesos de negocio críticos de los efectos de fallas o desastres mayores de los sistemas de información, y asegurar su oportuna reanudación.		
A.14.1.1	Incluyendo la seguridad de la información en la gestión de la continuidad del negocio	Control Deberá desarrollarse y mantenerse un proceso gestionado de continuidad del negocio en toda la organización, que se encargue de los requerimientos de seguridad de la información necesarios para la continuidad del negocio de la organización.

A.14.1.2	Continuidad del negocios y evaluación de riesgos	Control Deberá identificarse los eventos que pueden causar interrupciones a los procesos de negocios, junto con la probabilidad e impacto de tales interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollando e implementando planes de continuidad que incluyen la seguridad de la información.	Control Deberá prepararse e implementarse planes para mantener o restaurar las operaciones y asegurar la disponibilidad de información al nivel requerido y en las escalas de tiempo requeridas luego de la interrupción o falla de procesos de negocios críticos.
A.14.1.4	Marco de planificación de la continuidad del negocio	Control Deberá mantenerse un solo marco de planes de continuidad de negocios para asegurar que todos los planes sean concordantes, para enfocar de modo uniforme los requerimientos de seguridad de la información, y para identificar prioridades de prueba y mantenimiento.
A.14.1.5	Probando, manteniendo y reevaluando los planes de continuidad del negocio	Control Los planes de continuidad de los negocios deberán probarse y actualizarse regularmente para asegurar que estén al día y sean efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento de requisitos legales Objetivo: Evitar violaciones de cualquier ley u obligación estatutaria, de regulación o contractual, y de cualquier requisito de seguridad.		
A.15.1.1	Identificación de la legislación aplicable	Control Deberá definirse, documentarse y mantenerse al día explícitamente todos los requisitos estatutarios, de regulación y contractuales pertinentes y el enfoque de la organización para cumplirlos, para cada sistema de información en la organización.
A.15.1.2	Derechos de propiedad intelectual (DPI)	Control Deberá implementarse procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de regulación y contractuales sobre el uso del material respecto al cual puedan existir derechos de propiedad intelectual y sobre el uso de productos de “software” propietario.
A.15.1.3	Salvaguarda de los registros de la organización	Control Los registros importantes deberán protegerse de pérdida, destrucción y

		falsificación, de conformidad con los requisitos estatutarios, de regulación, contractuales y de negocios.
A.15.1.4	Protección de datos y privacidad de la información personal	Control La protección y privacidad de los datos deberá asegurarse como sea necesario mediante la legislación y reglamentos pertinentes y, si corresponde, mediante las cláusulas contractuales.
A.15.1.5	Prevención en el mal uso de las instalaciones de procesamiento de la información	Control A los usuarios se les deberá disuadir de utilizar las instalaciones de procesamiento de información para fines no autorizados.
A.15.1.6	Regulación de los controles criptográficos	Control Los controles criptográficos deberán usarse cumpliendo con todos los convenios, leyes, y reglamentos pertinentes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y del cumplimiento técnico Objetivo: Asegurar que los sistemas cumplan con las políticas y normas de seguridad de la organización		
A.15.2.1	Cumplimiento con los estándares y la política de seguridad	Control Los gerentes deberán asegurar que todos los procedimientos de seguridad dentro de sus áreas de responsabilidad se efectúan correctamente para lograr el cumplimiento de las políticas y normas de seguridad.
A.15.2.2	Comprobación del cumplimiento técnico	Control Deberá comprobarse regularmente el cumplimiento de las normas de implementación de seguridad en los sistemas de información.
A.15.3 Consideraciones sobre la auditoría de sistemas Objetivo: Maximizar la efectividad del proceso de auditoría de sistemas de información y minimizar la interferencia de dicho proceso.		
A.15.3.1	Controles de auditoría de sistemas	Control Los requerimientos y actividades de auditoría que involucren comprobaciones de los sistemas operativos deberán planearse y acordarse cuidadosamente para minimizar el riesgo de perturbaciones a los procesos de negocios.
A.15.3.2	Protección de las herramientas de auditoría de sistemas	Control Deberá protegerse el acceso a las herramientas de auditoría de sistemas de información para impedir cualquier posible mal uso o compromiso.

Anexo Nº 4: Cuadro de distribución de la Sede Central Administrativa de la MPCH

	AREA	# de Trabajadores	% de Trabajadores	
PRIMER PISO	Programa Sociales	5	3	%
	Sicología	1	1	%
	Defensoría de la Mujer	1	1	%
	Defensoría del Niño	2	1	%
	Secretaria de la DEMUNA	1	1	%
	Programa Nutricional	0	0	%
	SISFOH	4	2	%
	Control de Asistencia	4	2	%
	Remuneración de Empleados	6	4	%
	Recursos Humanos	8	5	%
	Tramite Documentario	5	3	%
	Secretaria General	5	3	%
	Bienestar Social	2	1	%
	Tecnología y Comunicaciones	9	6	%
	SUBTOTAL	**53**	**33**	%
SEGUNDO PISO	Gerencia General	5	3	%
	Relaciones Publicas	6	4	%
	Asesoría Jurídica	6	4	%
	Procuraduría	12	7	%
	Coordinación de Alcaldía	10	6	%
	SUBTOTAL	**39**	**24**	%
TERCER PISO	Administración y Finanzas	7	4	%
	Planem. Y Prog/Presup. y Estad/OPI	14	9	%
	Tesorería	16	10	%
	Contabilidad	18	11	%
	Logística	14	9	%
	SUBTOTAL	69	43	%
	TOTAL	**161**	**100**	**%**

Fuente: Gerencia de Tecnología y Comunicaciones Área de Redes – Marzo 2015

Anexo Nº 5: Glosario de términos

Con el propósito de unificar significados de algunos términos utilizados en la presente investigación, a continuación se definen las siguientes:

- Activos: recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

- Amenazas: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

- Contraseña: Una contraseña es un código o una palabra que se utiliza para acceder a datos restringidos de una computadora. Mientras que las contraseñas crean una seguridad contra los usuarios no autorizados, el sistema de seguridad sólo puede confirmar que la contraseña es válida si el usuario está autorizado a disponer de la información.

- Criptografía: Es la rama del conocimiento que se encarga de la escritura secreta, originada en el deseo humano por mantener confidenciales ciertos temas. Este procedimiento permite la transmisión de informaciones privadas por las redes públicas desordenándola matemáticamente (encriptándola) de manera que sea ilegible para cualquiera excepto para la persona que posea la “llave” que pueda ordenar (desencriptar) la información nuevamente.

- Detección de Intrusos: Sistemas utilizados para detectar las intrusiones o los intentos de intrusión; cualquier mecanismo de seguridad con este propósito puede ser considerado sistema de detección de intrusos, pero generalmente sólo se aplica esta denominación a los sistemas automáticos.

- Dirección IP: Una dirección IP es un código numérico que identifica a una computadora específica en una red de área local o Internet.

- Eficacia: Consecución de los objetivos; logro de los efectos deseados.

- Eficiencia: Logro de los fines con la menor cantidad de recursos; el logro de los objetivos al menor costo u otras consecuencias no deseadas.

- Firewalls: Una combinación de hardware y software que proporciona un sistema de seguridad, usualmente para ayudar a evitar el acceso de externos no autorizados a una red interna o Intranet.

- Gestión: Es el proceso mediante el cual se obtiene, despliega o utiliza una variedad de recursos básicos para apoyar los objetivos de la organización.

- Hacker: Persona que obtiene acceso no autorizado a una red de computación para obtener provecho, realizar actos delictivos o por placer personal.

- Información: La información es el resultado de haber organizado o analizado los datos de alguna manera y con un propósito.

- Intrusión: Se denomina intrusión a un conjunto de acciones que intentan comprometer la integridad, confidencialidad o disponibilidad; además una intrusión no tiene por qué consistir solo en un acceso no autorizado a una máquina, también puede ser una negación de servicio, es decir dejar sin funcionamiento al sistema informático.

- Mecanismo de Salvaguarda: procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

- Política de seguridad de la información: Una política de seguridad de la información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el

propósito de proteger la información, los recursos y la reputación de la misma.

- Permisos: Regla asociada con un objeto, como un archivo, para regular qué usuarios pueden obtener acceso al objeto y de qué manera. El dueño del objeto otorga o niega los permisos.

- Riesgo: posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la organización

- Redes informáticas: Están formadas por conexiones entre grupos de computadoras y dispositivos asociados que permiten a los usuarios la transferencia electrónica de información.

- Red inalámbrica: una red inalámbrica posibilita la unión de dos o más dispositivos sin la medición de cables. Es una red en la cual los medios de comunicación entre sus componentes son ondas electromagnéticas.

- Seguridad: Es la protección de los activos frente acciones o situaciones no deseadas mediante la implantación de controles.

- Sistema de información: Se puede definir como un conjunto de componentes interrelacionados que reúne, procesa, almacena y distribuye información para apoyar la toma de decisiones y el control de la organización.

- Servicios críticos: Son los servicios de redes, sistemas y comunicaciones y de apoyo que brinda la MPCH y que manejan información muy valiosa como los datos financieros y presupuestal, base de datos, sistemas informáticos, etc.

- Software Antivirus: Es el software diseñado específicamente para la detección, eliminación y prevención de virus informáticos.

- Sistema Operativo: Un sistema operativo (SO) es un conjunto de programas software que permite comunicar al usuario con una computadora y gestionar sus recursos de manera cómoda y eficiente. Comienza a trabajar cuando se enciende el ordenador, y gestiona el hardware de la máquina desde los niveles más básicos. Hoy en día un sistema operativo se encuentra normalmente en ordenadores o productos electrónicos como teléfonos móviles.

- Tecnologías de la Información y Comunicaciones (TIC): Es un término que se utiliza actualmente para hacer referencia a una gama amplia de servicios, aplicaciones, y tecnologías, que utilizan diversos tipos de equipos y de programas informáticos, y que a menudo se transmiten a través de las redes de telecomunicaciones.

- Usuario: Persona que accede a los recursos y servicios que ofrece una red informática. Puede ser un trabajador o tercero.

- Virus informático: Un virus informático es un programa creado especialmente para invadir computadores y redes y crear el caos. El daño puede ser mínimo, como hacer aparecer una imagen o un mensaje en la pantalla, o puede hacer mucho daño alterando o incluso destruyendo archivos dentro de la computador.