UNIVERSIDAD AUTÓNOMA DEL ESTADO DE MÉXICO

Centro Universitario UAEM Texcoco

LICENCIATURA EN INFORMÁTICA ADMINISTRATIVA

"MANUAL PARA LA APLICACIÓN DEL ESTÁNDAR ISO/IEC 27001 (SEGURIDAD DE LA INFORMACIÓN)"

T E S I N A

QUE PARA OBTENER EL TITULO DE:

LICENCIADO EN INFORMÁTICA ADMINISTRATIVA

P R E S E N T A:

NELLY CÁRDENAS GUILLEN

DIRECTOR:
M. EN C. LETICIA ARÉVALO CEDILLO

REVISORES:
ING. JOSÉ ROBERTO RAMÍREZ CERVANTES
ING. FÉLIX RAMÍREZ CERVANTES

ESTADO DE MÉXICO

Texcoco México a 8 de Noviembre de 2013

M.ENC. JUAN MANUEL MUÑOZ ARAUJO
SUBDIRECTOR ACADEMICO DEL
CENTRO UNIVERSITARIO UAEM TEXCOCO.
PRESENTE:

AT´N M. EN P.P. ANTONIO INOUE CERVANTES
RESPONSABLE DEL DEPARTAMENTO DE TITULACION.

Con base en las revisiones efectuadas al trabajo escrito titulado "Manual para la aplicación del estándar ISO/IEC 27001 " que para obtener el título de Licenciado en Informática Administrativa presente la sustentante Cárdenas Guillen Nelly, con número de cuenta 0825871 respectivamente, se concluye que cumple con los requisitos teorico-metodologicos por lo que se le otorga el voto aprobatorio para su sustentación, pudiendo continuar con la etapa de digitalización del trabajo escrito.

ATENTAMENTE

Ing. Fernando Robles Gil

Ing. José Roberto Ramírez Cervantes

M. en C. Arévalo Cedillo Leticia

TITULACION
RECIBIDO
COPIA
Texcoco, Méx., a 08 de 11 del 2013

AGRADECIMIENTOS Y DEDICATORIAS

A dios por permitirme estar aquí concluyendo una nueva etapa en mi vida.

A mis hijos que le dan la razón y la chispa perfecta a una vida que vivo solo por ellos y para ellos, gracias mis peques por ser el motor de mi vida.

A mis hermanos sin los cuales seguramente nunca hubiera descubierto el camino, se que nunca podría levantarme sin su ayuda, mil gracias por estar siempre en los momentos más importantes y más divertidos, los amo queridos “sol y luna”.

A mis padres, en especial a madre quien me ha demostrado que nunca se cansara amarme a pesar de todo y sé que ella es quien agradecerá mas el que yo esté aquí.

A mis amados sobrinos a quienes solo por tanto amar no podía dejar de mencionar.

A mis profesores que me ayudaron de todas las maneras posibles e imposible a la culminación de este trabajo.

A cualquier persona que se tome el tiempo de leerlo ya sea para juzgarla, criticarla o como apoyo “Gracias”.

ÍNDICE GENERAL

I INTRODUCCIÓN

La seguridad de la información es un tema importante dentro de una organización sin importar el giro que tenga o su tamaño, involucra las medidas tanto preventivas como reactivas que se incluyen al resguardar información confidencial o su tratamiento dentro de la empresa.

Dado ese panorama tan delicado es que se tiene que buscar un método que garantice a los agentes externos de la empresa la confianza del resguardo que se da a los datos que le ha proporcionado.

Dos ejemplos de instituciones mexicanas que se encuentran certificadas bajo ISO / IEC 27001 es el área de informática y estadística de la operación del Programa de Resultados Electorales Preliminares (PREP) y la Contraloría General ambas del IEEM las cuales desde el 12 de septiembre del 2012 y el 2011 respectivamente cuentan con la susodicha certificación, siendo las primera instituciones electorales en México que se certifican.

El presente proyecto de investigación permitirá al lector conocer sobre el estándar de calidad en la seguridad informática, ya que hoy en día, la seguridad en todo lo que implica este tema es de suma importancia el conocer y saber cómo prevenir y controlar riesgos con información que es la parte vital de una organización, independientemente del giro de esta.

La estructura de la tesina que se presenta, cuenta con tres capítulos que permite su fácil comprensión del tema. En el capítulo 1 se habla sobre las generalidades de un estándar y por supuesto nos conlleva al capítulo 2 en el que se describe la norma ISO / IEC 2700, considerando que esta norma es muy amplia y que en este trabajo solo se habla en particular de la 27001, para con ello guiarnos en el capítulo 3 en un manual que interpreta a la norma en cuestión, mostrando cuadros descriptivos sobre ésta.

II. PLANTEAMIENTO DEL PROBLEMA

En el 2010 en México se puso en marcha la Ley de protección y Privacidad de la información dando como resultado que las empresas buscaran una certificación la cual les permitiera garantizar que la información manejada en la empresa está siendo tratada de manera adecuada y al mismo tiempo cumplan con lo dispuesto en la ley.

Adquirir una certificación para la seguridad de la información no es fácil ya que las empresas no cuentan con los conocimientos necesarios y surgen preguntas como ¿Donde podría adquirirlo?, ¿Qué abarca esta norma?, ¿Qué beneficios obtiene una empresa al certificarse bajo este lineamiento? este trabajo pretende aclarar este tipo de dudas para poder realizar una certificación teniendo conocimientos previos sirviendo de guía antes y durante la certificación.

III. JUSTIFICACIÓN

Datos del INEGI tomados en el año 2009 revelan que en México existen 5.144.05 empresas de las cuales 36 se encuentran certificadas por ISO/IEC 27001, esto pareciera poco sin embargo cada año aumentan el número de empresas certificadas en esta norma; resultados tomados de encuestas realizadas por ISO sobre las empresas Mexicanas muestran un aumento significativo en la certificación de normas ISO / IEC 27001 para la seguridad de la información del 12% en el 2010. En México tan solo en el 2011 las empresas certificadas en ISO 27001 fueron casi el doble comparadas con el año 2008, lo que nos dice que las empresas están haciendo conciencia en cuanto a la seguridad de su información.

En la actualidad las empresas se enfrentan al reto que resulta una certificación ya que no basta con conocer la norma como una oportunidad de crecimiento y mejora en la organización, habrá que contar con una guía que ayude a la implementación de un sistema de seguridad beneficiando a toda aquella organización que desee adquirir una certificación específicamente en seguridad de la información, dando pauta a la competitividad, crecimiento, control de la empresa esto para poder entender el funcionamiento y la terminología utilizada, minimizando los esfuerzos, así como aclaración de las dudas más comunes que se tiene al implantar esta certificación invitando a que mas organismos no solo conozcan sino aprendan a utilizar una certificación en ISO/IEC 27001.

IV. OBJETIVOS

Objetivo general

Generar un manual de aplicación sobre el estándar ISO/IEC 27001 en el que se indique como funciona y aclare las dudas que puedan surgir al adquirir este estándar.

Objetivos específicos

1. Conocer las generalidades de la seguridad de la información
2. Investigar las generalidades del estándar ISO/IEC 27001
3. Desarrollar un manual que permita aplicar el estándar ISO/IEC 27001.

Capítulo I. Generalidades del Estándar de Gestión

1.1 ¿Qué es ISO?

ISO es el mayor desarrollador de estándares reconocido a nivel mundial creada en 1947, su finalidad es promover el desarrollo de la estandarización y actividades relacionadas para desarrollar la cooperación en la esfera del ámbito intelectual, científico, tecnológico y económico. ISO no tiene fines lucrativos, facilita el intercambio de bienes y servicios a nivel mundial.

En la actualidad ISO ha publicado más de 19 500 normas internacionales, cuenta con miembros de 163 países. La secretaría central se encuentra en Ginebra, Suiza y es quien coordina el sistema [3].

1.1.1 Historia de ISO

ISO se deriva del griego "isos", que significa igual. Los fundadores decidieron darle la forma corta ISO. Se puede decir que una manera rápida y corta es "Organización Internacional de Normalización".

La historia ISO comenzó en 1946 cuando los delegados de 25 países se reunieron en Londres y decidieron crear una nueva organización internacional *"para facilitar la coordinación y unificación de normas industriales internacionales"*. En febrero de 1947 comenzó oficialmente sus operaciones.

ISO nació de la unión de dos organizaciones. Uno era el ISA (Federación Internacional de las Asociaciones Nacionales de Normalización), establecido en Nueva York en 1926, y administrada desde Suiza. El otro fue el UNSCC (Comité Coordinador de Normas de las Naciones Unidas), establecido hasta 1944 y se administra en Londres.

1.2 ¿Qué es IEC?

La Comisión Internacional de Electrotecnia (IEC) es una organización de normalización, publica las técnicas pertinentes a nivel mundial que permitan a millones de dispositivos y sistemas que utilizan, producen o almacenan electricidad, funcionar con seguridad juntos en cualquier lugar del mundo. IEC no es gubernamental y no tiene fines de lucro.

Este organismo normaliza la amplia esfera de la electrotécnica, desde el área de potencia eléctrica hasta las áreas de electrónica, comunicaciones, conversión de la energía nuclear y la transformación de la energía solar en energía eléctrica.

Esencialmente la IEC enfoca su atención a la existencia de un lenguaje técnico universal, que comprenda definiciones, símbolos eléctricos y electrónicos o unidades de medición, rangos normalizados, requisitos y métodos de prueba, características de los sistemas como tensión e intensidad y frecuencia, requisitos dimensionales, requisitos de seguridad eléctrica, tolerancias de componentes de equipo eléctrico y electrónico, entre otros.

A diferencia de ISO, IEC se enfoca a los campos de la electrónica y tecnologías relacionadas. A la fecha la IEC cuenta con 82 miembros, cada uno de ellos representando a un país.

1.2.2 Historia de IEC

Fue creado en 1906, cuya sede se encuentra en Ginebra, Suiza. Fundada como resultado del Congreso Eléctrico Internacional que se llevó a cabo en la ciudad de St. Luis, USA en 1904. Durante el mismo fue tomada una resolución que señaló la necesidad de crear una comisión mundial que desarrollara y publicara normas para el sector eléctrico, electrónico y las tecnologías relacionadas con los mismos.

El trabajo de la IEC es llevado a cabo por Comités Técnicos, Subcomités y su trabajo se refleja finalmente como normas internacionales o guías.

1.3 ¿Cómo se desarrolla un estándar?

Un estándar es un documento establecido por consenso, aprobado por un cuerpo reconocido, y que ofrece reglas, guías o características para que se use repetidamente.

México ha implementado el Sistema Nacional de Normalización, Metrología y Sistema de evaluación de la conformidad, que es coordinado por la DGN (*Dirección General de Normas*).

DGN es responsable de coordinar el sistema de normalización y evaluación de la conformidad, para fomentar la competitividad de la industria y el comercio en el ámbito nacional e internacional.

- Participa en las organizaciones internacionales y otros foros pertinentes para representar los intereses de los sectores nacionales.
- Coordina la elaboración de los reglamentos nacionales y las normas de su competencia.
- Autoriza a las entidades de acreditación y supervisa su trabajo, así como el cumplimiento de los reglamentos bajo la responsabilidad de DGN.

Los estándares existen gracias a que un grupo de gobierno ampliamente reconocido (en la mayoría de los casos de ámbito mundial) ha llegado a un acuerdo sobre un conjunto específico de principios o protocolos y los ha publicado para que todo el mundo pueda utilizarlos. Los estándares son establecidos normalmente por comités que trabajan bajo diversas organizaciones de comercio e internacionales.

Otros estándares menos técnicos definen que actividades deberían implementarse y, a menudo, añaden un código de prácticas para determinar qué nivel deberían alcanzar estas actividades. El órgano de estándares internacionales más predominante es ISO que cuenta con organizaciones miembros en cada país desarrollado en el mundo.

La ISO opera en Europa junto con la IEC por lo que la nomenclatura correcta para los estándares es ISO/IEC xxxxx. Este número de estándares normalmente va seguido por el año de publicación. De esta forma se informa de la versión del estándar.

La IEC tiene grupos de cooperación mutua con la ISO y con la ITU (*Unión Internacional de Telecomunicaciones*) entre otros, así como grupos conjuntos de trabajo tales como el JTC 1 "Tecnología de la información".

La principal tarea de estos grupos conjuntos de trabajo o comités técnicos es preparar las normas internacionales, los organismos nacionales votan y la publican como norma internacional con al menos 27 votos.

En la actualidad, nuestro país es miembro pleno de la IEC a través del CEM (*Comité Electrotécnico Mexicano*) quien representa a IEC en México [4].

Entre las actividades de la CEM se encuentran:

- Coordinar la participación de México en los trabajos y reuniones de la IEC.
- Promover la cooperación internacional en todos los aspectos relacionados con la normalización integral en los campos antes citados.
- Difundir en el país los trabajos y las normas de la IEC.

1.4 La acreditación

Acreditación es el acto que da la seguridad y avala que los laboratorios (calibración, ensayo y /o clínicos), organismos de inspección, organismos de certificación, proveedores de ensayos de aptitud y a los organismos verificadores/validadores de emisión de gases efecto Invernadero, ejecuten las regulaciones, normas o estándares correspondientes con

precisión para que comprueben, verifiquen o certifiquen los productos y servicios que consume la sociedad.

Los organismos de acreditación de cada país están abiertos a cualquier entidad, tanto pública como privada y sin ánimo de lucro, por tanto objetivamente independientes de las empresas de certificación, lo cual conlleva a tener resultados reales, sabiendo que si una empresa es acreditada es gracias a que cumplió con los requisitos puestos por los organismos de acreditación.

En algunos países existen varios proveedores de servicios de acreditación, en México existe solo uno la EMA (Entidad Mexicana de Acreditación). EMA es la primera entidad de gestión privada en México que acredita a los organismos de la evaluación de conformidad como son los laboratorios de ensayo, laboratorios de calibración, laboratorios clínicos, unidades de verificación (organismos de inspección) y organismos de certificación.

EMA brinda la acreditación a todas aquellas certificadoras mexicanas que deseen ofrecer un servicio de certificación en producto, personas y sistemas de gestión. Se evalúa regularmente a las entidades acreditadas, mediante visitas de seguimiento y auditorías de reevaluación. La organización que desee una acreditación tiene que ser legalmente identificable.

En México DGN autoriza a las entidades de acreditación y supervisa su trabajo.

La norma que EMA brinda a los organismos de certificación para su acreditación es NMX-EC-17021-IMNC-2008 ISO/IEC 17021: 2006 Evaluación de la conformidad-Requisitos para los organismos que realizan la auditoria y certificación de sistemas de gestión [http://www.economia.gob.mx/comunidad-negocios/competitividad-normatividad/normalizacion/normalizacion-internacional/iec].

1.4.1 Pasos para la acreditación

- Envió de solicitud y documentación.- La certificadora interesada deberá realizar una solicitud y enviarla a la acreditadora quien le brindara una serie de formatos que deberá llenar y enviar junto con la documentación correspondiente.
- Revisión de documentos.- La acreditadora revisa que los documentos estén completos, en orden y que cumpla con los requerimientos que la ley imponga para su funcionamiento. En caso de que la documentación no sea la adecuada la

certificadora deberá llenarlos nuevamente y solo entonces podrá continuar con la acreditación.

- Designación del equipo auditor.- La acreditadora asignará al equipo auditor y a un jefe auditor, en caso de que la entidad tenga algún motivo por el cual piense que la auditoria podría ser imparcial llenará una solicitud expresando los motivos de su inconformidad y se le asignara otro equipo. Se asignará una fecha y se le indicará los puntos que deberá llenar para la acreditación.
- Auditoría.- Durante la auditoría se evaluará a la certificadora y su funcionamiento.
- Informe de la evaluación.- El equipo auditor realiza un informe detallado y lo emite a la entidad quien realizara todas las correcciones necesarias hasta que el equipo auditor apruebe las correcciones.
- Emisión del certificado.- Al ser aprobadas las correcciones por el equipo auditor, éste manda el informe con la autorización a la acreditadora quien emite el certificado de aprobación en el que la entidad puede hacer uso de la marca de la acreditación aceptando evaluaciones regulares por medio de auditorías de reevaluación.

La figura 1 muestra un diagrama de flujo que sirve de guía para la acreditación.

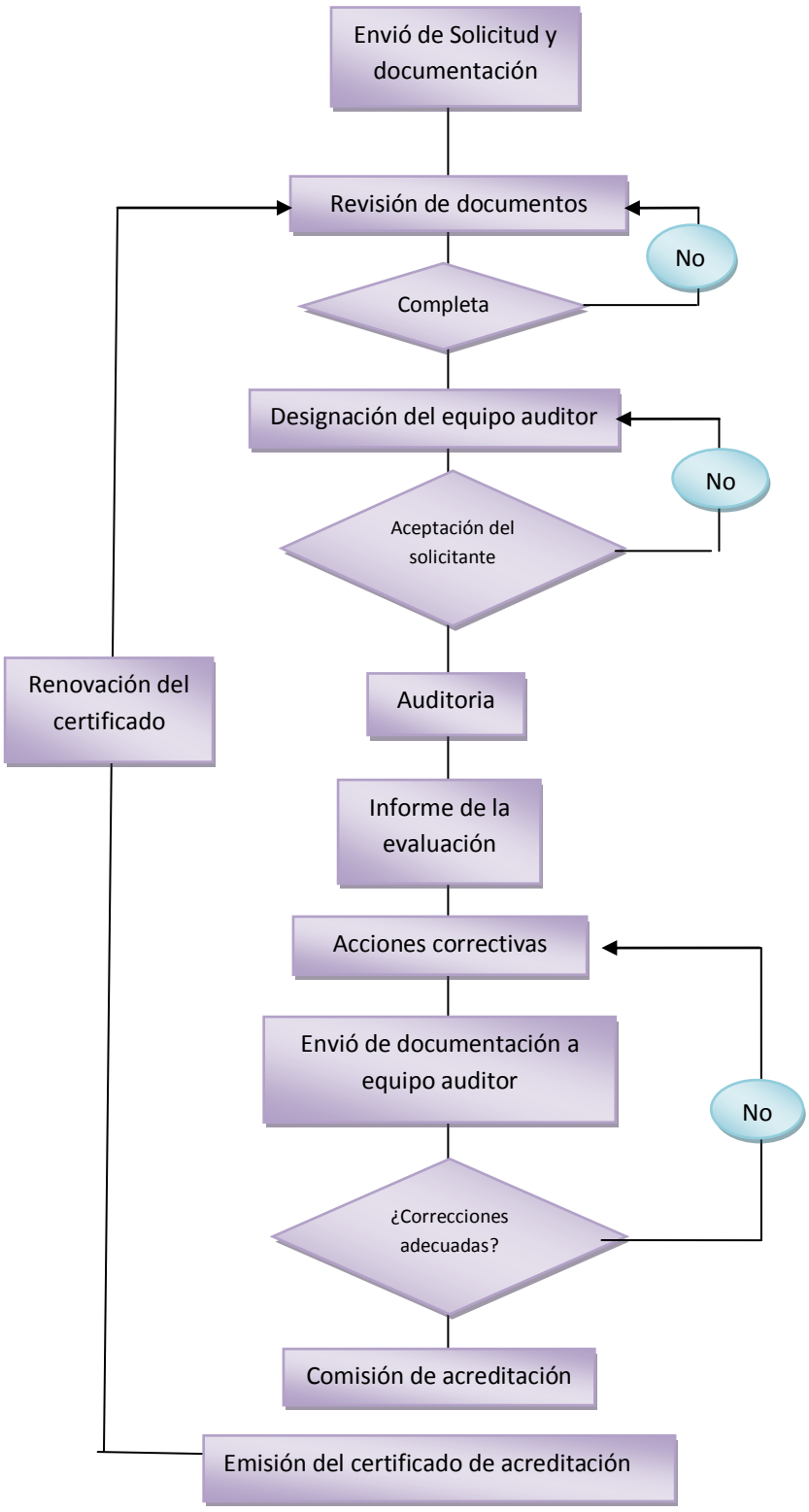


Figura 1. Guía de acreditación

1.5 La certificación

La certificación es la acción llevada a cabo por una entidad reconocida como independiente de las partes interesadas mediante la que se manifiesta la conformidad de una empresa, producto, servicio, proceso o persona con los requisitos definidos en normas o especificaciones [http://www.iso.org/iso/home/standards/certification.htm.]

Las entidades de certificación deben ser acreditadas por algún organismo de acreditación y para ello deben cumplir a su vez con unos requisitos marcados por las directivas correspondientes.

El procedimiento de certificación demuestra la capacidad de la empresa para producir un producto o prestar un servicio y da respuesta a la necesidad de generar la confianza del cliente respecto del producto o servicio que recibirá de la empresa suministradora.

El procedimiento de certificación evalúa que:

1.- El producto responde a sus especificaciones.
2.- La empresa fabrica siempre de la misma forma.

En México existen tres instituciones capaces de brindar una certificación ISO/IEC 27001.

- AENOR México. [http://www.aenormexico.com/]
- American Trust Requister, S.C. [http://www.americantrust.com.mx/]
- Normalización y Certificación Electrónica S.C. (NYCE) [http://www.nyce.org.mx/]

1.5.1 Pasos para la certificación

Los pasos para la certificación son muy similares a la acreditación, sin embargo hay que tener en cuenta que los objetivos son muy distintos en ambos casos.

- Envió de solicitud y documentación.- La empresa interesada deberá realizar una solicitud y enviarla a la certificadora quien le brindará una serie de formatos que deberá llenar y enviar junto con la documentación correspondiente.
- Revisión de documentos.- La certificadora revisa que los documentos estén completos, en orden y que cumpla con los requerimientos. En caso de que la documentación no sea la adecuada la empresa deberá llenarlos nuevamente y solo entonces podrá continuar con la certificación.

- Designación del equipo certificador.- La certificadora asignará al equipo auditor y a un jefe auditor, en caso de que la empresa tenga algún motivo por el cual piense que la auditoria podría ser imparcial llenará una solicitud expresando los motivos de su inconformidad y se le asignará otro equipo. Se asignará una fecha y se le indicará los puntos que deberá llenar para la certificación.
- Auditoria.- Durante la auditoria se evaluara el sistema gestor y su funcionamiento.
- Informe de la evaluación.- El equipo auditor realiza un informe detallado y lo emite a la entidad quien realizara todas las correcciones necesarias hasta que el equipo auditor apruebe las correcciones.
- Emisión del certificado.- Al ser aprobadas las correcciones por el equipo auditor, este manda el informa con la autorización a la certificadora quien emite el certificado de aprobación en el que la entidad puede hacer uso de la marca de la certificadora, aceptando evaluaciones regulares por medio de auditorías de reevaluación.

La figura 2 muestra un diagrama de flujo que sirve de guía para la certificación.

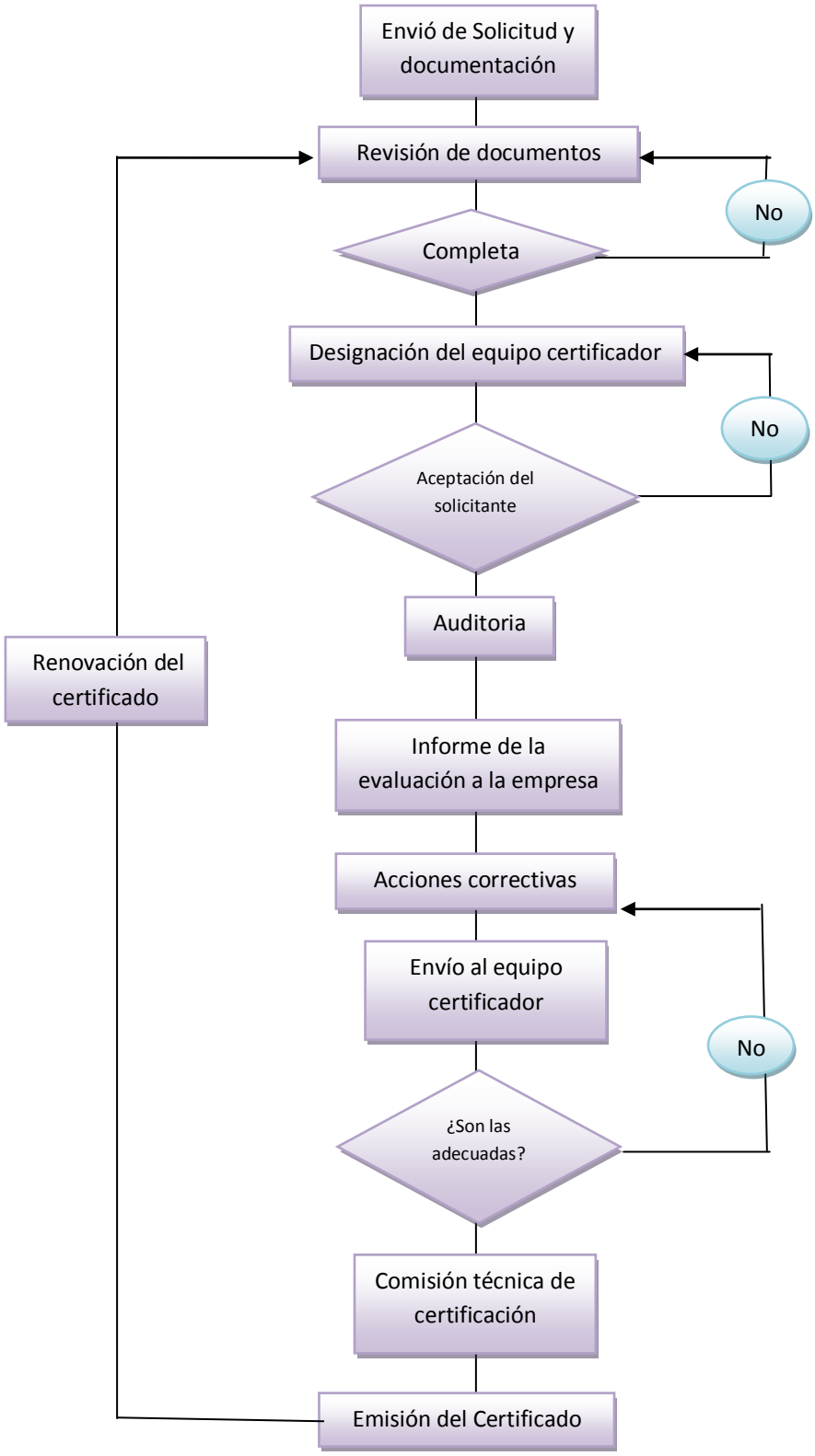


Figura 2 Guías para la certificación

Capítulo II Seguridad informática y la ISO 27001

2.1 Conceptos Generales de Seguridad Informática

Antes de iniciar con este tema tan importante y que es el la parte vital del presente trabajo escrito, es necesario que se muestren algunos conceptos que encuadran el marco teórico de esta tesina.

2.1.1 Seguridad

Según la Real Academia Española, "seguridad se refiere a estar libre y exento de todo peligro, daño o riesgo".

Según Leonard H. Fime, seguridad de centros de cómputo Políticas y procedimientos [1], la seguridad depende, en última instancia, de la integridad de los individuos que conforman una institución. No existe la seguridad total y cada institución depende de su personal para lograr los niveles de seguridad requeridos.

Partiendo de estas definiciones concluyo entonces que la seguridad general no pude existir siendo esta solo un intento por minimizar el riesgo o impacto a fin de causar el menor daño posible, buscando que sea una seguridad confiable más que absoluta.

2.1.2 Seguridad informática

Disciplina que se ocupa de diseñar las normas, métodos y técnicas destinados a conseguir un sistema de información lo más seguro posible.

2.1.3 Seguridad de la información

De acuerdo a la norma ISO 27000, se define como preservación de la confidencialidad, integridad y la disponibilidad de la información, en adición también de otras propiedades como autenticación, autorización, registro de actividad, no repudio y confiabilidad pueden ser también consideradas.

2.2 Sistema de Gestión de Seguridad de la Información (SGSI)

Un SGSI es un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la organización. Consta de las políticas, procedimientos, pautas y recursos asociados y actividades de gestión colectiva de una organización, en la búsqueda de la protección de sus activos de información.

2.3. Familia ISO/IEC 27000

La familia de estándares ISO/IEC 27000 se compone de 19 estándares publicados hasta el año 2013, en el cuadro 1 se da una breve descripción de cada uno de ellos.

ESTÁNDAR	CONTENIDO
ISO/IEC 27000: 2009	Proporciona una visión general de las normas que componen la serie 27000, términos y definiciones que se emplean en toda la serie 27000.
ISO/IEC 27001: 2005	Especifica los requisitos para establecer, implementar, operar, monitorizar, revisar, mantener y mejorar un SGSI (*Sistema de Gestión de la Seguridad de la información*) documentado, en el contexto de los riesgos del negocio globales de la organización. Esta es la más importante de toda la serie de ISO 27000.
ISO/IEC 27002: 2005	Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
ISO/IEC 27003: 2010	Es una guía que se centra en los aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI *(Sistema de Gestión para la Seguridad de la Información)* de acuerdo ISO/IEC 27001:2005.
ISO/IEC 27004: 2009	Es una guía para el desarrollo y utilización de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles o grupos de controles implementados según ISO/IEC 27001.
ISO/IEC 27005: 2011	Está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos.
ISO/IEC 27006: 2011	Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los SGSI.
ISO/IEC 27007: 2011	La norma abarca los aspectos específicos del SGSI de la auditoría de cumplimiento y se centra en la auditoría del sistema de gestión.
ISO/IEC 27008: 2011	Esta norma sobre SGSI "auditoría técnica" complementa la norma ISO / IEC 27007. Se concentra en la auditoría de los controles de seguridad de la información.
ISO/IEC 27010: 2012	Es una norma en 2 partes, que consiste en una guía para la gestión de la seguridad de la información en comunicaciones inter-sectoriales.
ISO/IEC 27011: 2008	Guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

ISO/IEC 27013: 2012	Guía de implementación integrada de ISO/IEC 27001 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).
ISO/IEC27015: 2012	Directrices de gestión de seguridad de información para los servicios financieros.
ISO/IEC 27031: 2011	Directrices para la preparación de la información y las comunicaciones para la continuidad del negocio.
ISO/IEC 27032: 2012	Proporciona orientación para mejorar el estado de seguridad cibernética.
ISO/IEC 27034: 2011	Guía para ayudar en las organizaciones en la integración de la seguridad en los procesos utilizados en la gestión de sus aplicaciones.
ISO/IEC 27035: 2011	Estándar para la Gestión de Incidentes de Seguridad de la Información.
ISO/IEC27037: 2012	Proporciona directrices para las actividades específicas en el manejo de la evidencia digital potencial.
ISO/IEC27799: 2008	Es una norma que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes. Esta norma, al contrario que las anteriores, no la desarrolla el subcomité JTC1/SC27, sino el comité técnico TC 215.

Cuadro 1 Breve descripción de la familia ISO/IEC 27000

2.4. Historia de ISO/IEC 27001

La norma ISO/IEC 27001 es creada en 1987 por la fundación del centro nacional de informatica del Reino Unido, con el objetivo de establecer un criterio de evaluación internacional en relación con la seguridad de las tecnologias de informacion y ayudar a los usuarios mediante un codigo de prácticas.

En 1993 es mejorado por el NCC (*Centro Nacional de Computacion*) y publicado como PD0003 un codigo de practicas para la gestión de la seguridad de la información.

En 1995 se adopta como estandar Británico de buenas prácticas denominado como BS 7799.

En 1998, la segunda parte de la BS 7799 se publica como BS 7799-2 el cual contenía una guía para la implantación de un SGSI (*Sistema de Gestion de Seguridad de la informacion*), siendo certificable a nivel Nacional. En el 2005 es certificable por la ISO dándola a conocer como 27001:2005.

La primera parte de la BS 7799 se publica como BS 7799-1 y resulta una guía de buenas prácticas no certificable. En el año 2000 pasa a ser parte de la ISO, lo que le da

certificación a nivel mundial y cambia su nombre a ISO 17799. En el 2005, es nuevamente revisada y en año 1997 es renombreda a ISO 27002:2005.

Se tiene también que considerar que ISO al ser una institución a nivel mundial pone a revisión sus normas cada cierto tiempo, haciéndolas extensas y completas provocando cambios significativos en las normas, lo que las hace bastante confiables ya que si bien es cierto que la tecnología cambia constantemente, también lo hacen los medios que brindan ayuda para proteger lo más valioso que una organización puede tener: la información.

2.5 Descripción de la familia ISO/IEC 27000 y como se relacionan.

2.5.1 ISO/IEC 27000

Esta norma contiene une serie de definiciones que ayudan a la implementación de un SGSI evitando duplicidades y malos entendidos en la implementación de ISO/IEC 27001, dando a todo el modelo un lenguaje común, evitando la ambigüedad y duplicidad de terminología utilizada en normas anteriormente publicadas, ayudando al entendimiento y la comprensión de la familia de ISO/IEC 27000.

A continuación se dan a conocer una lista de los términos más utilizados durante la implementación del estándar ISO/IEC 27001.

- Activo.- Cualquier elemento que tenga valor para la organización.
- Autenticidad.- Propiedad de que una entidad es lo que dice ser.
- Disponibilidad.- Propiedad de ser accesible y utilizable a petición por una entidad autorizada.
- Confidencialidad.- Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos.
- Confidencialidad.- Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos.
- Conformidad.- Cumplimiento de un requisito.
- Eficacia.- Resultados a medida que se realizan las actividades planificadas y previstas alcanzados.
- Eficiencia.- Relación entre los resultados obtenidos y los recursos utilizados.
- Seguridad de la información: Preservación de la confidencialidad, integridad y la disponibilidad de la información; además, otras propiedades, tales como autenticidad, la responsabilidad, no repudio y fiabilidad también pueden estar involucrados.

- Integridad.- Propiedad de la protección de la exactitud e integridad de los activos. SGSI: Proyecto actividades estructuradas llevadas a cabo por una organización para implementar un SGSI.
- Sistema de gestión.- Marco de las directrices, políticas, procedimientos, procesos y los recursos asociados destinada a garantizar una organización cumple con sus objetivos.
- Política.- Intención y dirección general como se expresan formalmente por la dirección.
- Procedimiento.- Forma especificado para llevar a cabo una actividad o un proceso.
- Proceso.- Conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados.
- Confiabilidad.- Característica de un comportamiento coherente previsto y resultado Gestión de riesgos.- Actividades coordinadas para dirigir y controlar una organización en lo que respecta al riesgo.
- Proceso de gestión del riesgo.- Aplicación sistemática de políticas de gestión, los procedimientos y de las prácticas a las actividades de comunicación de riesgos, consultoría, estableciendo el contexto y la identificación, análisis, evaluación, tratamiento, seguimiento y revisión.
- Amenaza.- Causa potencial de un incidente no deseado.
- Validación.- Confirmación, mediante la aportación de evidencia objetiva, de que los requisitos para un uso específico previsto o aplicación que se hayan cumplido.
- Vulnerabilidad.- Debilidad de un activo o de control que puede ser explotado por una o más amenazas.
- Política.- Intención y dirección general expresada formalmente por la gerencia Riesgo.- Combinación de la probabilidad de un evento y su ocurrencia.
- Análisis del riesgo.- Uso sistemático de la información para identificar las fuentes y calcular el riesgo.

El enfoque basado en procesos en la familia de normas de SGSI se basa en el principio de funcionamiento adoptado en las normas ISO de sistemas de gestión comúnmente conocido por sus siglas en ingles como PDCA que significa Plan - Do - Check - Act (Planeación, Implementación, Revisión y Mantenimiento), *Ver figura 3*.

a) Plan.- Establecer objetivos y hacer planes, analizar la situación de la organización, establecer los objetivos generales y las metas establecidas, y desarrollar planes para alcanzarlos.
b) Implementación.- Implementar planes.
c) Revisar.- Resultados de monitorear el grado de los logros del cumplimiento con los objetivos previstos.

d) Mantenimiento.- Corregir y mejorar las actividades, aprender de los errores para mejorar las actividades para lograr mejores resultados.

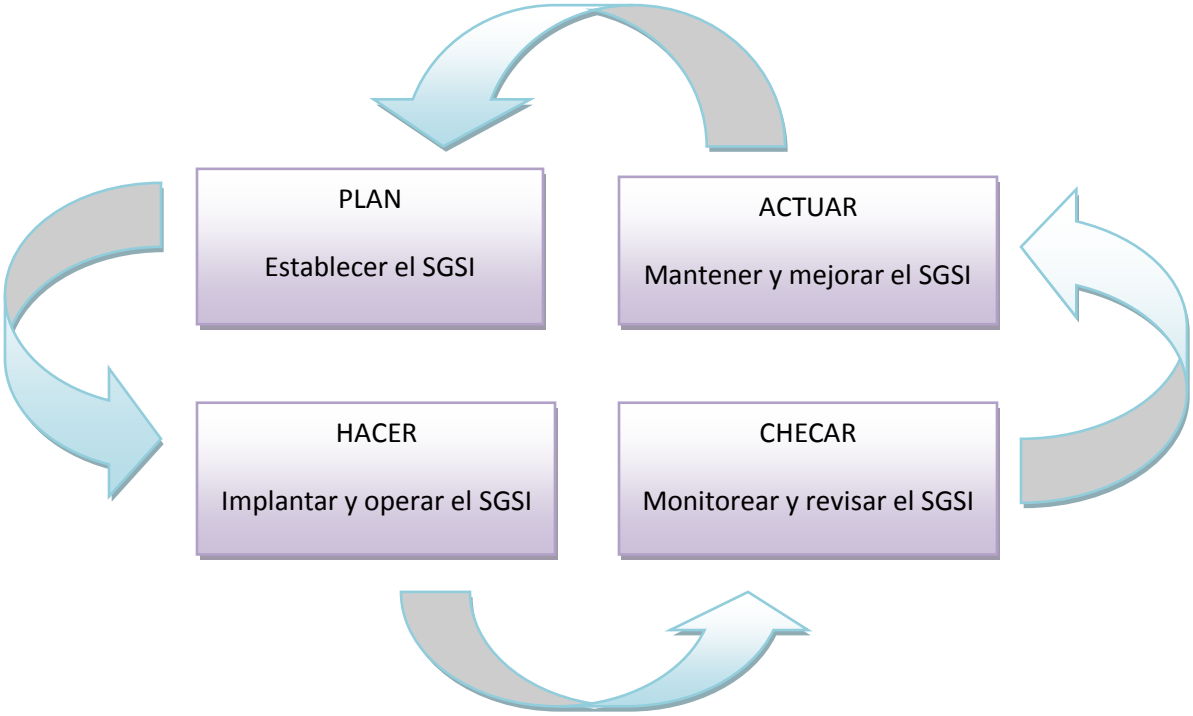


Figura 3 Fases del modelo PDCA

2.5.2 ISO/IEC 27002

Proporcionan una guía general basada en objetivos comúnmente aceptados para la gestión de la seguridad de la información. Esta norma establece principios generales para el comienzo, la implantación, el mantenimiento y la mejora de la gestión de la seguridad de la información en una organización.

En esta norma se dan a conocer aspectos como la documentación y la revisión para su mejoramiento de las políticas en la seguridad de la información. La forma en cómo se organiza la seguridad de la información de manera interna, el compromiso de la dirección con la seguridad de la información.

2.5.3 ISO/IEC 27003

Permite realizar una planeación clara para de cómo implementar la ISO 27001 en sus numeral 4,5, y 7, y definir las estrategias de seguridad relacionadas con el negocio acorde con los requisitos de ISO 27001.

Ayudará a las organizaciones a implementar un SGSI, principalmente enfocado en las clausulas 4,5 y 7 de estándar.

4. Sistema de gestión de la seguridad de la información
5. Responsabilidad de la dirección
7. Revisión del SGSI por la dirección

2.5.4 ISO/IEC 27004

Es una estructura que enlaza los atributos medibles con una entidad relevante. Estas entidades, incluyen procesos, productos, proyectos y recursos. Este modelo debe describir cómo estos atributos son cuantificados y convertidos a indicadores que provean bases para la toma de decisiones, sustentados en necesidades de información específica.

Se debe desarrollar un programa de cómo ejecutar la medición de la seguridad de la información. El éxito de este programa, se basará en la asistencia o ayuda que estas mediciones aporten para adoptar decisiones o determinar la eficiencia de los controles de seguridad.

Una organización debe describir cómo se interrelacionan el SGSI y las mediciones, desarrollando guías que aseguren, aclaren y documenten esta relación, con todo el detalle posible.

Los métodos de medición pueden abarcar varios tipos de actividades y un mismo método puede aplicar a múltiples atributos. Algunos ejemplos de métodos son:

- Encuestas/indagaciones
- Observación
- Cuestionarios
- Valoración de conocimientos
- Inspecciones
- Consulta a sistemas de información
- Muestreo

2.5.5 ISO/IEC 27005

Se basa en el análisis de riesgo, implica la adquisición de toda la información pertinente sobre la organización y la determinación de los criterios básicos, finalidad, alcance, límites y organización de las actividades de gestión de riesgos. El objetivo es el cumplimiento de los requisitos legales y proporcionar la prueba de la debida diligencia el apoyo de un SGSI

que puede ser certificado. El alcance puede ser un plan de notificación de incidentes y un plan de continuidad del negocio.

Los indicadores de riesgo muestran si la organización está sujeta o tiene una alta probabilidad de ser sometida a un riesgo que excede el nivel permitido.

Gestión del Riesgo es una actividad recurrente que se refiere al análisis, planificación, ejecución, control y seguimiento de las medidas implementadas y la política de seguridad impuesta.

2.5.6 ISO/IEC 27006

Permite a los organismos de acreditación armonizar con mayor eficacia su aplicación de las normas contra las que están obligados a evaluar los organismos de certificación. Esta norma puede ser utilizada como un documento de criterios para la acreditación, la evaluación por pares u otra auditoría procesos.

El organismo de certificación debe disponer de criterios para la capacitación de los equipos de auditoría que garantice:

a) El conocimiento de la norma SGSI y otros documentos normativos pertinentes.
b) Conocimiento de seguridad de la información.
c) La comprensión de la evaluación del riesgo y gestión del riesgo desde la perspectiva de negocio.
d) Conocimientos técnicos de la actividad a ser auditada.
e) Conocimiento general de los requisitos normativos correspondientes al SGSI.
f) Conocimiento de los sistemas de gestión.
g) Conocimiento de los principios de la auditoría basada en la norma ISO 19011.
h) Conocimiento de SGSI, examen de la eficacia y la medición de la eficacia del control.

El organismo de certificación debe tener un procedimiento para:

1. La selección de los auditores y expertos técnicos sobre la base de sus competencias, la formación, cualificación y experiencia.
2. La evaluación inicial de la conducta de los auditores y expertos técnicos en las auditorías de certificación y seguimiento, posteriormente, el desempeño de los auditores y expertos técnicos.

2.5.7 ISO/IEC 27007

ISO/IEC 27007 proporciona orientación sobre la realización de auditorías SGSI, esta guía ayuda a los auditores para asegurarse de que están llevando a cabo una auditoría del SGSI de la manera correcta.

Los auditores pueden utilizar la orientación proporcionada por esta norma, en cualquier tipo o tamaño de organización. Es de aplicación general, y su uso se asegura se sigue un enfoque de mejores prácticas en la realización de auditorías SGSI.

Ofrece orientación a los auditores sobre la forma de llevar a cabo auditorías SGSI. Auditoría de un SGSI siguiendo las instrucciones de este estándar permitirá a una organización para identificar las lagunas que es preciso abordar antes de someterse a una auditoría de certificación formal.

Busca desarrollar su organización al proporcionar los conocimientos y habilidades necesarias para alcanzar la excelencia de auditoría esencial.

2.5.8 ISO/IEC 27008

Proporciona una guía en la revisión de la implementación y operación de los controles. Está dirigido principalmente a los auditores de seguridad de la información para verificar el cumplimiento técnico de los controles de seguridad de la información de una organización según la norma ISO / IEC 27002 y otras normas de control utilizadas por la organización.

Ayuda a:

- Identificar y comprender el alcance de los posibles problemas y deficiencias de los controles de seguridad de la información
- Identificar y comprender los impactos potenciales en la organización mitigando las amenazas y las vulnerabilidades de seguridad de la información y gestionándolas de forma inadecuada.
- Priorizar las actividades la seguridad de la información y de mitigación de riesgos.
- Confirmar que previamente se han identificado debilidades de emergencia o deficiencias y que han sido abordadas adecuadamente.
- Apoyo a las decisiones presupuestarias en el proceso de inversión y otras decisiones de gestión relacionadas con la mejora de la gestión de seguridad de la información en la organización.

2.5.9 ISO/IEC 27010

ISO / IEC 27010 una guía sobre seguridad de la información y las comunicaciones entre las industrias en los mismos sectores, en diferentes sectores industriales y con los gobiernos, ya sea en tiempos de crisis y para proteger la infraestructura crítica o para el reconocimiento mutuo en circunstancias normales de trabajo para cumplir con reglamentación legal, y las obligaciones contractuales.

Brinda orientación en relación con el intercambio de información sobre los riesgos de seguridad de la información, los controles, los problemas, incidentes que se extienden los límites entre los sectores de la industria, en particular las que afectan a "infraestructura crítica".

A veces es necesario compartir la información confidencial relativa a las amenazas, vulnerabilidades de seguridad de la información entre o dentro de una comunidad de organizaciones, dicha información es a menudo muy sensible. Las fuentes de información posiblemente tengan que ser protegidas con el anonimato.

La norma proporciona orientación sobre los métodos, modelos, procesos, políticas, controles, protocolos y otros mecanismos para el intercambio de información de forma segura con las entidades de confianza en el entendimiento de que importantes principios de la seguridad de la información será respetada.

2.5.10 ISO/IEC 27011

Apoya a la aplicación de la gestión de seguridad de la información en las organizaciones de telecomunicaciones.

BS ISO / IEC 27011 es para los organismos de telecomunicaciones, para los responsables de seguridad de la información, junto con los proveedores de seguridad, auditores, vendedores de terminales de telecomunicaciones y proveedores de contenido de la aplicación. Proporciona un conjunto común de objetivos de control de seguridad general en base a la norma ISO / IEC 27002, controles específicos para el sector de telecomunicaciones, y las directrices de gestión de seguridad de la información que permitan la selección y aplicación de esos controles.

2.5.11 ISO/IEC 27013

Proporciona orientación sobre la implementación de una seguridad de la información integrada y sistema de gestión de servicios de TI, basado en las normas ISO / IEC 27001:2005 (SGSI) y la norma ISO / IEC 20000-1:2011.

Con esta norma se demuestra la visión estratégica de integrar y homogeneizar cada vez más los sistemas de gestión existentes, así se facilita a las organizaciones la optimización de los recursos dedicados a la implementación y mantenimiento de sus sistemas de gestión.

2.5.12 ISO/IEC 27015

Se enfoca en organizaciones de servicios del sector financiero. Proporciona asesoramiento y orientación sobre la aplicación de la gestión de seguridad de la información dentro de las organizaciones. Los requisitos y controles dentro de estas normas son generales y genéricos, por lo que construye un puente entre estos requisitos y controles generalizados y los hace utilizables por las organizaciones de servicios financieros.

2.5.13 ISO/IEC 27031

Describe los conceptos y principios de la tecnología de información y comunicación (TIC) y la preparación para la continuidad del negocio.

Abarca todos los eventos e incidentes que podrían tener un impacto en la infraestructura y los sistemas de TIC. Se incluye y se extiende a las prácticas de seguridad de la información y el manejo de la gestión de incidentes y los servicios de planificación y preparación para las TIC.

Ayuda a comprender las amenazas y vulnerabilidades de los servicios TIC, lo que le permite asegurarse de que su organización está protegida contra esas amenazas y vulnerabilidades.

Proporciona un marco de métodos y procesos para identificar y especificar todos los aspectos para mejorar la preparación para las TIC de una organización para garantizar la continuidad del negocio. Esto le ayudará a asegurarse de que su organización está preparada en caso de desastre.

2.5.14 ISO/IEC 27032

Esta norma está centrada en cerrar las brechas en materia de seguridad**,** derivadas de la falta de comunicación entre los diferentes usuarios y proveedores del ciberespacio. También aborda los riesgos no cubiertos por la Internet actual, las redes y la seguridad de las tecnologías de la información y de la comunicación.Proporciona una solución global y de colaboración de múltiples partes interesadas para reducir riesgos.

El ciberespacio es un entorno complejo que consta de las interacciones entre las personas, software y servicios, apoyados por la distribución mundial de la información y la comunicación los dispositivos y redes de tecnología. La norma facilita la colaboración segura y confiable protegiendo la privacidad de las personas en todas partes del mundo. De esta forma, se puede ayudar a preparar, detectar, controlar y responder a los ataques.

2.5.15 ISO/IEC 27034

Guía para ayudar en las organizaciones en la integración de la seguridad en los procesos utilizados en la gestión de sus aplicaciones.

Las aplicaciones deben estar protegidas contra las vulnerabilidades como defectos de software que aparecen en el curso del ciclo de vida de la aplicación como cambios en la aplicación, o surgen debido a la utilización de la aplicación en un contexto para el que no estaba previsto.

Las aplicaciones pueden ser adquiridas a través del desarrollo interno, la subcontratación o la compra de un producto comercial. Las aplicaciones también pueden ser adquiridas a través de una combinación de estos enfoques que podrían introducir nuevas implicaciones de seguridad que deben ser considerados y gestionados.

A lo largo de su ciclo de vida, una aplicación segura necesita características de requisitos previos de la calidad del software como la ejecución y cumplimiento, además de cumplir los requisitos de seguridad de un desarrollo, la gestión, la infraestructura tecnológica, y la perspectiva de la auditoría.

2.5.16 ISO/IEC 27035

Esta primera edición de la norma ISO / IEC 27035 anula y sustituye a la norma ISO / IEC TR 18044:2004.
En general, las políticas o los controles de seguridad de la información por sí sola no garantizan una protección total de la información, sistemas de información, servicios o

redes. Después que han sido implementados los controles, vulnerabilidades residuales son probables que se mantengan y pueden hacer de la seguridad de información errónea, por lo tanto es posible tener incidentes de seguridad informática .Es inevitable que se produzcan nuevos casos de amenazas no identificados previamente.

El término "seguridad de la información de gestión de incidentes" se utiliza en esta norma para abarcar la gestión no sólo de los incidentes de seguridad de información, sino también las vulnerabilidades de seguridad de información.

2.5.17 ISO/IEC 27037

Proporciona orientaciones sobre mejores prácticas en la identificación, adquisición y preservación del potencial de la evidencia digital que puede ser de valor probatorio. Su orientación es adecuada para su uso en investigaciones forenses digitales.

Ayuda al manejo de la evidencia digital, siguiendo las directrices de esta norma ayudará a asegurarse de potencial evidencia digital se recoge de manera válida a efectos legales para facilitar el enjuiciamiento exitoso.

Se enfoca a situaciones frecuentes durante todo el proceso de manipulación de la evidencia digital, ayuda a las organizaciones en sus procedimientos disciplinarios y de facilitar el intercambio de potencial evidencia digital entre las jurisdicciones.

2.5.18 ISO/IEC 27799

Especifica un conjunto detallado de controles para la gestión de la seguridad de la información para el ámbito sanitario y proporciona una serie de claras directrices de seguridad sobre las mejores prácticas a seguir en los temas relacionados con la salud. Representa directrices sobre el sector y se implanta y desarrolla bajo el sistema de gestión definido sobre ISO 27001.

Mediante la aplicación de esta norma internacional, las organizaciones sanitarias y entidades afines serán capaces de garantizar un nivel mínimo de seguridad necesaria para que pueda mantenerse en ellas de manera coherente la confidencialidad, integridad y disponibilidad de los datos personales referentes a la salud.

Capítulo III Manual de interpretación para la operatividad del ISO 27001

3.1 Previo a la Implementación

Para la realización de este manual se consideran plantillas, cuadros y cuestionarios para su claro desarrollo y entendimiento, sirviendo como apoyo al comité de gestión.
Antes de buscar una certificación considere que:

- La certificación ISO/IEC 27001 le permite establecer políticas, procedimientos y controles con objeto de disminuir los riesgos de su organización, considerando que ningún mecanismo podría brindar una seguridad absoluta.
- La certificación es una decisión estratégica que debe involucrar a toda la organización y que debe ser apoyada y dirigida desde la dirección, si no hay apoyo de estos la implementación no podrá ser realizada.
- La implementación lleva entre 6 meses y un año.
- Se considera a todo el personal para poder realizar el SGSI.
- En ocasiones, no es necesario un sistema que implique a toda la organización, puede ser que sea sólo necesario en un departamento, una sede en concreto o un área de negocio.
- Se debe determinar a los responsables de la implementación y mantenimiento del SGSI, el auditor del sistema no debe haber participado en la implantación del mismo.

Se consideran tres niveles de responsabilidades *(Ver figura 4).*

1. Estratégico: Define los grandes lineamientos gerenciales para la seguridad de la información y política global del SGSI, coordina y aprueba los recursos.

2. Táctico: Diseño e Implementación del SGSI, establece objetivos concretos y gestiona los recursos.

3. Operacional: Intenta alcanzar los objetivos específicos mediante procesos técnicos.

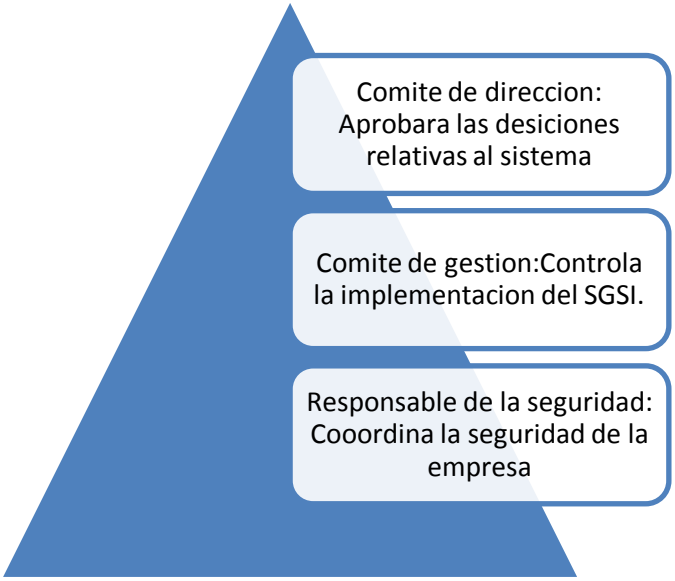


Figura 4 Niveles de Responsabilidad

3.2 Etapas del SGSI

Planear (P): Es el primer paso del SGSI *(Ver figura 3),* en esta etapa se debe establecer el SGSI y para esto se deben realizar diez pasos:

1.- Alcance y limites

2.- Políticas

- Objetivos
- Principios para la acción en relación con la seguridad de la información
- Requerimientos comerciales y legales
- Apruebe la gerencia

3.- Definir enfoque de evaluación del riesgo

- Definir metodología para calcular el riesgo.
- Criterio para identificar los niveles de riesgo y su aceptación.

4.- Identificar los riesgos

- Activos
- Vulnerabilidades
- Amenazas
- Impactos

5.- Analizar y evaluar el riesgo

- Calcular el impacto
- Probabilidad de que la falla ocurra
- Calcular el nivel del riesgo
- Calcular si el riesgo es aceptable o requiere tratamiento utilizando el criterio de evaluación establecido

6.- Identificar y evaluar las opciones para tratamiento del riesgo
- Aplicación de controles
- Asumir los riesgos
- Transferir los riesgos

7.- Aprobación de la gerencia para los riesgos residuales propuestos

8.- Aprobación de la gerencia para implementar el SGSI.

9.- Realizar un enunciado de aplicabilidad.

3.2.1 Alcance y limites

El alcance es todo aquel abarcamiento o hasta donde se desea que tenga lugar el SGSI, en este se dan a conocer las áreas o procesos a certificar, su actividad, la ubicación física del área a proteger y aquellas que se verán afectadas, así como las excluidas y la tecnología involucrada.

El alcance del SGSI dependerá de los objetivos, la estructura y necesidades de la empresa, se puede utilizar como base las respuestas obtenidas del Cuestionario 1.

Logotipo de la empresa	***Cuestionario 1***
Comité gestor: Lo realizará ***Comité de seguridad: Lo actualizará y llevara a cabo*** ***Comité gerencial: Revisará y aprobará*** ***Auditor: Revisará y aprobará***	
Cuestionario 1	
1.- ¿Cual es el proceso o área que se certifica?	
2.- ¿Describa la actividad del proceso o área a certificar?	
3.- ¿Dónde se encuentra físicamente ubicado el área o proceso a certificar?	
4.- ¿Cuales son las aéreas o procesos que se verán afectados en la implementación del SGSI?	
5.- ¿Cuales son las aéreas o procesos que no se verán afectados en la implementación del SGSI?	
6.- ¿Qué tipo de tecnología utiliza el proceso o área a certificar?	
_____ ***Nombre y firma del comité gerencial***	_____ ***Nombre y firma del Comité de seguridad***
_____ ***Nombre y firma del comité gestor***	_____ ***Nombre y firma del auditor***

Cuestionario 1. Alcance, objetivos y necesidad de la empresa

3.2.2 Políticas de seguridad

Las políticas son el comienzo real de la seguridad de la información de la empresa, trazan el camino de la seguridad de la información enfocándose en las necesidades de la organización y la legislación vigente.

Durante la realización de las políticas se considera el personal que labora en la organización para realizar acuerdos en las normas y reglas establecidas, con esto no solo se concede transparencia al proceso, se da un aire de concienciación con el fin de crear en la empresa una cultura de seguridad al mismo tiempo se busca que el personal conozca las actuaciones llevadas a cabo y el motivo de su realización. El mantener involucrado al

personal logra que este desarrolle las nuevas actividades de acuerdo a la normativa y a los términos establecidos.

Todo el personal se dará por enterado y entendido de todas las políticas aplicables las cuales serán de fácil acceso y dominio del personal que labora en la empresa.

Para formular políticas de seguridad se debe hacer uso de conocimientos previos:

- Definir seguridad de la información en la empresa
- Especificar cuál es el alcance de la seguridad y su importancia como mecanismo de control que permita compartir la información.
- Definir los objetivos de la empresa con respecto a la seguridad de la información.
- Debe indicar que lo que se protege en la organización incluye tanto al personal como a la información.
- Dar a conocer las normas, reglas y medidas de seguridad que llevará a cabo la organización.
- Explicación general de las políticas.
- Definición de responsabilidades generales y específicas en las que se incluirán los roles pero nunca a personas concretas dentro de la organización.
- Debe definir responsabilidades teniendo en cuenta que éstas van asociadas a la autoridad dentro de la compañía. En función de las responsabilidades se decidirá quién está autorizado a acceder a qué tipo de información.
- Debe delimitar qué se tiene que proteger, de quién y por qué.
- Debe explicar qué es lo que está permitido y qué no, determinar los límites del comportamiento aceptable y cuál es la respuesta si estos se sobrepasan; e identificar los riesgos a los que está sometida la organización.

Se presenta un cuestionario y dos cuadros con el objetivo de ayudar a la realización de las políticas.

Logotipo de la empresa	***Cuestionario 2***
Comité gestor: Lo realizará ***Comité de seguridad: Lo actualizará y llevara a cabo*** ***Comité gerencial: Revisará y aprobará*** ***Auditor: Revisará y aprobará***	
Cuestionario 2	
1.- Define seguridad de la información	
2.- Especifica el alcance de la seguridad y la importancia de llevar un buen control	
3.- ¿Cual es el objetivo de la empresa al llevar a cabo la seguridad de la información?	
4.- Realiza un enlistado de las normas, reglas y medidas de seguridad que se llevaran a cabo por parte de la organización.	
5.- Explica de manera general en qué consisten las políticas implementadas por la organización.	
_____ ***Nombre y firma del comité gerencial***	_____ ***Nombre y firma del Comité de seguridad***
_____ ***Nombre y firma del comité gestor***	_____ ***Nombre y firma del auditor***

Cuestionario 2 Políticas de seguridad

¿Que se tiene que proteger?	¿De quién?	¿Por qué?

Cargo en la compañía	¿Cuál es su responsabilidad general en la compañía?	¿Cuál es sus responsabilidades especifica en la compañía?	Departamento o área a la que está autorizado	Tipo de información a la que tiene acceso

Cargo que tiene en la compañía	Lo que tiene permitido	Lo que no tiene permitido	Acciones a tomar por la realización de algo no permitido	Riesgos para la organización por algo no permitido

Nota: En función de las responsabilidades se dará respuesta a quien está autorizado a qué tipo de información.

Cuadro 2. Formulación de políticas de seguridad

Una vez terminadas las políticas, deben ser aprobadas por la gerencia mediante un documento con la firma de autorización previa a la implementación y hacer del conocimiento a todo el personal que labora en la empresa, asegurándose que serán de fácil acceso y dominó de todo el personal que labora en la empresa.

La Política de Seguridad debe ser un documento completamente actualizado, por lo que debe ser revisado y modificado anualmente.
Las políticas serán revisadas cada que:

- Exista un incidente de seguridad.
- Después de una auditoría del sistema sin éxito.
- Existan cambios que afectan a la estructura de la organización.

3.2.3 Definir enfoque de evaluación del riesgo

3.2.3.1 Definir metodología para calcular el riesgo.

No toda la información que disponemos tiene el mismo valor o está sometida a los mismos riesgos. Por ello, es importante realizar un análisis de riesgos que valore los activos de información y vulnerabilidades a las que están expuestas. Así mismo, es necesaria una evaluación de dichos riesgos para reducirlos en la medida de lo posible.

Se deberá elegir una metodología para calcular el riesgo en que se encuentra sometido cada activo. La metodología a utilizar dependerá del comité gestor, a continuación se muestran una lista de metodologías comúnmente utilizadas para la evaluación del riesgo.

- MARGERIT
- CONTROL-IT
- CRAMM
- CRITI_CALC
- COBRA
- BUDDY SYSTEM
- DBSS
- BDS RISK ASSESOR
- ANALYZ
- RISC
- CCTA
- DDIS
- XRM
- SISSI
- RANK-IT
- PSICHE
- PREDICT

- MINIRISK
- LAVA

3.2.3.2 Criterio para identificar los niveles de riesgo y su aceptación.

Se aclara el criterio que utilizará la empresa para los riesgos, esto es, hasta qué punto un riesgo será aceptado en la empresa y hasta qué punto tendrá que ser resuelto.

El comité de dirección será quien apruebe el nivel de riesgo al que se pretenderá dar solución y el nivel en el que se asumirán las consecuencias, mediante una pequeña escala de evaluación, en la cual se marcará el nivel más adecuado para la empresa.

Nivel de riesgo			
80% al 100%	Muy alto	MA	Tendran que ser resueltos y requerirán de una cuidadosa administración
40% al 79%	Alto	A	Tendran que ser recueltos y requerirán de una cuidadosa administración.
20% al 39%	Normal	N	Deben ser tratados y controlados siempre.
9% al 19%	Bajo	B	Serán aceptados por la empresa, pudiendo no ser necesaria una acción adicional.
<ó=10%	Muy bajo	MB	Serán aceptados por la empresa, pudiendo no ser necesaria una acción adicional.

_____

Nombre y firma del comité gerencial

_____ _____

Nombre y firma del comité gestor ***Nombre y firma del auditor***

Figura 5. Niveles de riesgo

3.2.4 Identificar los riesgos

Para poder identificar los riesgos es necesario realizar en forma de inventario todos los activos con los que cuenta la organización *(Ver cuadro 3)*, clasificándolos de la siguiente manera:

- Datos: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la organización.

- Aplicaciones: El software que se utiliza para la gestión de la información.

- Personal: En esta categoría se encuentra tanto la plantilla propia de la organización, como el personal subcontratado, los clientes, usuarios y, en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la organización.

- Servicios: Aquí se consideran tanto los servicios internos, aquellos que una parte de la organización suministra a otra (por ejemplo la gestión administrativa), como los externos, aquellos que la organización suministra a clientes y usuarios (por ejemplo la comercialización de productos).

- Tecnología: Los equipos utilizados para gestionar la información y las comunicaciones (servidores, PCs, teléfonos, impresoras, routers, cableado, etc.).

- Instalaciones: Lugares en los que se alojan los sistemas de información (oficinas, edificios, vehículos, etc.).

- Equipamiento auxiliar: En este tipo entrarían a formar parte todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos (equipos de destrucción de datos, equipos de climatización, etc.).

- Intangibles.- Son aquellos que re presentan un valor a la empresa pero no están presentes de manera física como son la imagen y la reputación de una empresa.

Logotipo de la empresa ***Formato 1***

Comité gestor: Lo realizará y contestará
Comité de seguridad: Actualizará
Comité gerencial: Revisará y aprobará
Auditor: Revisará y aprobará

Inventario

*Activo	Código asignado	Clasificación	Unidades con la que se cuenta	Descripción	Localización	*Propietario

_____ _____
Nombre y firma del comité gerencial ***Nombre y firma del Comité de seguridad***

_____ _____
Nombre y firma del comité gestor ***Nombre y firma del auditor***

Cuadro 3. Formato para inventario

Nota:
**Activo.- Cualquier elemento que tenga valor para la organización.*
**Propietario.- Persona que tiene la responsabilidad gerencial aprobada para controlar la producción, desarrollo, mantenimiento, uso y grado de seguridad que requiere el activo, no tiene que ser el dueño de la empresa.*

Una vez que se tiene el inventario de activos, se procede a identifican los factores que introducen una amenaza, existen formas de identificarlos como:

- Cuestionarios de análisis de riesgos: descubrir amenazas a través de una serie de preguntas y en algunas instancias.

- Listas de chequeo de exposiciones a riesgo: Una de las más comunes herramientas en el análisis de riesgos son las listas de chequeo, las cuales son simplemente unas listas de exposiciones a riesgo.

- Listas de chequeo de políticas de seguridad: Esta herramienta incluye un catálogo de varias políticas de seguridad que un negocio dado puede necesitar.

- Sistemas expertos: Un sistema experto usado en la administración de riesgos incorpora los aspectos de las herramientas descritas anteriormente en una sola herramienta.

3.2.5 Valoración del activo

No todos los activos tienen la misma importancia para la organización, ni generan los mismos problemas sin son atacados, es por eso que a cada activo se le tiene que asignar un valor propio.

La valoración del activo se puede realizar de dos maneras ya sea cuantitativa o cualitativamente.

La cualitativa se establece de acuerdo a una escala, por ejemplo del 0 al 5 o con valores del tipo: bajo, medio y alto. En esta los cuestionarios y entrevistas son los más utilizados, el comité de gestión es el encargado de realizarlos y los propietarios de los activos de responderlas, Ver cuadro 4.

Ejemplo de preguntas realizadas en una valoración cualitativa:

¿Qué impacto tendría en la integridad del activo XXXXX si alguien entrara a la base de datos y modificara los datos?

☐ Bajo ☐ Muy Bajo ☐ Medio ☒ Alto ☐ Muy alto

Ejemplo de llenado de un cuadro cualitativo:

	Dimensiones de origen de la seguridad			
Código	Integridad	confidencialidad	disponibilidad	* valoración
XXXXX	10	10	10	10

**Nota:*
La valoración cualitativa dependerá del grado de integridad, confidencialidad y disponibilidad que el propietario asigne en las entrevistas y cuestionarios realizados.

Abreviatura	Significado
10	Muy Alto
7	Alto
5	Medio
3	Bajo
1	Muy Bajo

Cuadro 4. Valoración cualitativa

La valoración cuantitativa se realiza mediante la asignación de valores económicos al activo, Ver cuadro 5.

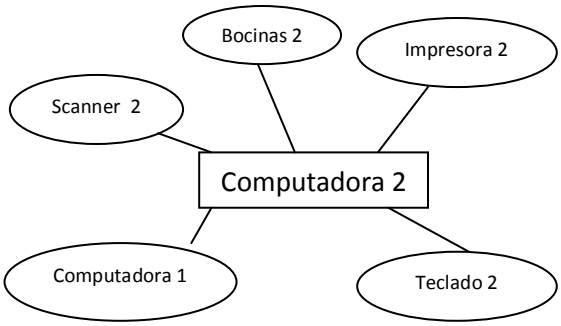
Valor del activo		
Código	Valor asignado	Valoración
XXX	$1'000 000.00	10

Rango de valor	Nivel de valoración
≥ $1'000 000.00	10
≥ $400 000.00 y < $1'000 000.00	7
≥ $90 000.00 y < $400 000.00	5
> $ 500.00 y < $90 000.00	3
≤ $ 500.00	1

Cuadro 5. Valoración cuantitativa

3.2.5.1 Relación entre los activos

La dependencia entre activos supone a una amenaza que afecte a un activo del que dependa otro activo superior, tendrá impacto directo sobre el activo superior, es por esto que se debe realizar un árbol de dependencias en donde se muestren las relaciones existentes entre los activos (*Ver figura 6*). El comité de gestión será el encargado de su realización.



Activo	¿En caso de algún inconveniente que activos se verán afectados?
1.1	2.2
	2.3
	3.7

Figura 6. Árbol de dependencias

3.2.6 Análisis y Evaluación del riesgo

En el analizar de riesgo existen multitud de metodologías, estas nos indican los pasos a seguir para su correcta ejecución, ya que suelen ser muy complejos. Los cuadros mencionados a continuación se basan en una metodología llamada Margerit y están dado como apoyo en la implementación de la metrología a elegir.

Se realiza el análisis del riesgo (*Ver cuadro 8*) con el objetivo de obtener los resultados que definen el nivel de riesgo al que está expuesta la organización pudiendo así tomar medidas al respecto para disminuir lo más posible el riesgo, dando respuesta a:

- Impacto que tiene sobre la organización.
- Probabilidad de que una falla ocurra.
- Calcular el nivel del riesgo al que está sometido.

Para cada activo se identifican las amenazas que le afectan y se calcula la frecuencia con que ocurre dicha amenaza por medio de un registro, *Ver cuadro 6*.

REGISTRO			
Responsable del registro:			
Activo:			
Registro realizado del _____al_____ (mínimo un año)			
Incidencia: 1.1			
Descripción:	**Fecha**	**Activos a los que afecta**	**Riesgo**
1.-			
Valor total de la frecuencia	**10**		

**Nota: Para el riesgo ver cuadro 7*

Frecuencia	Valor de la frecuencia
= o > 15 veces al año	10
10 a 14 veces al año	7
5 a 9 veces al año	5
2 a 4 veces al año	3
= o < 1 vez al año	1

Cuadro 6. Registro de amenazas

Una vez que se tiene documentadas las amenazas, se procede a calcular el riesgo y la prioridad que se tiene para dar solución.
El riesgo se define como la probabilidad de que ocurra una amenaza y se calcula por medio de la formula: Riesgo = Impacto × Frecuencia.

Amenaza	Frecuencia	Impacto	Riesgo
1.1	10	10	100 %

**Nota: El impacto será la valoración del activo Ver cuadros 4 Y 5.*

La prioridad de respuesta a cada amenaza detectada dependerá de la valoración asignada. A mayor impacto menor tiempo de respuesta para la corrección.

Impacto	Tiempo de respuesta
10	Muy Bajo
7	Bajo
5	Medio
3	Alto
1	Muy Alto

Cuadro 7. Riesgo

Logotipo de la empresa						**Formato 2**
Comité gestor: Lo realizará y contestará ***Comité de seguridad: Actualizará*** ***Comité gerencial: Revisará y aprobará*** ***Auditor: Revisará y aprobará***						
Análisis de riesgo						
Activo	***Vulnerabilidad**	***Amenaza**	***Impacto (Valoración del activo)**	**Frecuencia**	**Riesgo**	**Tiempo de respuesta**
		1.1-	10	10	100%	Muy bajo
		1.2.-				
		1.3.-				
_____ ***Nombre y firma del comité gerencial***				_____ ***Nombre y firma del Comité de seguridad***		
_____ ***Nombre y firma del comité gestor***				_____ ***Nombre y firma del auditor***		

Cuadro 8. Formato análisis y evaluación del riesgo

Nota
**Vulnerabilidad.- Debilidad de un activo o de control que puede ser explotado por una amenaza*
**Amenaza.- Causa potencial de un incidente no deseado*
**Impacto.- Consecuencia de la materialización de una amenaza sobre un activo.*

3.2.7 Calcular si el riesgo es aceptable o requiere tratamiento utilizando el criterio de evaluación establecido

Una vez obtenido el nivel de riesgo al que está sometido el activo, se evaluará para conocer si está en un nivel aceptado por la organización o requiere pasar a la siguiente etapa de tratamiento de riesgo para poder disminuirlo hasta un nivel aceptable (*Ver figura 5*).

3.2.8 Identificar y evaluar las opciones para tratamiento del riesgo

Ya que se ha realizado el análisis de riesgo, se buscan y determinan cuáles serán las alternativas existentes para disminuir los riesgos a un punto aceptable por la empresa *(Ver formato 3*).

Existen varias medidas para llevar a cabo el tratamiento del riesgo de manera que se encuentren por debajo del riesgo asumido por la organización, algunos de ellos son:

1.- Aplicación de controles: Los controles son políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

En el *Anexo A* se da un enlistado de controles, se deberán seleccionar cuales son los más viables para disminuir lo más que se pueda el riesgo.

La norma ISO/IEC 27002 es una guía más completa de controles aplicados a la mayoría de las organizaciones.

2.- Aceptar el riesgo: Se asume la responsabilidad por escrito y de una manera consciente, siempre que satisfagan un nivel de riesgo aceptado por el comité de dirección, de lo contrario no se podrá aceptar el riesgo y se buscarán otras alternativas.

3.- Transferir el riesgo: Se valorará la subcontratación del servicio externamente o la contratación de un seguro que cubra los gastos en el caso de que ocurra una incidencia. En el caso de que el activo sea altamente confidencial, la subcontratación no será una opción viable.

4.- Evitar el riesgo: Se consigue eliminando los activos a los que tengan un cierto grado de riesgo, es una elección generalmente costosa y drástica por lo que suelen buscarse medidas alternativas.

Logotipo de la empresa				**Formato 3**
Comité gestor: Lo realizará y contestará ***Comité de seguridad: Actualizará*** ***Comité gerencial: Revisará y aprobará*** ***Auditor: Revisará y aprobará***				
Tratamiento del riesgo				
Amenaza	Aplicación de controles	Aceptar el riesgo	Transferir el riesgo	Evitar el riesgo
1.1	X			
_____ ***Nombre y firma del comité gerencial***			_____ ***Nombre y firma del Comité de seguridad***	
_____ ***Nombre y firma del comité gestor***			_____ ***Nombre y firma del auditor***	

Cuadro 9. Formato para tratamiento del riesgo

3.2.9 Aprobación de la gerencia para los riesgos residuales

La gerencia debe aprobar por escrito todos los riesgos sobre los que está dispuesto a asumir la responsabilidad sobre las amenazas existentes, a esto se le conocerá como riesgo residual *Ver cuadro 10*.

Logotipo de la empresa	**Formato 4**
Comité gestor: Lo realizara ***Comité gerencial: Contestara y aprobará*** ***Comité de seguridad: Actualizará*** ***Auditor: Revisará y aprobará***	
Aceptación del riesgo	
Amenaza	¿Razón por la cual se acepta el riesgo?
1.1	

_____ _____

Nombre y firma del comité gerencial ***Nombre y firma del Comité de seguridad***

_____ _____

Nombre y firma del comité gestor ***Nombre y firma del auditor***

Cuadro 10. Formato aceptación del riesgo

3.2.10 Aprobación de la gerencia para la Implementación del SGSI

El comité de gestión buscara la aprobación del comité gerencial para la implementación y operación del sistema de mediante la firma y revisión de:

- Cuestionario 1
- Cuestionario 2
- Figura 5 Niveles de riesgo
- Cuadro 3 Formato para inventario
- Cuadro 7 Riesgo
- Cuadro 8 Formato análisis y evaluación del riesgo
- Cuadro 9 Formato para el tratamiento del riesgo
- Cuadro 10 Aceptación del riesgo

3.2.11 Enunciado de aplicabilidad

El enunciado de aplicabilidad es un escrito que sirve para mostrar la racionalidad de haber elegido ciertos controles, y deberá contener los siguientes puntos:

- Los controles seleccionados e implementados.
- Los controles seleccionados y la razón de su implementación.
- Los controles que no seleccionados y la razón de su exclusión.

Logotipo de la empresa				**Formato 5**
Comité gestor: Lo realizara ***Comité gerencial: Contestara*** ***Comité de seguridad: Actualizará*** ***Auditor: Revisará y aprobará***				
Enunciado de aplicabilidad				
Amenaza encontrada	**Controles no seleccionados**	**Razón de la exclusión**	**Control a implementar**	**Razón de la elección de este control:**
			A.1	
Amenaza encontrada	**Controles no seleccionados**	**Razón de la exclusión**	**Control a implementar**	**Razón de la elección de este control:**
_____ ***Nombre y firma del comité gerencial***			_____ ***Nombre y firma del Comité de seguridad***	
_____ ***Nombre y firma del comité gestor***			_____ ***Nombre y firma del auditor***	

Cuadro 11. Formato para enunciado de aplicabilidad

3.3 Hacer (D)

Es la segunda etapa del SGSI, básicamente es poner en marcha lo realizado en la planeación; implementando las políticas, controles, procesos y procedimientos del SGSI.

Requerimientos para esta etapa:

1.- Llevar a cabo plan tratamiento de riesgo a cada riesgo encontrado.

2.- Implementar los controles seleccionados.

3.- Definir cómo medir la efectividad de los controles seleccionados

4.- Implementar programas de capacitación y conocimiento

5.- Manejar los recursos y operaciones del SGSI

6.- Implementar procedimientos y otros controles capaces de permitir una pronta detección para dar respuestas de seguridad.

7.- Tener evidencia documentada de lo realizado

3.3.1 Plan de tratamiento de riesgos

Se debe tener evidencia de un plan de tratamiento de riesgos firmado por la gerencia, este es un documento donde se especifican todo las acciones necesarias para poner en marcha los controles elegidos.

Dentro de este plan pueden quedar recogidos los objetivos definidos para medir la eficacia de los controles, el tiempo en que se realizará, los responsables y los recursos necesarios, *Ver cuadro 12*.

Logotipo de la empresa **Formato 6**

Comité gestor: Lo realizara
Comité gerencial: Lo contestara
Auditor interno: Revisará y aprobará

Plan de tratamiento de Riesgos

Código del activo:	Código del control a implementar:	Plazo para la implementación:	Nivel de riesgo en que se encuentra			Nivel de riesgo objetivo	
			A	MA	N	B	MB

¿Cómo se llevara a cabo la implementación?

Responsable de la implementación del control:

Recursos para la implementación:

Código del activo:	Código del control a implementar:	Plazo para la implementación:	Nivel de riesgo en que se encuentra			Nivel de riesgo objetivo	
			A	MA	N	B	MB

¿Cómo se llevara a cabo la implementación?:

Responsable de la implementación:

Recursos para la implementación:

_____ _____

Nombre y firma del comité gerencial ***Nombre y firma del Comité de seguridad***

_____ _____

Nombre y firma del comité gestor ***Nombre y firma del auditor***

Cuadro 12. Formato riesgos y controles

3.3.2 Definir cómo medir la efectividad de los controles seleccionados

Tras la implantación de los controles, se debe especificar la manera en que será evaluada su eficacia mediante indicadores, asegurándose que proporcionaran la protección prevista y que continuarán aplicándose.

Los pasos que se proponen por la norma ISO 27004 con el fin de medir la eficacia de los controles se pueden resumir de la siguiente manera:

- Seleccionar los procesos y objetos de medición.- Las organizaciones deben definir lo que hay que medir. Sólo los procesos bien documentados que son repetibles deben ser considerados para la medición.

- Definir las líneas de base.- los valores de referencia que indican el punto de referencia debe definirse para cada objeto que se está midiendo.

- Recopilar datos.- Recopilación oportunos y preciso de los sistemas y procesos que están en el ámbito de la medición sería la actividad más importante en la creación de métricas de seguridad.

- Desarrollar un método de medición.- Aplican diversos atributos del objeto seleccionado para la medición, con el fin de llegar al "indicador" de una salida que tenga sentido para los interesados.

- Interpretar los valores medidos.- Tener procesos y la tecnología para el análisis y la interpretación de los valores de medición. El análisis de los resultados del proceso de medición debe identificar las diferencias entre el valor inicial y el valor de medición actual *(Ver cuadro 12).*

- Comunicar los valores de medición: Las salidas de medida SGSI deben comunicarse a las partes interesadas. Los valores de medición se pueden comunicar en forma de tablas, cuadros de mando operacionales, informes o boletines de noticias.

3.3.3 Implementar programas de capacitación y conocimiento

La organización debe asegurarse que todo el personal a quien se asignó las responsabilidades definidas en el SGSI sea competente para realizar las tareas requeridas mediante capacitaciones, evaluando las decisiones tomadas, nivel de educación y experiencia.

Logotipo de la empresa				*Formato 7*
Comité gestor: Lo realizara ***Comité gerencial: Contestará y aprobará*** ***Comité de seguridad: Actualizará*** ***Auditor interno: Revisará y aprobará***				
Capacitación del personal				
Personal	**Nivel de educación**	**Años de experiencia trabajos en el área**	**Cursos a los que ha asistido**	**Cursos y capacitaciones a los que deberá asistir**
Auditor interno				
Comité gestor				
Comité de seguridad				
_____ ***Nombre y firma del comité gerencial***			_____ ***Nombre y firma del Comité de seguridad***	
_____ ***Nombre y firma del comité gestor***			_____ ***Nombre y firma del auditor***	

Cuadro 14. Formato capacitación del personal

**Nota: Los cursos y capacitaciones a los que deberán asistir el comité gestor solo aplicara si son empleados de la misma empresa y buscan la implementación del sistemas gestor sin la certificación.*

3.3.4 Manejar los recursos y operaciones del SGSI

El comité gerencial debe llevar a cabo los recursos necesarios brindados para la implementación, monitoreo, mantenimiento, mejora, establecimiento y operación el SGSI; además de:

- Identificar y tratar los requerimientos legales y reguladores y las obligaciones de seguridad contractuales.
- Mantener una seguridad adecuada mediante la correcta aplicación de todos los controles implementados.
- Llevar a cabo revisiones cuando sea necesario, y reaccionar apropiadamente ante los resultados de estas revisiones.

3.3.6 Implementar procedimientos y otros controles capaces de permitir una pronta detección para dar respuestas de seguridad.

Se implementarán otros controles para garantizar que los eventos y debilidades en la seguridad asociados con los sistemas de información se comuniquen de modo que se puedan realizar acciones correctivas oportunas.

Ejemplo: A los propietarios de los activos, se les deberá exigir que informen de cualquier evento o debilidad en la seguridad de información lo más rápido posible y al punto de contacto designado *Ver formato 15*.

Logotipo de la empresa			**Formato 8**
Comité gestor: Lo realizara ***Comité gerencial: Revisará y aprobará*** ***Comité de seguridad: Actualizará y llevará a cabo*** ***Auditor interno: Revisará y aprobará***			
Notificación			
Activo	**Responsable del activo**	**A quien acudir en caso de alguna amenaza detectada**	**Firma**
_____ ***Nombre y firma del comité gerencial***		_____ ***Nombre y firma del Comité de seguridad***	
_____ ***Nombre y firma del comité gestor***		_____ ***Nombre y firma del auditor***	

Cuadro 15. Formato notificación

3.3.7 Documentación

La gerencia deberá tener evidencia de:

1.- Políticas de seguridad, objetivos, alcance del SGSI, roles y responsabilidades para la seguridad de la información (*Ver cuestionario 1 y cuestionario 2).*
2.- Hacer del conocimiento a la organización sobre la importancia de los objetivos de la seguridad de la información, responsabilidad y necesidad de mejora continuo.
3.- Criterio para la aceptación del riesgo y niveles de riesgo aceptables, *Ver figura 5 y cuadro 10*.
4.- Sugerencias de personal como usuarios, clientes, proveedores, publico. Esto se lleva a cabo por medio de cuestionarios, entrevistas o colocación de buzones de quejas y sugerencias.
5.- Auditorías realizadas a la organización (*Ver 3.4.5*).
6.- Recursos para el desarrollo, implementación, operación, monitoreo, revisión, mantenimiento y mejoras del SGSI *(Ver cuadro 16).*

Logotipo de la empresa *Formato 9*

Comité gestor: Lo realizará
Comité gerencial: Lo revisará y aprobará
Comité de seguridad: Lo llevará a cabo
Auditor: Revisará

Recursos para el SGSI						
Formato	**Implementación**	**operación**	**monitoreo**	**Revisión**	**Mantenimiento**	**Mejora**
Cuestionario 1						
Cuestionario 2						
Figura 5 Nivel del riesgo						
Cuadro 1 formato para inventario.						
Cuadro 4 valoración cualitativa del activo						
Cuadro 5 valoración cuantitativa del activo						
Cuadro 6 registro de amenazas						
Cuadro 7 Riesgo						
Cuadro 8 formato Análisis de riesgo						
Cuadro 9 formato para tratamiento del riesgo						
Cuadro 10 formato Aceptación del riesgo						
Cuadro 11 formato para enunciado de aplicabilidad						

Cuadro 14 formato capacitación del personal						
Cuadro 15 formato notificación						
Cuadro 16 formato recursos para el SGSI						

_____ _____

Nombre y firma del comité gerencial ***Nombre y firma del Comité de seguridad***

_____ _____

Nombre y firma del comité gestor ***Nombre y firma del auditor***

Cuadro 16. Formato recursos para el SGSI

3.4 Monitorear y revisar el SGSI

En esta tercera y penúltima etapa se incluirán los informes de revisión que surgen a partir de la realización de las etapas pasadas y sus requerimientos son:

1. Ejecutar procedimientos de monitoreo.
2. Realizar revisiones regulares de la efectividad del SGSI.
3. Revisar las evaluaciones del riesgo a intervalos planeados
4. Realizar las auditorías internas a intervalos planeados.
5. Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso.
6. Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de las actividades de monitoreo y revisión.
7. Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI.

3.4.1 Ejecutar procedimientos de monitoreo

Se llevarán a cabo revisiones de monitoreo al SGSI para detectar lo antes posible:

- Errores de procesamiento.
- Incidencias y violaciones de seguridad fallidas y exitosas.
- Permitir a la gerencia determinar si las actividades de seguridad delegadas a las personas o implementadas mediante la tecnología de información se están realizando como se esperaban.
- Ayudar a detectar los eventos de seguridad, evitando así los incidentes de seguridad mediante el uso de indicadores.
- Determinar si son efectivas las acciones tomadas para resolver una violación de seguridad.

3.4.2 Realizar revisión a la efectividad del SGSI.

El comité gestor emitirá un reporte al comité gerencial informado sobre el estado del SGSI y las sugerencias para mejorarlo, *Ver cuadro 17 y 18*.

Logotipo de la empresa			***Formato 10***
Comité gestor: Realizará y contestará ***Comité gerencial: Revisará y aprobará***			
Revisiones al SGSI			
A revisar	**Código**	**Estado en que se encuentra**	**Si existe algún inconveniente ¿Qué acción que se tomará para disminuirlo?**
Cuestionario 1			
Cuestionario 2			
Figura 5 Nivel del riesgo			
Cuadro 1 formato para inventario.			
Cuadro 4 valoración cualitativa del activo			
Cuadro 5 valoración cuantitativa del activo			
Cuadro 6 registro de amenazas			
Cuadro 7 Riesgo			
Cuadro 8 formato Análisis de riesgo			
Cuadro 9 formato para tratamiento del riesgo			

Cuadro 10 formato Aceptación del riesgo			
Cuadro 11 formato para enunciado de aplicabilidad			
Cuadro 14 formato capacitación del personal			
Cuadro 15 formato notificación			
Cuadro 16 formato recursos para el SGSI			
Cuadro 20 Programa de auditoria			
Cuadro 26 Formato causa de las des conformidades			
Cuadro 27 Formato acciones preventivas			
_____ ***Nombre y firma del comité gestor***		_____ ***Nombre y forma del comité gerencial***	

Cuadro17. Formato revisiones al SGSI

Logotipo de la empresa			***Formato 11***
Comité gestor: Realizará y contestará ***Comité gerencial: Revisará y aprobará***			
Acciones tomadas			
Código del estado en que se encuentra	**Responsable de llevarla a cabo la corrección**	**Recursos**	**Tiempo**
_____ ***Nombre y firma del comité gestor***		_____ ***Nombre y forma del comité gerencial***	

Cuadro 18. Acciones tomadas

3.4.3 Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad

Se lleva a cabo la medición de los controles implementados para verificar que se hayan cumplido los requerimientos de seguridad.

Ejemplo de cómo medir un control:

1. Se realiza una comparación de los registros de amenazas pasados *(Ver cuadro 6)* con los registros actuales.
2. Se mide el riesgo en que se encuentra *(Ver cuadro 7)*
3. Si el riesgo disminuyo el control es optimo, pero si el riesgo aumento, el control no es adecuado y tendrá que ser remplazado.

Registro				
Responsable del registro:				
Registro realizado del _____al_____ (mínimo un año)				
Activo:				
Control implementado:				
Incidencia:				
Descripción:	**Responsable de la incidencia**	**Fecha**	**Valor de activos afectados**	**Riesgo**
1.-		3/2 /12		
2.-				
Valor total de la frecuencia	**10**			

Cuadro 19. Registro para medir la efectividad de controles

3.4.4 Revisar las evaluaciones del riesgo a intervalos planeados

Cada año se realizarán revisiones a la evaluación del riesgo para verificar el nivel de riesgo residual.

Se deberá revisar cada que existan cambios en:

- La organización
- La tecnología
- Objetivos y procesos comerciales
- Amenazas identificadas
- Efectividad de los controles implementados
- Eventos externos como cambios en el ambiente legal o regulador, cambios en obligaciones contractuales y cambios en el clima social

3.4.5 Realizar las auditorías internas a intervalos planeados.

Es necesario llevar a cabo una revisión anual del SGSI denominada auditoría interna (además de la revisión del sistema que realiza la dirección). Esta auditoría puede ser realizada por personal de la propia entidad. El comité de dirección será el encargado de designar al auditor. El auditor del sistema no debe haber participado en la implantación del mismo para mantener la objetividad y la independencia entre la implantación y la auditoría.

Durante la auditoria se realiza un listado de todos los controles a revisar y todos los aspectos del sistema que necesitan ser analizados, con este listado el auditor realizará una revisión del sistema e indicará aquellos aspectos de mejora que se han detectado, así como la prioridad o gravedad de cada uno de ellos.

A manera de facilitar la realización de la auditoria, se presentan una serie de pasos:
1.- Realizar un programa de auditoría interna: Es un documento donde se planificaran las fechas, a/los auditores, áreas a auditar y los resultados de las auditorias pasadas.

Logotipo de la empresa	***Formato 12***
Auditor: Lo realizará y contestará. ***Comité gerencial: Revisara y aprobará***	
Programa de auditoría interna	
Encargado de la realización de la auditoría interna:	
¿Cada cuando se realizara la auditoria (mínimo cada año)?:	
Fecha de inicio de la auditoria:	
Códigos de auditorías pasadas:	
Área a auditar:	
Activo a auditar:	
_____ ***Nombre y firma del Comité gerencial***	_____ ***Nombre y firma del Auditor interna***

Cuadro 20. Programa de auditoria

2.- El auditor deberá realizar cuestionarios y entrevistas a los empleados, para poder realizar la auditoria. Ejemplo de preguntas realizadas:
El personal de Comunicaciones ¿Puede entrar directamente en la Sala de Computadoras?
R= No, solo tiene tarjeta el Jefe de Comunicaciones. No se la da a su gente más que por causa muy justificada, y avisando casi siempre al Jefe de Explotación.

3.- Se lleva a cabo una revisión, para verificar que cumpla con los requerimientos del estándar.

Logotipo de la empresa						***Formato 13***	
Auditor interno: Realizara y contestará ***Comité gerencial: Revisara***							
Requerimientos del SGSI							
Planeación		**Hacer**		**Monitorear y revisar el SGSI**		**Mantener y mejorar el SGSI**	
Alcance y limites	X	Elaboración del plan de tratamiento de riesgo		Ejecutar procedimientos de monitoreo		Implementar las mejoras identificadas en al SGSI	
Políticas		Implementar el plan de tratamiento de riesgo		Realizar revisiones regulares de la efectividad del SGSI		Tomar las acciones correctivas y preventivas apropiadas	
Definir enfoque de evaluación de riesgos		Levar a cabo el tratamiento de riesgo elegido a cada riesgo encontrado.		Medir la efectividad de los controles para verificar que se hayan cumplido los requerimientos de seguridad.		Comunicar los resultado y acciones a todas las partes interesadas con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar como proceder	
Identificar riesgos		Implementar los controles seleccionados		Revisar las evaluaciones del riesgo a intervalos planeados		Asegurar que las mejoras logren sus objetivos señalados	
Analizar y evaluar los riesgos		Definir como medir la efectividad de los controles seleccionados		Realizar las auditorías internas a intervalos planeados			
Tratamiento del riesgo		Implementar programas de capacitación y conocimiento		Realizar una revisión gerencial del SGSI sobre una base regular para asegurar que el alcance permanezca adecuado y se identifiquen las mejoras en el proceso SGSI.			
Seleccionar controles para tratamiento del riesgo		Manejar los recursos y operaciones del SGSI		Actualizar los planes de seguridad para tomar en cuenta los descubrimientos de			

				las actividades de monitoreo y revisión.			
Aprobación de la gerencia para los riesgos residuales propuestos		Implementar procedimientos y otros controles capaces de permitir una pronta detección para dar respuestas de seguridad.		Registrar las acciones y eventos que podrían tener un impacto sobre la efectividad o desempeño del SGSI.			
Aprobación de la gerencia para implementar el SGSI							
Realizar un enunciado de aplicabilidad							

_____ _____

Nombre y firma del Comité gerencial ***Nombre y firma del Auditor interno***

Cuadro 21. Requerimientos del SGSI

4.- Se llevara a cabo revisión de los controles, objetivos de control, las áreas que serán auditadas y sus activos para verificar que cumplen con lo esperado.

Logotipo de la empresa	***Formato 14***
Auditor: Lo realizará y contestará. ***Comité gerencial: Revisara y aprobará***	
Auditoría interna	
Encargado de la realización de la auditoría interna:	
Fecha de inicio de la auditoria:	**Fecha termino de la auditoria:**
Área a auditar:	
Activo a auditar:	
_____	_____
Nombre y firma del Comité gerencial	***Nombre y firma del Auditor interna***

Cuadro 22. Formato auditoría interna

5.- El auditor documentará las des conformidades (*Ver cuadro 23),* mejoras detectadas *(Ver cuadro 24)* y acciones preventivas *(Ver cuadro 27).*

Logotipo de la empresa			***Formato 15***
Auditor: Realizará y contestará ***Comité gerencial: Revisará y aprobará.***			
Des conformidades			
Nombre del auditor:			
área/activo/control	**Responsable del área/activo/control**	**¿Se detecto alguna des conformidad?**	
		Si (¿Cual?)	**No**
_____ ***Nombre y firma del Comité gerencial***		_____ ***Nombre y firma del Auditor interno***	

Cuadro 23. Formato des conformidades

Logotipo de la empresa			***Formato 16***
Auditor: Realizará y contestará ***Comité gerencial: Revisará y aprobará.***			
Mejoras			
Nombre del auditor:			
área/activo/control	**Responsable del área/activo/control**	**¿Se detecto alguna mejora?**	
		Si (¿Cual?)	**No**
_____ ***Nombre y firma del Comité gerencial***		_____ ***Nombre y firma del Auditor interno***	

Cuadro 24. Formato mejoras

6.-El comité de seguridad será el encargado de llevar a cabo las correcciones detectadas en la auditoria *(Ver cuadro 25).*

Logotipo de la empresa				*Formato 17*
Auditor: Realizará ***Comité de seguridad: Contestará*** ***Comité gerencial: Revisara y aprobará***				
Acciones correctivas				
área/activo/control	**Acción correctiva**	**Responsable de corregirla**	**Tiempo que llevará corregirla**	**Recursos para corregirla**
_____ ***Nombre y firma del Comité gerencial*** _____ _____ ***Nombre y firma del Comité de gestión*** ***Nombre y firma del Auditor interno***				

Cuadro 25. Formato acciones correctivas

3.4.6 Realizar una revisión gerencial del SGSI.

La gerencia deberá revisar y aprobar informes sobre el estado del SGSI. Esta revisión tiene como objetivo conocer si es adecuado, apropiado y efectivo para los propósitos y contexto de la organización.

3.4.7 Actualizar los planes de seguridad, registrar las acciones y eventos que podrían tener impacto sobre la efectividad y desempeño del SGSI

Con los resultados obtenidos durante la revisión del SGSI, se actualizarán los planes de seguridad. Se mantendrán registros para proporcionar evidencia de conformidad con los requerimientos y la operación efectiva del SGSI, estos documentos deben ser protegidos, controlados y mantenerse:

- Legibles
- Fácilmente inidentificables
- Recuperables.

Se documentará e implementará los controles necesarios para:

- Identificación
- Almacenaje
- Protección
- Recuperación
- Tiempo de retención
- Disposición de registro

3.5 Mantener y mejorar el SGSI

En esta última etapa la organización debe mejorar de forma continua la eficacia del SGSI por medio de:

1.- Implementar las mejoras identificadas al SGSI.

2.- Tomar las acciones correctivas y preventivas apropiadas.

- Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.

3.- Comunicar los resultados y asegurar que las mejoras logren sus objetivos señalados

4.- Asegurar que las mejoras logren sus objetivos señalados.

3.5.1 Implementar las mejoras identificadas en el SGSI

Al terminar la auditoria, es necesario llevar a cabo mejoras al SGSI asegurando así su actualización *(Ver cuadro 24*).

3.5.2 Tomar las acciones correctivas y preventivas apropiadas

3.5.2.1 Acciones correctivas

La organización debe tomar acciones para eliminar la causa de las no conformidades respecto de los requisitos del SGSI para evitar que éstas vuelvan a ocurrir.

El documento para la acción correctiva debe definir los requisitos para:

- Identificar no conformidades.
- Determinar la causa de las no conformidades.
- Determinar e implementar la acción correctiva requerida.
- Registrar los resultados de la acción acometida.

Logotipo de la empresa			***Formato 18***
Auditor: Realizará y contestará ***Comité gerencial: Revisará*** ***Comité de seguridad: Llevará a cabo***			
Causa de des conformidad			
Nombre del auditor:			
Código del activo/ área/control	***Impacto:**	**Fecha inicio de eliminación de la causa:**	**Fecha termino de eliminación de la causa:**
¿Qué fue lo que causo la des conformidad?:			
¿Acción tomada para evitar que vuelva a ocurrir?:			
Recursos otorgado para disminuir la causa:			
Responsable de disminución de la causa:			
_____ ***Nombre y firma del Comité gerencial*** _____ _____ ***Nombre y firma del Comité de gestión*** ***Nombre y firma del Auditor interno***			

Cuadro 26. Formato causa de las des conformidades

3.5.2.2 Acciones preventivas

El auditor interno emitirá un informe sobre las acciones preventivas existentes, *(Ver cuadro 27).*

Las acciones preventivas son usualmente más eficaces en cuanto a coste que las acciones correctivas.

Logotipo de la empresa		***Formato 19***
Auditor interno: Realizará y contestará ***Comité gerencial: Revisará*** ***Comité de seguridad: Llevará a cabo***		
Acciones preventivas		
Nombre del auditor:		
Código del activo/ área/control	**Fecha inicio de eliminación de la causa:**	**Fecha termino de eliminación de la causa:**
¿Acción preventiva detectada?:		
Recursos otorgados:		
Responsable de llevarla a cabo:		
_____ ***Nombre y firma del Comité gerencial*** _____ ***Nombre y firma del Comité de gestión*** _____ ***Nombre y firma del Auditor interno***		

Cuadro 27. Formato acciones preventivas

3.5.3 Aplicar las lecciones aprendidas de las experiencias de seguridad de otras organizaciones y aquellas de la organización misma.

La organización deberá llevar a cabo un registro de incidentes de seguridad llevados a cabo por otras organizaciones, el comité de seguridad será el encargado de registrar estos eventos, previniendo los percances similares que se pudieran dar en la organización.

Ejemplo: Descuido en materia de seguridad de datos, por la cual los datos de empleados en la empresa XXXX fueron expuestos afectando a los empleados, la reputación y confianza de la empresa.

3.5.4 Comunicar los resultados y asegurar que las mejoras logren sus objetivos señalados

Se darán a conocer los resultados de las mejoras, acciones preventivas y correctivas a todas las partes interesadas, con un nivel de detalle apropiado de acuerdo a las circunstancias y, cuando sea relevante, acordar como proceder.

3.5.5 Asegurar que las mejoras logren sus objetivos señalados.

Una vez que las mejoras se han realizado por el personal asignado, deberán ser revisadas por el comité de seguridad y el comité gerencial, con el objetivo de asegurar que se estas se han llevando a cabo.

CONCLUSIONES

En este trabajo escrito se ha tratado el tema de seguridad de la información bajo el estándar ISO / IEC 27001. Para poder hablar del tema se tuvo que partir desde el desglose de cada elemento del tema principal, esto es, hablar desde ISO hasta aterrizar con un manual interpretativo sobre el ISO 27001.

Para muchos de nosotros, ya es muy común observar a nuestro alrededor empresas u organizaciones que "presumen" una certificación, y los usuarios finales sentimos gusto y admiración por saber que en quien se ha depositado la confianza para adquirir un producto o servicio cumple con características tan particulares en sus procesos que hablan de la calidad que se nos ofrece. Sin embargo, al estudiar que es un estándar nos damos cuenta que calidad no solo se ve al final de la producción o al palpar un servicio, se inicia desde el proceso de suministro de materiales, de la forma de como transformarlos y como llega al usuario final. Pero ahora bien, y con respecto a la seguridad ¿Qué se puede decir?. Primeramente que seguridad es un término ambiguo, cada persona (física o moral) va a interpretarla de acuerdo a sus lineamientos y políticas, pero si estaremos todos de acuerdo en que este término puede ser sinónimo de resguardo y protección. Seguridad de la información, es tan ambiguo como el primero, la información es un activo vital para el éxito y la continuidad en el mercado de cualquier organización. El aseguramiento de dicha información y de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para la organización, pues bien, el tesoro más valioso de una empresa es su información por tanto, al ser este el tesoro por el cual se da todo se busca tener un control implementado para ello nos apoyamos de un estándar internacional como lo es ISO 27000.

Este estándar, es muy amplio, consta de más de veinte apartados pero lo interesante de ello es que se pueden entrelazar garantizando una máxima seguridad en la organización.

ISO 27001 es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información, en México es conocida con el nombre de NMX-I-041/02-NYCE, lo que se realizó en este trabajo fue una interpretación de la norma y generar pasos muy concretos de los elementos solicitados para así tener una base que sirva al gestor de la información y poder aspirar a una evaluación con fines de certificación en dicha norma.

Las empresas requieren en la actualidad contar con certificaciones pues ello las hace más competitivas, sin embargo, éstas son en primera instancia costosas, seguido de que no todas han sido traducidas al idioma natal de los miembros de la empresa, por tanto es importante generar un manual en el que se describan muy concretamente que se busca y que elementos se deben colocar, ya que cuando la empresa se somete a la certificación el

grupo evaluador traerá su checklist e irá palomeando el cumplimiento y nivel alcanzado, es por ello que se considera que se alcanzó el objetivo planteado para este trabajo de tesina, pues se tiene información relevante de ISO, IEC, se habló de ISO 27000 y se interpretó a ISO 2001. Se espera que el trabajo sea útil para alguien interesado en el mundo de la calidad globalizada.

ANEXO A

CONTROLES A IMPLEMENTAR EXTRAÍDOS DE LA NORMA ISO/IEC 27001

A.5 POLÍTICA DE SEGURIDAD		
A.5.1 Política de seguridad de la información **Objetivo de control: Proporcionar dirección general y apoyar a la seguridad de la información en concordancia con los requerimientos comerciales, leyes y regulaciones relevantes.**		
5.1.1	Documentar política de seguridad de la información	Control: La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
A.5.1.2	Revisión de la política de la seguridad de la información	Control: La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continuidad, idoneidad, eficiencia y efectividad.
A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN		
A.6.1 Organización interna **Objetivo: Manejar la seguridad de la información dentro de la organización.**		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control: La gerencia debe apoyar activamente a la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explicita y reconocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de la información	Control: Las actividades de la seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.

A.6.1.3	Asignación de las responsabilidades de la seguridad de la información	Control: Se deben definir claramente las responsabilidades de la seguridad de la información.
A.6.1.4	Proceso de la autorización para los medios de procesamiento de la información.	Control: Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A.6.1.5	Acuerdo de la confidencialidad	Control: Se deben identificar y revisar regularmente los requerimientos de confidencialidad a los acuerdos de no divulgación, reflejando las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	Control: Se debe mantener los contactos apropiados con autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	Control: Se deben mantener contacto a apropiados con los grupos de interés especial y otros foros de seguridad especializados y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para mejorar la seguridad de la información y su implementación (es decir; objetivo de control, controles, políticas procesos y procedimientos para la seguridad de la información) se debe realizar independientemente a intervalos planeados, o cuando ocurran cambios para la implementación de la seguridad.
A.6.2 Entidades externas **Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tiene acceso y procesan; y son comunicados a o manejados por entidades externas.**		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control: Se deben identificar los riesgos que corren la información y los medios de procesamiento de la información de la organización y se debe implementar los controles apropiados antes de otorgar acceso.

A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes.	Control: Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas.	Control: Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregan productos o servicios a los medios de procesamiento de la información deben abarcar los requerimiento de seguridad necesarios relevantes.
A.7 GESTIÓN DE ACTIVOS		
A.7.1 Responsabilidad de los activos **Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.**		
A.7.1.1	Inventarios de los activos	Control: Todos los activos deben de estar claramente identificados y se deben elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control: Toda la información y los activos asociados con los medios de procesamiento de la información deben ser propiedad de una parte designada de la organización.
A.7.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
A.7.2 Clasificación de la información **Objetivo: Asegurarse que la información reciba un nivel de protección apropiado.**		
A.7.2.1	Lineamientos de clasificación	Control: la información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico de la organización.
A.7.2.2	Etiquetado y manejo de la	Control: Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el

	información	esquema de clasificación adoptado por la organización.
A.8 SEGURIDAD DE LOS RECURSOS HUMANOS		
A.8.1 Antes del empleo **Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.**		
A.8.1.1	Roles y responsabilidades	Control: Se debe definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de la información.
A.8.1.2	Selección	Control: Se debe llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.8.1 .3	Términos y condiciones de empleo	Control: Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la organización para la seguridad de la información.
A.8.2 Durante el empleo **Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de la información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal y reducir los riesgos de error humano.**		
A.8.2.1	Gestión de responsabilidades	Control: La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.

A.8.2.2	Capacitación y educación en seguridad de la información	Control: Todos los empleados de la organización y, cuando sea relevante los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actuaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	Control: Debe existir un proceso formal disciplinario para los empleados que han cometido una violación en la seguridad.
A.8.3 Terminación o cambio de empleo **Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.**		
A.8.3.1	Responsabilidades de terminación	Control: Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio de empleo.
A.8.3.2	Devolución de los activos.	Control: Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posición a la terminación de su empleo, contrato o acuerdo.
A.8.3.3	Eliminación de derechos de acceso.	Control: Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
A.9 SEGURIDAD FÍSICA Y AMBIENTAL		
A.9.1 Áreas seguras **Objetivo: Evitar el acceso físico no autorizado, daño o interferencia la local y la información de la organización.**		
A.9.1.1	Parámetro de seguridad física	Control: Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger aéreas que contiene información y medios de procesamiento de información.

A.9.1.2	Controles de entrada física	Control: se deben de proteger las áreas seguras mediante controles de entrada apropiados para asegurar que solo se permita acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones y medios	Control: Se deben diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4	Protección contra amenazas externas y ambientales	Control: se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5	Trabajo en áreas seguras	Control: Se deben diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso público, entrega y carga	Control: Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no autorizadas pueden ingresar a los locales, cuando fuese posible, se deben de aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.
A.9.2 Seguridad del equipo **Objetivo: Evitar la pérdida, daño, robo compromiso de los activos y la interrupción de las actividades de la organización.**		
A.9.2.1	Ubicación y protección del equipo	Control: El equipo debe estar ubicado o protegido para reducir los riesgos o las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2	Servicios públicos	Control: El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

A.9.2.3	Seguridad en el cableado	Control: El cableado de la energía y las telecomunicaciones que llevan data o sostiene los servicios de información deben ser protegidos de la de la interrupción o daño.
A.9.2.4	Mantenimiento de equipo	Control: El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera del local	Control: Se debe aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6	Eliminación de seguro o re uso del equipo	Control: Todos los ítems del equipo que tengan medios de almacenaje deben ser checados para asegurar que se hayan removido o sobre-escrito de manera segura, cualquier data confidencial y software con licencia antes de su eliminación.
A.9.2.4	Trasladado de la propiedad	Control: Equipos, información o software no deben ser sacados de la propiedad sin previa autorización.
A.10 GESTIÓN DE COMUNICACIONES Y OPERACIONES		
A.10.1. Procedimientos y responsabilidades operacionales **Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información.**		
A.10.1.1	Procedimiento de operación documentados	Control: Se deben documentar y mantener los procedimientos de operación y se deben poner a disposición de todos los usuarios que los necesite
A.10.1.2	Gestión de cambio	Control: Se deben controlar los cambios en los medios y sistemas de procesamiento de la información
A.10.1.3	Segregación de deberes	Control: Se deben segregar los deberes de responsabilidad para reducir las oportunidades de una modificación no autorizada o no intencionada o un mal uso de los activos de la información

A.10.1.4	Separación de los medios de desarrollo y operacional	Control: Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de acceso no autorizado o cambios en el sistema operacional.
A.10.2 Gestión de la entrega de servicios de terceros **Objetivo: Implementar y mantener el nivel apropiado de la seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.**		
A.10.2.1	Entrega del servicio	Control: Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega fluidos con el control de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2	Monitoreo y revisión y de los servicios de terceros	Control: Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorias se deben llevar a cabo regularmente.
A.10.2.3	Manejar los cambios en los servicios de terceros	Control: Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y controles de seguridad existentes, tomando en cuenta el grado critico de los sistemas y procesos comerciales involucrados y la reevaluación de los riesgos.
A.10.3 Planeación y aceptación del sistema. **Objetivo: Minimizar el riesgo de fallas en los sistemas.**		
A.10.3.3	Gestión de capacidad	Control: Se deben monitorias, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2	Aceptación del sistema	Control: Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cobo pruebas actualizadas del/los sistema(s) durante su desarrolla y su aceptación.
A.10.4 Protección contra software malicioso y código móvil **Objetivo: Proteger la integridad del software y la información.**		

A.10.4.1	Controles contra software malicioso	Control: Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos maliciosos y se deben implementar procedimientos de conciencia apropiados.
A.10.4.2	Controles contra códigos móviles	Control: Cuando se autoriza el uso de código móvil, a configuración debe asegurar que el código móvil autorizado actué de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no autorizado.
A.10.5 Respaldo (back-up) **Objetivo: Mantener la integridad y disciplina de los servicios de procesamiento de información y comunicación.**		
A.10.6.1	Controles de red	Control: Las redes deben ser adecuadamente controladas y manejadas para poderlas proteger de amenazas y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad en los servicios de red	Control: Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya que estos servicios sean provistos en casa o sean abastecidos externamente.
A.10.6 Gestión de medios **Objetivos: Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos; y la interrupción de las actividades comerciales.**		
A.10.7.1	Gestión de los medios removibles	Control: Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Eliminación de medios	Control: Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiera.

A.10.7.3	Procedimientos de manejos de la información	Control: Se deben establecer los procedimientos para el manejo y almacenaje de la información de una divulgación no autorizada o un mal uso.
A.10.7.4	Seguridad de documentación del sistema.	Control: Se debe proteger la documentación de un acceso no autorizado.
A.10.8 Intercambio de la información. **Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.**		
A.10.8.1	Procedimientos y políticas de información y software	Control: Se deben establecer políticas, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2	Acuerdos de intercambio	Control: Se debe establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	Medios físicos en transito	Control: Los medios que tiene información deben de ser protegidos contra un acceso no autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajes electrónicos	Control: Se deben proteger adecuadamente los mensajes electrónicos.
A.10.8.5	Sistemas de información comercial	Control: Se deben desarrollar e implantar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.10.9 Servicios de comercio electrónico **Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro.**		
A.10.9.1	Comercio electrónico	Control: Se debe proteger la información involucrada en el comercio electrónico que se transmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual, divulgación y modificación no autorizada.

A.10.9.2	Transacciones en línea	Control: Se debe proteger la información involucrada en las transacciones en línea para evitar la transmisión incompleta, rutas equivocadas, alteración no autorizada del mensaje, divulgación no autorizada y duplicación o reenvío no autorizado del mensaje.
A.10.9.3	Información disponible públicamente	Control: Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada
A.10.10 Monitoreo **Objetivo: Detectar actividades de procesamiento de información no autorizadas.**		
A.10.10.1	Registro de auditoria	Control: Se deben producir registros de la actividad de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un periodo acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2	Uso del sistema de monitoreo	Control: Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3	Protección de la información del registro	Control: Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no autorizado.
A.10.10.4	Registros del administrador y operador	Control: Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5	Registro de fallas	Control: Las fallas se deben registrar, analizar y se deben tomar las acciones adecuadas.
A.10.10.6	Sincronización de los relojes	Control: Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben ser sincronizados con una fuente de tiempo externa.
A.11 CONTROL DE ACCESO		

A.11.1 Requerimiento comercial para el control del acceso **Objetivo: Controlar acceso a la información**		
A.11.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
A.11.2 Gestión del acceso al usuario **Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.**		
A.11.2.1	Inscripción del usuario	Control: Debe existir un procedimiento formal para la inscripción y des inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control: Se debe restringir y controlar la asignación y uso de privilegios.
A.11.2.3	Gestión de la clave del usuario	Control: La asignación de claves se debe de controlar a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso del usuario	Control: La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario **Objetivo: Evitar el acceso de usuario no autorizado y el compromiso a robo de la información y los medios de procesamiento de la información.**		
A.11.3.1	Uso de clave	Control: Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2	Equipo de usuario desatendido	Control: Se debe requerir que los usuarios se aseguren de dar protección apropiada al equipo desatendido.
A.11.3.3	Política de pantalla y escritorio limpio	Control: Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje movibles y una política de pantalla limpia para los medios de procesamiento de información.
A.11.4 Control de acceso a redes		

Objetivo: Evitar el acceso no autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios de red	Control: Los usuarios solo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.11.4.2	Autenticación del usuario para conexiones externas	Control: Se debe de utilizar métodos de autentificación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación del equipo en red	Control: Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección del puerto de diagnóstico remoto	Control: Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Segregación en redes	Control: Los servicios de información, usuarios y sistemas de información se deben segregar en redes.
A.11.4.6	Conexión de redes.	Control: Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizacionales, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales.
A.11.4.7	Routing de redes	Control: Se deben implementar controles routing para las redes, para asegurar que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema de operación **Objetivo: Evitar acceso no autorizado a los sistemas operativos.**		
A.11.5.1	Procedimiento de registro en el terminal	Control: Se deben controlar el acceso a los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2	Identificación y autentificación del usuario	Control: Todos los usuarios deben tener identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una

		técnica de autenticación adecuada para verificar la identidad del usuario.
A.11.5.3	Sistema de gestión de claves	Control: Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4	Uso de utilidades del sistema	Control: Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5	Sesión inactiva	Control: Las sesiones inactivas deben serrase después de un periodo de inactividad definido.
A.11.5.6	Limitación de tiempo de conexión	Control: Se deben utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a la aplicación e información **Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.**		
A.11.6.1	Restricción al acceso a la información	Control: Se debe restringir el acceso a los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2	Aislamiento del sistema sensible	Control: Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
A.11.7 Computación móvil y tele trabajo **Objetivo: Asegurar la seguridad de la información cuando se utilicen medios de computación móvil y tele trabajo.**		
A.11.7.1	Computación móvil y comunicaciones	Control: Se debe de establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios computación y comunicación móviles.
A.11.7.2	Tele-trabajo	Control: Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.		

A.12.1.4	Análisis y especificación de los requerimientos de seguridad	Control: Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
A.12 .2 Procesamiento correcto en las aplicaciones **Objetivo: Evitar errores, perdida, modificación no autorizada a mal uso de la información en las aplicaciones.**		
A.12.2.1	Validación de datos de insumo	Control: El insumo de datos en las aplicaciones debe ser válido para asegurar que este dato sea válido y aprobado.
A.12.2.2	Control de procesamiento interno	Control: Se debe incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción en la información a través de errores de procesamiento o actos deliberados.
A.12.2.3	Integridad del mensaje	Control: Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones y se debe identificar e implementar los controles de apropiados.
A.12.2.4	Validación de data de output (salida de datos)	Control: Se debe validar el output de data (salida de datos) de una aplicación para asegurar que el procesamiento de la información almacenada sea el correcto y apropiado para las circunstancias.
A.12 .3 Controles criptográficos **Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.**		
A.12.3.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión clave	Control: Se debe usar una gestión clave para el uso de las técnicas de criptografía en la organización.
A.12 .4 Seguridad de los archivos del sistema **Objetivo: Garantizar la seguridad de los archivos del sistema**		

A.12.4.1	Control de software operacional	Control: Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.4.2	Protección de los datos de prueba del sistema	Control: Se debe seleccionar cuidadosamente, proteger y controlar los datos de prueba.
A.12.4.3	Control de acceso al código fuente del programa	Control: Se debe restringir el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte. **Objetivo: Mantener la seguridad del software e información del sistema de aplicación.**		
A.12.5.1	Procedimientos de control de cambios	Control: La implementación de cambios debe controlar mediante el uso de procedimientos formales de control de cambio.
A.12.5.2	Revisión técnica en las aplicaciones después de cambios en el sistema operativo.	Control: Cuando se cambian los sistemas operativos, se deben revisar y aprobar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	Control: No se deben fomentar las aplicaciones a los paquetes de software, que deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
A.12.5.4	Filtración de información	Control: Se debe evitar la oportunidades de filtración de la información
A.12.5.5	Desarrollo de subcontratados de software	Control: El desarrollo de software que ha sido subcontratado debe ser supervisado y monitoreado por la organización.
A.12.6. Gestión de vulnerabilidad técnica **Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.**		
A.12.6.1	Control de vulnerabilidades técnicas	Control: Se debe tener información oportuna sobre la vulnerabilidad técnica de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y deben tomas las medidas apropiadas para tratar el riesgo asociado.
A.13. GESTIÓN DE INCIDENTES DE LA INFORMACIÓN.		

A.13.1 Reporte de eventos y debilidades en la seguridad de la información **Objetivo: Asegurar la información de los eventos y debilidades en la seguridad de la información asociada con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.**		
A.13.1.1	Reporte de eventos en la seguridad de la información.	Control: Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2	Reporte de debilidades en la seguridad	Control: Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
A.13.2. Gestión de incidentes y mejoras en la seguridad de la información. **Objetivo: Asegurar que se aplique consistente y efectivo a la gestión de la seguridad de la información.**		
A.13.2.1	Responsabilidades y procedimientos	Control: Se debe establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de la seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información.	Control: Deben existir mecanismos para monitorear y cuantificar los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3	Recolección de evidencia	Control: Cuando la acción de seguimiento contra persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia estable en la(s) jurisdicción (es) relevantes.
A.14. GESTIÓN DE LA CONTINUIDAD COMERCIAL		
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial **Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los**		

procesos comerciales críticos de los efectivos de fallas o desastres importantes o desastres en los sistemas de información y asegurar la reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de continuidad comercial.	Control: Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2	Continuidad comercial y evaluación del riego	Control: Se deben identificar los eventos que causan interrupciones en los procesos comerciales de la organización.
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control: Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	Control: Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las propiedades de prueba y mantenimiento.
A.14.1.5	Prueba, mantenimiento y re-evaluación de planes de continuidad comerciales.	Control: Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que sean actualizados y sean efectivos.
A.15 CUMPLIMIENTO		
A.15.1 Cumplimiento con requerimientos legales **Objetivo: Garantizar el uso legal de información**		
A.15.1.1	Identificación de legislación aplicable	Control: Se deben definir explícitamente, documentar y actualizar todos los requerimientos estatuarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.

A.15.1.2	Derechos de propiedad intelectual (IPR)	Control: Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3	Protección de los registros organizacionales	Control: Se den proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatuarios, reguladores, contractuales y comerciales.
A.15.1.4	Protección de datos y privacidad de información personal	Control: Se debe asegurar la protección y privacidad del cómo se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
A.15.1.5	Prevención de mal uso de medios de procesamiento de información.	Control: Se debe desanimar a los usuarios de utilizar los medios de procesamiento de información para propósitos no autorizados.
A.15.1.6	Regulación de controles criptográficos	Control: Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad y el cumplimiento técnico. **Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.**		
A.15.2.1	Cumplimiento con las políticas y estándares de seguridad	Control: Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2	Chequeo de cumplimiento técnico	Control: Los sistemas de información deben checarse regularmente para el cumplimiento con los estándares de la seguridad.
A.15.3 Consideraciones de auditoría de los sistemas de información. **Objetivo: Maximizar la efectividad y minimizar la interferencia de/desde el proceso de auditoría de los sistemas de información.**		
A.15.3.1	Auditoría de sistemas	Control: Se debe planear cuidadosamente los requerimientos y actividades de las auditorias

	de información	que involucran chequeos de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información	Control: Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

BIBLIOGRAFÍA

[1] [H. fime] Leonard, *Seguridad de centro de cómputo políticas y procedimientos*, Editorial Trillas.

[2] [Daniel Diosdado Rivera]. *La seguridad de la información requiere de una certificación.* Fecha de creación 10 de Mayo del 2011. Fecha de consulta: 7/01/2013

[3]http://www.iso.org/iso/home.html. Fecha de consulta 28/04/2013

[4]http://www.iec.ch/. Fecha de consulta: 28/05/2012.

[5] http://www.inegi.org.mx/. Fecha de consulta: 2/08/2012.

[6]www.iee.org.mx/cs/boletin/2012/sep/B_01_020912.doc.
Fecha de consulta: 7/01/2013. Fecha de creación: 2/09/2012.

[7] http://www.aenormexico.com/ Fecha de consulta: 7/01/2013.

[8] http://www.ema.org.mx/ema/ema/index.php Fecha de consulta: 12/04/2013.

[9] http://www.nyce.org.mx/index.php/sistemas/iso-27001 Fecha de consulta: 25/06/2013.

[10] ISO / IEC Comité Técnico Conjunto 1 - JTC 1, *El multiplicador de fuerza para la innovación en TIC Estándares de tecnología de la información.* Fecha de consulta: 29/07/2013.

[13] ISO/IEC 27000:2012 Tecnología de la información-Técnicas de seguridad - Sistemas de gestión de seguridad de la información - Información general y vocabulario (segunda edición).

[14] ISO/IEC 27001: 2005 Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de seguridad de la información – Requisitos

[15]ISO/IEC 27002:2005 Tecnología de la información-Técnicas de seguridad - Código de buenas prácticas para la gestión de seguridad de la información.

[16]ISO/IEC 27003:2010 Tecnología de la información-Técnicas de seguridad - Información de gestión de seguridad de la Guía de Implementación del sistema.

[17]ISO/IEC 27004: 2009 Tecnología de la información-Técnicas de seguridad - gestión de seguridad de la información – Medición.

[16]ISO/IEC 27005: 2011 Tecnología de la información-Técnicas de seguridad - Gestión del riesgo de seguridad de la información (segunda edición)

[17]ISO/IEC 27006:2011 Tecnología de la información-Técnicas de seguridad - Requisitos para los organismos que presten servicios de auditoría y certificación de sistemas de gestión de seguridad de la información

[18]ISO/IEC 27007: 2011 Tecnología de la información-Técnicas de seguridad - Directrices para la gestión de información de seguridad de los sistemas de auditoría.

[19]ISO/IEC 27008: 2011 Tecnología de la información-Técnicas de seguridad - Directrices para los auditores de sistemas de gestión de seguridad de la información controla

[20]ISO/IEC 27010: 2012 Tecnología de la información-Técnicas de seguridad - Gestión de seguridad de la información para las comunicaciones entre los sectores.

[21]ISO/IEC 27011:2008 Tecnología de la información-Técnicas de seguridad - Directrices de gestión de seguridad de la información para las organizaciones de telecomunicaciones basado en la norma ISO / IEC 27002.

[22]ISO/IEC27015:2012 Tecnología de la información-Técnicas de seguridad - Directrices de gestión de seguridad de la información de los servicios financieros.

[23]ISO/IEC 27031: 2011 Tecnología de la información-Técnicas de seguridad - Directrices para la información y las comunicaciones preparación tecnológica para la continuidad del negocio.

[24]ISO/IEC 27032: 2012 Tecnología de la información-Técnicas de seguridad - Directrices para la ciberseguridad

[25]ISO/IEC 27034: 2011 Tecnología de la información-Técnicas de seguridad - la seguridad de aplicaciones.

[26]ISO/IEC27037:2012 Tecnología de la información - Técnicas de seguridad - Directrices para la identificación, recolección, adquisición y preservación de evidencia digital

[27]ISO/IEC27799:2008 Informática de la Salud - Gestión de seguridad de la información en materia de salud.