UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE INGENIERÍA

LA UNAM COMO ORGANISMO CERTIFICADOR DE LA NORMA ISO/IEC 27001:2005

INFORME DE ACTIVIDADES

QUE PARA OBTENER EL TÍTULO DE

INGENIERO EN COMPUTACIÓN

P R E S E N T A N :

ACOSTA REZA JAZMIN

LOMA AMEL FRANCISCO

ASESORA: M.C. MARÍA JAQUELINA LÓPEZ BARRIENTOS

CIUDAD UNIVERSITARIA, 2010

Dios me brindó la oportunidad de tener dos pilares fundamentales en mi vida, quienes me enseñaron que para lograr mis sueños, metas y objetivos se tiene que trabajar arduamente y que la base de todo éxito es la humildad, el sacrificio, la oración y la felicidad, el resultado de sus enseñanzas, así como de mi esfuerzo y dedicación es la presente tesis.

La cual dedico con amor y cariño:

A Dios, a mis Padres, los pilares que Dios me obsequió, a mí por el empeño, constancia y compromiso que demostré durante la realización de la tesis y a ti Francisco mi amigo, compañero y primer amor.

Jazmín

La culminación de la presente tesis es el resultado de un gran esfuerzo y dedicación, pero esto no hubiese sido posible sin el apoyo de las personas que estuvieron a mi lado,

Por lo que esta tesis la dedico con cariño:

A Dios por la vida prestada y por las personas que puso en mi camino,

A mis padres, pilar fundamental en mi desarrollo personal,

A mis hermanos, por su compañía, amistad y apoyo,

A mi Hermano Oscar por su gran apoyo incondicional, y

A Jazmín por ser mi complemento, mi amiga y mi amor.

Francisco

AGRADECIMIENTOS

Doy especial agradecimiento a:

Dios, por darme la vida y porque con cada prueba que me pone me hace más fuerte.

Mis Padres, por brindarme su apoyo, comprensión y amor, pero sobre todo por confiar en mí y tenerme paciencia.

Mis hermanos y a sus familias, por apoyarme y creer en mí.

Francisco, por estar conmigo en las buenas y en las malas, por compartir mis sueños y ayudarme a cumplirlos.

La Maestra Jaquelina, por haber dirigido el trabajo de investigación, por compartirnos su conocimiento y experiencia, por la paciencia y apoyo que siempre nos demostró.

La Facultad de Ingeniería, por la formación que recibí dentro y fuera de sus aulas, y por permitirme ser orgullosamente Universitaria.

Todos los profesores que contribuyeron en mi formación como Ingeniera.

Mis amigos, porque siempre estuvieron apoyándome y motivándome, además de enseñarme el verdadero valor de la amistad.

Finalmente, a todas aquéllas personas que directa e indirectamente contribuyeron a la realización de esta tesis.

Jazmín.

AGRADECIMIENTOS

Quiero dar un especial agradecimiento a:

Mis padres, por brindarme su cariño, amor, bondad, paciencia, comprensión, apoyo incondicional y consejos, por sus regaños y llamada de atención y, sobre todo, por la formación y valores inculcados.

Mis hermanos, por su compañía, comprensión, consejos y por todo lo aprendido conviviendo con ellos.

Oscar, por todo el apoyo recibido, por los sacrificios hechos para brindarme todo lo que estuvo a tu alcance, por tus consejos y palabras de aliento.

Jazmín, por emprender y concluir este proyecto conmigo y permanecer a mi lado, por soportarme, por brindarme tu comprensión, cariño y amor, por tus palabras de aliento y consuelo en los momentos de desesperación y decepción, por compartir tus ideas, sueños e ilusiones, por ser una parte fundamental de mi vida.

Los señores Roberto Acosta y Francisca Reza, por brindarme su apoyo, amistad y confianza y a sus hijos que me brindaron su amistad y compañía.

La M.C. María Jaquelina López Barrientos, quien dirigió esta tesis, que con sus consejos y recomendaciones hicieron posible la culminación de ésta, que siempre estuvo al pendiente de nuestros avances y nuestra situación personal, siempre motivándonos a seguir adelante.

A la Facultad de Ingeniería, por abrigarme dentro de sus instalaciones y por la formación académica que recibí.

A todos los profesores, que con sus conocimientos fueron parte de mi formación académica.

A mis amigos, por sus consejos, su apoyo y su amistad desinteresada.

Y por último, a todas aquellas personas que ayudaron y contribuyeron de manera directa o indirecta al desarrollo de esta tesis, en especial a los jefes de los laboratorios que muy amablemente nos brindaron parte de su valioso tiempo.

Francisco

ÍNDICE

Capítulo 3:

Requisitos para definir el proceso de Certificación 54

Capítulo 4:

Evaluación de la Facultad de Ingeniería 77

PRÓLOGO

Prólogo

PRÓLOGO

En un mundo globalizado definido por la competitividad y por normativas cada vez más exigentes en lo que a seguridad y a calidad se refieren, la acreditación, se ha convertido en un elemento indispensable para garantizar la confianza de las evaluaciones y certificaciones realizadas sobre productos o servicios.

Hoy en día las organizaciones, tanto públicas como privadas, asumen estándares que exigen que los productos y servicios sean evaluados por motivos de seguridad, salud, protección del medio ambiente, lucha contra el fraude o para asegurar la competencia leal. Por ello algunas de las organizaciones han creado un sistema voluntario de evaluación para alcanzar un alto grado de fiabilidad así como una competencia en condiciones equitativas.

Así, surge la necesidad de los Organismos de Evaluación de la Conformidad (OEC), conformados por Laboratorios, Unidades de Verificación y Organismos de Certificación, que son los organismos encargados de determinar objetivamente el cumplimiento de las normas establecidas en una empresa. Figura 1.

Para que los OEC sean confiables en sus evaluaciones necesitan demostrar al comprador, a la autoridad responsable y al público en general que son organismos competentes en la labor que realizan. Por ese motivo necesitan ser evaluadas imparcialmente por los Organismos de Acreditación.

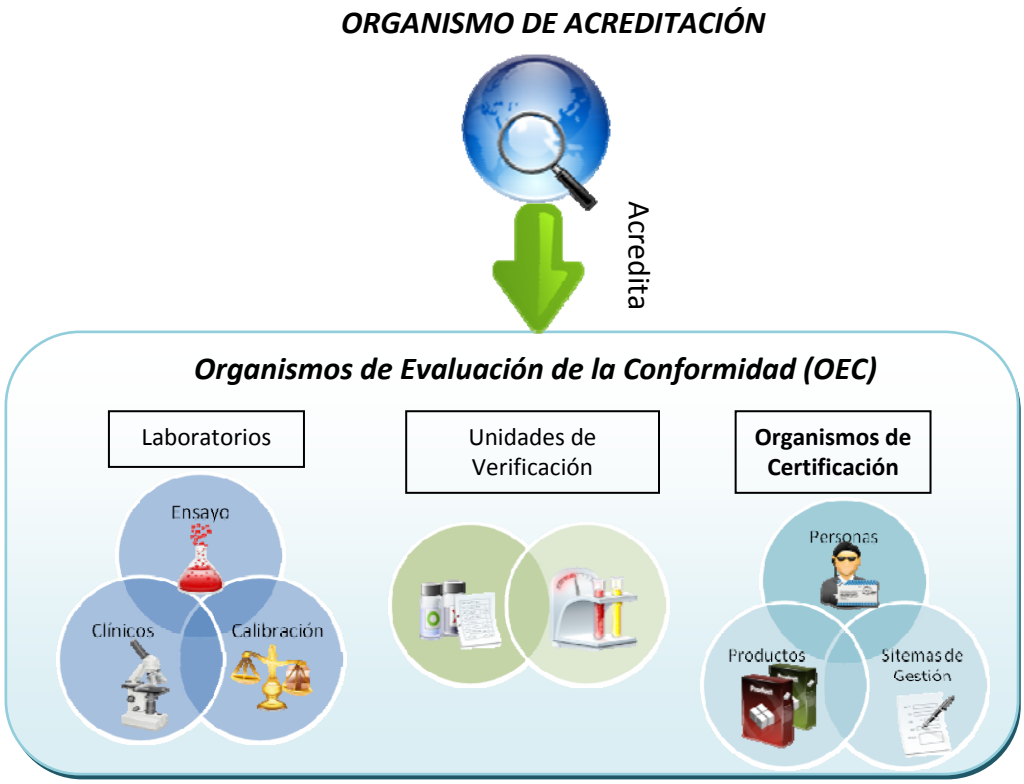


Figura 1. Relación entre un Organismo Acreditador y los Organismos de Evaluación de la Conformidad.

De acuerdo a la figura 1, un Organismo de Acreditación, es el encargado de comprobar, mediante evaluaciones independientes e imparciales, la competencia de los OEC con objeto de dar confianza al comprador y a la Administración, contribuyendo, así, a facilitar tanto el comercio nacional como internacional.

Los Organismos de Acreditación de los distintos países desempeñan su tarea conforme a los mismos criterios internacionales, utilizando métodos de evaluaciones equivalentes y transparentes, generando la adecuada confianza que posibilita la aceptación mutua de resultados.

La acreditación es el acto que da la seguridad y avala que los laboratorios, unidades de verificación y OEC ejecuten las regulaciones, normas o estándares correspondientes con precisión para que comprueben o verifiquen los productos y servicios que consume la sociedad.

La acreditación implica que el OEC ha demostrado que:

- Cuenta con personal calificado y con experiencia.
- Dispone del equipamiento adecuado, calibrado y mantenido correctamente, y de las infraestructuras necesarias para el desarrollo de su actividad.
- Aplica métodos y procedimientos de evaluación válidos y apropiados.
- Emplea técnicas de control de calidad de los resultados.
- Asegura la trazabilidad de las mediciones y calibraciones a patrones internacionales.
- Informa adecuadamente a sus clientes de los resultados de sus actividades, emitiendo informes o certificados claros y precisos.
- Cuenta con un sistema de aseguramiento de la calidad para gestionar su actividad.

El Proceso de acreditación, subordinado al Organismo Acreditador, y consiste de tres pasos:

- PASO 1: Solicitud de acreditación.
- PASO 2: Evaluación.
- PASO 3: Decisión y Mantenimiento de acreditación.

La acreditación en México es una herramienta de crecimiento y productividad, para fortalecer la competitividad.

Los Organismos de Certificación se basan en normas nacionales o internacionales para asegurar la imparcialidad de sus evaluaciones. Para que estos Organismos de Certificación sean confiables es necesario demostrar que han pasado por un proceso de acreditación y éste ha sido superado satisfactoriamente. Dicho proceso avala que un Organismo de Certificación cumple con los requisitos establecidos en una norma para poder realizar actividades de evaluación de Sistemas de Gestión, productos, laboratorios y/o personas.

La certificación es la confirmación que una organización ha implementado un sistema de gestión conforme a ciertos requisitos, es decir, es el procedimiento por el cual se asegura que un producto, proceso, sistema o servicio se ajusta a las normas o lineamientos o recomendaciones de organismos dedicados a la normalización nacional o internacional.

Es recomendable certificarse porque:

- El mercado, los usuarios de los servicios y las relaciones inter-institucionales lo están exigiendo.
- La certificación promueve la identificación y satisfacción de las necesidades y expectativas de confiabilidad de sus clientes y otras partes interesadas.
- Incrementa la ventaja competitiva.
- Ayuda a definir métodos de trabajo.
- Fomenta la comunicación entre las áreas de la organización.
- Si se toma como un compromiso interno, se inducirá a todos los integrantes de la organización al trabajo con orden y a la larga esto se convierte en un hábito.
- Ayuda a mejorar la eficacia y eficiencia de la operación y capacidades de la organización.

Los beneficios de implementar un Sistema de Gestión Certificado son:

- Permite identificar las fortalezas y debilidades de la organización.
- Proporciona una base para la Mejora Continua.
- Posibilita el reconocimiento externo.
- Mejoras en los resultados operativos, tales como, ingresos, costos y participación de mercado.
- Aumenta la fidelidad del cliente con la reiteración de los negocios y la recomendación de la empresa.
- Alineación de los procesos para alcanzar los resultados deseados.
- Uso eficaz y eficiente de los recursos.
- Mayor compresión y motivación del personal hacia los objetivos de la organización y participación en la mejora continua.
- Habilidad para crear valor para la organización y sus proveedores, con la optimización de recursos, flexibilidad y velocidad de respuesta de las exigencias de los mercados.
- Los directivos, empleados y operarios mejoran su conocimiento acerca de la labor que desempeñan, lo cual les proporciona un mejor control de sus tareas (Proceso de optimización).
- Debido a que es un proceso voluntario, la puesta en marcha y mejora continua ocurren naturalmente y saca lo mejor de los empleados, de tal suerte que empiezan a contribuir espontánea e inteligentemente a la resolución de los problemas en la organización. Por otro lado, permite que las inspecciones de la autoridad se afronten fácilmente y con seguridad.
- Los muestreos a producto final, que se destruyen durante la realización de los ensayos y que son productos en buenas condiciones, pueden ser reducidos notablemente.

En México los marcos regulatorios han comenzado a incorporar la seguridad informática como un punto crítico, esto debido al incremento de ataques informáticos en los últimos años.

Por otra parte en la Industria mexicana hay varios errores de cómo se está atacando el problema de la inseguridad informática. Hoy en día las empresas piensan que la seguridad se va a resolver sólo con la compra de productos antivirus, firewall, etc., pero no se dan cuenta de que lo que se protege son los activos, más no los datos, es decir, se protege el medio, el sistema operativo y la

red, sin embargo, la mayor cantidad de fraudes están relacionados con las bases de datos y aplicaciones, lo que implica que se conviertan en empresas reactivas y correctivas en lugar de empresas preventivas.

Otro problema real es que las instituciones o empresas no saben cuál es el nivel de seguridad que requiere su organización y esto es porque no se sabe cuáles son realmente los riesgos que pudieran poner en peligro la capacidad de operación, servicios y en algunos casos hasta la supervivencia de la organización.

Por lo anterior, es importante saber que la información tiene una importancia fundamental. El hecho de disponer de una certificación, según ISO/IEC 27001:2005, ayuda a gestionar y proteger sus valiosos activos de información.

Por lo tanto, el hecho de certificar un Sistema de Gestión de la Seguridad de la Información (SGSI) según la norma ISO/IEC 27001:2005 puede aportar las siguientes ventajas a la organización:

- Demuestra la garantía independiente de los controles internos y cumple los requisitos de gestión corporativa y de continuidad de la actividad comercial.
- Demuestra independientemente que se respetan las leyes y normativas que sean de aplicación.
- Proporciona una ventaja competitiva al cumplir los requisitos contractuales y demostrar a los clientes que la seguridad de su información es primordial.
- Verifica independientemente que los riesgos de la organización estén correctamente identificados, evaluados y gestionados al tiempo que formaliza los procesos, procedimientos y documentación de protección de la información.
- Demuestra el compromiso de la cúpula directiva de su organización con la seguridad de la información.
- El proceso de evaluaciones periódicas ayudan a supervisar continuamente el rendimiento y la mejora.

Aunado a esto, la norma ISO/IEC 27001:2005 es la única norma internacional auditable, para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo, que define los requisitos para un Sistema de Gestión de la Seguridad de la Información (SGSI). La norma se ha concebido para garantizar la selección de controles de seguridad adecuados y proporcionales.

La norma adopta un enfoque por procesos para establecer, implementar, operar, supervisar, revisar, mantener y mejorar un SGSI.

La *auditoría informática* es el proceso de recoger, agrupar y evaluar evidencias para determinar si un Sistema de Información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos.

Una vez obtenidos los resultados, se detalla, archiva y reportan a los responsables quienes deberán establecer medidas preventivas de refuerzo, siguiendo siempre un proceso secuencial que permita a los administradores mejorar la seguridad de sus sistemas aprendiendo de los errores cometidos con anterioridad.

Cuando se generalizó el uso de las nuevas tecnologías, surgió también la necesidad de realizar auditorías sobre los sistemas de información. En este sentido se podría decir que la Auditoría informática comprende el conjunto de actividades encaminadas a la validación y verificación de los sistemas, procesos y resultados en los que se utilizan tecnologías automatizadas, ya sea en cumplimiento de la legislación, como garantía de la integridad y veracidad de la información aportada por un sistema o por alineamiento con determinados estándares relacionados con el buen uso de los sistemas.
Las auditorías de Sistemas de Información permiten conocer en el momento de su realización cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad.

La auditoría informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además, debe evaluar todo: Informática, Organización de centros de información, Hardware y Software.

La auditoría del sistema de información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental, mejorar la rentabilidad, la seguridad, la eficacia, y la eficiencia del sistema mecanizado de información en que se sustenta.

Es por ello que realzamos la necesidad de crear un Organismo de Evaluación de la Conformidad, capaz de cumplir con las normas y estándares relacionados con la seguridad informática, así como, las expectativas de nuestro País.

Por lo descrito en los párrafos anteriores el objetivo principal de esta tesis es:

"Elaborar un estudio de análisis y propuesta que permita a la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (UNAM) convertirse en un Organismo de Evaluación de la Conformidad de Sistemas de Gestión de Seguridad de la Información, y de esta manera ser un Organismo Certificador de SGSI y adicionalmente generar una cultura y conciencia por la seguridad de la información en México, promoviendo así empresas más seguras y confiables en nuestro país disminuyendo las posibilidades de pérdida y robo de la información".

Para lo cual la tesis se desarrolla a través de cinco capítulos organizados de la siguiente manera:

En el primer capítulo se da un panorama general de la presencia de organismos acreditadores y certificadores de origen mexicano o extranjero en México y cuáles son sus alcances y objetivos.

El segundo capítulo presenta una introducción a las normas utilizadas para llevar a cabo el desarrollo de la presente tesis, un panorama general de los recursos, documentación e implementación para un Sistema de Gestión de la Seguridad de la Información (SGSI), así como la documentación necesaria previa al proceso de acreditación y una descripción general del proceso de acreditación.

En el tercer capítulo se detalla el proceso de certificación, basado en la norma ISO/IEC 27006:2007, que debe implementarse en cualquier Organismo de Certificación bajo la norma

ISO/IEC 27001, así como los recursos necesarios y las condiciones óptimas necesarias para realizar las actividades de certificación.

En el cuarto capítulo se lleva a cabo una evaluación de la situación actual de los laboratorios de la carrera de Ingeniería en Computación de la Facultad de Ingeniería, con el objetivo de encontrar un laboratorio con las condiciones adecuadas que lo conviertan en candidato para llevar a cabo el proceso de implementación, acreditación y certificación del SGSI.

En el quinto capítulo se desarrolla la propuesta para que la Universidad Nacional Autónoma de México en conjunto con la carrera de Ingeniería en Computación de la Facultad de Ingeniería se convierta en un Organismo Certificador de la norma ISO/IEC 27001:2005, siendo así uno de los primeros organismos de esta naturaleza en el país.

Finalmente, se presentan las conclusiones a las que llegamos después de desarrollar el presente trabajo de tesis.

MESOGRAFÍA

www.ema.org.mx
http://netmedia.info/articulo-31-7295-1.html
http://www.bsigroup.com.mx/es-mx/Auditoria-y-Certificacion/Sistemas-de-Gestion/Normas-y-estandares/ISO-27001/
http://www.seguridadit.com.mx/
http://www.enac.es
http://html.rincondelvago.com/auditoria-informatica_1.html
http://es.wikipedia.org/wiki/Auditor%C3%ADa_de_seguridad_de_sistemas_de_informaci%C3%B3n
http://es.wikipedia.org/wiki/Auditor%C3%ADa_inform%C3%A1tica
http://www.aenor.es/
http://www.cesmec.cl/noticias/Certificacion/inspeccion1.act
http://www.cesmec.cl/noticias/Certificacion/certificacion.act
http://www.normex.com.mx/certificacion.html

http://www3.inn.cl/pdfs/acreditacion/Evalu_de_la_conform.pdf//Conceptos

CAPÍTULO 1

Empresas Acreditadoras y Certificadoras en México

1.1 Empresas Acreditadoras en México

En el pasado quien realizaba en México la acreditación de los Organismos de Evaluación de la Conformidad era el gobierno federal a través de la Dirección General de Normas de la Secretaría de Comercio y Fomento Industrial (hoy Secretaría de Economía).

De cara a los cambios en el mercado exterior, a la competencia que implicaba abrir las fronteras en el comercio globalizado, y apoyar a la planta productiva nacional se reformó la Ley Federal sobre Metrología y Normalización, estos cambios ocurrieron en 1992 y 1997. Las transformaciones en el orden legal abrieron la posibilidad de que una entidad de gestión privada, de tercera parte, imparcial, incluyente y profesional realice esta importante labor para el sector productivo mexicano. Y a partir de la publicación, el 15 de enero de 1999, en el Diario Oficial de la Federación de la autorización de la Secretaría de Comercio y Fomento Industrial, EMA comienza a operar como el primer órgano acreditador en México. [1]

La Ley Federal sobre Metrología y Normalización (LFMN) expedida el 1 de julio de 1992, constituye el fundamento para la expedición de las NOMs (Normas Oficiales Mexicanas) de carácter obligatorio y las Normas Mexicanas (NMX) de carácter voluntario, además, establece la creación de diferentes organismos con el objetivo de apoyar al sistema mexicano de normalización.

De los organismos creados en la LFMN destacan los siguientes:

- Sistema General de Unidades de Medida.
- Sistema Nacional de Calibración.
- Centro Nacional de Metrología.
- Comisión Nacional de Normalización.
- Sistema Nacional de Acreditamiento.

El objetivo del sistema mexicano de normalización es incrementar la calidad de los productos y servicios nacionales, estimular la concurrencia del sector privado, público y científico y de consumidores en la elaboración y observancia de la normatividad, determinar las normas de carácter obligatorio y la forma en que se acreditará el cumplimiento de las mismas, así como el desarrollo de los recursos humanos especializados para lograr esos fines. [2]

Entidad Mexicana de Acreditación, A.C. (EMA)

Desde 1999, EMA es la primera y única entidad acreditadora que opera en nuestro país dando certidumbre y confianza a los Organismos de Evaluación de la Conformidad (laboratorios de prueba, laboratorios de calibración, organismos de certificación y unidades de verificación u organismos de inspección). Es una asociación civil imparcial y de gestión privada que fortalece nuestro Sistema Nacional de Metrología, Normalización y Evaluación de la Conformidad.

Su creación se impulsó al detectar los retos que nos presenta el intercambio de productos, bienes y servicios en el mundo globalizado; para dotar a la industria y comercio de herramientas para competir equitativamente, e insertarnos ampliamente al comercio internacional. [1]

EMA forma parte de:

- Foro Internacional de Acreditación (IAF).
- Cooperación Internacional de Acreditación de Laboratorios (ILAC).
- Cooperación Interamericana de Acreditación (IAAC).
- Cooperación Norteamericana de Calibración (NACC).
- Cooperación de Acreditación de Laboratorios de Asia-Pacífico (APLAC).
- Cooperación de Acreditación del Pacífico (PAC).

Lo que asegura el reconocimiento de la acreditación expedida por EMA a cada Organismo de Certificación y que este certificado sea válido en todo el mundo.

Los alcances de acreditación de EMA, de acuerdo con la información publicada en su página web son:

1. Agricultura, pesca.
2. Minería y canteras.
3. Productos alimenticios, bebidas y tabaco.
4. Textiles y productos textiles.
5. Pieles y productos de piel.
6. Madera y productos de madera.
7. Pulpa, papel y productos de papel.
8. Compañías de publicación.
9. Compañías de impresión.
10. Fabricación del coque y productos de petróleo refinados.
11. Combustible nuclear.
12. Químicos, productos químicos y fibras.
13. Farmacéuticos.
14. Hule y productos de plástico.
15. Productos minerales no metálicos.
16. Concreto, cemento, cal, yeso, etc.
17. Metales básicos y productos de metal fabricados.
18. Maquinaría y equipo.
19. Equipo eléctrico y óptico.
20. Construcción naval.
21. Aeroespacial.
22. Otro equipo de transporte.
23. Fabricación no clasificada en otra parte.
24. Reciclado.
25. Suministro de electricidad.
26. Suministro de gas.
27. Suministro de agua.
28. Construcción.
29. Comercio al mayoreo y menudeo; reparación de vehículos de motor, motocicletas y bienes personales y domésticos.
30. Hoteles y restaurantes.
31. Transporte, almacenamiento y comunicación.
32. Intervención financiera; bienes raíces; alquiler.
33. Información tecnológica.
34. Servicios de ingeniería.
35. Otros servicios.
36. Administración pública.
37. Educación.
38. Salud y asistencia social.
39. Otros servicios sociales.

Además EMA se apega a las siguientes normas nacionales e internacionales: NMX-EC-058-IMNC-2000, para acreditar laboratorios de pruebas y calibración; NMX-CC-021, para acreditar organismos de certificación e ISO/IEC/TR 17010, para acreditar unidades de verificación. Los organismos acreditados deben cumplir con la NMX-EC-17025-IMNC-2000 para laboratorios, NMX-EC-062-IMNC-2000 para organismos de certificación, y la NMX-EC-17020-IMNC-2000 para unidades de verificación. Además, las acreditaciones y dictámenes las realizan integrantes del

Padrón Nacional de Evaluadores, contando actualmente con 121 evaluadores líderes, 90 evaluadores y 135 expertos técnicos.

La entidad ha logrado realizar sus actividades y cumplir con sus objetivos por sus fuentes de financiamiento, que son:

1) Servicios de acreditación.
2) Cuotas de sus asociados.
3) Cursos de capacitación.
4) Apoyos y Estímulos Públicos y/o Donativos de dependencias federales, estatales, organismos nacionales, regionales e internacionales, ya que la entidad es una persona moral no contribuyente, por el hecho de no tener fines de lucro.

1.2 Empresas Certificadoras en México

EMA por ser la única empresa acreditadora en México, tiene una gran lista de organismos acreditados de los cuales se presenta una breve descripción así como las normas en las que certifican.

BVQI Mexicana, S.A DE C.V. (BVQI).

BVQI, es el organismo de certificación independiente de Bureau Veritas, está ampliamente reconocida por autoridades nacionales e internacionales a través de 30 acreditaciones, avalando la legitimidad de sus actividades. Una clave importante de BVQI es su incomparable gama de servicios en las áreas de Calidad, Seguridad y Salud, Medio Ambiente, Responsabilidad Social y Seguridad. BVQI ofrece la posibilidad de combinar certificaciones con el mayor rango de estándares reconocidos, brindando consistencia, optimización y eficiencia.

Normas acreditadas:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.
- NMX-SAA-14001-IMNC-2004, Sistemas de gestión ambiental - Requisitos con orientación para su uso.

Calidad Mexicana Certificada, A.C. (CALMECAC).

CALMECAC tiene por objeto mediante la práctica de auditorías, de programas de verificación y en coordinación con laboratorios de pruebas acreditados, certificar la calidad de los sistemas, productos, servicios y personal de las actividades económicas de acuerdo a las Normas Oficiales Mexicanas, Normas Mexicanas y Normas Internacionales de Empresa o Asociación.

Normas acreditadas:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

- NMX-SAST-001-IMNC-2000, Sistemas de Administración de Seguridad y Salud en el Trabajo.

Certificación Mexicana, S.C.

Su misión es apoyar a la SEMARNAT, por conducto de la CONAGUA, a SAGARPA, Organismos Operadores de agua públicos y privados, fabricantes, asociaciones y demás usuarios, en la verificación y certificación del cumplimiento de las normas de productos, instalación y sistemas emitidas en el Sector Agua, Construcción y Riego, con el fin de colaborar en iniciativas que promuevan una cultura del cuidado del agua y su uso eficiente, recursos que requieren del cuidado en su calidad y desarrollo sustentable.

Normas acreditadas:

- NMX-SAA-14001-IMNC-2004, Sistemas de gestión ambiental - Requisitos con orientación para su uso.
- NMX-SAST-001-IMNC-2000, Sistemas de Administración de Seguridad y Salud en el Trabajo.

Det Norske Veritas México, SA de CV.

Det Norske Veritas es una fundación de origen Noruego creada en el año de 1864, bajo el principio fundamental de salvaguardar la vida, la propiedad y el medio ambiente. Desde sus orígenes funciona como una clasificadora de barcos, con sus propias Normas y estándares, mismos que son ampliamente reconocidos y aceptados por todo el mundo, razón por la cual en la actualidad el 20 por ciento de la flota naval en el mundo está clasificada por DNV. En el contexto actual de los negocios la Globalización es una constante y una de las herramientas principales es la estandarización, razón por la cual DNV amplía su campo de acción e incursiona en los sistemas de Certificación. En la actualidad tiene más de 300 oficinas alrededor del mundo y un poco más de 7000 empleos directos y ha emitido más de 48000 certificados. En nuestro país se establece a partir de finales de los años setentas brindando los mismos servicios que se disponen alrededor del mundo.

Normas acreditadas:

- NMX-CC-9001-IMNC-2000/COPANT/ ISO 9001/ ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

Factual Services, S.C.

Factual Services, S.C. es una empresa que proporciona servicios de certificación de sistemas de calidad y servicios de verificación de Normas Mexicanas de manera objetiva, imparcial y eficiente, comprometiéndose a lograr la satisfacción de sus clientes. Es un organismo con reconocimiento oficial que cuenta con la acreditación nacional e internacional, en función a los acuerdos de reconocimiento suscrito por la EMA.

Normas acreditadas:

- NOM-001-SCFI-1993, Aparatos electrónicos de uso doméstico alimentados por diferentes fuentes de energía eléctrica – Requisitos de seguridad y métodos de prueba para la aprobación de tipo.
- NOM-003-SCFI-2000, Productos eléctricos – especificaciones de seguridad.
- NOM-016-SCFI-1993, Aparatos electrónicos de uso en oficina y alimentados por diferentes fuentes de energía eléctrica – Requisitos de seguridad y métodos de prueba.
- NOM-019-SCFI-1998, Seguridad de equipo de procesamiento de datos.
- NOM-058-SCFI-1999, Productos eléctricos – Balastros para lámparas de descarga eléctrica en gas - Requisitos de Seguridad.

Instituto Mexicano de Normalización y Certificación, A.C. (IMNC).

El Instituto Mexicano de Normalización y Acreditación AC es una Asociación Civil no lucrativa de carácter privado, multisectorial, independiente e imparcial de tercera parte, que nace para contribuir en el proceso de inserción de la economía mexicana en la globalización de los mercados y el incremento de la competitividad y productividad de las organizaciones mexicanas. Cuentan con expertos reconocidos internacionalmente en los campos de Normalización, Certificación de Sistemas de Gestión, Productos y Personas, y disponen de una Unidad de Verificación del cumplimiento con Normas Oficiales Mexicanas. Sus servicios están avalados por Registros otorgados por el Gobierno Mexicano, a través de la Dirección General de Normas de la Secretaría de Economía y la Acreditación con reconocimiento internacional otorgado por la Entidad Mexicana de Acreditación (EMA) de acuerdo con los lineamientos establecidos por la Ley Federal sobre Metrología y Normalización y su Reglamento, así como por las Guías y Normas Nacionales e Internacionales aplicables; acuerdos de reconocimiento mutuo y multilaterales. Además, participan activamente en el desarrollo de Normas Internacionales, como las ISO 9000, ISO 14000, ISO 19011 y Normas sobre Evaluación de la Conformidad y Metrología.

Normas acreditadas:

- NMX-SAST-001-IMNC-2000, Sistemas de Administración de Seguridad y Salud en el Trabajo.

Sociedad Mexicana de Normalización y Certificación, S.C. (NORMEX).

NORMEX es el primer Organismo Nacional de Normalización y Certificación con más de 50 años de experiencia en el ámbito de las tecnologías para la calidad, ya que es el resultado de la privatización de los Laboratorios Nacionales de Fomento Industrial (LANFI) ocurrida en el año de 1993.

NORMEX está integrada por tres instituciones nacionales: La Universidad del Valle de México (UVM), el Instituto Politécnico Nacional (IPN) y la Cámara Nacional de la Industria de la Transformación (CANACINTRA), por lo que NORMEX tiene la representación de los sectores académicos, científicos, tecnológicos e industriales.

NORMEX está acreditado y aprobado por diversas dependencias públicas y entidades de acreditación:

- Secretaría de Economía (SE).
- Secretaría de Salud (SS).
- Secretaría de Turismo (SECTUR).
- Secretaría del Medio Ambiente, Recursos Naturales (SEMARNAT).
- Secretaría de Comunicaciones y Transporte (SCT).
- Secretaría de Agricultura, Ganadería y Desarrollo Rural (SAGARPA).
- Entidad Mexicana de Acreditación (EMA).
- Consejo de Normalización y Certificación de la Competencia Laboral (CONOCER).

Normas acreditadas:

- NOM-155-SCFI-2003, Leche, fórmula láctea y producto lácteo combinado-Denominación, especificaciones físico químicas, información comercial y métodos de prueba.

Normalización y Certificación Electrónica A.C (NYCE).

Normalización y Certificación Electrónica A. C., NYCE, es una asociación civil sin fines de lucro creada en noviembre de 1994 por un grupo de empresas líderes de los sectores de Electrónica, Telecomunicaciones y Tecnologías de Información de México, convencidas de la necesidad de contar con un organismo de jurisdicción nacional que tomará en cuenta sus necesidades, en la certificación del cumplimiento con las Normas Oficiales Mexicanas aplicables a los productos de la rama.

NYCE nace al amparo de la Ley Federal sobre Metrología y Normalización (LFMN), que promulgada en 1992 abrió la posibilidad de que en México al igual que en otros países, se conformaran organismos privados para realizar actividades de certificación y verificación, las cuales anteriormente sólo eran llevadas a cabo por dependencias gubernamentales.

NYCE está acreditado y autorizado por las instancias legales y las dependencias del Gobierno Federal conducentes y forma parte del Sistema Mexicano de Metrología, Normalización y Evaluación de la Conformidad (SISMENEC), que está totalmente reglamentado y opera de manera consistente en el ámbito nacional.

El SISMENEC está integrado por organizaciones de tercera parte, de normalización, de certificación de producto, de certificación de sistemas, de certificación de personas, de verificación, de pruebas, de metrología y de acreditación, así como por las dependencias que conforme a la propia LFMN deben abocarse a estos aspectos.

Normas acreditadas:

- NMX-CC-SAA-19011-IMNC-2002 / ISO 19011:2002, Directrices para la auditoría de los sistemas de la calidad o ambiental.
- NMX-I-006/03-NYCE-2006, Tecnología de la información - Evaluación de los procesos - Parte 03: Guía para la realización de una evaluación.

Organismo de Certificación de Establecimientos T.I.F., A.C. (OCETIF)

El Organismo de Certificación de Establecimientos TIF, A.C. (OCETIF) es una asociación civil que participa activamente en el desarrollo de la industria mexicana de los alimentos. El Sistema de Inspección Federal es un conjunto de preceptos, limitaciones, obligaciones y vigilancias del más elevado nivel sanitario, que ejerce el Gobierno Federal, a través de la Secretaría de Agricultura, Ganadería, Desarrollo Rural, Pesca y Alimentación (SAGARPA), de acuerdo a ciertas normas aceptadas internacionalmente, sobre los locales, su construcción, conservación e higiene; los procedimientos de inspección de los ganados de abasto y de las carnes que se obtienen de ellos; sobre la maquinaria, equipo, indumentaria y enseres que se utilizan en el proceso y obtención de las carnes, productos cárnicos y subproductos de las empresas que operan bajo él.
Normas acreditadas:

- NOM-005-ZOO-1993, Campaña Nacional contra la Salmonelosis Aviar.
- NOM-007-ZOO-1994, Campaña Nacional contra la enfermedad de Aujeszky.
- NOM-008-ZOO-1994, Especificaciones zoosanitarias para la construcción y equipamiento de establecimientos para el sacrificio de animales y los dedicados a la industrialización de productos cárnicos.
- NOM-009-ZOO-1994, Proceso sanitario de la carne.
- NOM-013-ZOO-1994, Campaña Nacional contra la enfermedad de Newcastle, presentación velo génica.
- NOM-033-ZOO-1995, Sacrificio humanitario de los animales domésticos y silvestres.
- NOM-037-ZOO-1995, Campaña Nacional contra la Fiebre Porcina Clásica.
- NOM-044-ZOO-1995, Campaña Nacional contra la Influenza Aviar.
- PC-002-2004, Pliego de condiciones para el uso de la marca oficial México Calidad Suprema en Carne de Cerdo.
- PC-003-2004, Pliego de condiciones para el uso de la marca oficial México Calidad Suprema en Carne de Bovino.

Organismo Nacional de Normalización y Certificación de la Construcción y Edificación, S. C. (ONNCCE).

El ONNCCE, es una Sociedad Civil reconocida en el ámbito Nacional, que tiene como propósito contribuir a la mejora de la calidad y de la competitividad de los productos, procesos, servicios y sistemas, particularmente a través de la normalización y de la certificación.

Actualmente está acreditado como Organismo Nacional de Normalización (ONN) por la Secretaría de Economía (SE) con la aprobación de la SEDESOL para el sector de la construcción y como Organismo de Certificación de Producto y de Sistemas de Calidad por la Entidad Mexicana de Acreditación (EMA), con la aprobación de la SE, la CNA y la CONAE.

El ONNCCE ofrece a las PYMES un programa de apoyo para la certificación de los Sistemas de Gestión de Calidad en toda la República Mexicana, de acuerdo con la norma NMX-CC-9001-IMNC-2000 Sistemas de gestión de la calidad - Requisitos.

Normas acreditadas:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

Q.S. Mexiko A.G., S.A. de C.V.

QS Significa servicios de calidad. Los orígenes de la organización, así como los de la Organización Internacional de Normalización ISO son suizos, lo que permite contar con la información de primera mano acerca del acontecer internacional en lo referente a emisión y aplicación de normas. Entre sus servicios cuenta con la certificación de Sistemas de Gestión de Calidad, ambiental, HACCP y aplicable a la industria fabricante de artículos y dispositivos médicos.

Normas acreditadas:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

SGS de México, S.A. de C.V.

Fundado en 1878, el grupo SGS es la mayor organización del mundo en el campo de la inspección y la calidad. Opera en 140 países a través de su red de compañías filiales con más de 850 oficinas, 340 laboratorios y 43,000 empleados. Es el líder mundial en Inspección, Verificación, Ensayos y Certificación, y su amplia gama de servicios lo convierte en una institución única en su género.

El núcleo de sus actividades lo constituyen los servicios de inspección y supervisión del comercio internacional de productos agrícolas, minerales, petróleo y petroquímicos, equipos industriales y bienes de consumo. A lo largo de los años, SGS ha ampliado sus actividades hacia campos no dependientes del comercio, como son la certificación de calidad y la gestión industrial. Todos los servicios que SGS brinda, poseen dos rasgos importantes en común: ayudan a minimizar los riesgos y proporcionan evaluaciones, verificaciones y asesoría de carácter independiente.
Normas acreditadas:

- PC-009-2004, Pliego de condiciones para el Uso de la Marca Oficial México Calidad Suprema en Arroz.
- PC-031-2005, Pliego de condiciones para el uso de la marca oficial México Calidad Suprema en Leche.

TÜV Rheinland de México, S.A. de C.V.

TÜV Rheinland es una organización que cuenta con más de 125 años sirviendo a la industria, con presencia en más de 40 países alrededor del mundo.

TÜV Rheinland de México inició sus operaciones en 1993 para cubrir la demanda de los servicios técnicos profesionales con reconocimiento Internacional requeridos en México.

Se dedican a la certificación de sistemas administrativos de calidad y ambientales bajo acreditaciones nacionales e internacionales como son:

- EMA (México).
- DAR (Alemania).
- RAB (USA).
- SCC (Canadá).

Además, TÜV Rheinland de México, realiza certificaciones de producto e imparte seminarios de capacitación con auditores nacionales calificados.
Norma acreditada:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

Asociación de Normalización y Certificación, A.C. (ANCE)

El 10 de diciembre de 1992 se constituyó la Asociación Nacional de Normalización y Certificación del Sector Eléctrico, A.C. (ANCE), institución privada sin fines de lucro, concebida con el fin de brindar apoyo y servicios en materia de normalización, laboratorio de pruebas, certificación de sistemas de calidad, certificación de productos y verificación.

Normas acreditadas:

- NMX-SAST-001-IMNC-2000, Sistemas de Administración de Seguridad y Salud en el Trabajo.
- NMX-SAA-14001-IMNC-2004.
- NMX-CC-003-1995 IMNC / ISO 9001:1994.
- NMX-CC-004-1995 IMNC / ISO 9002:1994.
- NMX-CC-005-1995 IMNC / ISO 9003:1994.
- NMX-SAA-14001-IMNC-2004/ ISO 14001:2004.

Además, cuenta con certificaciones de productos como:

- Certificación de aparatos domésticos.
- Certificación de productos eléctricos.
- Certificación de productos y accesorios a base de gas y seguridad industrial.

International Certification of Quality Systems, S.C.

Es una organización de servicios profesionales entre los cuales destacan capacitación, conferencias y certificaciones. Cuenta con acreditaciones por parte de la EMA, IAR y ANAB.

Norma acreditada:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

Germanischer Lloyd Certification, S. de R.L. de C.V. (GLC)

GLC, es la certificadora de la sociedad de clasificación Germanischer Lloyd, creada en 1867. Germanischer Lloyd Certification Services es representante único de GLC en España y es por ello que está acreditada por ENAC en España y por otras entidades de acreditación europeas, además, es una entidad independiente que ofrece servicios de certificación de sistemas de gestión de Calidad, Gestión Ambiental, Higiene y Seguridad, Prevención de Riesgos, Benchmarking y Auditorías de todo tipo de normas.

Norma acreditada:

- NMX-SAA-14001-IMNC-2004, Sistemas de gestión ambiental - Requisitos con orientación para su uso.

Consejo Mexicano de Certificación, A.C.

El Consejo Mexicano de Certificación en Medicina Familiar busca a través de la Certificación, brindar a la sociedad la certidumbre de que los médicos especialistas en Medicina Familiar poseen la capacidad necesaria para prestar atención médica integral y continua al individuo y su familia con elevados estándares de calidad.

Normas acreditadas:

- NOM-005-CNA-1996, Fluxómetros – Especificaciones y métodos de prueba.
- NOM-008-CNA-1998, Regaderas empleadas en el aseo corporal - Especificaciones y métodos de prueba.
- NOM-009-CNA-2001, Inodoros para uso sanitario - Especificaciones y métodos de prueba.
- NOM-010-CNA-2000, Válvulas de admisión y válvula de descarga para tanque de inodoro. - Especificaciones y métodos de prueba.

Quality Solution Register, S.A. DE C.V. (QSR)

Es un organismo de Certificación de Gestión acreditado por la EMA que desde su inicio se ha preocupado y comprometido por mejorar los procesos de Certificación, tomando como base el servicio personalizado.

Norma acreditada:

- ISO 14001, Sistemas de Gestión ambiental.
- ISO 19011, calificación de auditores de Calidad.
- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

Underwriters Laboratories Inc, México. (UL)

Underwriters Laboratories Inc. (UL) es un organismo independiente de pruebas/ensayos de seguridad y certificación, que evalúa productos, materiales y sistemas trabajando por la seguridad de los consumidores y sus bienes desde 1894. UL es líder mundial en el desarrollo de normas de

seguridad de productos, las cuales son frecuentemente actualizadas y revisadas para responder a los cambios en la tecnología o responder a nuevos usos de estos productos. A través de esquemas de certificación internacionales y acuerdos de cooperación con organizaciones de normas internacionales, pruebas / ensayos y, certificación de gestión de calidad, UL está en condiciones de evaluar productos según las normas de otros países, facilitando su aceptación por las diferentes agencias de certificación, mediante un sometimiento único del producto.

Normas acreditadas:

- ISO 9000:2000.
- ISO 14000.
- OHSAS 18001.
- QS 9000.
- TS 16949.
- TL 9000.
- SA 8000.

Además, cuenta con certificaciones de productos como:

- Certificación de conformidad para producto electrónico en las normas:
  - NOM-001-SCFI-1993.
  - NOM-016-SCFI-1993.
  - NOM-019-SCFI-1998.
- Certificación de conformidad de producto eléctrico en las normas:
  - NOM-058-SCFI-1999.
  - NOM-003-SCFI-2000.
- Emisión de Dictamen de Equipo Altamente Especializado.
- Ampliación de Titularidad. Este servicio sólo aplica para fabricantes nacionales o extranjeros.
- Cambios o modificaciones de alcance de certificados y dictámenes otorgados, tales como:
  - Ampliación o cancelación de modelos.
  - Cambios de razón social o domicilio.
- Cartas de validación de muestras en aduana.
- Dictámenes de producto.
- Agrupamiento de Familias.
- Cualquier otro tipo de servicio relacionado con la evaluación de la conformidad.

EQA Certificación México, S.A. de C.V.

EQA es una Entidad Internacional de Certificación. Audita sistemas de gestión de la calidad (ISO 9000), de gestión medioambiental (ISO 14001), de gestión de calidad en el sector aeroespacial (EN 9100) y calidad en Internet (IQA).

European Quality Assurance nace en 1993, en Newark Inglaterra, país en donde se forjó la idea de las normas ISO-9000. En tan solo 2 años de operar se amplían las operaciones en diversas delegaciones, abarcando el Continente Americano, Europeo, Asiático, Africano y Oceanía.

Norma acreditada:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

Consejo Regulador del Tequila, A.C. (CRT)

El Consejo Regulador del Tequila, CRT, A. C. es una organización interprofesional donde se reúnen desde el 16 de Diciembre de 1993 todos los actores y agentes productivos ligados a la elaboración de Tequila con el fin de promover la cultura y la calidad de esta bebida que se ha ganado un lugar importante entre los símbolos de identidad nacional.

El CRT cuenta con un sistema de Aseguramiento de Calidad que garantiza la confiabilidad de sus servicios. A partir de Junio de 1999 el CRT obtuvo la certificación ISO - 9002.

Reconocimientos otorgados:

- AENOR (Asociación Española de Normalización) 22-Junio-1999 con reconocimiento en la red IQ net (más de 25 países miembros).
- ANCE (Asociación de Normalización y Certificación) 16-Julio-1999.

El CRT no tiene fines de lucro, es de carácter privado, y tiene personalidad jurídica propia. Su alcance es Nacional e Internacional, donde el fin es el de Certificar el cumplimiento de la Norma Obligatoria del Tequila.

Normas acreditadas:

- NMX-V-049-NORMEX-2004, Bebidas alcohólicas-Bebidas alcohólicas que contienen Tequila-Denominación, etiquetado y especificaciones.
- NOM-006-SCFI-2005, Bebidas alcohólicas - Tequila - Especificaciones.

Consejo para el Fomento de la Calidad de la Leche y sus Derivados, A.C. (COFOCALEC)

El Consejo para el Fomento de la Calidad de la Leche y sus Derivados, es un organismo privado, sin fines de lucro, que se integra con el propósito fundamental de promover la calidad de la leche y sus productos en México a través de la normalización, el fomento y la evaluación de la conformidad, es decir, la determinación del grado de cumplimiento de las normas mexicanas y oficiales mexicanas o internacionales, prescripciones o características que aplican a este alimento importante.

Proporciona servicios de certificación, verificación, laboratorio, normalización, asistencia técnica y capacitación, a través de profesionales especializados y de un sistema de calidad que brinda confianza sobre los servicios a sus clientes y certeza sobre la leche y sus productos a la sociedad en general.

Norma acreditada:

- NOM-155-SCFI-2003, Leche, fórmula láctea y producto lácteo combinado -Denominación, especificaciones físico químicas, información comercial y métodos de prueba.

American Trust Register, S. C. (ATR)

American Trust Register, S.C., se establece en México en 2002, como una Sociedad Civil y se encarga de Certificar Sistemas de Gestión de la Calidad y Sistemas de Gestión Ambiental. Cuenta con Auditores de más de 20 años de experiencia lo que hace que ATR, aunque el Organismo es joven, cuenta con la mejor relación de calidad-precio del mercado y el reconocimiento de sus clientes debido al valor agregado de nuestras auditorías de certificación.

Normas acreditadas:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.
- NMX-SAA-14001-IMNC-2004, Sistemas de gestión ambiental - Requisitos con orientación para su uso.

Centro de Normalización y Certificación de Productos, A.C. (CNCP)

El Organismo de Certificación de Producto del CNCP, cuenta con la acreditación 35/07 por la Entidad Mexicana de Acreditación, A.C. (EMA) conforme a los requisitos establecidos en la Norma Mexicana NMX-EC-065-IMNC-2000 “Requisitos generales para organismos que operan sistemas de certificación de producto” para llevar a cabo actividades de certificación en las Normas Mexicanas (NMX) o Normas Oficiales Mexicanas (NOM) indicadas en el alcance de su acreditación. Dicha acreditación tiene una vigencia hasta agosto del 2011.

Normas acreditadas:

- NMX-E, Plásticos (tubos, conexiones, válvulas, bolsas).
- NMX-C, Tinacos, tubos de concreto.
- NMX-T, Anillos de hule.
- NOM-CNA, Regaderas, inodoros, fluxómetros, válvulas y Fosas Sépticas.
- NOM-SCFI, Seguridad en aparatos electrónicos, productos eléctricos y equipos de procesamiento de datos.

DQS de México, S.A. de C.V.

Asociación alemana para la certificación de sistemas administrativos de calidad y del medio ambiente. DQS es la primera certificadora alemana en sistemas de gestión, fundada el 1 de febrero de 1985 por DGQ (Deutsche Gesellschaft für Qualität e.V. Asociación alemana de calidad) y por DIN (Deutsches Institut für Normung e.V. Instituto alemán para la estandarización).

Actualmente tienen 7 socios: DIN, DGQ, ZVEI, VDMA, VCI, HvBi y Spectaris, todas asociaciones alemanas en diferentes rubros de la industria.

Normas acreditadas:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.
- NMX-SAA-14001-IMNC-2004, Sistemas de gestión ambiental - Requisitos con orientación para su uso.

TÜV SÜD América de México, S.A. de C.V.

TÜV (Technisher Überwachungs Verein- Asociación de Inspección Técnica) fue fundada en el año de 1870 por la industria alemana de calderas de vapor.

En el año de 1986, TÜV SÜD Group creó TÜV America Inc. y es precisamente TÜV SÜD America Inc. la Organización que el 20 de Septiembre de 1995 instituye oficialmente TÜV SÜD América de México, S.A. de C.V. en la ciudad de Monterrey, Nuevo León.

El grupo TÜV SÜD es una Organización de servicios técnicos líder en segmentos de negocios estratégicos como son la INDUSTRIA (INDUSTRY), el campo AUTOMOTRIZ (MOBILITY) y la GENTE (PEOPLE). Su gama de servicios abarca, pero no se limita, a servicios de inspecciones, pruebas técnicas, servicios de certificación y de entrenamiento. Los objetivos del Grupo TÜV SÜD son la confiabilidad, la seguridad y la calidad así como la protección del medio ambiente y la rentabilidad. TÜV SÜD América de México, S.A. de C.V. tiene como misión incrementar la seguridad y agregar valor a las operaciones de sus clientes, así como ofrecer servicios de forma independiente, objetiva, y profesional.

Normas acreditadas:

- HACCP.
- SQF.
- ISO 22000:2005.
- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.

Consejo Mexicano Regulador de la Calidad del Mezcal, A. C. (COMERCAM)

El Consejo Mexicano Regulador de la Calidad del Mezcal A.C. (COMERCAM) se constituye el 12 de diciembre de 1997, como un organismo del sector privado con fines no lucrativos, tiene personalidad jurídica propia y es de alcance nacional.

El COMERCAM vigila el cumplimiento de la NORMA Oficial Mexicana NOM-070-SCFI-1994, Bebidas alcohólicas-Mezcal-Especificaciones, para tal efecto se ha obtenido la acreditación del Organismo de Certificación: Reg. No. 33/03 y Unidad de Verificación No. UVNOM 030 por parte de la Entidad Mexicana de Acreditación A.C.

Norma acreditada:

- NOM-070-SCFI-1994, Bebidas alcohólicas-Mezcal-Especificaciones.

Comité Estatal de Sanidad Vegetal de Puebla

El CESAVEP es un organismo integrado por productores agrícolas de la entidad, que opera campañas y programas fitosanitarios con asesoría especializada para prevenir, detectar, controlar o erradicar plagas y enfermedades bajo la normatividad de la Secretaría de Agricultura, Desarrollo Rural, Pesca y Alimentos (SAGARPA) y apoyados por la Secretaría de Desarrollo Rural (SDR).

El CESAVEP trabaja de manera coordinada con el gobierno federal (SAGARPA) y el gobierno estatal (SDR) los cuales son los ejes rectores de la operación.

Normas acreditadas:

- PC-010-2004, Pliego de Condiciones para el uso de la marca México Calidad Suprema en Café Verde.
- PC-011-2004, Pliego de condiciones para el uso de la Marca Oficial México Calidad Selecta en Chile poblano, serrano y jalapeño.
- PC-012-2004, Pliego de condiciones para el uso de la Marca Oficial México Calidad Selecta en Limón Persa.
- PC-020-2005, Pliego de condiciones para el uso de la marca oficial México Calidad Suprema en Tomate.

Primus Laboratorios de México, S. de R.L. de C.V.

La firma se ha distinguido por enfocar sus recursos dirigiéndolos hacia temas como inocuidad y calidad en la industria de perecederos. PrimusLabs.com históricamente ha adoptado y desplazado continuamente los esfuerzos técnicos para poner mayor énfasis en dirigir los problemas que emergen en la industria de productos frescos, en lugar de tratar de buscar un Producto con habilidades técnicas específicas.

Actualmente, la lista de servicios que ofrece PrimusLabs.com incluye análisis de residuos de pesticidas, análisis para organismos microbiológicos, provee auditorías de tercería para crecimiento y manejo de las operaciones de Buenas Prácticas Agrícolas (BPA) o Buenas Prácticas de Manufactura (BPM), HACCP desarrollo de sistemas de manejo de datos para proporcionar a los compradores y vendedores una cadena efectiva de sus programas de inocuidad y calidad.

Norma acreditada:

- PC, Pliego de condiciones para el uso de la Marca Oficial México Calidad Selecta en diferentes productos agrícolas.

Quality Management Institute (QMI).

Quality Management Institute (QMI) es el más grande certificador de Sistemas de Gestión en Norte América, ha sido líder en la certificación de los Sistemas de Gestión desde la llegada de las normas y del movimiento de certificación. Desde 1984, QMI ha certificado casi 11, 000 firmas en ISO 9001 y otras normas de la industria a través de un amplio rango de industrias, ayudando a los

negocios a no solo obtener su certificado de registro, sino también a alcanzar un mejoramiento real y duradero en sus operaciones del negocio.

QMI está calificado para certificar el cumplimiento de las normas más importantes que rigen un amplio rango de negocios e industrias.

Normas acreditadas:

- ISO 9001, ISO/TS 16949, AS9100 – Series.
- ISO 14001, OHSAS 18001, RC14001, RCMS®, Sistemas Integrados de Gestión.
- CSA Z809 SFM.
- SFI.
- Seguridad de Alimentos (HACCP).
- ISO 22000.

Empresas que certifican bajo la norma ISO/IEC 27001

En México, son pocas las empresas que certifican bajo la norma ISO/IEC 27001, cabe mencionar que el origen de estas empresas es extranjero, a excepción de la empresa OCICERT que es de origen mexicano.

OCICERT México, S.A. de C.V.

Multinacional de origen mexicano con reconocimiento y presencia internacional en el ámbito de la evaluación de la conformidad en normas oficiales, voluntarias, de marca propia y de terceros, con personal altamente calificado y especializado por sector de actividad económica.

Norma acreditada:

- NMX-CC-9001-IMNC-2000/COPANT/ISO 9001/ISO 9001:2000, Sistemas de Gestión de la Calidad – Requisitos.
- ISO-9000.
- ISO-14001.
- ISO-22000.
- OSHAS.

BSI British Standards.

Desde su fundación en 1901 como el comité de estándares de ingeniería, el grupo BSI ha crecido como una organización de servicios a las empresas de forma independiente. BSI, Inc. es la compañía líder mundial en inspecciones y certificaciones.
Actualmente, el grupo BSI opera a través de sus tres unidades de negocio: BSI British Standards (estándares), BSI Management Systems (certificación de sistemas) y BSI Product Services (certificación de productos).

El grupo BSI:

- Certifica sistemas de gestión y productos.
- Desarrolla estándares nacionales e internacionales.
- Proporciona formación e información sobre estándares y comercio internacional.

Normas Acreditadas:

- ISO 9001 - Administración de calidad.
- ISO 14001 - Administración del medio ambiente.
- QS-9000 - Administración de calidad para la industria automotriz.
- TE Supplement to QS-9000 - Administración de calidad para los proveedores de herramientas y equipo a la industria automotriz.
- VDA 6.1 - Administración de calidad para la industria automotriz (requisitos Alemanes).
- ISO/TS 16949 - Sistemas de calidad - Proveedores automotrices - Requisitos particulares para la aplicación del ISO 9001:1994.
- ISO/IEC 27001, Seguridad de la Información.
- BS OHSAS 18001 Salud y seguridad en el trabajo.
- ISO 22000 Seguridad e Inocuidad en los alimentos.

American Bureau of Shipping (ABS)

American Bureau of Shipping (ABS) es una Sociedad de Clasificación con sede en Houston, Texas. ABS fue fundada en 1862 y actualmente es una de las tres empresas líderes en su sector a nivel mundial, junto a la británica Lloyd's Register y la noruega Det Norske Veritas.

ABS opera una estructura descentralizada por medio de tres divisiones localizadas en Houston (ABS Americas), Londres (ABS Europe) y Singapur (ABS Pacific), contando con más de 150 oficinas en 70 países.

La misión de ABS es buscar el interés general así como las necesidades de sus clientes promoviendo la seguridad de la vida humana y propiedades así como la protección del entorno natural marino por medio del desarrollo y verificación de estándares para el diseño, construcción y mantenimiento de buques y plataformas offshore.

ABS es miembro de la Asociación Internacional de Sociedades de Clasificación (IACS), a la cual pertenecen las diez Sociedades de Clasificación más importantes del mundo.

Normas acreditadas:

- Aeroespacial - AS9003, AS9100.
- Automotriz - ISO/TS 16949.
- Químico - RCMS®, RC14001®.
- Pressure Equipment Directive – PED.
- Ambiental - ISO 14001.
- Seguridad Alimenticia – HACCP.
- Evaluación de Información de Sistemas - ISO/IEC 27001.

- Seguridad - OHSAS 18001.
- Responsabilidad Social - SA 8000.
- Telecomunicaciones - TL9000.
- Calidad - ISO 9001.

Perry Johnson Registrars, Inc. (PJR)

Desde la acreditación inicial con ANAB (anteriormente RAB) y el RvA en enero de 1995, Perry Johnson Registrars ha sido la certificadora de más rápido crecimiento en Norteamérica, y ha abierto más oficinas que cualquier otra certificadora en el mundo.

PJR está actualmente acreditado por ANSI-ASQ National Accreditation Board **(ANAB - anteriormente RAB)**, Raad voor Acreditatie **(RvA)**, Japanese Acretitation Board **(JAB)**, United Kingdom Acreditation Sevices **(UKAS)**, Brazilian National Institute of Metrology **(INMETRO)**, Italian National Service for Acreditation of Certification and Inspection Body **(SINCERT)**, German Association for Accreditation **(TGA),** Federal Motor Transport Authority of Dresden **(KBA)** y por la Entidad Mexicana de Acreditación **(EMA)**. TGA y KBA están bajo la autoridad del cuerpo de acreditación alemán Deutscher Akkreditierungs Rat **(DAR)**.

Normas acreditadas:

- ISO 9001:2000.
- ISO 13485.
- ISO 14001:2004.
- TL 9000.
- AS9100.
- OHSAS 18001.
- AS9120.
- ISO 27001:2005.
- ISO 22000:2005.

Asociación Española de Normalización y Certificación (AENOR) MÉXICO

AENOR MÉXICO es una de las entidades de certificación más importantes del país, con 450 certificados emitidos tanto en México como en países de Centroamérica. En cuanto a los clientes de la entidad, los sectores más representados en las certificaciones concedidas son el químico, eléctrico, industrial y los servicios. También destaca la administración pública mexicana, a la que AENOR MÉXICO ha certificado 16 dependencias.

AENOR MÉXICO está acreditada por la Entidad Nacional de Acreditación (ENAC) en España, por la Entidad Mexicana de Acreditación (EMA) en México, por el Instituto Nacional de Normalización (INN) en Chile, por el Sistema Nazionale per l'Accreditamento degli Organismo di Certificazione e Ispezione (SINCERT) en Italia y por Internacional Automotive Task Force (IATF).
Normas acreditadas:

- ISO 9001, Sistemas de Gestión de la Calidad.
- ISO 14001, Sistemas de Gestión Ambiental.

- ISO 22000, Sistemas de Gestión de inocuidad de los alimentos.
- OHSAS 18001, Sistemas de Gestión de seguridad y salud en el trabajo.
- QS 9000 Sector de Automoción.
- ISO 27001, Sistemas de Gestión de la Seguridad de la Información.

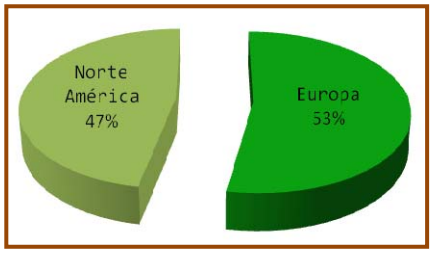
Intertek Testing Services de México, S.A. DE C.V. (INTERTEK)

Intertek es un líder internacional en certificación de sistemas y de pruebas, inspección y certificación de productos y materias primas. Con nuestra extensa red de 1000 oficinas y laboratorios en 100 países, somos la organización más grande de inspección y ensayo de productos de consumo.

Normas acreditadas:

- ISO 9001, ISO 14001, ISO 14971
- ISO 14001.
- ISO 14971.
- AS 9100.
- ISO/TS 16949.
- OHSAS 18001.
- ISO 22000 (HACCP).
- TL 9000.
- ISO 20000.
- ISO 27001.
- QC 080000.
- NOM-001-SCFI-1993, Aparatos electrónicos de uso doméstico alimentados por diferentes fuentes de energía eléctrica – Requisitos de seguridad y métodos de prueba para la aprobación de tipo.
- NOM-003-SCFI-2000, Productos eléctricos – especificaciones de seguridad.
- NOM-016-SCFI-1993, Aparatos electrónicos de uso en oficina y alimentados por diferentes fuentes de energía eléctrica – Requisitos de seguridad y métodos de prueba.
- NOM-019-SCFI-1998, Seguridad de equipo de procesamiento de datos.

1.3 Análisis

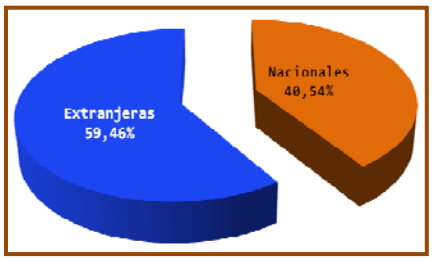


Gráfica 1.1. Comparación del origen de las entidades certificadoras en México

De la información anterior podemos obtener la gráfica 1.1, en donde observamos que en México la mayoría de las entidades certificadoras son de origen Norteamericano (principalmente México, E.U.A y Canadá) y de origen Europeo.

También podemos observar que las empresas de origen Europeo predominan sobre las de origen Norteamericano, aunque la diferencia es mínima.

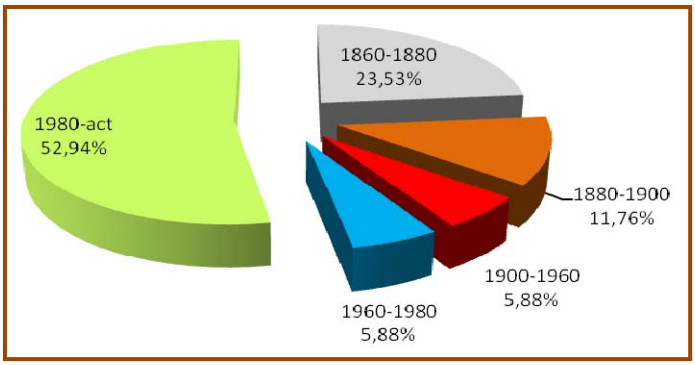
Sin embargo, en la siguiente gráfica (1.2) podemos apreciar que las empresas certificadoras nacionales tienen menos presencia en nuestro país, a diferencia de las extranjeras que tienen una presencia mayor.



Gráfica 1.2. Tipo de empresas certificadoras en México

De acuerdo al año de origen de las empresas certificadoras en México, podemos obtener la grafica 1.3, de la cual observamos que la mayoría de estas empresas tienen su origen a partir del año de 1980, incluyendo las empresas certificadoras de origen mexicano, y las primeras empresas certificadoras con sede en México datan de los años de 1860, es decir, hubo un periodo de casi 100 años sin avances en este ramo.

Los motivos de este hecho pueden deberse a diferentes factores históricos, entre los que podemos destacar el inicio de la Revolución Industrial (1750-1840), en donde se da el auge de diversas empresas industriales, el origen de la International Organization for Standardization (ISO) en 1947, en 1957 se funda en Europa la Organización Europea para la Calidad (EOQ) y en 1988 se crea la Fundación Europea para la Gestión de la Calidad (EFQM) con el objetivo de promocionar la Gestión Total de la Calidad.



Gráfica 1.3. Año de origen de las empresas certificadoras en México

En cuanto al auge de las empresas certificadoras mexicanas y extranjeras con sede en México, probablemente se debió a la creación de la Entidad Mexicana de Acreditación (EMA), que como anteriormente mencionamos, es la encargada de realizar las acreditaciones en México.

De acuerdo a lo visto durante el presente capítulo, la mayoría de las empresas certificadoras en México certifican principalmente bajo tres tipos de normas. En la tabla 1.1 se presenta una descripción general de éstas.

Tabla 1.1. Descripción general de los tres tipos de normas principales certificadas en México

Tipo de Norma	Descripción	Regulada por:	De carácter
ISO	Son normas internacionales cuya finalidad es la coordinación de las normas nacionales, de acuerdo con el Acta Final de la Organización Mundial de Comercio, con el propósito de facilitar el comercio, el intercambio de información y contribuir con normas comunes al desarrollo y a la trasferencia de tecnologías.[3]	ISO (International Organization for Standardization) y la Organización Mundial de Comercio.	Voluntario
NOM (Norma Oficial Mexicana)	Es la regulación técnica de observancia obligatoria expedida por las dependencias competentes, conforme a las finalidades establecidas en el artículo 40 de la LFMN, que establece reglas, especificaciones, atributos, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio, o método de producción u operación, así como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado, y las que se refieren a su cumplimiento o aplicación.[4]	LFMN (Ley Federal sobre Metrología y Normalización).	Obligatorio
NMX (Norma Mexicana)	Es la que elabore un organismo nacional de normalización, o la Secretaría, en los términos de esta Ley, que prevé para un uso común y repetido reglas, especificaciones, atributos, métodos de prueba, directrices, características o prescripciones aplicables a un producto, proceso, instalación, sistema, actividad, servicio o método de producción u operación, así como aquellas relativas a terminología, simbología, embalaje, marcado o etiquetado.[4]	LFMN (Ley Federal sobre Metrología y Normalización).	Voluntario. Sin embargo, si una NOM hace referencia a una NMX, dicha NMX adquirirá el carácter de obligatoria

Como información adicional a la tabla 1.1, en México podemos encontrar Normas Mexicanas cuyo nombre tiene el siguiente formato NMX-XX-0000-XXXX-0000/XXXXXX/ISO XXXX/ISO XXXX:XXXX, estas normas son copias exactas de las normas internacionales ISO.

Finalmente, con este análisis hacemos énfasis en la necesidad de impulsar la acreditación de nuevas empresas mexicanas, por lo que en el siguiente capítulo se da un panorama general sobre los requerimientos previos necesarios (recursos, documentos, etc.) para empezar el proceso de acreditación y la descripción de este proceso.

CAPÍTULO 2

Acreditación

Hoy en día en un mundo globalizado existen muchos estándares enfocados a la Seguridad tanto de la información como de las Tecnologías de la información, en la figura 2.1 presentamos a los Organismos que destacan tanto a nivel nacional como internacional en el ámbito de la Seguridad de la Información y de las Tecnologías de la Información.

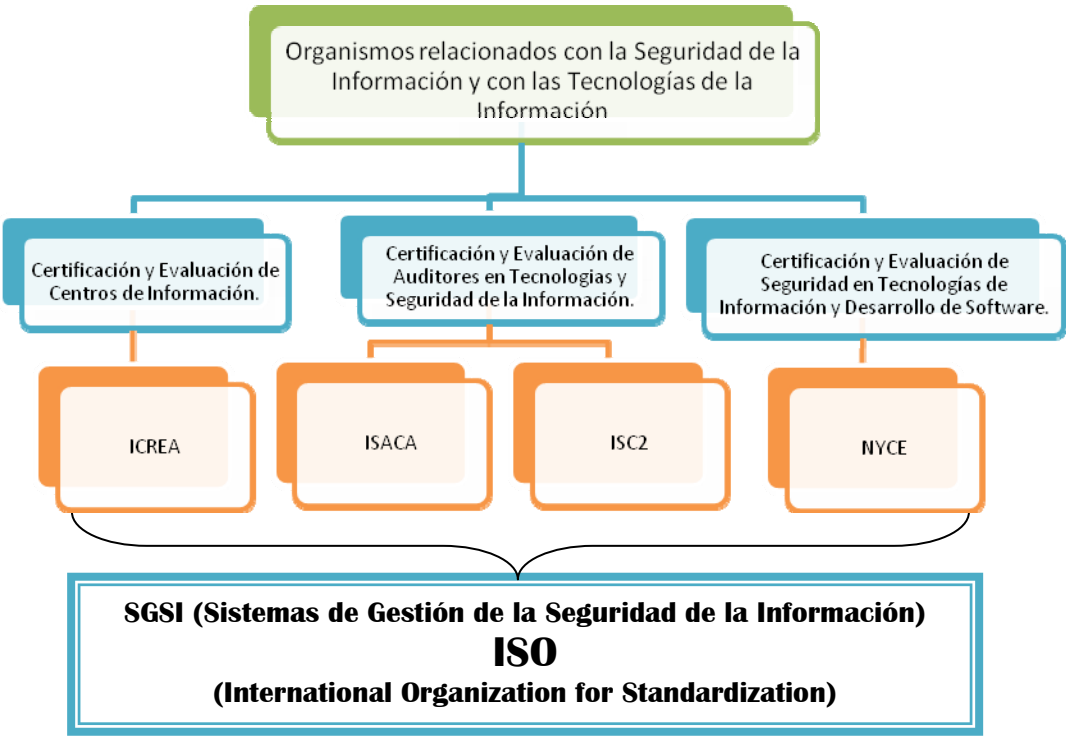


Figura 2.1. Organismos con actividades enfocadas a la Seguridad de las Tecnologías de la Información y de la Seguridad de ésta.

Los organismos mencionados en la figura 2.1 de manera directa o indirecta, se relacionan con el ciclo de vida de la información (ver figura 2.2).

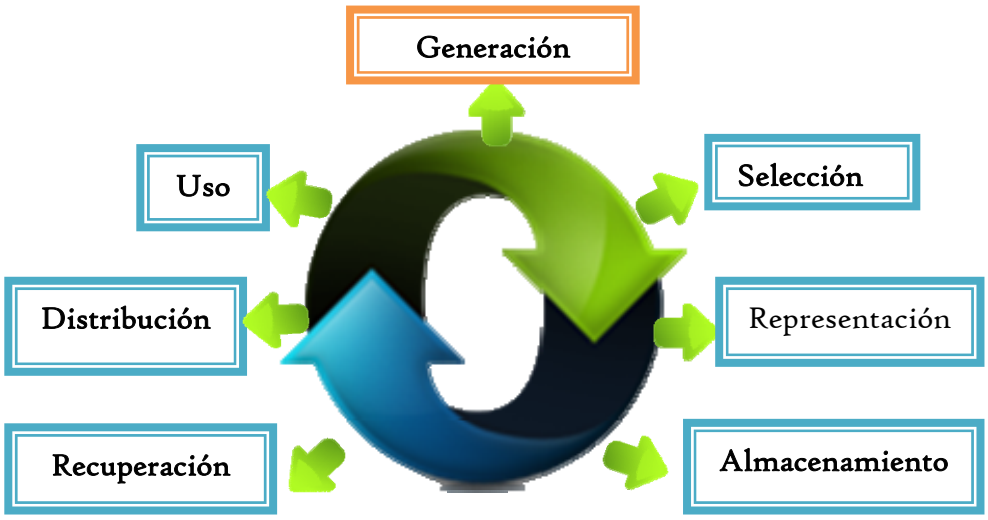


Figura 2.2 Ciclo de vida de la información.

ISO es un organismo que ha tratado de unificar y englobar estos métodos y procesos a través de una serie de normas las cuales se conocen como la serie ISO/IEC 27000.

La Organización Internacional para la Estandarización (ISO) con sede en Ginebra, Suiza, es el organismo encargado de promover el desarrollo de normas internacionales de fabricación, comercio y comunicación para todas las ramas industriales a excepción de la eléctrica y la electrónica. Estas normas son de carácter voluntario. Su función principal es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

En México existen normas mexicanas (NMX) que tratan sobre seguridad en Tecnologías de la Información, publicadas por la Secretaria de Economía en conjunto con NYCE. Además, cuenta con una serie de normas mexicana sobre la seguridad de la información que son idénticas a las normas internacionales de la serie ISO/IEC 27000, las cuales se describen a continuación:

- NMX-I-041/01-NYCE-2005: Tecnologías de la información-Seguridad de la información-Parte 01: Código de buenas prácticas para la gestión de la seguridad de la información. Esta norma es idéntica a la norma internacional ISO/IEC 17799, Primera edición (2000-12-01).
- NMX-I-041/02-NYCE-2006: Tecnologías de la información-Técnicas de seguridad-Sistemas de gestión de la seguridad de la información-Requisitos.
  Esta norma es idéntica a la norma internacional ISO/IEC 27001 (2005).

De acuerdo a lo antes mencionado hay varios organismos y normas enfocadas a preservar la seguridad de la información, sin embargo, la única norma internacional auditable que implementa un Sistema de Gestión de la Seguridad de la Información es la norma ISO/IEC 27001. Por lo tanto el presente capitulo trata sobre los requisitos previos y el proceso para acreditar a un organismo que realice actividades de Certificación basándonos en la norma ISO/IEC 27001:2005.

2.1 Requerimientos previos

2.1.1 Implementación del Sistema de Gestión de Seguridad de la Información (SGSI)

Antecedentes

ISO/IEC 27000 es un conjunto de estándares desarrollado por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La norma BS 7799 de BSI (British Standards Institution) aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa, un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es una guía de buenas prácticas, para la que no se establece un esquema de certificación. La segunda parte (BS 7799-2), publicada por primera vez en 1998, establece los requisitos de un sistema de seguridad de la información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adoptó por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000.
En 2002, se revisó BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

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

A continuación se hace un breve resumen del contenido de las normas ISO 27001 e ISO 27002. Si desea acceder a las normas completas, debe saber que éstas no son de libre difusión sino que han de ser adquiridas.

ISO 27001:2005

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

ISO 27002:2005 (anterior ISO 17799:2005)

- **Introducción:** conceptos generales de seguridad de la información y SGSI.
- **Campo de aplicación:** se especifica el objetivo de la norma.
- **Términos y definiciones:** breve descripción de los términos más usados en la norma.
- **Estructura del estándar:** descripción de la estructura de la norma.
- **Evaluación y tratamiento del riesgo:** indicaciones sobre cómo evaluar y tratar los riesgos de seguridad de la información.
- **Política de seguridad:** documento de política de seguridad y su gestión.

- **Aspectos organizativos de la seguridad de la información:** organización interna; terceros.
- **Gestión de activos:** responsabilidad sobre los activos; clasificación de la información.
- **Seguridad ligada a los recursos humanos:** antes del empleo; durante el empleo; cese del empleo o cambio de puesto de trabajo.
- **Seguridad física y ambiental:** áreas seguras; seguridad de los equipos.
- **Gestión de comunicaciones y operaciones:** responsabilidades y procedimientos de operación; gestión de la provisión de servicios por terceros; planificación y aceptación del sistema; protección contra código malicioso y descargable; copias de seguridad; gestión de la seguridad de las redes; manipulación de los soportes; intercambio de información; servicios de comercio electrónico; supervisión.
- **Control de acceso:** requisitos de negocio para el control de acceso; gestión de acceso de usuario; responsabilidades de usuario; control de acceso a la red; control de acceso al sistema operativo; control de acceso a las aplicaciones y a la información; ordenadores portátiles y teletrabajo.
- **Adquisición, desarrollo y mantenimiento de los sistemas de información:** requisitos de seguridad de los sistemas de información; tratamiento correcto de las aplicaciones; controles criptográficos; seguridad de los archivos de sistema; seguridad en los procesos de desarrollo y soporte; gestión de la vulnerabilidad técnica.
- **Gestión de incidentes de seguridad de la información:** notificación de eventos y puntos débiles de la seguridad de la información; gestión de incidentes de seguridad de la información y mejoras.
- **Gestión de la continuidad del negocio:** aspectos de la seguridad de la información en la gestión de la continuidad del negocio.
- **Cumplimiento:** cumplimiento de los requisitos legales; cumplimiento de las políticas y normas de seguridad y cumplimiento técnico; consideraciones sobre las auditorías de los sistemas de información.
- **Bibliografía:** normas y publicaciones de referencia.

Además de las normas 27001 y 27002, la serie ISO 27000 cuenta con otros estándares que complementan a estas normas.

Sistema de Gestión de Seguridad de la Información

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

ISO 27001 exige que el SGSI contemple los siguientes puntos:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.

- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

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

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

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

La confidencialidad, la integridad y disponibilidad de información sensible pueden llegar a ser esenciales para mantener los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial necesarios para lograr los objetivos de la organización y asegurar beneficios económicos. El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios. El modelo de la gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos (Ver figura 2.3).

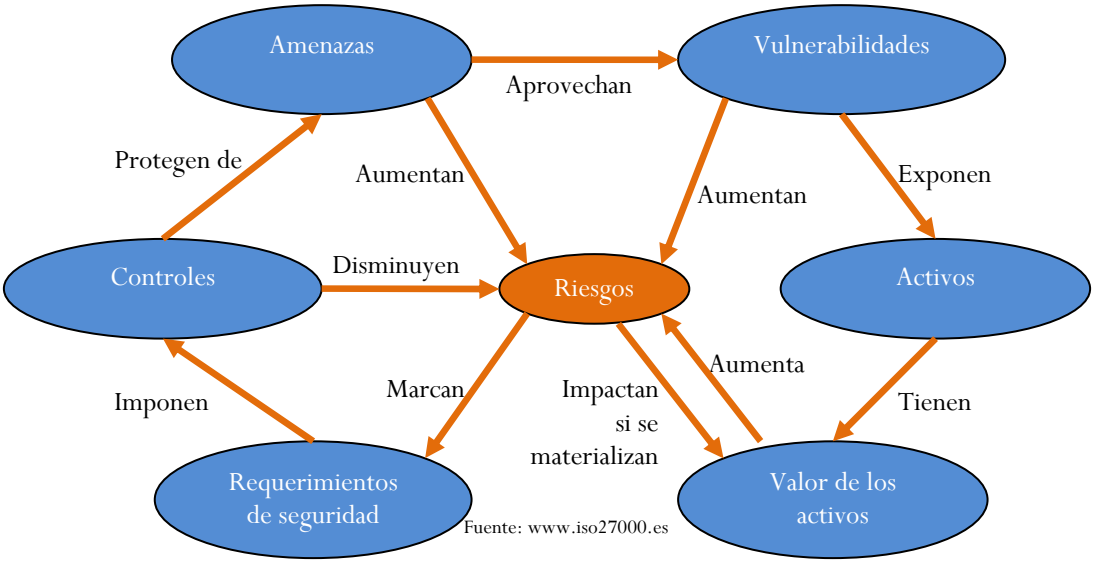


Figura 2.3. Modelo de la Gestión de la Seguridad.

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

Documentación

La documentación del modelo de un SGSI basado en ISO 27001 se puede mostrar gráficamente con una pirámide de cuatro niveles, como se muestra en la figura 2.4:

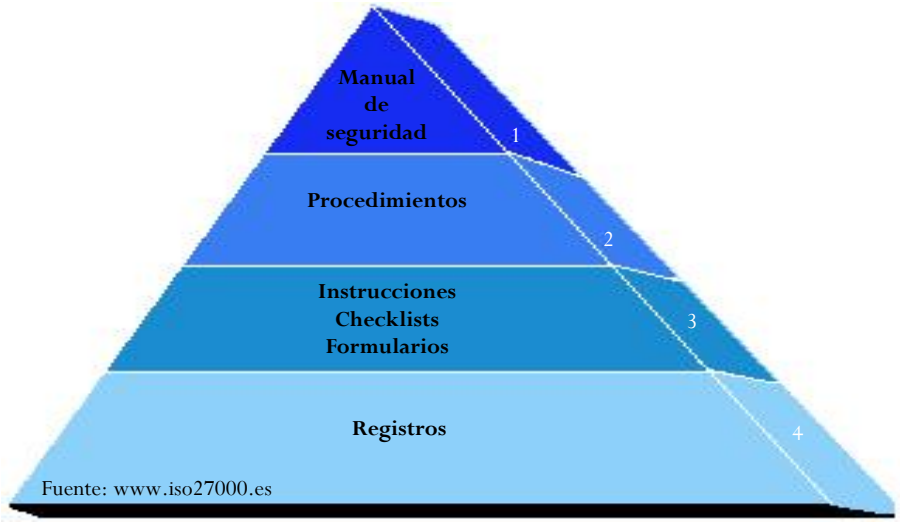


Figura 2.4. Pirámide documental de un SGSI

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

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

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

Registros: Documentos que proporcionan una evidencia objetiva del cumplimiento de los requisitos del SGSI; están asociados con los documentos antes mencionados como resultado que demuestran que se ha cumplido lo indicado en los mismos.

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

- ***Alcance del SGSI:*** ámbito de la organización que queda sometido al SGSI, incluyendo una identificación clara de las dependencias, relaciones y límites que existen entre el alcance y aquellas partes que no hayan sido consideradas (en aquellos casos en los que el ámbito de influencia del SGSI considere un subconjunto de la organización como delegaciones, divisiones, áreas, procesos, sistemas o tareas concretas).

- ***Política y objetivos de seguridad:*** documento de contenido genérico que establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- ***Procedimientos y mecanismos de control que soportan al SGSI:*** son aquellos procedimientos que regulan el propio funcionamiento del SGSI.

- ***Enfoque de evaluación de riesgos:*** es la descripción de la metodología a emplear (como se realizará la evaluación de las amenazas, vulnerabilidades, probabilidades de ocurrencia e impactos en relación a los activos de información contenidos dentro del alcance seleccionado), desarrollo de criterios de aceptación de riesgo y fijación de niveles de riesgo aceptables.

- ***Informe de evaluación de riesgos:*** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.

- ***Plan de tratamientos de riegos:*** documento que identifica las acciones de la dirección, los recursos, las responsabilidades y las prioridades para gestionar los riesgos de seguridad de la información, en función de las conclusiones obtenidas de la evaluación de riesgos, de los objetivos de control identificados, de los recursos disponibles, etc.

- ***Procedimientos documentados:*** todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- ***Registros:*** documentos que proporcionan evidencia de la conformidad (cumplimiento de un requisito de la norma) con los requisitos y del funcionamiento eficaz del SGSI.

- ***Declaración de aplicabilidad (SOA- Statements of applicability):*** documento que contiene los objetivos de control y los controles contemplados por el SGSI, basados en los

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

Control de la documentación

Para los documentos generados se debe establecer cómo documentar, implantar y mantener un procedimiento que defina las acciones de gestión necesarias para:

- Aprobar documentos apropiados antes de su emisión.
- Revisar y actualizar documentos cuando sea necesario y renovar su validez.
- Garantizar que los cambios y el estado actual de revisión de los documentos están identificados.
- Garantizar que las versiones relevantes de documentos vigentes están disponibles en los lugares de empleo.
- Garantizar que los documentos se mantienen legibles y fácilmente identificables.
- Garantizar que los documentos permanecen disponibles para aquellas personas que los necesiten y que son transmitidos, almacenados y finalmente destruidos acorde con los procedimientos aplicables según su clasificación.
- Garantizar que los documentos procedentes del exterior están identificados.
- Garantizar que la distribución de documentos está controlada.
- Prevenir la utilización de documentos obsoletos.
- Aplicar la identificación apropiada a documentos que son retenidos con algún propósito.

Implementación

Para establecer y gestionar un SGSI con base en ISO 27001, se utiliza el ciclo continúo PDCA (Plan - Do – Check - Act) tradicional en los sistemas de gestión de la calidad.

Plan (planificar): Establecer el SGSI

- Definir el alcance de SGSI en términos del negocio, la organización, su localización, activos y tecnologías, incluyendo detalles y justificación de cualquier exclusión.
- Definir una política de seguridad que:
  - incluya el marco general y los objetivos de seguridad de la información de la organización;
  - considere requerimientos legales o contractuales relativos a la seguridad de la información;
  - esté alineada con el contexto estratégico de gestión de riesgos de la organización en el que se establecerá y mantendrá el SGSI;
  - establezca los criterios con los que se va a evaluar el riesgo;
  - esté aprobada por la dirección.
- Definir una metodología de evaluación del riesgo apropiada para el SGSI y los requerimientos del negocio, además de establecer los criterios de aceptación de riesgo y especificar los niveles de riesgo aceptable. Lo primordial de esta metodología es que los resultados obtenidos sean comparables y repetibles.
- Identificar los riesgos:
  - identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;

- identificar las amenazas en relación a los activos;
- identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
- identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

- Analizar y evaluar los riesgos:
  - evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
  - evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
  - estimar los niveles de riesgo;
  - determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.
- Identificar y evaluar las distintas opciones de tratamiento de los riesgos para:
  - aplicar controles adecuados;
  - aceptar el riesgo, siempre y cuando se siga cumpliendo con las políticas y criterios establecidos para la aceptación de los riesgos;
  - evitar el riesgo, p. ej., mediante el cese de las actividades que lo originan;
  - transferir el riesgo a terceros, p.ej., compañías aseguradoras o proveedores de *outsourcing.*
- Seleccionar los objetivos de control y los controles del Anexo A de ISO 27001 para el tratamiento del riesgo que cumplan con los requerimientos identificados en el proceso de evaluación del riesgo.
- Aprobar por parte de la dirección tanto los riesgos residuales (El riesgo que permanece tras el tratamiento del riesgo) como la implantación y uso del SGSI.
- Definir una declaración de aplicabilidad que incluya:
  - los objetivos de control y controles seleccionados y los motivos para su elección;
  - los objetivos de control y controles que actualmente ya están implementados;
  - los objetivos de control y controles del Anexo A excluidos y los motivos para su exclusión; este es un mecanismo que permite, además detectar posibles omisiones involuntarias.

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

Do (hacer): Implementar y utilizar el SGSI

- Definir un plan de tratamiento de riesgos que identifique las acciones como recursos, responsabilidades y prioridades en la gestión de los riesgos de seguridad de la información.
- Implantar el plan de tratamiento de riesgos, con el fin de alcanzar los objetivos de control identificados, incluyendo la asignación de recursos, responsabilidades y prioridades.

- Implementar los controles anteriormente seleccionados, que lleven a los objetivos de control.
- Definir un sistema de métricas que permita obtener resultados reproducibles y comparables para medir la eficacia de los controles o grupos de controles.
- Procurar programas de formación y concienciación en relación a la seguridad de la información a todo el personal.
- Gestionar las operaciones del SGSI.
- Gestionar los recursos necesarios asignados al SGSI para el mantenimiento de la seguridad de la información.
- Implantar procedimientos y controles que permitan una rápida detección y respuesta a los incidentes de seguridad.

Check (verificar): Monitorizar y revisar el SGSI

La organización deberá:

- Ejecutar procedimientos de monitorización y revisión para:
  - detectar a tiempo los errores en los resultados generados por el procesamiento de la información;
  - identificar brechas e incidentes de seguridad;
  - ayudar a la dirección a determinar si las actividades, desarrolladas por las personas y dispositivos tecnológicos para garantizar la seguridad de la información, se desarrollan en relación a lo previsto.
  - detectar y prevenir eventos e incidentes de seguridad mediante el uso de indicadores;
  - determinar si las acciones realizadas para resolver brechas de seguridad fueron efectivas.
- Revisar regularmente la efectividad del SGSI, atendiendo el cumplimiento de la política y objetivos del SGSI, los resultados de auditorías de seguridad, incidentes, resultados de las mediciones de eficacia, sugerencias y observaciones de todas las partes implicadas.
- Medir la efectividad de los controles para verificar que se cumple con los requisitos de la seguridad.
- Revisar regularmente en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables, teniendo en cuenta los posibles cambios que hayan podido producirse en la organización, la tecnología, los objetivos y procesos de negocio como las amenazas identificadas, la efectividad de los controles implementados y el entorno exterior -requerimientos legales, obligaciones contractuales, etc.
- Realizar periódicamente auditorías internas del SGSI en intervalos planificados.
- Revisar el SGSI por parte de la dirección periódicamente para garantizar que el alcance definido sigue siendo el adecuado y que las mejoras en le proceso del SGSI son evidentes.
- Actualizar los planes de seguridad en función de las conclusiones y nuevos hallazgos encontrados durante las actividades de monitorización y revisión.
- Registrar acciones y eventos que puedan haber impactado sobre la efectividad o el rendimiento del SGSI.

Act (actuar): Mantener y mejorar el SGSI

La organización deberá regularmente:

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

El Plan-Do-Check-Act (PDCA) es un ciclo de vida continuo, lo cual quiere decir que la fase de Act lleva de nuevo a la fase de plan para iniciar un nuevo ciclo de las cuatro fases. No hay una secuencia estricta de las fases, por ejemplo, puede haber actividades de implantación que ya se llevan a cabo cuando otras de planificación aún no han finalizado; o que se monitoricen controles que aún no están implantados en su totalidad.

Funciones de la gerencia dentro de un SGSI

Uno de los componentes primordiales en la implantación exitosa de un Sistema de Gestión de Seguridad de la Información es la implicación de la dirección. No se trata de una expresión retórica, sino que debe asumirse desde un principio que un SGSI afecta fundamentalmente a la gestión del negocio y requiere, por tanto, de decisiones y acciones que sólo puede tomar la gerencia de la organización. No se debe caer en el error de considerar un SGSI una mera cuestión técnica o tecnológica relegada a niveles inferiores del organigrama; se están gestionando riesgos e impactos de negocio que son responsabilidad y decisión de la dirección.

El término Dirección debe contemplarse siempre desde el punto de vista del alcance del SGSI. Es decir, se refiere al nivel más alto de gerencia de la parte de la organización afectada por el SGSI (el alcance no tiene por qué ser toda la organización).

Algunas de las tareas fundamentales del SGSI que ISO 27001 asigna a la dirección se detallan en los siguientes puntos:

Compromiso de la dirección

La dirección de la organización debe comprometerse con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI. Para ello, debe tomar las siguientes iniciativas:

- Establecer una política de seguridad de la información.
- Asegurarse de que se establecen objetivos y planes del SGSI.
- Establecer roles y responsabilidades de seguridad de la información.
- Comunicar a la organización tanto la importancia de lograr los objetivos de seguridad de la información y de cumplir con la política de seguridad, como sus responsabilidades legales y la necesidad de mejora continua.
- Asignar suficientes recursos al SGSI en todas sus fases.

- Decidir los criterios de aceptación de riesgos y sus correspondientes niveles.
- Asegurar que se realizan auditorías internas.
- Realizar revisiones del SGSI, como se detalla más adelante.

Revisión del SGSI

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

- Resultados de auditorías y revisiones del SGSI.
- Observaciones de todas las partes interesadas.
- Técnicas, productos o procedimientos que pudieran ser útiles para mejorar el rendimiento y eficacia del SGSI.
- Información sobre el estado de acciones preventivas y correctivas.
- Vulnerabilidades o amenazas que no fueran tratadas adecuadamente en evaluaciones de riesgos anteriores.
- Resultados de las mediciones de eficacia.
- Estado de las acciones iniciadas a raíz de revisiones anteriores de la dirección.
- Cualquier cambio que pueda afectar al SGSI.
- Recomendaciones de mejora.

Basándose en todas estas informaciones, la dirección debe revisar el SGSI y tomar decisiones y acciones relativas a:

- Mejora de la eficacia del SGSI.
- Actualización de la evaluación de riesgos y del plan de tratamiento de riesgos.
- Modificación de los procedimientos y controles que afecten a la seguridad de la información, en respuesta a cambios internos o externos en los requisitos de negocio, requerimientos de seguridad, procesos de negocio, marco legal, obligaciones contractuales, niveles de riesgo y criterios de aceptación de riesgos.
- Necesidades de recursos.
- Mejora de la forma de medir la efectividad de los controles.

Aspectos Clave

- ***Fundamentales:***

  - Compromiso y apoyo de la Dirección de la organización.
  - Definición clara de un alcance apropiado.
  - Concienciación y formación del personal.
  - Evaluación de riesgos exhaustiva y adecuada a la organización.
  - Compromiso de mejora continúa.
  - Establecimiento de políticas y normas.
  - Organización y comunicación.
  - Integración del SGSI en la organización.

❖ ***Factores de éxito:***

- La concienciación del empleado por la seguridad. Principal objetivo a conseguir.
- Realización de comités de dirección con descubrimiento continuo de No conformidades (incumplimiento de un requisito) o acciones de mejora.
- Creación de un sistema de gestión de incidencias que recoja notificaciones continuas por parte de los usuarios (los incidentes de seguridad deben ser reportados y analizados).
- La seguridad absoluta no existe, se trata de reducir el riesgo a niveles asumibles.
- La seguridad no es un producto, es un proceso.
- La seguridad no es un proyecto, es una actividad continua y el programa de protección requiere el soporte de la organización para tener éxito.
- La seguridad debe ser inherente a los procesos de información y del negocio.

❖ ***Riesgos:***

- Exceso de tiempos de implantación: con los consecuentes costes descontrolados, desmotivación, alejamiento de los objetivos iniciales, etc.
- Temor ante el cambio: resistencia de las personas.
- Discrepancias en los comités de dirección.
- Delegación de todas las responsabilidades en departamentos técnicos.
- No asumir que la seguridad de la información es inherente a los procesos de negocio.
- Planes de formación y concienciación inadecuados.
- Calendario de revisiones que no se puedan cumplir.
- Definición poco clara del alcance.
- Exceso de medidas técnicas en detrimento de la formación, concienciación y medidas de tipo organizativo.
- Falta de comunicación de los progresos al personal de la organización.

❖ ***Consejos básicos***

- Mantener la sencillez y restringirse a un alcance manejable y reducido: un centro de trabajo, un proceso de negocio clave, un único centro de proceso de datos o un área sensible concreta; una vez conseguido el éxito y observados los beneficios, ampliar gradualmente el alcance en sucesivas fases.
- Comprender en detalle el proceso de implantación: iniciarlo en base a cuestiones exclusivamente técnicas es un error frecuente que rápidamente sobrecarga de problemas la implantación; adquirir experiencia de otras implantaciones, asistir a cursos de formación o contar con asesoramiento de consultores externos especializados.
- La autoridad y compromiso decidido de la Dirección de la empresa -incluso si al inicio el alcance se restringe a un alcance reducido- evitarán un muro de excusas para desarrollar las buenas prácticas, además de ser uno de los puntos fundamentales de la norma.
- No reinventar la rueda: aunque el objetivo sea ISO 27001, es bueno obtener información relativa a la gestión de la seguridad de la información de otros métodos y marcos reconocidos.

- Servirse de lo ya implementado: otros estándares como ISO 9001 son útiles como estructura de trabajo, ahorrando tiempo y esfuerzo y creando sinergias; es conveniente pedir ayuda e implicar a auditores internos y responsables de otros sistemas de gestión.
- Reservar la dedicación necesaria diaria o semanal: el personal involucrado en el proyecto debe ser capaz de trabajar con continuidad en el proyecto.
- Registrar evidencias: deben recogerse evidencias al menos tres meses antes del intento de certificación para demostrar que el SGSI funciona adecuadamente.

2.1.2 Recursos: humanos, materiales y tecnológicos para implementar un SGSI

Asignación de recursos

Para el correcto desarrollo de todas las actividades relacionadas con el SGSI, es imprescindible la asignación de recursos. Es responsabilidad de la dirección garantizar que se asignen los suficientes para:

- Establecer, implementar, operar, monitorizar, revisar, mantener y mejorar el SGSI.
- Garantizar que los procedimientos de seguridad de la información apoyan los requerimientos de negocio.
- Identificar y tratar todos los requerimientos legales y normativos, así como las obligaciones contractuales de seguridad.
- Aplicar correctamente todos los controles implementados, manteniendo de esa forma la seguridad adecuada.
- Realizar revisiones cuando sea necesario y actuar adecuadamente según los resultados de las mismas.
- Mejorar la eficacia del SGSI donde sea necesario.

Formación y concienciación

La formación y la concienciación en seguridad de la información son elementos básicos para el éxito de un SGSI. Por ello, la dirección debe asegurar que todo el personal de la organización al que se le asignen responsabilidades definidas en el SGSI esté suficientemente capacitado. Se deberá:

- Determinar las competencias necesarias para el personal que realiza tareas en aplicación del SGSI.
- Satisfacer dichas necesidades por medio de formación o de otras acciones como, p. ej., contratación de personal ya formado.
- Evaluar la eficacia de las acciones realizadas.
- Mantener registros de estudios, formación, habilidades y experiencia.

Además, la dirección debe asegurar que todo el personal relevante esté concienciado de la importancia de sus actividades de seguridad de la información y de cómo contribuye a la consecución de los objetivos del SGSI.

2.1.3 Documentación

Para solicitar la acreditación el Organismo Solicitante debe conocer y disponer de los siguientes documentos.

2.1.3.1 Documentos de referencia

Estos documentos son necesarios para que el Organismo Solicitante tenga un panorama general sobre el proceso de acreditación que debe seguir el Organismo de Acreditación.

- **Procedimiento de acreditación del Organismo de Acreditación**

Estos documentos tienen como objetivo establecer los pasos y las diferentes etapas que debe seguir la solicitud de un Organismo de Certificación para otorgar, mantener, renovar, ampliar, reducir, actualizar, suspender y cancelar la acreditación con el Organismo de Acreditación.

El contenido de este documento puede variar de acuerdo al Organismo de Acreditación, sin embargo, los puntos que normalmente deberán abarcar son los siguientes:

a) Objetivo y campo de aplicación.
b) Documentación de referencia.
c) Alcance de acreditación.
d) Criterios de acreditación.
e) Solicitud de acreditación.
f) Procedimiento de acreditación.
g) Mantenimiento de la acreditación.
h) Ampliación del alcance de una acreditación.
i) Notificaciones.
j) Derechos y obligaciones.
k) Suspensión y retirada de la acreditación.

Estos documentos pueden ser solicitados directamente en las oficinas del Organismo de Acreditación o pueden descargarse de la página web del Organismo de Acreditación.

- **ISO/IEC 17021: 2006 Requisitos generales para los organismos que realizan la auditoría y la certificación de sistemas de gestión.**

La norma ISO/IEC 17021:2006 establece los requisitos generales relativos a la competencia técnica de las entidades de certificación que realizan certificación de sistemas de gestión.

En algunos casos es conveniente aclarar o precisar el contenido o interpretación de algunos apartados de la norma cuando ésta va a ser usada en un proceso de acreditación con el fin de asegurar la coherencia en la evaluación.

La norma ISO/IEC 17021 está conformada de la siguiente manera:

INDICE

PRÓLOGO

PRÓLOGO DE LA VERSIÓN EN ESPAÑOL

INTRODUCCIÓN

1. OBJETO Y CAMPO DE APLICACIÓN

2. NORMAS PARA CONSULTA
3. TÉRMINOS Y DEFINCIONES

4. PRINCIPIOS
4.1. Generalidades
4.2. Imparcialidad
4.3. Competencia
4.4. Responsabilidad
4.5. Transparencia
4.6. Confidencialidad
4.7. Receptividad y respuesta oportuna a las quejas

5. REQUISITOS GENERALES
5.1. Asuntos legales y contractuales
5.2. Gestión de imparcialidad
5.3. Responsabilidad legal y financiamiento

6. REQUISITOS RELATIVOS A LA ESTRUCTURA
6.1. Estructura de la organización y alta dirección
6.2. Comité para la preservación de la imparcialidad

7. REQUISITOS RELATIVOS A LOS RECURSOS
7.1. Competencia de la dirección y del personal
7.2. Personal que interviene en las actividades de certificación
7.3. Empleo de auditores externos y expertos técnicos externos individuales
7.4. Registros relativos al personal
7.5. Contratación externa

8. REQUISITOS RELATIVOS A LA INFORMACIÓN
8.1. Información accesible al público
8.2. Documentos de certificación
8.3. Lista de clientes certificados
8.4. Referencia a la certificación y utilización de marcas
8.5. Confidencialidad
8.6. Intercambio de información entre el organismo de certificación y sus clientes
9. REQUISITOS RELATIVOS A LOS PROCESOS

9.1. Requisitos generales
9.2. Auditoría inicial y certificación
9.3. Actividades de vigilancia
9.4. Renovación de la certificación
9.5. Auditorías especiales
9.6. Suspender, retirar o reducir el alcance de la certificación
9.7. Apelaciones
9.8. Quejas
9.9. Registros relativos a solicitantes y clientes

10. REQUISITOS RELATIVOS AL SISTEMA DE GESTIÓN DE LOS ORGANISMOS DE CERTIFICACIÓN
10.1. Opciones
10.2. Opción 1: Requisitos del sistema de gestión de acuerdo con la Norma ISO 9001
10.3. Opción 2: Requisitos generales del sistema de gestión

ANEXO I: COMITÉ DE PARTES.

ANEXO II: REGLAS PARA EL USO DE LAS MARCAS DE CERTIFICACIÓN DE SISTEMAS DE GESTIÓN.

ANEXO III: TRATAMIENTO DE QUEJAS SOBRE EL PRODUCTO O EL SERVICIO DE UNA ORGANIZACIÓN CUYO SISTEMA DE GESTIÓN ESTA CERTIFICADO.

Esta norma puede adquirirse a través de la página electrónica de AENOR: (http://www.aenor.es/desarrollo/normalizacion/normas/resultadobuscnormas.asp).

- **ISO/IEC 27006:2007 Information Technology – Security techniques-requirements for bodies providing audit and certification of information security management systems.**

Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA7/03 (Requisitos para la acreditación de entidades que operan certificación / registro de SGSI) que añade a ISO/IEC 17021 (requisitos para las entidades de auditoría y certificación de sistemas de gestión). Los requisitos específicos relacionados con ISO 217001 y los SGSI‘s. Es decir, ayuda a interpretar los criterios de acreditación de ISO/IEC 17021, cuando se aplican a entidades de certificación de ISO 27001, pero no es una norma de acreditación por sí misma. En España, esta norma aún no está traducida, y la forma de adquirir esta norma en México, es a través de AENOR, que es una entidad certificadora de origen español, sin embargo, el original en inglés puede adquirirse en “http://iso.org/”.

Esta norma está conformada por los siguientes puntos:

- **Preámbulo:** presentación de las organizaciones ISO e IEC y sus actividades.
- **Introducción:** antecedentes de ISO 27006 y guía de uso para la norma.
- **Campo de aplicación:** a quién aplica este estándar.
- **Referencias normativas:** otras normas que sirven de referencia.
- **Términos y definiciones:** breve descripción de los términos más usados en la norma.
- **Principios:** principios que rigen esta norma.

- **Requisitos generales:** aspectos generales que deben cumplir las entidades de certificación de SGSI's.
- **Requisitos estructurales:** estructura organizativa que deben tener las entidades de certificación de SGSI's.
- **Requisitos en cuanto a recursos:** competencias requeridas para el personal de dirección, administración y auditoría de el Organismo de Certificación, así como para auditores externos, expertos técnicos externos y subcontratas.
- **Requisitos de información:** información pública, documentos de certificación, relación de clientes certificados, referencias a la certificación y marcas, confidencialidad e intercambio de información entre el Organismo de Certificación y sus clientes.
- **Requisitos del proceso:** requisitos generales del proceso de certificación, auditoría inicial y certificación, auditorías de seguimiento, re-certificación, auditorías especiales, suspensión, retirada o modificación de alcance de la certificación, apelaciones, reclamaciones y registros de solicitantes y clientes.
- **Requisitos del sistema de gestión de entidades de certificación:** opciones, opción 1 (requisitos del sistema de gestión de acuerdo con ISO 9001) y opción 2 (requisitos del sistema de gestión general).
- **Anexo A - Análisis de la complejidad de la organización de un cliente y aspectos específicos del sector:** potencial de riesgo de la organización (tabla orientativa) y categorías de riesgo de la seguridad de la información específicas del sector de actividad.
- **Anexo B - Áreas de ejemplo de competencia del auditor:** consideraciones de competencia general y consideraciones de competencia específica (conocimiento de los controles del Anexo A de ISO 27001:2005 y conocimientos sobre SGSI).
- **Anexo C - Tiempos de auditoría**: introducción, procedimiento para determinar la duración de la auditoría y tabla de tiempos de auditoría (incluyendo comparativa con tiempos de auditoría de sistemas de calidad -ISO 9001- y medioambientales -ISO 14001-).
- **Anexo D - Guía para la revisión de controles implantados del Anexo A de ISO 27001:2005:** tabla de apoyo para el auditor sobre cómo auditar los controles, sean organizativos o técnicos.

2.1.3.2 Documentos necesarios

Estos documentos son los que se deberán entregar junto con la solicitud de acreditación como anexos. La entrega de dichos documentos dependerá del Organismo de Acreditación y generalmente son los siguientes:

- Documentación justificativa de la personalidad jurídica del Organismo de Certificación (Acta constitutiva).
- Listado de delegaciones.
- Organigrama del Organismo Solicitante.
- Documentación donde se identifique la estructura y denominación del comité.
- Documentación sobre organismos relacionados.
- Listado del personal de la entidad de certificación.
- Copia de los procedimientos: requisitos de calificación y supervisión y selección del equipo auditor.
- Lista de auditores cualificados.
- Copia de los documentos/procedimientos.
- Listado de subcontrataciones y subcontratistas.

- Listado de todas las certificaciones concedidas. En caso de no haber expedido alguna certificación, debe ingresar un escrito en el que se declara esta situación y la disponibilidad de contar con un cliente potencial para continuar con el proceso.
- Copia de un certificado emitido.
- Listado actualizado de documentos en vigor.
- Tabla cruzada de las clausulas de la norma ISO/IEC 17021 e ISO/IEC 27006:2007 con los documentos de su sistema de gestión.
- Comprobante de pago por el servicio para realizar la apertura del expediente.

En caso de no adjuntar alguno de los documentos anteriores, el Organismo Solicitante deberá indicar los motivos. Cada documento deberá estar debidamente identificado y fechado.

La documentación del SGSI deberá incluir:

- Política y objetivos de seguridad.
- Alcance del SGSI.
- Procedimientos y controles que apoyan al SGSI.
- Descripción de la metodología de evaluación del riesgo.
- Informe resultante de la evaluación del riesgo.
- Plan de tratamiento de riesgos.
- Procedimientos de planificación, manejo y control de los procesos de seguridad de la información y de la medición de la eficacia de los controles.
- Registros.
- Declaración de aplicabilidad (SOA – Statement of Applicability-).
- Procedimiento de gestión de toda la documentación del SGSI.

Como recomendación, hay una serie de controles clave que un auditor va a examinar siempre en profundidad:

- Política de seguridad.
- Asignación de responsabilidades de seguridad.
- Formación y capacitación para la seguridad.
- Registro de incidencias de seguridad.
- Gestión de continuidad del negocio.
- Protección de datos personales.
- Salvaguarda de registros de la organización.
- Derechos de propiedad intelectual.

2.1.4 Experiencia

Una vez implantado el SGSI en la organización, y con un historial demostrable de al menos 3 meses, se puede pasar a la fase de auditoría y acreditación.

2.2 Solicitud de acreditación

La solicitud de acreditación se complementará por el Organismo Solicitante en el formulario de solicitud de acreditación, en el que un representante autorizado del Organismo Solicitante:

- Define el alcance de la acreditación,
- Declara tener conocimiento del sistema de acreditación del Organismo de Acreditación, de los derechos y obligaciones de los Organismos Acreditados definidos en el procedimiento de acreditación del Organismo de Acreditación,
- Efectúa la demanda oficial de acreditación,
- Se compromete a cumplir con los requisitos de acreditación y las otras obligaciones de los Organismos acreditados, a respetar el procedimiento de acreditación, y en particular, a recibir y prestar colaboración al equipo auditor, permitiendo cualquier comprobación razonable para verificar el cumplimiento de los requisitos de acreditación, hacerse cargo de los gastos que ocasione la evaluación y los que le corresponden como consecuencia de controles posteriores.

El pago de la tarifa vigente de apertura de expediente será condición necesaria para poder iniciar el proceso de acreditación.
La información recibida por el Organismo de Acreditación, tanto en a solicitud como a lo largo del procedimiento, será considerada como confidencial en todos los aspectos.

Cuando la acreditación solicitada tiene implicaciones reglamentarias o va a ser utilizada por la administración en procesos de autorización o similares, es responsabilidad del Organismo Solicitante el asegurarse de que el alcance de la acreditación que solicita sea requerido por la autoridad competente en cada caso.

2.2.1 Alcance

El alcance de acreditación es una parte fundamental de la solicitud de acreditación, ya que constituirá finalmente el anexo técnico que acompaña al "Certificado de Acreditación".

El alcance de la acreditación es la declaración que define el área, rama, campo, sector, técnica o norma, pliego de condiciones o cualquier prescripción técnica susceptible de evaluación, en las que se demuestra la competencia técnica del organismo de certificación.

La acreditación debe basarse en alcances de acreditación definidos de forma clara, precisa y sin ambigüedades que proporcionen tanto al cliente del acreditado como otras partes interesadas una información concreta sobre la competencia técnica demostrada.

El Organismo Solicitante deberá definir el alcance para el que desea ser acreditado. El Organismo de Acreditación limitará las evaluaciones y la decisión de acreditación al alcance definido por el Organismo Solicitante.

El alcance definirá con referencia a:

a) ***El propio Organismo Solicitante:*** Cada acreditación estará referida a una Unidad Técnica. Se entenderá por "Unidad Técnica" a un conjunto de medios técnicos y humanos perfectamente definido y adscrito a los fines propios de la acreditación solicitada. Una Unidad Técnica puede coincidir con la organización que solicita la acreditación o ser una parte de ésta, por ejemplo, un departamento dentro de una empresa.

b) ***Lo que es objeto de certificación:*** Los sistemas a certificar, que podrían estar limitados, cuando corresponda, a una serie de sectores industriales o de actividad. En los formularios de solicitud correspondientes a cada sistema de gestión se indican, en su caso, los sectores aplicables. El alcance del SGSI debe realizarse en términos referidos al negocio o actividad que desempeña la organización, a la propia organización y su estructura, dónde se encuentra situada y en qué términos (instalaciones físicas, remotas, sucursales, etc.), sus activos y la tecnología afectada (WI-FI, cable, etc.). Asimismo, la organización debe incluir en detalle los motivos que justifiquen las exclusiones que va a realizar en su SGSI.

c) ***Los documentos normativos según los cuales son certificados:*** La acreditación estará referida a los documentos normativos según los cuales son certificados, los sistemas, los productos o personas.

Una vez llenado la solicitud de acreditación deberá ser enviada al Organismo de Acreditación.

2.3 Evaluación

Una vez recibida la solicitud de acreditación por el Organismo de Acreditación, ésta acusará recibo de la misma y revisará la documentación suministrada con objeto de comprobar que la actividad es susceptible de ser acreditada o si existe algún motivo legal, estatutario o de otra índole que lo impida, en cuyo caso se lo comunicará al Organismo Solicitante. Se evaluará también si la actividad corresponde al esquema de acreditación bajo el que se solicita y que el Organismo de Acreditación está capacitado para atender dicha solicitud. Así mismo se verificará que el alcance esté claramente definido, y la documentación sea completa y adecuada, si la documentación no fuera completa o adecuada se pedirá al Organismo Solicitante que la complete.

La evaluación de la competencia se lleva a cabo mediante el **estudio de los documentos** que describen el modo en que el Organismo Solicitante realiza sus actividades (sistema de gestión, métodos y procedimientos de trabajo, competencia del personal, etc.) y la **evaluación "In Situ" (en sitio)** de cómo trabaja el Organismo Solicitante. Los resultados de la evaluación se recogen en un informe que se envía al Organismo Solicitante al que debe dar respuesta con las acciones correctivas que considere pertinentes.

Con el informe de evaluación y la respuesta del Organismo Solicitante, la Comisión de Acreditación toma una decisión. Si es positiva se emite el certificado de acreditación.

2.3.1 Designación del equipo auditor

Esta etapa consiste en designar y notificar al Organismo Solicitante los nombres de los miembros del equipo auditor, así como la organización a la que pertenecen.

El equipo auditor designado es el que realiza la evaluación documental, la evaluación en sito y la evaluación de seguimiento en caso de que se requiera.

El número de integrantes del equipo auditor estará en función del alcance de la acreditación solicitado pero, contará en cualquier caso, con un auditor jefe, responsable final de la auditoría y tantos técnicos como sean necesarios.

El Organismo Solicitante será informado con suficiente antelación de los miembros del equipo auditor y, en su caso, de la organización a la que pertenecen. El Organismo Solicitante podrá rechazar a cualquier miembro del equipo auditor por escrito presentando los motivos. Esto no implica que el Organismo de Acreditación esté obligado a aceptar dicho rechazo.

2.3.2 Criterios

La evaluación se llevará a cabo de la siguiente manera:

a) **Estudio de la documentación técnica:**

Esta etapa de proceso de evaluación define las responsabilidades y actividades para que el equipo auditor lleve a cabo la evaluación documental de procedimientos técnicos y del SGSI documentados, para determinar que el Organismo Solicitante cuenta con los elementos necesarios para proceder a realizar la evaluación en sitio.

Esta evaluación puede realizarse en las instalaciones del Organismo Solicitante, en las oficinas del Organismo de Acreditación o en su caso, en las oficinas del equipo auditor.

Si el resultado de dicho estudio documental es satisfactorio, continuará la evaluación (auditoría) en sitio. En caso contrario, se informará al Organismo Solicitante para que resuelva los problemas detectados.

b) Evaluación In Situ:

Esta etapa consiste en evaluar en las instalaciones del Organismo Solicitante el SGSI para verificar que se cumplen los requisitos establecidos en la(s) norma(s) correspondiente(s).

En la evaluación In Situ, el responsable asignado del Organismo Solicitante, realiza los arreglos necesarios para llevar a cabo la visita de evaluación In Situ y prepara la carpeta de trabajo para el equipo auditor.

La evaluación In Situ, tiene como objetivo verificar el cumplimiento de los criterios de acreditación.

La evaluación In Situ se desarrolla en tres fases:

1) **Reunión inicial:** Entre los representantes del Organismo Solicitante y el equipo auditor, durante la cual se harán las presentaciones oportunas, se confirmará el plan de la evaluación y el alcance de la misma y se describirá la dinámica a seguir.
2) **Desarrollo de la evaluación:** En esta fase se procederá a observar el funcionamiento del Organismo Solicitante e investigar el cumplimiento de los requisitos de la acreditación.
3) **Reunión final** del equipo auditor con los representantes del Organismo Solicitante con el objetivo de presentar a los responsables del mismo un resumen verbal de los resultados de la investigación.

En el caso de que el Organismo Solicitante realice su actividad en diversos emplazamientos, la evaluación In Situ se realizará tanto a las oficinas centrales del Organismo Solicitante como en todas aquellas oficinas en las que se realicen actividades clave.

Se considerarán actividades clave las relativas a la formulación de políticas, desarrollo de procedimientos, revisión de contratos, designación de equipos auditores y toma de decisiones.

2.3.3 Informe

Tras la realización de la auditoría se facilita al Organismo Solicitante un informe escrito elaborado por el equipo auditor con los resultados e información recopilada durante la evaluación realizada.

En caso de haber No conformidades, al final del informe de evaluación se indica el periodo de tiempo para la entrega de acciones correctivas con evidencias y/o programas de implementación de acuerdo al tipo de servicio.

Una vez recibido el informe de auditoría, el Organismo Solicitante deberá analizar cada una de las No conformidades identificadas para:

- Evaluar si la No conformidad se repite en otros casos diferentes de los estudiados durante la auditoría.
- Determinar las causas que las han motivado.
- Establecer las acciones correctivas destinadas a evitar su repetición
- Establecer, en su caso, acciones correctivas inmediatas pertinentes.
- Establecer el plazo en el que está previsto que la No conformidad esté resuelta.

El Organismo Solicitante puede alegar aquellas partes del informe con las que no esté de acuerdo.

El Organismo Solicitante deberá enviar al Organismo de Acreditación el resultado del análisis anterior aportando las evidencias que demuestren que los problemas detectados han recibido el tratamiento adecuado para su corrección. Esta información será estudiada por el equipo auditor para determinar si las acciones propuestas y las evidencias presentadas aportan, a su entender, la suficiente confianza en que los problemas detectados han sido adecuadamente resueltos.

2.3.4 Acciones correctivas

Si durante el proceso de evaluación el equipo auditor encuentra No conformidades, el Organismo Solicitante podrá analizarlas y en su caso presentar las Acciones correctivas de forma inmediata, por lo tanto, éstas ya no serán indicadas en el informe.

La Acción correctiva es una acción tomada para corregir y eliminar la causa de una No conformidad detectada u otra situación indeseable.

2.4 Deliberación

En esta etapa se definen las responsabilidades y actividades que permiten al Organismo de Acreditación otorgar, negar, ampliar, actualizar, reducir, suspender o cancelar la acreditación, una vez que el Organismo Solicitante ha concluido el proceso de evaluación.

El Comité de Evaluación es el órgano técnico independiente encargado del estudio, tramitación y concesión de la acreditación, tanto su composición como sus responsabilidades deberán estar establecidas en los estatutos del Organismo de Acreditación.

Para conceder la acreditación, el Comité de Evaluación debe obtener la confianza adecuada en que se cumplen los requisitos de acreditación y en que las desviaciones detectadas en su caso, han sido convenientemente tratadas. Para ello analizará la información generada durante el proceso de evaluación y basándose en ello adoptará una de estas decisiones:

a) Conceder la acreditación, emitiendo el certificado correspondiente.
b) Determinar las actividades de evaluación extraordinarias que sean necesarias para asegurarse de la subsanación de las deficiencias detectadas.
c) Elevar propuesta denegatoria de la concesión al Comité Permanente, notificándolo al Organismo Solicitante.

2.4.1 Alegaciones

En caso de inconformidad con la decisión, el Organismo Solicitante podrá dirigirse al Comité Permanente en un determinado plazo, definido por el Organismo de Acreditación, el cual abarca desde la recepción de la notificación. La inconformidad se hace mediante un escrito redactado por el presidente o representante legal del Organismo Solicitante, en el que se formulan tantas insatisfacciones como dicha entidad considere. El Comité Evaluador emitirá un informe el cual será analizado por el Comité Permanente y éste estará en posición de dar una respuesta.

2.4.2 Certificado de Acreditación

Tras una decisión favorable, el Organismo de Acreditación emitirá un Certificado de Acreditación, que atestigüe la concesión de la acreditación a favor del Organismo Solicitante firmado por el presidente del Organismo de Acreditación.

En dicho certificado se expresarán específicamente los puntos siguientes como mínimo:

- El nombre del Organismo Solicitante y el número de la acreditación concedida.
- Alcance de la acreditación concedida.
- La fecha de entrada en vigor de la acreditación y la vigencia de la misma.

Este documento es propiedad del Organismo de Acreditación y por lo tanto está bajo su control. Por lo que, no podrá ser modificado si no es por el propio Organismo de Acreditación.

2.4.3 Uso de la marca del Organismo de Acreditación

Una vez acreditada, el Organismo Solicitante tiene derecho a hacer uso de la marca del Organismo de Acreditación o referencia a su condición de acreditado en las condiciones establecidas en un documento de referencia propio del Organismo de Acreditación.

Está explícitamente prohibido por dicho documento el uso de la marca o la referencia a la condición de acreditado por parte del Organismo Solicitante mientras la acreditación no se haya concedido o que ésta no se encuentre vigente.

El incumplimiento con lo anterior provocará el cierre del expediente independientemente de la fase en la que se encuentre el proceso de acreditación.

2.5 Mantenimiento de la acreditación

Una vez obtenida la acreditación el Organismo de Acreditación efectuará evaluaciones (auditorías) de seguimiento con el objetivo de verificar que se mantienen las condiciones bajo las cuales se concedió la acreditación y así mantener la vigencia de la misma.

La acreditación de un organismo, concedida con base en el procedimiento de acreditación del Organismo de Acreditación, se considerará vigente siempre y cuando el Organismo Solicitante continúe cumpliendo con los criterios establecidos por el Organismo de Acreditación, por lo que el Organismo de Acreditación define el periodo o requisitos para que una acreditación sea considerada vigente.

Los Organismos acreditados pueden, en cualquier momento, solicitar una suspensión temporal voluntaria de la totalidad o parte del alcance de la acreditación, lo que implica la prohibición temporal de expedir certificados/informes que hagan referencia a la acreditación del Organismo de Acreditación.

Para realizar este trámite el Organismo acreditado debe consultar la documentación o el procedimiento del Organismo de Acreditación.

2.5.1 Evaluaciones de Seguimiento

Se realizarán evaluaciones de seguimiento a los Organismos acreditados por los auditores suficientes de manera periódica. Los objetivos fundamentales de estas evaluaciones de seguimiento son:

- Comprobar que el organismo ha respetado durante el periodo transcurrido los criterios establecidos para la concesión de la acreditación.
- Verificar el cierre de las desviaciones detectadas en evaluaciones previas.
- Examinar cualquier cambio en la organización, procedimientos y recursos del Organismo acreditado para la realización de las actividades incluidas en el alcance de su acreditación.
- Comprobar que se han respetado las obligaciones resultantes de la acreditación.
- Comprobar la actividad del Organismo acreditado para el alcance acreditado.

La frecuencia de las evaluaciones de seguimiento se establecerá en función de los resultados de visitas previas.

La primera evaluación de seguimiento se programará en un plazo establecido por el Organismo de Acreditación y éste no debe ser mayor a doce meses.

Las evaluaciones de seguimiento se pueden hacer a través de una evaluación documental o a través de una evaluación In Situ y el Comité Evaluador determinará lo conducente de acuerdo con la gravedad de la situación que lo genere.

2.5.2 Renovación

Esta etapa consiste en realizar nuevamente el proceso completo de evaluación y acreditación para evaluar las condiciones bajo las cuales se concede la acreditación, al término de su vigencia, con fines de que se vuelva a expedir la acreditación.
Esta renovación se realiza de forma programada por el Organismo de Acreditación, en caso de no requerir la renovación el Organismo Solicitante, a través de su representante autorizado debe notificarlo por escrito al Organismo de Acreditación, el plazo para realizar dicho trámite quedará establecido por el Organismo de Acreditación.

2.6 Ampliación del alcance de la acreditación

Cuando una entidad ya acreditada desea ampliar el alcance de su acreditación, deberá solicitar formalmente dicha ampliación. Para ello deberá utilizarse el formulario de solicitud correspondiente que podrá obtenerse en la página web del Organismo de Acreditación.

La ampliación a la acreditación se puede realizar en los siguientes casos:

a) Ampliación de normas;
b) Ampliación de sectores.

La evaluación para dictaminar la ampliación solicitada podrá realizarse en forma documental y en caso de ser procedente se realizará In Situ.

2.7 Costo total de la acreditación

El costo del proceso de acreditación incluye una tarifa correspondiente a la tramitación y gestión del proceso y el costo correspondiente al número de días de auditor necesarias para llevar a cabo las evaluaciones necesarias que están en función del alcance de acreditación y las características de la entidad.

En algunos Organismos de Acreditación los Organismos acreditados pagan una tarifa anual por el mantenimiento de la acreditación.

Puede consultar las tarifas aplicables a la acreditación en una sección de la página web del Organismo de Acreditación.
Además del costo total de la acreditación, se debe tener en cuenta que es necesario adquirir las normas necesarias para la acreditación, lo que implica un costo adicional.

El costo de las normas al mes de febrero de 2010, se obtuvo de las siguientes páginas:

- http://www.aenor.es/desarrollo/normalizacion/normas/buscadornormas.asp?pag=p
- http://www.iso.org/iso/iso_catalogue.htm

Dichos precios se muestran en la tabla 2.1

Tabla 2.1. Costo de las normas en Aenor e ISO

norma	Descripción	precio	
		ISO[USD]	AENOR[USD]
ISO/IEC 27001:2005	Information technology -- Security techniques -- Information security management systems -- Requirements	120.769	41.836
ISO/IEC 17021:2006	Conformity assessment -- Requirements for bodies providing audit and certification of management systems	104.060	41.836
ISO/IEC 27002:2005 (UNE-ISO/IEC 17799:2002)	Information technology -- Security techniques -- Code of practice for information security management	193.253	77.249
ISO/IEC 27006:2007	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems	126.354	n/a

2.8 Compromisos

Después de que el Organismo Solicitante ha obtenido la acreditación, el Organismo Solicitante tendrá una serie de derechos y obligaciones, las cuales deberán cumplir en todo momento tal y como se establece en los documentos aplicables del Organismo de Acreditación.

Algunos derechos que el Organismo acreditado deberá tener, son:

1) Hacer uso de la marca del Organismo de Acreditación y hacer constar su acreditación en los actos de su vida social, profesional y mercantil.
2) Conocer los informes que se generen con motivo de las auditorías, visitas de acompañamiento o de seguimiento que haya recibido.
3) Solicitar al Organismo de Acreditación la suspensión temporal voluntaria de la acreditación o la retirada de la misma.
4) Formar parte de la asociación del Organismo de Acreditación, si así lo solicita.

En cuanto a las obligaciones que la entidad acreditada deberá tener, se encuentran las siguientes:

1) Cumplir con los criterios de acreditación aplicables en las actividades amparadas por la acreditación.
2) Enviar en tiempo y forma la documentación solicitada por el Organismo de Acreditación para el mantenimiento de la acreditación.
3) Declarar que está acreditado únicamente para los sistemas de certificación y actividades para los que se le ha concedido la acreditación.
4) Fomentar la utilización de los certificados o informes acreditados como medio de aumentar la confianza general en las actividades de certificación, absteniéndose de cualquier actividad que dañe la reputación del Organismo de Acreditación.

5) Mantener en correcto estado de funcionamiento todos los medios que determinaron la concesión de la acreditación y mantener un equipo suficiente de personas debidamente cualificadas
6) Demostrar que realiza anualmente un volumen de certificaciones suficientes para mantener su competencia técnica.
7) Informar del alcance exacto de su acreditación, incluyendo, en su caso, las actividades suspendidas.
8) Cumplir en todo momento con todos los requisitos reglamentarios que la administración haya establecido, en su caso, para desarrollar la actividad para la que esta acreditada.

2.9 Resumen

Para finalizar con el presente capítulo, en la figura 2.5 se ilustran los requisitos previos al proceso de acreditación.

Figura 2.5 Requisitos previos al proceso de acreditación

En la figura 2.6 se muestra la implementación de un SGSI por medio del ciclo continuo PDCA, el cual es uno de los requisitos previos para el proceso de acreditación.

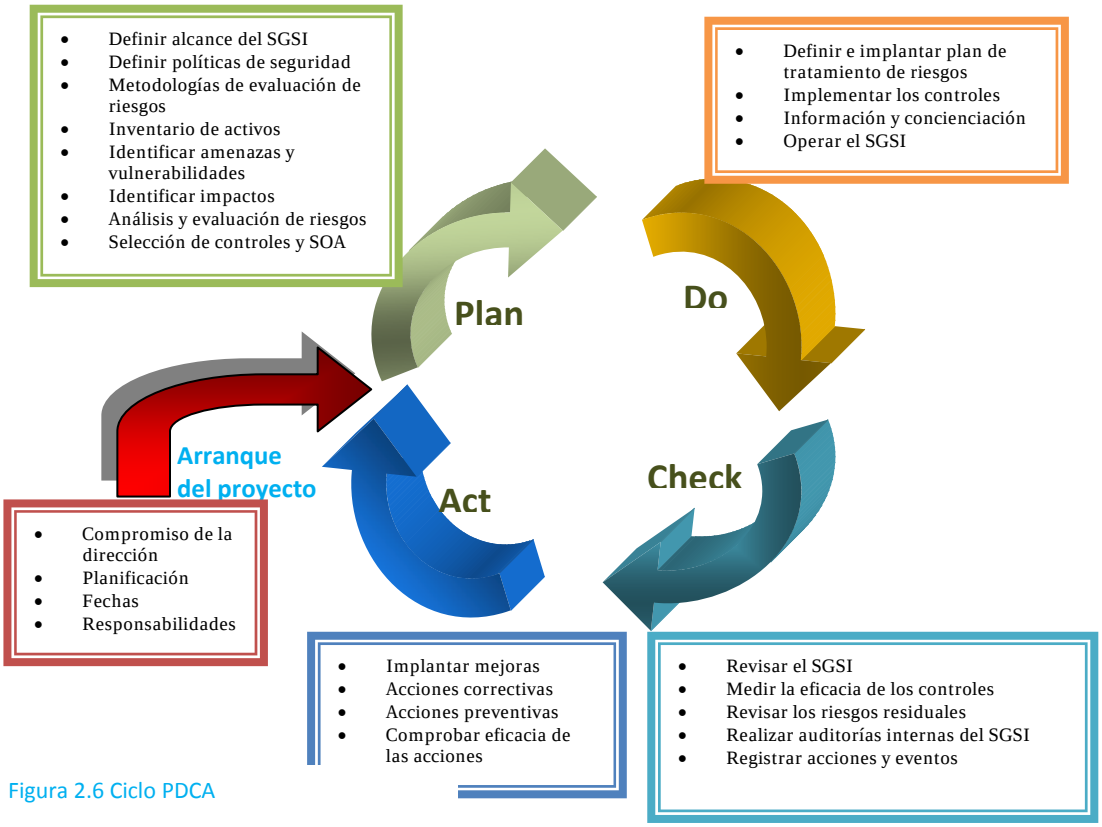


Figura 2.6 Ciclo PDCA

Por último, en la figura 2.7 resumimos el proceso de acreditación mediante el cual un Organismo de Acreditación evalúa los requisitos establecidos en la norma ISO/IEC 27006 donde se pide que el Organismo de Certificación tenga definido un proceso de Certificación, por lo que en el siguiente capítulo se verán de manera general los requisitos para definir dicho proceso.

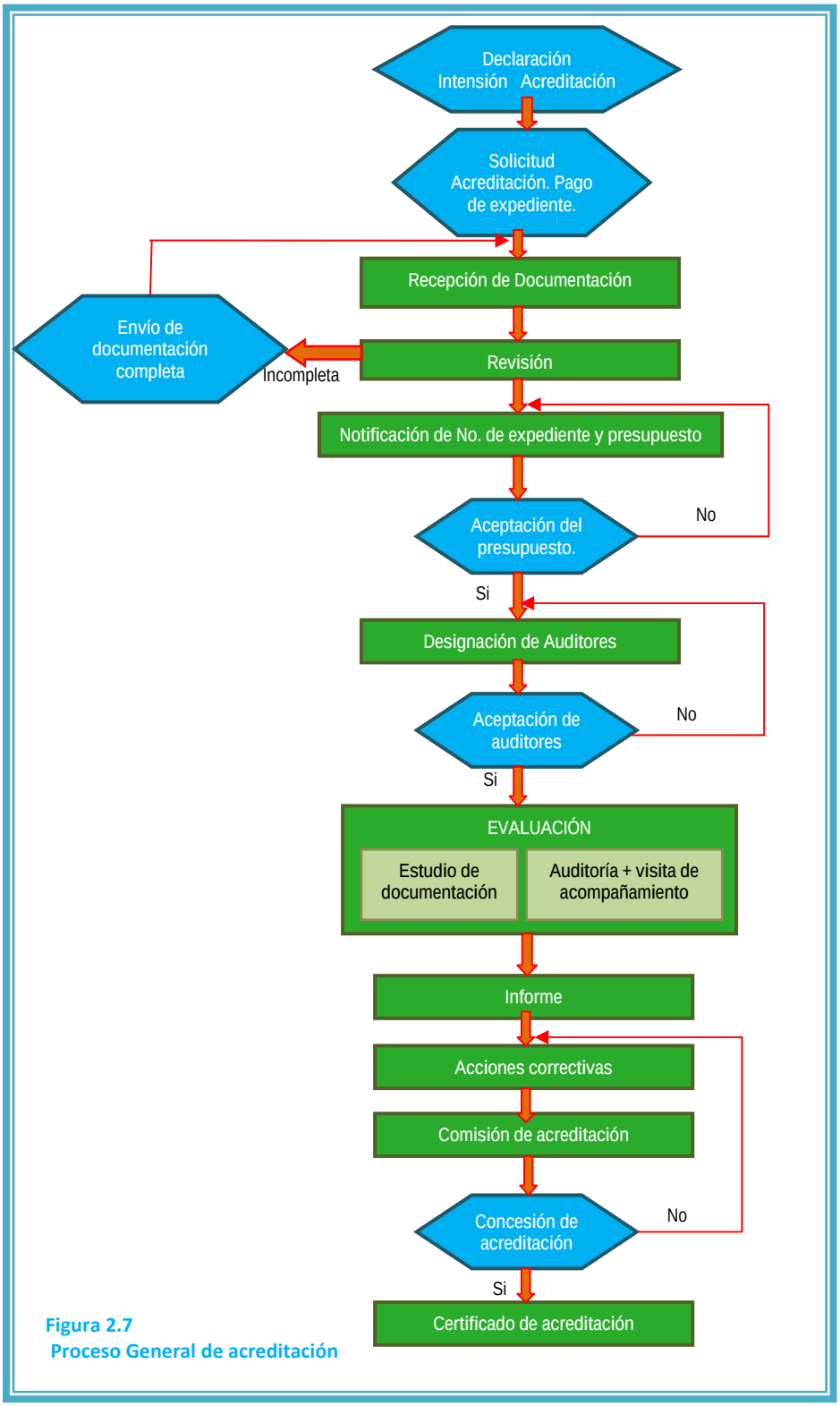


Figura 2.7
Proceso General de acreditación

CAPÍTULO 3

Requisitos para definir el proceso de Certificación

3.1 Requisitos para definir el proceso de Certificación

Un Organismo de Certificación debe definir un Proceso de certificación, mediante el cual certificará o evaluará a las Organizaciones Solicitantes.

Para darnos una idea de cómo definir dicho proceso nos basaremos en las siguientes normas emitidas por International Organization for Standardization (ISO):

1. ISO/IEC 17021:2006 Requisitos generales para los organismos que realizan la auditoría y la certificación de Sistemas de Gestión.
2. ISO/IEC 27006: 2007 Information Technology – Security techniques-requirements for bodies providing audit and certification of information security management systems.

A continuación presentamos una descripción general de estas dos normas:

1. ISO/IEC 17021:2006 Requisitos generales para los organismos que realizan la auditoría y la certificación de Sistemas de Gestión.

ISO ha elaborado esta norma con requisitos internacionalmente aprobados para ayudar a los Organismos de Certificación y auditores que trabajan con las normas de gestión de ISO en su trabajo. La norma ISO/IEC 17021:2006, no sólo le dará una mayor fiabilidad y confianza al trabajo de quienes evalúan y certifican sino que también contribuirá a difundir esta buena práctica.

Esta norma tiene como objetivo atender a la importancia de formalizar y armonizar los procesos de acreditación abordando tres cuestiones importantes: la imparcialidad, la competencia y el proceso, además de que, esta norma es aplicable a cualquier Sistema de Gestión.

La norma ISO/IEC 17021 incorpora los últimos adelantos tecnológicos. Como ejemplo, esta norma incluye disposiciones para la certificación y evaluación tanto de organizaciones "virtuales" como aquellas que no poseen una casa central y aquellas que brindan servicios online (a través de internet).

ISO/IEC 17021 es la primera norma elaborada acerca de la evaluación de la conformidad que incluye una sección entera sobre "principios". Esta sección resume los objetivos que la certificación debería reunir para conseguir y fomentar la confianza en el mercado sobre los Sistemas de Gestión de las organizaciones. Imparcialidad, competencia, responsabilidad, confidencialidad e interés en resolver las quejas son algunos de los principios. Estos no son requisitos per se, pero se proporcionan especificaciones en esta norma.

La norma incluye 13 requisitos específicos para asegurar que el Organismo de Certificación y sus auditores estén libres de conflictos de interés. También incorpora conceptos de la guía IAF (Internacional Acreditation Forum) respecto de las competencias de los Organismos de Certificación con particular énfasis en los integrantes del equipo auditor. Los requisitos proporcionan un proceso para asegurar que el equipo auditor asignado posea una adecuada competencia para cada cliente específico.

Para reducir alguno de los aspectos negativos de la competencia comercial entre los Organismos de Certificación, la norma "normaliza" el Proceso de certificación y las auditorías para que incluya:

- una auditoría de dos etapas para la certificación inicial;
- un ciclo de certificación de tres años que comienza con la decisión de la certificación o re-certificación y que tiene una fecha de vencimiento inequívoca;
- examinar auditorías en los primeros y segundos años del ciclo de tres años; y
- una auditoría previa al vencimiento para la re-certificación durante el tercer año.

2. ***ISO/IEC 27006: 2007 Information Technology – Security techniques-requirements for bodies providing audit and certification of information security management systems.***

Esta norma define los requisitos exigibles a los Organismos de Certificación de SGSI, y por tanto regula el Proceso de Acreditación. Además, esta norma también servirá para aclarar en cierta medida los términos en los que se debe interpretar la norma ISO/IEC 27001 desde el punto de vista de la auditoría.

Para empezar a desarrollar el Proceso de Certificación es necesario tomar en cuenta los siguientes puntos contenidos en la norma ISO/IEC 27006:2007, la cual está enfocada a los SGSI, sin embargo, es importante aclarar que dicha norma hace referencia a la norma ISO/IEC 17021, por lo que es recomendable que se cuente con ella.

Dentro de la norma nos encontraremos con la palabra “deberá (Shall)” la cual indica que es un requisito y por lo tanto es obligatorio. También encontraremos la palabra "podrá (should)" que se utiliza para indicar las disposiciones que, a pesar de que constituyen una guía para la aplicación de los requisitos, se espera que sean adoptados por el Organismo de Certificación.

3.2 Proceso de Certificación

A continuación describiremos los requisitos y procesos necesarios para llevar a cabo una correcta evaluación a las Organizaciones Solicitantes para obtener una certificación bajo la norma ISO/IEC 27001. Por lo que, el siguiente contenido es una interpretación nuestra de la norma ISO/IEC 27006:2007.

Términos y definiciones

Para los fines de esta interpretación son de aplicación las definiciones siguientes:

Acciones correctivas: Acciones para eliminar una no conformidad detectada.
Acciones preventivas: Medida orientada a prevenir no conformidades.
Acreditación: Es el proceso por medio del cual se evalúa a un Organismo de Certificación para comprobar que cumplen con los requisitos de una norma.
Alcance: Es la delimitación de lo que será auditado.
Amenaza: Causa potencial de un incidente no deseado, el cual puede causar daño a un sistema o a la organización.
Análisis de riesgos: Utilización sistemática de la información disponible para identificar peligros y estimar los riegos.

Análisis de significado: Analizar y determinar que tan significativa es una vulnerabilidad o amenaza.
Auditor: Persona que realiza actividades de auditoría.
Auditor externo: Auditor que no pertenece a l Organismo de Certificación.
Auditor Interno: Auditor que pertenece al Organismo de Certificación.
Auditoría: Es el proceso realizado por un auditor para evaluar y recabar evidencias objetivas (requisitos de una norma) de un Sistema de Gestión.
Auditoría de seguimiento: Auditoría realizada para verificar el funcionamiento del SGSI en caso de algún cambio o de re-certificación.
Auditoría externa: Auditoría realizada por un auditor externo al organismo a evaluar para recabar evidencias objetivas conforme a una norma.
Auditoría interna: Auditoría realizada por un auditor que pertenece al organismo a evaluar para recabar evidencias objetivas conforme a una norma.
Certificación: Es la confirmación de que un Organismo ha cumplido con los requisitos establecidos en una norma.
Competencia: Es el conjunto de atributos que posee una persona u organización que le permiten desarrollarse en un determinado ámbito.
Conformidad: Cumplimiento de un requisito de la norma.
Controles: Medidas de seguridad orientadas a mitigar los riesgos encontrados en el análisis de riesgos.
Criterio: Es una condición o regla que permite realizar una elección, lo que implica que sobre un criterio se pueda basar una decisión o un juicio de valor.
Evaluación de la conformidad: Es la verificación de los cumplimientos de los requisitos de una norma.
Evaluación de riesgo: Es una evaluación de las vulnerabilidades que puedan existir en el SGSI y de su probable ocurrencia.
Incidente: Un único o una serie de eventos inesperados o no deseados con probabilidad significativa de comprometer las operaciones de la organización.
Legislación: Conjunto de leyes que regulan una determinada materia.
No conformidad: incumplimiento de un requisito de la norma.
Norma: Documento técnico y legal que contiene especificaciones técnicas de aplicación voluntaria que están basadas en los resultados de la experiencia y desarrollo tecnológico.
Normalizar: Hacer que una cosa se ajuste a una norma, regla o a un modelo común.
Organismo de Certificación: Organismo que realiza actividades de certificación bajo la norma ISO/IEC 27001.
Organización Solicitante: Es aquella empresa que solicita una Certificación.
Política: Son las guías elaboradas para llegar a un fin específico.
Políticas de Seguridad: Es un documento que contiene las directrices que debe seguir la seguridad de la información, la respuesta a incidentes y la definición y asignación de responsabilidades.
Principios: Reglas de conducta que una Organización debe seguir.
Procedimientos: Son los documentos claramente definidos y desarrollados para cumplir con los objetivos marcados por las políticas.
Proceso: Es un conjunto de actividades que se realizan o suceden con un fin determinado.
Registros: Evidencia objetiva sobre los cumplimientos de los requisitos de una norma, además, estos incluyen métricas e indicadores de seguridad.
Regular: Medir y controlar algo.
Requisito: Condición de carácter obligatorio en una norma.

Riesgos: Es la posibilidad de que una amenaza cause perdida o daño en la información y su entorno.
Vulnerabilidad: Debilidad de la seguridad de la información de un organismo y que potencialmente permite que una amenaza afecte un activo.

3.2.1 Requisitos Generales

3.2.1.1 Conflictos de Intereses

Los Organismos de Certificación pueden llevar a cabo las siguientes funciones sin que se les considere como consultoría o que tengan un conflicto potencial de intereses:

a) La certificación, incluyendo reuniones de información, reuniones de planificación, la revisión de documentos, la auditoría (no auditorías internas del SGSI o revisiones internas de la seguridad) y seguimiento de las No conformidades.
b) Organizar y participar como conferencista en cursos de formación, siempre y cuando estos cursos se refieran a la gestión de la Seguridad de la Información, relacionados con los Sistemas de Gestión o auditoría, los Organismos de Certificación deben limitarse a proveer información genérica y asesoramiento de libre acceso al dominio público, es decir, el Organismo de Certificación no debe proporcionar a la Organización Solicitante asesoramiento específico que vaya en contra de los requisitos del inciso c.
c) Poner a disposición o solicitar información sobre la publicación que describe el Organismo de Certificación de la interpretación de los requisitos de la certificación de normas de auditoría.
d) Actividades antes de la auditoría, cuyo único fin sean determinar la preparación para la auditoría de certificación, sin embargo, estas actividades no deben resultar en la prestación de recomendaciones o asesoramiento que puedan afectar a la presente cláusula y el Organismo de Certificación debe ser capaz de confirmar que esas actividades no contravengan estos requisitos y que no se utilicen para justificar una reducción de la eventual duración de la auditoría de certificación.
e) La realización de la segunda y la tercera parte de las auditorías de acuerdo con las normas u otros reglamentos que no sean parte del alcance de la Acreditación.
f) Valor añadido durante las auditorías de certificación y las visitas de seguimiento, por ejemplo, mediante la identificación de oportunidades de mejora, que sean evidentes durante la auditoría, sin recomendar las posibles soluciones específicas.

El Organismo de Certificación deberá ser independiente del Organismo u Organismos (incluidas las personas) que proporcionen auditorías internas del SGSI de la Organización Solicitante sujeta a la certificación del SGSI.

3.2.2 Requisitos relativos a los recursos

Los elementos esenciales de competencia requeridos para llevar a cabo la certificación del SGSI son para seleccionar, proveer y administrar las personas cuyos conocimientos y competencia colectiva son adecuadas a las actividades que se van a auditar y relacionadas con las cuestiones de la Seguridad de la Información.

3.2.2.1 Análisis de Competencia y Revisión de Contrato

El Organismo de Certificación deberá asegurarse que tiene el conocimiento de los avances tecnológicos y jurídicos pertinentes con el SGSI de la Organización Solicitante, que evalúa.

El Organismo de Certificación deberá tener un sistema efectivo para el análisis de la competencia en cuanto a la Gestión de la Seguridad de la Información que necesite tener disponible con respecto a todas las áreas técnicas en las que se opera.

Para cada cliente, el Organismo de Certificación deberá ser capaz de demostrar que ha llevado a cabo un análisis de competencia (evaluación de las habilidades en respuesta a las necesidades evaluadas) de los requerimientos de cada sector pertinente antes de empezar la revisión del contrato. El Organismo de Certificación deberá revisar el contrato con la Organización Solicitante, basados en los resultados de este análisis de competencia. En particular, el Organismo de Certificación deberá ser capaz de demostrar que tiene la competencia para realizar las siguientes actividades:

a) Entender las áreas de actividad de la Organización Solicitante, así como los riesgos asociados al mismo.
b) Definir las competencias necesarias en el Organismo de Certificación para certificar en relación con las actividades identificadas, y la Seguridad de la Información relacionada con las amenazas a los activos, vulnerabilidades e impactos en la organización del cliente.
c) Confirmar la disponibilidad de la competencia requerida.

Recursos

La Dirección del Organismo de Certificación deberá contar con los procesos y los recursos que le permitan determinar si los auditores individuales son o no competentes para las tareas que requieran llevar a cabo dentro del alcance de la certificación en la que operan. La competencia de los auditores puede ser establecida verificando sus antecedentes y experiencias específicas de formación o de información. El Organismo de Certificación deberá ser capaz de comunicarse eficazmente con todos sus clientes, a quienes presta sus servicios.

3.2.2.2 Personal que interviene en las actividades del Proceso de certificación

Competencia del personal del Organismo de Certificación.

El Organismo de Certificación deberán contar con el personal competente para:

a) Seleccionar y verificar la competencia de los auditores del SGSI para los equipos apropiados de auditorías.
b) Informar y dar la capacitación necesaria a los auditores del SGSI.
c) Decidir sobre la concesión, el seguimiento, el retiro, la suspensión, la ampliación o reducción de las certificaciones.
d) Definir, crear y operar un proceso de apelaciones y quejas.

Capacitación de los equipos auditores:

El Organismo de Certificación deberá disponer de criterios para la formación de los equipos auditores que garanticen:

a) El conocimiento de la norma referente a los SGSI y otros documentos normativos.
b) La comprensión de la Seguridad de la Información.
c) La comprensión de la evaluación de riesgos y la gestión de éstos desde la perspectiva empresarial.
d) Los conocimientos técnicos de la actividad que será auditada.
e) Los conocimientos generales de los requisitos reglamentarios pertinentes para el SGSI.
f) El conocimiento de los Sistemas de Gestión.
g) La comprensión de los principios de auditoría basados en ISO 19011.
h) Conocimiento de la eficacia del SGSI, por medio de la revisión y medición de la eficacia del control.

La capacitación deberá ser para todos los miembros del equipo auditor, con excepción del inciso d), que puede ser compartida entre los miembros del equipo auditor.

Cuando el Organismo de Certificación seleccione un equipo auditor para una determinada auditoría de certificación, deberá asegurarse que las habilidades para cada misión son las apropiadas. Para ello el equipo auditor deberá:

a) Tener los conocimientos técnicos apropiados de las actividades específicas dentro del alcance del SGSI para el cual se busca la certificación y, en su caso, con los procedimientos asociados y sus posibles riesgos para la Seguridad de la Información (expertos técnicos que no son auditores pueden cumplir esta función).
b) Tener un grado suficiente de comprensión de la Organización Solicitante para llevar a cabo una auditoría de certificación confiable de su SGSI en la gestión de la Seguridad de la Información, los aspectos de sus actividades, productos y servicios.
c) Tener conocimientos apropiados de los requisitos reglamentarios aplicables al SGSI de la Organización Solicitante.

Cuando sea requerido, el equipo auditor puede ser complementado por expertos técnicos quienes pueden demostrar su competencia específica en un campo de la tecnología adecuada para la auditoría. Cabe señalar que los expertos técnicos no pueden reemplazar a los auditores del SGSI, pero pueden asesorar a los auditores sobre la adecuación técnica en el contexto del sistema de gestión sometido a la auditoría. El Organismo de Certificación deberá tener un procedimiento para:

a) Seleccionar auditores y expertos técnicos con base a su competencia, capacitación, habilidades y experiencia.
b) Inicialmente, evaluar la conducta de los auditores y expertos técnicos durante las auditorías de certificación y, subsecuentemente supervisar el desempeño de los auditores y expertos técnicos.

Gestión del proceso de la toma de decisiones:

La Dirección de la Organización de certificación deberá poseer la competencia técnica y capacidad de administrar los procesos de la toma de decisiones referentes a la concesión, seguimiento, ampliación, reducción, suspensión y retiro de la certificación de acuerdo a los requerimientos de la norma ISO/IEC 27001.

Prerrequisitos en cuanto al nivel de educación, experiencia laboral, capacitación como auditor y experiencias en auditorías para los auditores que llevan a cabo la realización de auditorías de SGSI.

Los siguientes criterios deben ser aplicados a cada auditor del equipo auditor del SGSI, por lo que el auditor deberá:

a) Tener una educación de nivel secundaria.
b) Tener por lo menos cuatro años de experiencia laboral en prácticas de tecnología de la información, de los cuales al menos dos años haya tenido un puesto relacionado con la Seguridad de la Información.
c) Haber completado con éxito cinco días de formación, cuyo ámbito de aplicación abarca las auditorías del SGSI y las auditorías de gestión que se consideren apropiadas.
d) Haber adquirido experiencia en todo el proceso de evaluación de la Seguridad de la Información antes de asumir la responsabilidad de desempeñarse como un auditor. Esta experiencia debería de haberse adquirido por la participación en mínimo cuatro auditorías de certificación por un total de al menos 20 días, incluyendo la revisión de la documentación y el análisis de riesgo, evaluación de la implementación e informes de la auditoría.
e) Tener experiencia razonablemente actualizada.
f) Ser capaz de explicar operaciones complejas desde una perspectiva amplia para comprender el papel de las unidades individuales en las grandes Organizaciones Solicitantes.

Los técnicos expertos deberán cumplir con los criterios a), b), e) y f).

Además de los requisitos anteriores, el auditor líder del equipo auditor deberá cumplir con los siguientes requisitos, los cuales deberán ser demostrados al orientar y supervisar una auditoría:

a) Tener los conocimientos y atributos para dirigir el proceso de auditoría de certificación.
b) Haber sido un auditor por lo menos en tres auditorías de SGSI completas.
c) Haber demostrado una capacidad efectiva de comunicación, tanto oral como escrita.

3.2.2.3 El uso de auditores externos o expertos técnicos externos como parte del equipo auditor

Cuando se hace uso de auditores externos o expertos técnicos externos como parte del equipo auditor, el Organismo de Certificación debe asegurarse que son competentes y que cumplen con las especificaciones aplicables de la norma ISO/IEC 27006:2007 y que no están involucrados, ya sea directamente o a través de su empleador con el diseño, implementación o seguimiento de un SGSI

o de gestión relacionado con el(los) sistema(s) de tal manera que la imparcialidad podría verse comprometida.

Uso de expertos técnicos

Los expertos técnicos con conocimientos específicos sobre el proceso y cuestiones de la Seguridad de la Información, así como de legislaciones que afecten a la Organización Solicitante, pero que no cumplen con todos los criterios de "Personal que interviene en las actividades del Proceso de certificación", pueden ser parte del equipo auditor. Los expertos técnicos deberán trabajar bajo la supervisión de un auditor.

3.2.3 Requisitos relativos a la información

3.2.3.1 Información Pública Accesible

Procedimientos para conceder, mantener, extender, reducir, suspender y retirar la certificación.

El Organismo de Certificación deberá documentar los procedimientos para:

a) La auditoría inicial de certificación del SGSI de la Organización Solicitante en acuerdo con las disposiciones de la norma ISO 19011, ISO / IEC 17021 y otros documentos pertinentes.
b) Auditorías de seguimiento y de re-certificación del SGSI de la Organización Solicitante de acuerdo con las normas ISO/IEC 19011 e ISO/IEC 17021 en forma periódica para seguir la conformidad de los requisitos pertinentes, así como para verificar y registrar que la Organización Solicitante tomó acciones correctivas a tiempo para corregir todas las no conformidades.

3.2.3.2 Documentos de la certificación del SGSI

El Organismo de Certificación deberá proporcionar a cada una de las Organizaciones Solicitantes que estén certificadas, un documento de certificación el cual puede ser una carta o un certificado firmado por un funcionario que ha sido asignado para esta responsabilidad. Para la Organización Solicitante y para cada uno de sus sistemas de información cubiertos por la certificación, este documento deberá identificar el alcance de la certificación concedida y la norma ISO/IEC 27001 para la cual el SGSI es certificado. Además, el Certificado deberá incluir una referencia específica de la versión de la Declaración de Aplicabilidad (SOA, por sus siglas en inglés Statement Of Applicability).

3.2.3.3 Control de las marcas de certificación

El Organismo de Certificación deberá ejercer un control adecuado sobre la propiedad, uso y exhibición de sus marcas de certificación SGSI. Si el Organismo de Certificación otorga el derecho a usar una marca para identificar la certificación de un SGSI, el Organismo de Certificación deberá asegurarse que la Organización Solicitante usa solo la marca especificada, autorizada y escrita por el Organismo de Certificación. El Organismo de Certificación no deberá permitir el uso de su marca en un producto de la Organización Solicitante, de manera que pueda interpretarse como indicación de conformidad del producto.

3.2.3.4 Confidencialidad

3.2.3.4.1 Acceso a los registros de la Organización Solicitante

Antes de la auditoría de certificación, el Organismo de Certificación deberá preguntar a la Organización Solicitante si algunos de sus registros del SGSI no pueden ser puestos a disposición para su revisión por el equipo auditor, ya que contienen información confidencial o susceptible.

El Organismo de Certificación deberá determinar si el SGSI puede ser auditado adecuadamente en la ausencia de estos registros. Si el Organismo de Certificación llega a la conclusión de que esto no es posible para una auditoría adecuada del SGSI sin la revisión de los registros identificados como confidenciales o susceptibles, el Organismo de Certificación deberá notificar a la Organización Solicitante que la auditoría de certificación no podrá tener lugar hasta que los acuerdos de acceso a los registros sean apropiados.

3.2.4 Requisitos relativos a los procesos

3.2.4.1 Requisitos generales de una auditoría del SGSI

Criterios de la auditoría de certificación

Los criterios, contra los cuales el SGSI de la Organización Solicitante, son auditados deberán estar indicados en la norma ISO/IEC 27001 y otros documentos requeridos para la certificación pertinente a la función que desempeñan.

Si se requiere una explicación en cuanto a la aplicación de estos documentos a un programa específico de certificación, en ese momento la explicación se hará por medio de un comité imparcial o por personas que tengan la competencia técnica necesaria, y será publicado por el Organismo de Certificación.

Políticas y procedimientos

La documentación del Organismo de Certificación deberá incluir la política y procedimientos para implementar el Proceso de certificación, incluyendo controles de uso y aplicación de documentos usados en la certificación de los SGSI´s y los procedimientos de auditoría y certificación del SGSI de la Organización Solicitante.

Equipo Auditor

El equipo auditor deberá ser nombrado oficialmente y provisto con los documentos de trabajo apropiados. El plan para las fechas de auditoría deberá ser acordado con la Organización Solicitante. El mandato otorgado al equipo auditor deberá estar claramente definido y dado a conocer a la Organización Solicitante, y deberá ser necesario que el equipo auditor examine la estructura, política y procedimientos de la Organización Solicitante, y confirmar que cumpla con todos los requisitos pertinentes o relevantes para el alcance de la certificación y que los procedimientos estén implementados y sean confiables en el SGSI de la Organización Solicitante.

3.2.4.1.1 Alcance de la certificación

El equipo auditor sólo deberá auditar el SGSI de la Organización Solicitante de acuerdo al alcance definido dentro de los requisitos aplicables a la certificación. El Organismo de Certificación deberá asegurar que el alcance y los límites del SGSI de la Organización Solicitante están claramente definidos en función a las características de la empresa, su organización, su ubicación, sus activos y su tecnología. El Organismo de Certificación deberá confirmar, en el alcance de su SGSI, que la Organización Solicitante entrega los requisitos establecidos en la cláusula 1.2 de la norma ISO/IEC 27001:2005.

El Organismo de Certificación deberá asegurarse de que la evaluación de riesgos de la Seguridad de la Información y el tratamiento de riesgos de la Organización Solicitante refleja adecuadamente sus actividades y se extiende a los límites de sus actividades, tal como se define en la norma ISO/IEC 27001 del SGSI. El Organismo de Certificación deberá confirmar que esto se refleje en el alcance del SGSI y el Statement of Applicability (SOA) de la Organización Solicitante.

El Organismo de Certificación deberá asegurarse que las interfaces con servicios o actividades que no están incluidos en el alcance del SGSI se abordan en el SGSI sujeto a la certificación y se incluyen en la evaluación de riesgos de Seguridad de la Información de la Organización Solicitante.

3.2.4.1.2 Tiempo de la auditoría

El Organismo de Certificación deberá asignar el tiempo suficiente a los auditores para llevar a cabo todas las actividades relativas a una auditoría inicial, auditoría de seguimiento o auditoría de re-certificación. El tiempo asignado se puede basar en factores tales como:

a) El tamaño del alcance del SGSI (por ejemplo, el número de sistemas de información usado, el número de empleados).
b) La complejidad del SGSI (ejemplo: sistemas de información crítico, situaciones de riesgo del SGSI).
c) El(los) tipo(s) de negocios realizados en el alcance del SGSI.
d) La amplitud y diversidad de la tecnología utilizada en la implementación de varios de los componentes del SGSI (tales como los controles implementados, documentación y/o control de procesos, acciones correctivas/preventivas).
e) El número de sitios.
f) El desempeño del SGSI demostrado previamente.
g) El alcance de la subcontratación (outsourcing) y acuerdos de terceras partes utilizadas dentro del alcance del SGSI.
h) Las normas y reglamentos que se aplican a la certificación.

El anexo C de la norma ISO/IEC 27006 provee una guía sobre el tiempo de la auditoría. El Organismo de Certificación deberá estar preparado para fundamentar o justificar la cantidad de tiempo empleado en cualquier auditoría inicial, auditoría de seguimiento y auditoría de re-certificación.

3.2.4.1.3 Sitios Múltiples

Las decisiones sobre muestras de sitios múltiples en el área de certificación del SGSI son más complejas que las decisiones para un Sistema de Gestión de Calidad. Cuando una Organización Solicitante tiene un número de sitios que reúnan los criterios de a) a c), el Organismo de Certificación puede considerar que se utilice una muestra basada en un enfoque de sitios múltiples de la auditoría de certificación:

Puede considerar la utilización de una muestra-base enfocada a la auditoría de certificación de sitios múltiples, sí:

a) Todos los sitios están operando bajo el mismo SGSI, los cuales son administrados centralmente y auditados y sujetos a evaluaciones de la gestión central.
b) Todos los sitios están incluidos dentro del programa de auditoría interna del SGSI de la Organización Solicitante.
c) Todos los sitios están incluidos dentro del programa de revisión de la gestión del SGSI de la Organización Solicitante.

El Organismo de Certificación que desee usar un enfoque basado en muestras deberá tener procedimientos que aseguren lo siguiente.

a) Que la revisión del contrato inicial identifique, en la mayor medida de lo posible, la diferencia entre los sitios de tal manera que un nivel de toma de muestras adecuado sea determinado.
b) Que un número representativo de sitios han sido muestreados por el Organismo de Certificación tomando en cuenta:

    1. El resultado de las auditorías internas de la oficina principal y de los sitios,
    2. El resultado de la revisión de la gestión,
    3. Variaciones en el tamaño de los sitios,
    4. Variaciones en los propósitos de los sitios del negocio,
    5. Complejidad de SGSI,
    6. Complejidad del Sistema de Información en los diferentes sitios,
    7. Variación en las prácticas de trabajo,
    8. Variación en las actividades emprendidas,
    9. Interacción potencial con los Sistemas de Información Críticos o Sistemas de Información que procesan información susceptible,
    10. Cualquier requisito legal diferente.

c) Que una muestra representativa es seleccionada de todos los sitios dentro del alcance del SGSI de la Organización Solicitante; esta selección puede estar basada en un juicio selectivo que refleje los factores presentados en el inciso anterior b), además de un elemento aleatorio.
d) Que cada sitio incluido en el SGSI que está sujeto a riesgos importantes es auditado por el Organismo de Certificación previo a la certificación.

e) Que el programa de seguimiento ha sido diseñado en función de los requisitos anteriores y abarca todos los sitios de la Organización Solicitante o dentro del alcance de certificación del SGSI dentro de un plazo razonable.
f) En el caso de que se haya observado una no conformidad, ya sea en la oficina central o en uno de los sitios de la Organización Solicitante, el procedimiento de acción correctiva se aplicará a la oficina central y en todos los sitios cubiertos por el Certificado.

La auditoría descrita a continuación deberá estar dirigida a las actividades de la oficina central de la Organización Solicitante para asegurarse que solo un SGSI es aplicado a todos los sitios y proporciona una Gestión en el Nivel operacional. En la auditoría se abordarán todos los problemas antes mencionados.

3.2.4.1.4 Metodología de una auditoría

El Organismo de Certificación deberá contar con procedimientos, que requiera la Organización Solicitante para poder demostrar que las auditorías internas del SGSI son programadas, y el programa y procedimientos están funcionando y puede demostrarse que son operativos.

Los procedimientos del Organismo de Certificación no pueden suponer una manera particular de la implementación de un SGSI o un formato particular para la documentación y los registros. Los procedimientos de certificación deberán enfocarse en que el SGSI de la Organización Solicitante cumple con los requisitos de la norma ISO/IEC 27001, así como con las políticas y objetivos de la Organización Solicitante.

El plan de auditoría puede establecer asistencia técnica de auditoría por red (“Network-assisted”), la cual puede ser utilizada durante la auditoría, según corresponda.

NOTA: La asistencia técnica de auditoría por red “Network-assisted” puede incluir, por ejemplo, teleconferencias, reuniones web, comunicación interactiva basada en web y acceso electrónico remoto a la documentación del SGSI y/o los procesos del SGSI. El propósito de estas técnicas puede ser mejorar la eficiencia y eficacia de la auditoría, y puede respaldar la integridad del Proceso de la auditoría.

3.2.4.1.5 Informe de la auditoría de la certificación

El Organismo de Certificación podrá adoptar procedimientos de presentación de informes que se adapten a sus necesidades, pero, como mínimo, estos procedimientos deberán asegurarse de que:

a) Se lleva a cabo una reunión entre el equipo de auditores y la dirección de la Organización Solicitante antes de salir de las oficinas de la Organización Solicitante, en dicha reunión el equipo auditor proporcionará:
    1. Una indicación oral o escrita en relación con la conformidad del SGSI de la Organización Solicitante con respecto a los requisitos particulares de la certificación.
    2. Una oportunidad para la Organización Solicitante, para hacer preguntas acerca de las conclusiones y sus bases.

b) El equipo auditor proporciona al Organismo de Certificación un informe de sus conclusiones sobre la conformidad del SGSI de la Organización Solicitante con todos los requisitos de certificación.

El informe de auditoría puede proporcionar la siguiente información:

a) Un reporte de la auditoría incluyendo un resumen de los documentos revisados.
b) Un reporte de la auditoría de certificación del análisis de riesgo de la seguridad de la Información de la Organización Solicitante.
c) El tiempo total empleado en la auditoría y una especificación detallada del tiempo dedicado a la revisión documental, la evaluación del análisis de riesgos, la auditoría in-situ y el reporte de la auditoría.
d) Las investigaciones de auditoría que se han seguido, los fundamentos para su selección y la metodología empleada.

El informe de auditoría de los resultados proporcionado al Organismo de Certificación deberá ser lo suficientemente detallado como para facilitar y apoyar una decisión de certificación y deberá contener:

a) Áreas abarcadas por la auditoría (por ejemplo, los requerimientos de certificación y los sitios que fueron auditados), incluyendo los caminos importantes de auditoría seguidos y las metodologías de auditoría empleadas.
b) Observaciones, tanto positivas (por ejemplo, las características notables) como negativas (por ejemplo, no conformidades potenciales).
c) Detalles de cualquier no conformidad identificada respaldados por evidencia objetiva y una referencia de estas no conformidades de los requisitos de la norma ISO/IEC 27001 u otros documentos requeridos para la certificación.
d) Comentarios sobre las conformidades del SGSI de la Organización Solicitante con los requisitos de certificación con, una declaración de las no conformidades, una referencia de la versión de la Declaración de Aplicabilidad (SOA) y, en su caso, cualquier comparación útil con los resultados de auditorías de certificación previas de la Organización Solicitante.

Cuestionarios, lista de verificación (Check list), observaciones, registros o notas del auditor, podrían formar una parte integral del informe de auditoría. Si estos métodos son usados, estos documentos deberán ser entregados al Organismo de Certificación como evidencia para respaldar la decisión de certificación. La información acerca de las muestras evaluadas durante la auditoría puede estar incluida en el informe de auditoría, o en otro documento de certificación.

El informe deberá considerar si la organización interna es la apropiada y los procedimientos del SGSI adoptados por la organización Solicitante son confiables.

Además de los requisitos para el informe bajo la norma ISO/IEC 17021:2006, el informe podrá abarcar:

- El grado de dependencia que puede ser puesto en las auditorías internas del SGSI y evaluaciones de la dirección.

- Un resumen de las observaciones más importantes, tanto positivas como negativas con respecto a la implementación y eficacia del SGSI.
- Las recomendaciones del equipo auditor en cuanto a si el SGSI de la Organización Solicitante puede ser Certificado o no, con la información que justifique esta recomendación.

3.2.4.2 Auditoría inicial y Certificación

3.2.4.2.1 Competencia del equipo auditor

Los siguientes requisitos se aplican a la evaluación de certificación, además de los requisitos que se enumeran en "El personal involucrado en las actividades de certificación". Para las actividades de seguimiento solo los requisitos que son apropiados para la aplicación de la actividad de seguimiento programada.

Se aplicaran los siguientes requisitos al equipo auditor en su conjunto.

a) En cada una de las siguientes áreas, al menos un miembro del equipo auditor debe satisfacer los criterios de la Organización de certificación para asumir responsabilidades dentro del equipo, como son:

    1. Dirección del equipo.
    2. Sistemas de Gestión y procesos aplicables al SGSI.
    3. Conocimiento de los reglamentos y requisitos legales en el campo de la Seguridad de la Información.
    4. Identificación de las amenazas relacionadas con la Seguridad de la Información y los incidentes.
    5. Identificación de las vulnerabilidades de la Organización Solicitante y la comprensión de la probabilidad de su explotación, su impacto, su mitigación y control.
    6. Conocimiento de los controles del SGSI y su implementación.
    7. Conocimientos de los análisis eficaces del SGSI y medición de los controles.
    8. Estándares relacionados y/o pertinentes del SGSI, mejores prácticas de la industria, políticas de seguridad y procedimientos.
    9. Conocimiento de métodos del manejo de incidentes y continuidad del negocio.
    10. Conocimiento acerca de los bienes activos de información, tangibles e intangibles y análisis de impacto.
    11. Conocimiento de la tecnología actual donde la seguridad podría estar relacionada o ser un tema.
    12. Conocimiento de procesos de gestión de riesgos y métodos.

b) El equipo auditor deberá ser competente para rastrear indicios de incidentes de seguridad del SGSI de la Organización Solicitante y restablecer los elementos apropiados del SGSI.
c) El equipo auditor deberá tener la experiencia necesaria y práctica para aplicar los puntos anteriores (esto no significa que un auditor necesita un mayor rango de experiencia en todas las áreas de la Seguridad de la Información, pero el equipo auditor en su conjunto

podrá tener suficiente crítica y experiencia para cubrir el alcance del SGSI objeto de la auditoría).

Un equipo auditor puede consistir de una sola persona, siempre y cuando ésta cumpla con los criterios vistos en el inciso anterior a).

Demostración de la competencia del auditor

Los auditores deben ser capaces de demostrar su conocimiento y experiencia, como se ha señalado anteriormente, por ejemplo, a través de:

a) Calificaciones reconocidas específicamente del SGSI.
b) Certificación como auditor.
c) Cursos aprobados de formación en SGSI.
d) Registros de desarrollo profesional hasta la fecha.
e) Demostración práctica a través de auditores testigos que han realizado Procesos de auditoría de sistemas de SGSI de Organizaciones Solicitantes reales.

3.2.4.2.2 Preparación General para la auditoría inicial

El Organismo de Certificación deberá exigir que la Organización Solicitante haga todo los arreglos necesarios para la realización de la auditoría de certificación, incluyendo la disposición para el estudio documental y acceso a todas las áreas, registros (incluyendo reportes de auditoría internas y reportes de evaluaciones independientes de la Seguridad de la Información) y personal para los propósitos de la auditoría de certificación, re-certificación y resolución de quejas.

Al menos la siguiente información debe ser proporcionada por la Organización Solicitante antes de llevar a cabo la auditoría de certificación In situ:

a) Información general con respecto al SGSI y las actividades que cubre.
b) Una copia de la documentación del SGSI requerida en la norma ISO/IEC 27001:2005, cláusula 4.3.1 y, cuando sea requerido, la documentación asociada.

3.2.4.2.3 Auditoría Inicial de certificación

Etapa 1 de la auditoría

En esta etapa de la auditoría, el Organismo de Certificación deberá obtener la documentación sobre el diseño del SGSI que abarca la documentación exigida en la cláusula 4.3.1 de la norma ISO/IEC 27001.
El objetivo de la etapa 1 de la auditoría es proporcionar un enfoque para la planificación de la etapa 2 de la auditoría para tener un mejor conocimiento del SGSI en el contexto de la política y objetivos del SGSI de la Organización Solicitante, y, en particular, el estado de preparación de la Organización Solicitante para la auditoría.

La etapa 1 de la auditoría incluye, pero no puede estar limitado a, la revisión de los documentos. El Organismo de Certificación deberá estar de acuerdo con la Organización Solicitante sobre cuándo

y dónde se llevará a cabo la revisión de los documentos. En todos los casos la revisión de los documentos deberá estar completa antes de comenzar con la etapa 2 de la auditoría.

Los resultados de la etapa 1 de la auditoría deberán ser documentados en un informe escrito. El Organismo de Certificación deberá revisar el informe de la etapa 1 de la auditoría antes de decidir continuar con la etapa 2 de la auditoría y para seleccionar a los miembros del equipo auditor con la competencia necesaria.

El Organismo de Certificación hará que la Organización Solicitante este al corriente de los tipos de información y registros adicionales que pueden ser requeridos para una revisión detallada durante la etapa 2 de la auditoría.

Etapa 2 de la auditoría.

La Etapa 2 de la auditoría siempre se llevará a cabo en las oficinas de la Organización Solicitante. Sobre la base de los resultados documentados en el informe de la etapa 1 de la auditoría, el Organismo de Certificación hará un borrador de un plan de auditoría para la realización de la Etapa 2 de la auditoría. Los objetivos de la Etapa 2 de la auditoría son:

a) Confirmar que la Organización Solicitante cumple con su propia política, objetivos y procedimientos.
b) Confirmar que el SGSI se ajusta a todos los requisitos de la norma ISO/IEC 27001 y es el logro de los objetivos de la política de la Organización Solicitante.

Para ello, la auditoría deberá centrarse en los siguientes puntos concernientes a la Organización Solicitante:

a) La evaluación de los riegos relacionados con la Seguridad de la Información, y que las evaluaciones presenten resultados comparables y reproducibles.
b) Los requisitos de documentación listados en la Cláusula 4.3.1 de la norma ISO/IEC 27001:2005.
c) La selección de controles objetivos y controles basados en la evaluación de riesgos y los procesos de tratamiento de riegos.
d) Revisión de la eficacia del SGSI y medida de la efectividad de los controles de la Seguridad de la Información, informando y revisando contra los objetivos del SGSI.
e) Auditorías Internas del SGSI y revisiones de la dirección.
f) Responsabilidad de la dirección para la información de la política de Seguridad
g) Correspondencia entre los controles seleccionados e implementados, el Statement of Applicability (SOA) y los resultados de la evaluación de riesgos y los procesos de tratamiento de riesgos, y la política y objetivos del SGSI.
h) La implementación de los controles, tomando en cuenta las medidas de eficacia de los controles de la Organización Solicitante, para determinar si los controles son implementados y efectivos para alcanzar los objetivos fijados.
i) Los programas, procesos, procedimientos, registros, auditorías internas y revisiones de la eficacia del SGSI para asegurar que éstos se representan en las decisiones de la dirección y en la política del SGSI y en los objetivos.

Elementos específicos de la auditoría del SGSI

El papel del Organismo de Certificación es establecer que la Organización Solicitante sea consistente en el establecimiento y seguimiento de los procedimientos para la identificación, revisión y evaluación de la Seguridad de la Información relacionada con las amenazas a los activos, vulnerabilidades e impactos sobre la Organización Solicitante. El Organismo de Certificación deberá:

a) Pedir a la Organización Solicitante que demuestre que los análisis de seguridad relacionados con las amenazas son relevantes y adecuados para la operación de la Organización Solicitante.

Nota: La Organización Solicitante es la responsable de definir los criterios por los cuales los riesgos relacionados con la Seguridad de la Información de la Organización Solicitante se identifican como importantes, y para desarrollar el (los) procedimiento(s) para hacer esto.

b) Establecer si los procedimientos de la Organización Solicitante para la identificación, revisión y evaluación de las amenazas a los activos relacionadas con la Seguridad de la Información, vulnerabilidades e impactos y los resultados de sus aplicaciones son consistentes con la política de la Organización Solicitante, objetivos y metas.

El Organismo de Certificación deberá establecer también si los procedimientos empleados en el análisis de significado son acertados y apropiadamente implementados. Si una de las amenazas a los activos relacionadas con la Seguridad de la Información, una vulnerabilidad, o un impacto sobre la Organización Solicitante es identificada como significativa, ésta deberá ser manejada dentro del SGSI.

Cumplimiento legal y reglamentario

El seguimiento y evaluación del cumplimiento legal y reglamentario es responsabilidad de la Organización Solicitante. El Organismo de Certificación deberá limitarse a los controles y muestras a fin de establecer la confianza de las funciones del SGSI en este sentido. El Organismo de Certificación deberá verificar que la Organización Solicitante tiene un Sistema de Gestión para lograr el cumplimiento legal y reglamentario aplicable a los riesgos e impactos de la Seguridad de la Información.

Integración de la documentación del SGSI con otros Sistemas de Gestión

La Organización Solicitante puede combinar la documentación para el SGSI y otros Sistemas de Gestión (tales como la Calidad, la Seguridad y la Salud, y el Medio Ambiente) mientras que el SGSI puede ser claramente identificado conjuntamente con las interfaces adecuadas a los demás sistemas.

Combinar auditorías de Sistemas de Gestión

Un Organismo de Certificación puede ofrecer certificación de otros Sistemas de Gestión ligados con la certificación de SGSI, o puede ofrecer solamente certificación de SGSI.

La auditoría del SGSI puede ser combinada con auditorías de otros Sistemas de Gestión. Esta combinación es posible siempre que pueda demostrarse que la auditoría satisface todos los requisitos para la certificación de SGSI. Todos los elementos importantes para un SGSI deberán aparecer claramente, y ser fácilmente identificables, en los informes de la auditoría. La calidad de la auditoría no deberá de verse negativamente afectada por la combinación de las auditorías.

Nota: La norma ISO/IEC 19011 proporciona una guía para llevar a cabo la combinación de auditorías de diferentes Sistemas de Gestión.

Información para la Concesión Inicial de certificación

Con el fin de proporcionar una base para la decisión de la certificación, el Organismo de Certificación deberá exigir informes claros, que proporcionen información suficiente para tomar esta decisión.

Los informes del equipo auditor para el Organismo de Certificación serán requeridos en varias etapas del Proceso de la auditoría de la certificación. En combinación con la información que se tiene en el expediente, estos informes podrían contener, al menos, la información requerida en el "Informe de auditoría de certificación"

Fallo de la certificación

El Organismo, el cual puede ser un individuo, puede tomar decisiones sobre la concesión o retiro de una certificación dentro del Organismo de Certificación, puede incorporar un nivel de conocimiento y experiencia en todas las áreas, lo cual es suficiente para evaluar el Proceso de auditoría y las recomendaciones formuladas por el equipo auditor.
La decisión de certificar o no el SGSI de la Organización Solicitante deberá ser tomada por el Organismo de Certificación en base a la información reunida durante el Proceso de certificación y alguna otra información relevante. Quiénes tomen la decisión de la certificación no deberán participar en la auditoría. Esta decisión deberá estar basada en las conclusiones y recomendaciones de certificación del equipo auditor, según lo previsto en su informe de auditoría de certificación y cualquier otra información relevante disponible para el Organismo de Certificación.

El Organismo de Certificación que toma la decisión sobre la concesión de la certificación no podrá anular una observación negativa del equipo auditor. Si se presenta esta situación, el Organismo de Certificación deberá documentar y justificar los fundamentos de la decisión de anular la observación.

Sobre el tema de decisión sobre la certificación, la norma ISO/IEC 17021 no menciona un tiempo específico en el cual una auditoría interna del SGSI completa y un examen de la Administración del SGSI de la Organización Solicitante deberá llevarse a cabo. El Organismo de Certificación podrá determinar dicho periodo. Independientemente de que si el Organismo de Certificación ha definido un tiempo mínimo, las medidas deberán ser establecidas por el Organismo de Certificación para asegurar la eficacia de la evaluación de la gestión de la Organización Solicitante y los Procesos de la auditoría interna.

La certificación no deberá ser concedida a la Organización Solicitante hasta que haya suficientes pruebas para demostrar que los arreglos para las evaluaciones de la gestión y las auditorías internas del SGSI han sido aplicadas, son eficaces y se mantendrán.

3.2.4.3 Actividades de Seguimiento

Auditorías de Seguimiento

Los procedimientos de la auditoría de seguimiento deberán ser consistentes con las relativas a la auditoría de certificación del SGSI de la Organización Solicitante tal y como se describe en la norma ISO/IEC 27006.

El objetivo del seguimiento consiste en verificar que el SGSI aprobado se sigue aplicando, para examinar las implicaciones de los cambios del sistema iniciados como resultado por los cambios del funcionamiento de la Organización Solicitante y para confirmar que se sigan cumpliendo los requisitos de certificación. El programa de seguimiento podría cubrir normalmente:

a) Los elementos de seguimiento del sistema los cuales son auditorías internas del SGSI, revisión de la gestión y acciones preventivas y correctivas.
b) Comunicaciones con las partes externas como lo exige la norma ISO/IEC 27001 y otros documentos requeridos para la certificación.
c) Cambios en la documentación del SGSI.
d) Áreas sujetas a cambios.
e) Elementos seleccionados de la norma ISO/IEC 27001.
f) Otras áreas seleccionadas según el caso.

Como mínimo, el seguimiento por parte del Organismo de Certificación debe revisar:

a) La eficacia del SGSI con respecto al cumplimiento de los objetivos de las políticas de Seguridad de la información de la Organización Solicitante.
b) El funcionamiento de los procedimientos para el periodo de evaluación y revisión de los cumplimientos con la legislación y los reglamentos en materia de la Seguridad de la Información pertinentes.
c) Medidas tomadas sobre las no conformidades identificadas durante las últimas auditorías.

El seguimiento por parte del Organismo de Certificación puede cubrir al menos los puntos necesarios para la auditoría de seguimiento de la norma ISO/IEC 17021. Además, pueden ser considerados los siguientes aspectos:

a) El Organismo de Certificación debería ser capaz de adaptar su programa de seguimiento a los riesgos de activos relacionados con las cuestiones de Seguridad de la Información, vulnerabilidades e impactos sobre la Organización Solicitante y justificar este programa de seguimiento.
b) El programa de seguimiento del Organismo de Certificación debería ser determinado por el mismo Organismo de Certificación. Las fechas específicas para las visitas pueden ser de acuerdo con la Organización Solicitante Certificado.

c) Las auditorías de seguimiento pueden ser combinadas con auditorías de otro Sistema de Gestión. El informe deberá indicar claramente los aspectos pertinentes de cada sistema de gestión.
d) El Organismo de Certificación será requerido para supervisar el uso apropiado del Certificado.

Durante las auditorías de seguimiento, el Organismo de Certificación deberá checar los registros de apelación y quejas presentadas ante el Organismo de Certificación y, en caso de encontrar alguna no conformidad o incumplimiento con los requisitos de certificación, se pone de manifiesto, que la Organización Solicitante ha investigado su SGSI, sus procedimientos y que ha tomado acciones correctivas apropiadas.

Un informe de seguimiento deberá contener, particularmente, información aclaratoria de las no conformidades manifestadas previamente. Como mínimo, los informes derivados del seguimiento podrán crearse para cubrir en su totalidad los requerimientos del inciso anterior a).

3.2.4.4 Re-Certificación

Auditorías de re-certificación

Los procedimientos de auditorías de re-certificación deberán ser consistentes con las auditorías concernientes a la auditoría de certificación del SGSI de la Organización Solicitante, tal y como se describe en la norma internacional ISO/IEC 27006.

El Organismo de Certificación deberá tener procedimientos claros en los que se establezcan las condiciones y circunstancias en las cuales la certificación se mantendrá. Si en la auditoría de seguimiento o re-certificación, se comprobó la existencia de no conformidades, tales no conformidades deberán ser corregidas efectivamente dentro de un plazo de tiempo acordado por el Organismo de Certificación. Si la corrección no es hecha durante el tiempo acordado, el alcance de la certificación deberá reducirse, o retirar o suspender el certificado retirado. El plazo de tiempo acordado para implementar las acciones correctivas deberá ser coherente con la gravedad de la no conformidad y los riesgos para la seguridad de los productos o servicios de la Organización Solicitante especificados en la junta de requisitos.

3.2.4.5 Auditorías Especiales

Casos Especiales

Las actividades de seguimiento deberán estar sujetas para la disposición especial en caso de que una Organización Solicitante certificada en SGSI haga grandes modificaciones a su sistema o en caso de llevar a cabo otros cambios que podría afectar la base de su certificación.

3.2.4.6 Quejas

Las quejas representan una fuente de información, en cuanto a, posibles no conformidades. El Organismo de Certificación podrá pedir a la Organización Solicitante Certificada que, en virtud de una queja, la Organización Solicitante Certificada podrá establecer, y en su caso, un reporte sobre

la causa de la queja, incluyendo cualquier factor pre determinante(o pre disponente) dentro del SGSI de la Organización Solicitante.

El Organismo de Certificación podrá cerciorarse de que la Organización Solicitante está usando tales investigaciones para desarrollar correcciones/acciones correctivas, las cuáles pueden incluir medidas para:

a) Notificar a las autoridades apropiadas si es requerido por el reglamento.
b) Restaurar la conformidad.
c) Prevenir recurrencias.
d) Evaluar y mitigar cualquier incidente de Seguridad adverso y sus impactos asociados.
e) Asegurar la interacción satisfactoria con otros componentes del SGSI.
f) Evaluar la eficacia de las medidas correctivas adoptadas.

El Organismo de Certificación deberá exigir a cada Organización Solicitante cuyo SGSI esté Certificado, poner a disposición del Organismo de Certificación, cuando sea requerido, los registros de todas la quejas y acciones correctivas tomadas de acuerdo con los requisitos de la norma ISO/IEC 27001.

3.3 Resumen

Para finalizar, ilustraremos el proceso general de certificación mediante la figura 3.1 que se muestra a continuación.

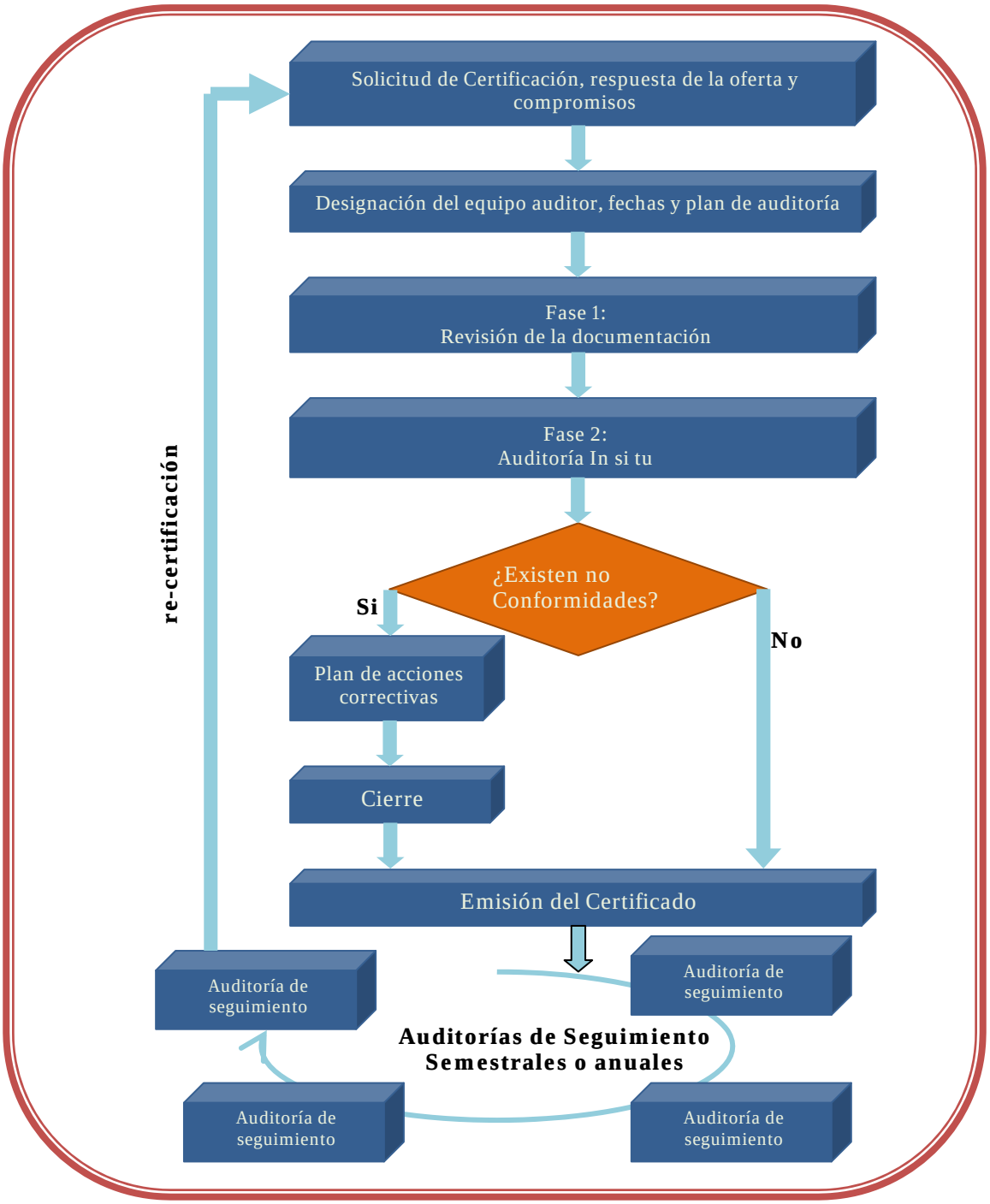


Figura 3.1. Proceso general de certificación

CAPÍTULO 4

Evaluación de la Facultad de Ingeniería

4.1 Facultad de Ingeniería

La Facultad de Ingeniería (Figura 4.1), con base a la información emitida oficialmente a través de su página web: “http://www.ingenieria.unam.mx”, forma parte del conjunto de facultades de la Universidad Nacional Autónoma de México y está ubicada frente a la alberca olímpica. Cuenta además con un conjunto anexo localizado en la parte sur (División de Ciencias Básicas y Posgrado).

Figura 4.1 Facultad de Ingeniería

La sede central de la Facultad de Ingeniería (Conjunto Norte, ver fig. 4.2) se ubica en el Circuito Escolar en Ciudad Universitaria. El conjunto original de la Facultad consta de tres edificios. En el primero se agrupan las áreas de teoría, los talleres, patio de maniobras, laboratorios, bodegas, salas de profesores y los servicios generales. En el segundo, aulas, laboratorios, patio de pruebas, el Auditorio “Javier Barros Sierra”, además de la dirección, sala de juntas, sala de profesores, la Biblioteca "Antonio Dovalí Jaime" y áreas de uso administrativo. El tercero se encuentra provisto de equipo de cómputo y maquinaria de perforación, además de disponer de tres laboratorios en los que se imparte la especialización de Ingeniería Petrolera.

Fuente: http://www.ingenieria.unam.mx/paginas/mapasFacultad.htm

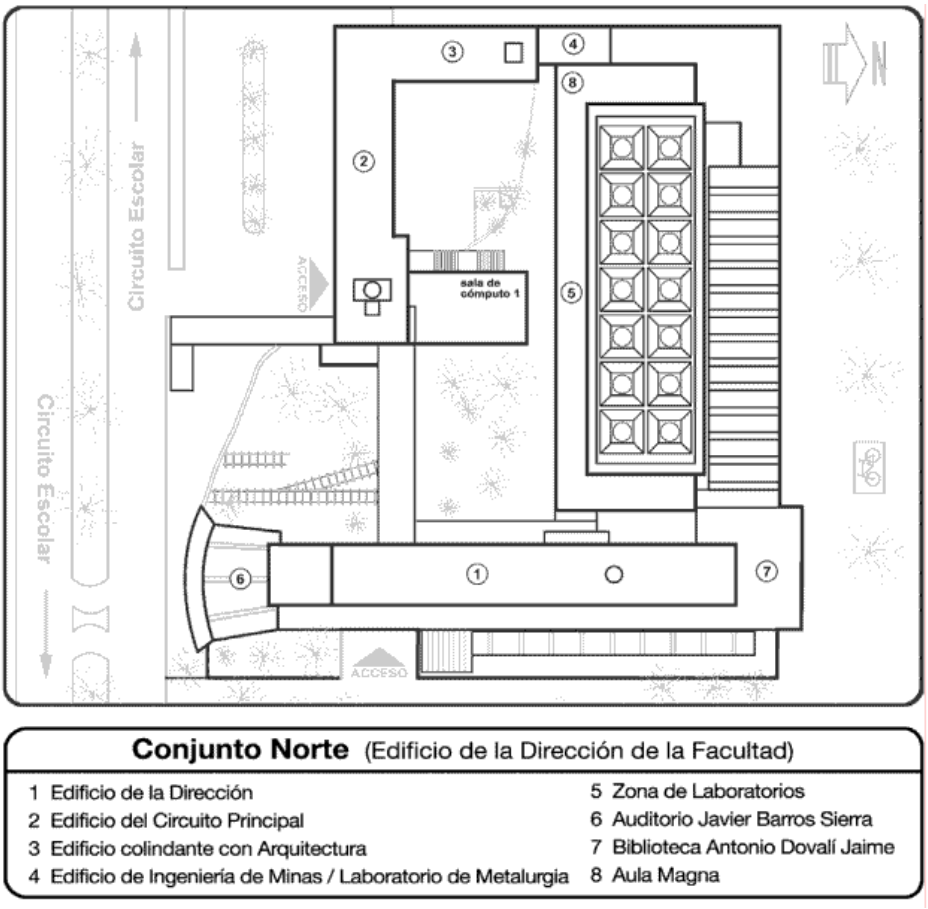


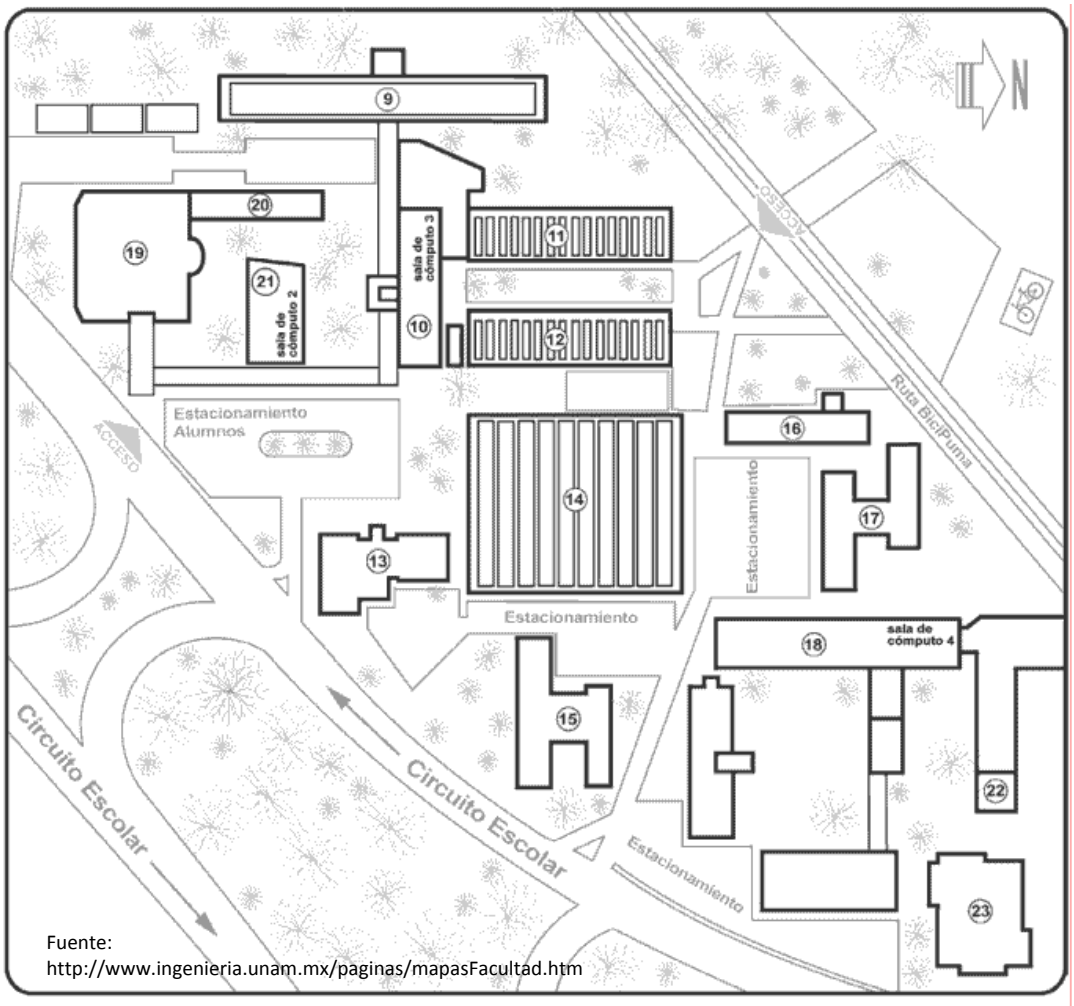
Figura 4.2 Ubicación de los edificios de la Facultad de Ingeniería conjunto Norte

Al sur de las instalaciones deportivas de la UNAM se encuentra el conjunto sur de la Facultad de Ingeniería, en el cual se localiza:

La División de Ciencias Básicas, compuesta por el Auditorio "Sotero Prieto", las salas de cómputo (2 y 3) para uso exclusivo de alumnos, los laboratorios de ciencias básicas, la Torre de Ciencias básicas utilizada como salones de clases, el Ala poniente que se utiliza como talleres de dibujo y la Biblioteca "Maestro Enrique Rivero Borrell", equipada con salas audiovisuales, de lectura, una videoteca y acceso a Internet inalámbrico a través de la RIU (Red Inalámbrica Universitaria)

La División de Ingeniería Mecánica e Industrial compuesta por el edificio "Alberto Camacho Sánchez" donde se imparten los talleres y laboratorios de Ingeniería Mecánica en donde se hacen prácticas de tratamientos térmicos, pruebas estáticas y dinámicas, afilado, rectificación y prensado.

La División de Ingeniería Eléctrica compuesta por el edificio "Luis G. Valdés Vallejo" donde están los laboratorios de Ingenierías en Computación, de Ingeniería Eléctrica Electrónica y de Ingeniería en Telecomunicaciones.



Fuente:
http://www.ingenieria.unam.mx/paginas/mapasFacultad.htm

Conjunto Sur (División de Ciencias Básicas y Posgrado)

9 Ala poniente de Ciencias Básicas
10 Torre de Ciencias Básicas
11 Laboratorios de Ciencias Básicas
12 Laboratorios de Ciencias Básicas
13 Laboratorio de Termofluidos
14 Laboratorios y Talleres de Ingeniería Mecánica Alberto Camacho Sánchez
15 División de Ingenierías Civil y Geomática
16 Divisiones de Ingeniería Mecánica e Industrial y de Ingeniería Eléctrica
17 Edificio Luis G. Valdés Vallejo
18 Edificio Bernardo Quintana Arrioja
19 Biblioteca Enrique Rivero Borrell
20 Centro de Docencia Ing. Gilberto Borja Navarrete
21 Auditorio Sotero Prieto
22 Auditorio Raúl J. Marsal
23 Biblioteca Dr. Enzo Levi

Figura 4.3 Ubicación de los edificios de la Facultad de Ingeniería conjunto Sur

La Secretaría de Posgrado e Investigación, integrada por el edificio "Bernardo Quintana Arrioja", la Biblioteca "Dr. Enzo Levi" y el auditorio "Raúl J. Marsal".

La División de Ingeniería Civil y Geomática.
Cuenta con 8 laboratorios de cómputo para distintos propósitos, laboratorio de materiales, gabinete de topografía, entre otros.

En este mismo conjunto sur de la Facultad, entre 1996 y 1998 se construyeron los laboratorios de Telecomunicaciones, de Termofluidos y el nuevo edificio de posgrado.

El antiguo Palacio de Minería es sede de la División de Educación Continua y de la Sociedad de Ex Alumnos de la Facultad de Ingeniería, así como del Museo Tolsá. El Real Seminario de Minas, aloja el Museo de los Minerales. Ambos edificios se ubican en el Centro Histórico de la Ciudad de México.

En Jiutepec, Morelos, se encuentra el inmueble de la Sección de Hidráulica de Posgrado.

En Juriquilla, Querétaro, se encuentra la Unidad de Desarrollo Tecnológico Querétaro (UDETEC), la cual está enfocad al desarrollo de tecnología y a la vinculación industrial como medio efectivo para formar profesionales de alto nivel.

Por otra parte, es importante mencionar que la totalidad de los laboratorios de la Facultad cuentan con el equipamiento necesario para impartir con calidad las prácticas curriculares correspondientes y realizar con éxito diversas actividades de investigación. Destacan la Estación Satelital ubicada en los Laboratorios de Telecomunicaciones y el equipo para análisis geofísico Stratagem a cargo de la División de Ingeniería en Ciencias de la Tierra.

Las perspectivas de la Facultad respecto a infraestructura, de cara al nuevo milenio, se encuentran plasmadas en el Plan de Desarrollo de la Facultad de Ingeniería 2007-20011, en el cual se establecen diversas estrategias y acciones tendientes a dar cabal cumplimiento a la misión de la institución.

La Facultad de Ingeniería tiene como misión y visión:

MISIÓN:

> *"Formar de manera integral recursos humanos en Ingeniería, realizar investigación acorde con las necesidades de la sociedad, y difundir ampliamente la cultura nacional y universal.*
> *Esta conjunción de elementos debe aportar a la sociedad ingenieros competitivos, nacional e internacionalmente, con habilidades, actitudes y valores que les permitan un desempeño pleno en el ejercicio profesional, la investigación y la docencia; con capacidad para actualizar continuamente sus conocimientos y poseedores de una marcada formación humanista que les dé sentido a sus actos y sus compromisos con la Universidad y con México."*

VISIÓN:

> *"La Facultad de Ingeniería ha sido y deberá ser la institución líder en la formación de profesionales en ingeniería del país; semillero fundamental donde se generan nuevos conocimientos al realizar investigación que impacte en el óptimo desarrollo nacional,*

con aportaciones a la cultura y al desarrollo de capacidades con sentido humanista, social y ecológico; por ello, sus profesionales deberán estar permanentemente actualizados gracias a la sólida oferta brindada a través de una educación continua y a distancia."

Además cuenta con las siguientes políticas y valores:

Políticas:

- **Liderazgo de la academia:** Revalorar la docencia y la vida colegiada, como los ejes principales que orientan el desarrollo de las actividades en la entidad académica.
- **Proactividad estudiantil:** Desarrollar una actitud inquisitiva, reflexiva y crítica como uno de los pilares principales en su formación personal, con repercusiones en el ejercicio profesional.
- **Calidad:** Satisfacer de manera natural las necesidades y expectativas de la comunidad, a través del óptimo desempeño en cada uno de los procesos encaminados al cumplimiento pleno de las funciones sustantivas de la Universidad.
- **Simplificación:** Facilitar los apoyos que merece la comunidad para dedicarle la mayor atención a las labores sustantivas de la entidad.
- **Seguridad:** Garantizar la integridad física de la comunidad, sus pertenencias y las de la Institución, así como a los sistemas de toda naturaleza.
- **Orden y limpieza:** Impulsar una tradición de la Facultad, que merece ser honrada con acciones en todos los ámbitos.
- **Transparencia:** Elevar, interna y externamente, los niveles de confianza al trabajar individualmente y en equipo. Necesidad y demanda justa en las actividades que se desarrollan en la Facultad.
- **Laboriosidad:** Incrementar la probabilidad de éxito en cualquier tarea que se emprenda mediante el talento y trabajo minucioso de la comunidad.

Valores:

- **Identidad:** Como consecuencia del orgullo que le genera su pasado histórico y su sentido de pertenencia a la Universidad Nacional Autónoma de México, la Facultad de Ingeniería tiene un arraigo profundo en el ser nacional, convirtiéndola en una institución fundamental para la sociedad, ya que está en posibilidad de aportar a la nación el recurso humano con los elementos técnicos y científicos necesarios para su transformación y desarrollo.
- **Pluralidad:** La Facultad, como parte indisociable de la Universidad, congrega en su seno a distintas voces, visiones y maneras de pensar enmarcadas en la dinámica continua de encontrar el camino más propicio, para ser tomadas en cuenta y apreciadas, siempre en el ámbito del respeto mutuo, y de la posibilidad de lograr una realimentación valiosa que será el punto de partida para la construcción del diálogo que hace vislumbrar el horizonte de un entendimiento más allá de las diferencias.
- **Equidad:** Es fundamental aceptar las diferencias que suelen suscitarse en las instituciones y llegar al entendimiento de que los individuos se configuran a partir de sus diferencias, y a través del reconocimiento de las mismas se da una relación armónica y justa en el núcleo de cualquier concentración humana.

- **Ética profesional:** Cobra especial relevancia la capacidad para tomar conciencia de ser persona con ética suficiente para actuar de una manera estable y honrada al servicio de los demás, y en beneficio propio a impulsos de la propia vocación y con la dignidad que corresponde al ser humano. Condición necesaria de cultivar entre los miembros de la Facultad.
- **Responsabilidad social:** Es imprescindible fomentar en las nuevas generaciones, a través de una formación integral, la conciencia social para darle sentido y valor a su actividad profesional, y favorecer su pleno desarrollo humano al permitirle aportar su capacidad y experiencia en favor de los sectores más necesitados. Es vital que el espíritu universitario se vea fortalecido, y que se preserven los ideales más elevados como consecuencia lógica de haber recibido una sólida formación en las aulas del pensamiento universitario.
- **Honestidad:** Todos los integrantes de la comunidad de la Facultad se deben comprometer a conducir sus acciones en el marco de la honestidad académica y administrativa; de tal modo, que sea una entidad modelo de rectitud en todos los niveles y ámbitos de competencia institucional y nacional sin excepciones.

La información académica y administrativa de la Facultad de Ingeniería se encuentra administrada por la Unidad de Servicios de Cómputo Administrativos, por tal motivo es importante mencionarla.

Unidad de Servicios de Cómputo Administrativos (USECAD)

Su objetivo publicado oficialmente en su página web http://servacad.fia.unam.mx/usecad/_info/, es proporcionar los servicios de cómputo, en forma eficiente y oportuna, para mejorar la vida académica de la Facultad.

Objetivos Específicos:

- Desarrollar los sistemas de cómputo que soporten las actividades académico-administrativas que generan los órganos de la Facultad.
- Mejorar la calidad de servicio a los usuarios.
- Garantizar la operación normal de los equipos de cómputo de la Secretaría de Servicios Académicos.
- Contar con sistemas de información flexibles en su operación y de fácil mantenimiento.
- Contar con personal capacitado en áreas de cómputo.
- Diseñar e incorporar nuevos productos y servicios que permitan el cumplimiento de los objetivos planteados.
- Crear la infraestructura para que la comunidad de la Facultad tenga acceso a la información que requiera.

Y los principales servicios que presta son:

- Procesamiento
- Captura de información
- Soporte Técnico
- Capacitación
- Diseño y desarrollo de sistemas
- Consultoría

Los principales procesos están enfocados a las actividades de administración escolar como son las reinscripciones y registro a exámenes extraordinarios.
La organización de USECAD contempla una coordinación y tres departamentos:

- Coordinación
- Desarrollo de Sistemas
- Soporte Técnico
- Producción

La Facultad de Ingeniería cuenta con siete divisiones, a través de las cuales se imparten 12 carreras organizadas como se muestra en la figura 4.4.

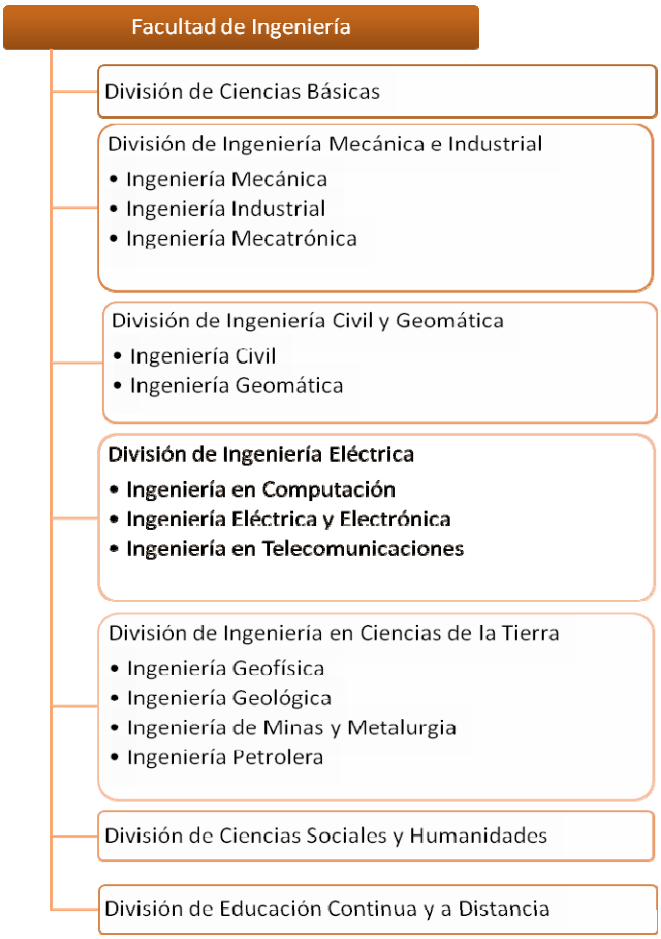


Figura 4.4 Organización de las divisiones de la Facultad de Ingeniería

División de Ingeniería Eléctrica

La División de Ingeniería Eléctrica de la Facultad de Ingeniería de la UNAM, con base en la información publicada en su página web “http://www.fi-b.unam.mx/”, tiene como misión y visión:

MISIÓN:

"Formar de manera integral recursos humanos con estricto rigor académico en ingeniería y tecnología, en los niveles de Licenciatura, Maestría y Doctorado. Proporcionando a los egresados conocimientos y una educación de alto nivel académico para poder realizar docencia, investigación de vanguardia y difusión de la cultura; todas comprometidas con las necesidades del país y en particular con los sectores industrial, empresarial y gubernamental."

VISIÓN:

"La División de Ingeniería Eléctrica de la Facultad de Ingeniería de la UNAM, es un centro de enseñanza superior público, que realiza actividades de docencia e investigación, agrupadas en siete Departamentos Académicos de Ingeniería (fig. 4.5)*: Computación, Control, Eléctrica, Electrónica, Procesamiento de Señales, Sistemas Energéticos y Telecomunicaciones. A través de estos Departamentos se persigue un liderazgo sostenido y acrecentado tanto a nivel nacional como internacional."*

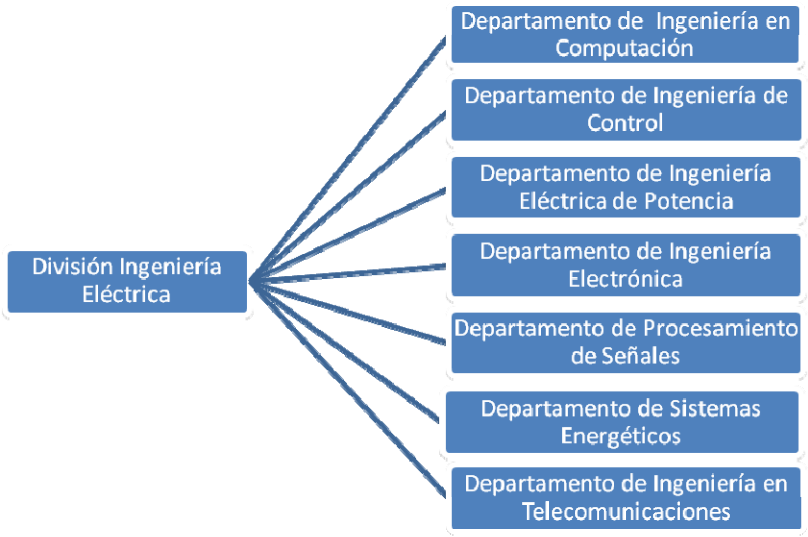


Figura 4.5 Organización de los Departamentos de la División de Ingeniería Eléctrica

Departamento de Ingeniería en Computación

La función del Departamento de Ingeniería en Computación se ve reflejada a través de su misión y visión publicadas oficialmente en su página Web "http://www.fi-b.unam.mx/Computacion.aspx", las cuales son:

MISIÓN:

"La misión del departamento de Ingeniería en Computación es formar a los alumnos dentro de las áreas de conocimiento de Computación y sus campos afines donde continuamente se vea reflejada la calidad, la integridad, la innovación y el nivel académico, para que sean competitivos en el ámbito profesional tanto nacional e

internacional, siendo profesionales calificados teniendo un buen reconocimiento en sus habilidades y actitudes en el desempeño de su profesión.

El departamento promueve la investigación y la docencia, favorece e induce tanto a los alumnos como al personal académico a especializarse en las áreas de Software y Hardware (Diseño de Sistemas Digitales, Redes y Seguridad, Multimedia e Internet, Bases y Minería de Datos, Microcomputadoras, etcétera), con capacidad para aprender toda la vida y mantenerse actualizado en los conocimientos de vanguardia, con las Universidades y empresas, para beneficio de toda la sociedad."

VISIÓN:

"La visión del Departamento de Ingeniería en Computación es fortalecer la investigación y la docencia a través de sus líneas de investigación (Bases y Minería de Datos, Diseño de Sistemas Digitales, Multimedia e Internet, Redes y Seguridad, Microcomputadoras, etcétera). Además de la vinculación con empresas tanto en proyectos o convenios. Y la participación en congresos con otras instituciones universitarias tanto nacionales como internacionales, así mismo la publicación de libros y artículos en revistas arbitradas."

Las áreas de investigación del Departamento de Ingeniería en Computación se muestran en la fig. 4.6.

Figura 4.6 Lista de Áreas de investigación del Departamento de Ingeniería en Computación

Carrera de Ingeniería en Computación

La Carrera de Ingeniería en Computación tiene como objetivo formar profesionales capaces de planear, diseñar, organizar, producir, operar y dar soporte técnico a los sistemas electrónicos para el procesamiento de datos, a los sistemas de programación -de base y de aplicación del equipo de cómputo-, así como efectuar el control digital de procesos automáticos.

El plan de estudios de estudios de la carrera de Ingeniería en Computación de acuerdo con el plan de estudios 2006, publicado oficialmente en la página de la Facultad de Ingeniería (http://www.ingenieria.unam.mx/paginas/Carreras/planes2009/ingComputo_Plan.htm), consta de

9 semestres con un total de 50 asignaturas, de las cuales 42 son obligatorias y 8 optativas, organizadas en 5 áreas del conocimiento, que son:

- Ciencias Básicas,
- Ciencias de la Ingeniería,
- Ingeniería Aplicada,
- Ciencias Sociales y Humanidades, y
- Otras de acuerdo al Módulo de salida.

Además, este plan de estudios cuenta con 6 Módulos de salida, los cuales se muestran (ver fig. 4.7) y se describen:

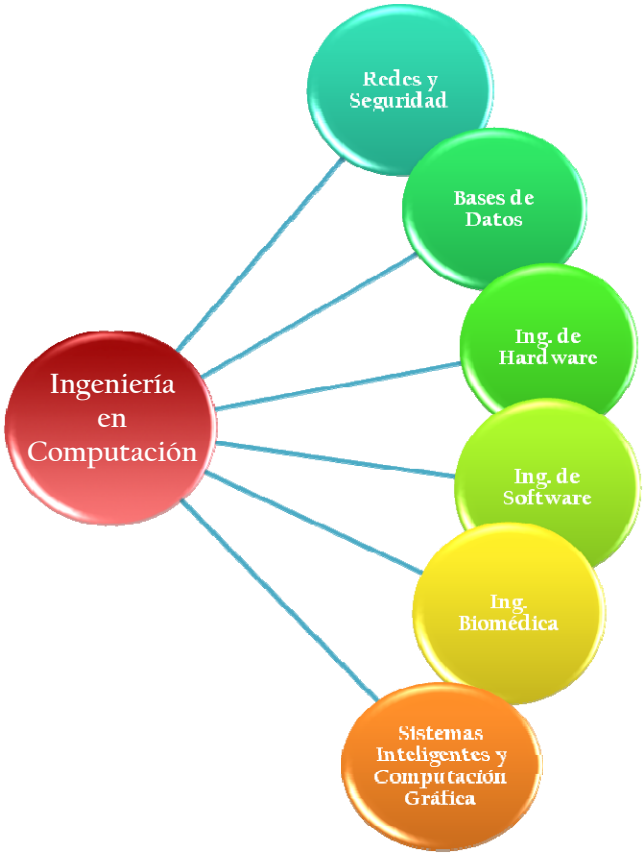


Figura 4.7 Lista de Módulos de Salida de la Carrera de Ingeniería en Computación

Redes y Seguridad

Objetivo:

El estudiante adquirirá conocimientos de protocolos, métodos, estándares, criptografía, calidad, normas y herramientas que le permitan, enmarcados en una base ética desarrollar: habilidades, aptitudes, actitudes y valores enfocados al diseño, desarrollo, mantenimiento y actualización de redes de datos, arquitecturas de seguridad, administración de redes, aplicaciones bajo el esquema cliente/servidor, mecanismos, soluciones y aplicaciones seguros y para la seguridad de la información.

Bases de Datos

Objetivo:

El alumno adquirirá conocimientos, habilidades y la experiencia necesaria en temas avanzados e innovadores del campo de las bases de datos, así como sus aplicaciones en la industria, mediante la elaboración de proyectos en los que analiza, diseña e implementa una aplicación de bases de datos específica.

Ingeniería del Hardware

Objetivo:

Formar profesionistas de alto nivel científico y tecnológico, con conocimientos sólidos y generales que les permitan ser capaces de identificar, analizar, planear, diseñar, organizar, producir, operar y dar soporte a los sistemas electrónicos, diseñando interfaces para ser conectadas en computadoras y describiendo el entorno y componentes de los sistemas de cómputo móvil; así mismo elaborará aplicaciones tanto en clientes inteligentes como en Internet inalámbrica comprendiendo los conceptos, las técnicas básicas y aplicaciones de los sistemas embebidos.

Ingeniería del Software

Objetivo:

El alumno aplicará procesos y herramientas mediante las cuales se analiza, diseña, implementa y administra una aplicación de software específica.

Ingeniería Biomédica

Este módulo ofrece a los alumnos de la carrera de Ingeniería Eléctrica Electrónica, a partir de las actividades académicas del Departamento de Ingeniería de Control, los conocimientos básicos y especializados para detectar, comprender, diseñar y construir equipos médicos, prótesis, dispositivos médicos, dispositivos de diagnóstico (imagenología médica) y de terapia, que permitan resolver los requerimientos de apoyo tecnológico de la medicina. El módulo es elegible a partir del octavo semestre y está conformado por siete asignaturas, tres en el octavo semestre y cuatro en el noveno semestre, de las cuales cuatro son de carácter obligatorio y tres son optativas.

Sistemas Inteligentes y Computación Gráfica

Este Módulo de Salida consta de tres submódulos, que son:

a) **Computación Gráfica**

Considerado uno de los campos de mayor crecimiento y de mayor valor agregado dentro del Cómputo, Informáticas y Tecnologías de la Información, Computación Gráfica ofrece una amplia diversidad de opciones para el desarrollo tanto profesional como académico.

Los egresados de este submódulo pueden desarrollarse en las áreas de:

- Visualización científica: médica, petrolera, astronómica, etc.
- Animación y producción digital.
- Desarrollo de videojuegos.
- Desarrollo de interfaces y Realidad Virtual.
- CAD y GIS.

b) Sistemas Inteligentes

Los egresados de este submódulo tienen enormes oportunidades de trabajo en el diseño y construcción de sistemas inteligentes.

Objetivos:

- Promover el conocimiento de las técnicas de Inteligencia Artificial para facilitar la toma de decisiones en problemas complejos.
- Diseñar, desarrollar e implementar sistemas inteligentes para la solución de problemas que involucran la toma de decisiones.
- Aplicar, en el desarrollo de sistemas inteligentes, técnicas de Inteligencia Artificial como son sistemas expertos, lógica difusa y bases de datos inteligentes, entre otras.

c) Tecnología del Lenguaje

Los egresados de este submódulo tienen enormes oportunidades de trabajo en:

- Empresas de telefonía celular como especialistas en el tratamiento de la voz.
- Empresas diseñadoras de software como especialistas en web semántica.
- Empresas bancarias, financieras, aseguradoras, y otras que manejen grandes bases de datos como especialistas en extracción y recuperación de información.

El Ingeniero en Computación deberá interrelacionarse con ingenieros en diversas especialidades, además de licenciados en informática, actuarios, abogados, administradores, economistas, entre otros, ya que su campo de acción abarca todas las áreas del conocimiento.

La labor que desempeña este profesionista es de una gran trascendencia desde diversos puntos de vista, ya que influye de manera directa tanto en los sectores productivo, económico, de planeación y de servicios, como en el área científica y de la investigación. Además, aporta indirectamente diversos beneficios a otros sectores de la población, ya sea por su contribución al desarrollo del país, o por el manejo que realiza de grandes volúmenes de información, con base en la planeación y la toma de decisiones.

El Ingeniero en Computación trabaja tanto en el sector público como en el privado, en donde existan computadoras o dispositivos de control automático.
Es importante señalar que actualmente el mercado de trabajo demanda en gran medida al Ingeniero en Computación, no sólo por el notable incremento que nuestro país ha tenido en los últimos años en materia de adquisición y uso de equipo de cómputo, sino también por la

utilización de un sinnúmero de lenguajes de programación y paquetes de uso comercial y científico.

Así, las múltiples empresas que disponen hoy en día de equipo de cómputo para el desarrollo de sus actividades, requieren de profesionistas capacitados en este campo.

La Facultad de Ingeniería mantiene un proceso permanente de revisión y actualización de sus planes de estudio, que están estructurados por un tronco común para las asignaturas de las Ciencias Básicas: Física, Matemáticas y Química; Ciencias de la Ingeniería, en las que se aplican las ciencias básicas para estructurar las teorías de la Ingeniería; Ingeniería Aplicada, en las que se aplican las ciencias de la Ingeniería para el desarrollo de metodologías a fin de resolver problemas de Ingeniería; y, finalmente, las Ciencias Sociales y las Humanidades, que proporcionan al alumno los elementos para ubicar su actividad como Ingeniero en la sociedad.

Para complementar la formación de los estudiantes, la Facultad de Ingeniería organiza diversas actividades académicas, culturales, deportivas y recreativas, así mismo, ofrece a sus alumnos la enseñanza de diversos idiomas, y distintos servicios como: Becas, Bolsa Universitaria de Trabajo, Servicio Bibliotecario, Centro de Información y Documentación, así como Centros de Cómputo que ofrecen capacitación a los alumnos. Además, los Laboratorios de Computación ofrecen servicios adicionales a los alumnos de esta carrera.

Laboratorios y Centros de Cómputo de la Facultad de Ingeniería

Los laboratorios de computación son una parte fundamental en la formación de los alumnos y es por ello que a continuación se presenta un panorama general del funcionamiento de cada uno de los laboratorios que en total son 11:

a) Unidad de Servicios de Cómputo Académico (UNICA)
b) Laboratorios de Computación (Salas A,B y C)
c) Laboratorio de Microsoft Research
d) Laboratorio de Investigación para el Desarrollo Académico (LINDA)
e) Laboratorio de Redes y Seguridad
f) Laboratorio de Multimedia e Internet
g) Laboratorio de Intel para la Academia
h) Laboratorio de JAVA
i) Laboratorio de Investigación y Desarrollo de Software Libre (LIDSOL) y Cómputo Gráfico
j) Laboratorios de Electrónica

a) Unidad de Servicios de Cómputo Académico (UNICA)

Misión

La misión de la Unidad de Servicios de Cómputo Académico es la de proporcionar eficaz y eficientemente en el ámbito institucional, los servicios de cómputo y el apoyo en actividades relacionadas que coadyuven al proceso integral de formación académica en la Facultad de Ingeniería.

Visión

La proyección de la Unidad de Servicios de Cómputo Académico al año 2010 es continuar siendo una Unidad líder en la prestación de servicios de cómputo de vanguardia a la Facultad de Ingeniería, al entorno universitario y a la sociedad en general.

- Contando con la organización, administración y los recursos adecuados.
- Siendo líderes en la formación, capacitación y difusión de la cultura informática
- Contando con las herramientas y convenios adecuados para el desarrollo y la investigación informática
- Contando con una infraestructura de red de cómputo moderna y tecnología de punta, brindando servicios de calidad y alta disponibilidad en tecnologías de la información y comunicación
- Contando con los servicios y procesos de atención sistematizados y actuales en apoyo a los eventos de seguridad informática
- Contando con la infraestructura adecuada y mecanismos para la actualización continúa del equipo de cómputo.

Estructura administrativa de UNICA

UNICA está organizada como lo indica la figura 4.2

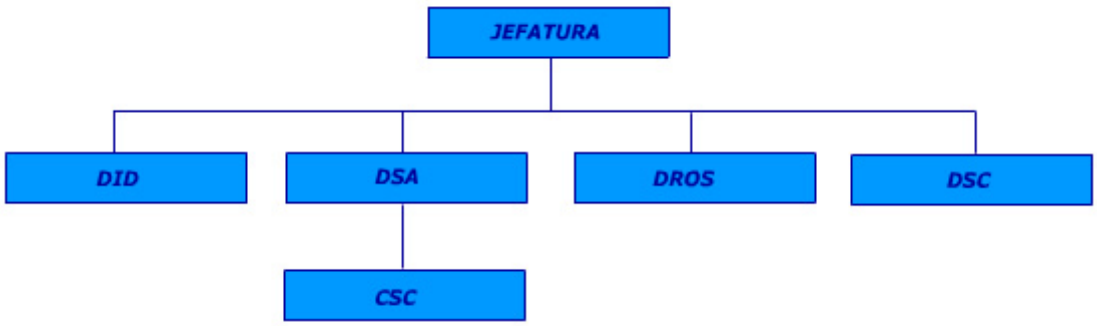


Figura 4.2 Organigrama de la estructura administrativa de UNICA

1) **DID: Departamento de Investigación y Desarrollo**

El Departamento de Investigación y Desarrollo (ver ubicación en fig. 4.3) se encarga de estar al día en la tecnología y avances en materia de cómputo. Así mismo, desarrolla sistemas de información administración y control de apoyo a las actividades académico-administrativas, internas de la Unidad, de la Facultad y eventualmente para la solución de problemas específicos de clientes externos.

Además, administra y da mantenimiento al servicio de Base de Datos, que se ofrece a los alumnos.

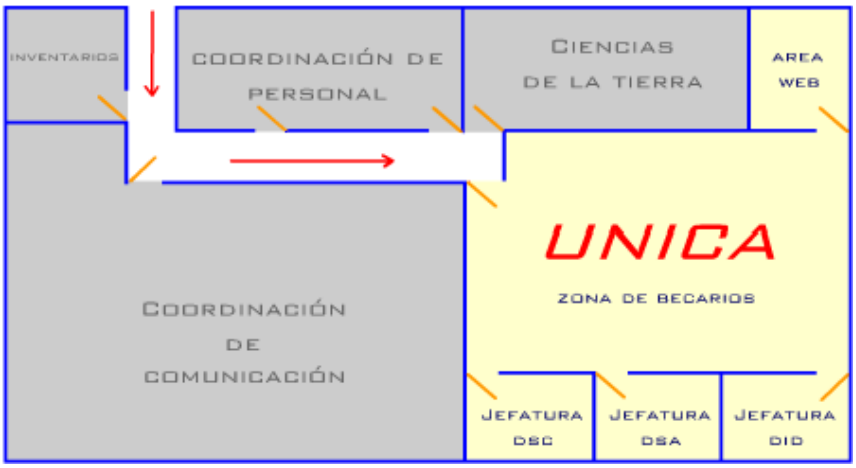


Figura 4.3 Ubicación de las áreas de UNICA en el edificio Principal, planta alta

2) DSA: Departamento de Servicios Académicos

El Departamento de Servicios Académicos (ver ubicación en fig. 4.3) se encarga de la planeación, organización e impartición de los cursos de cómputo que la Unidad ofrece sistemáticamente semestre a semestre, así como, los cursos requeridos para la formación de los alumnos becarios de UNICA.
Se encarga de la formación de los recursos humanos que la Unidad necesita para el cumplimiento de sus funciones; esto es mediante la coordinación del Programa de Formación de Becarios de UNICA.

Se imparten aproximadamente 120 cursos al año en los que se atienden del orden de 760 alumnos en promedio al semestre.

3) DSC: Departamento de Seguridad en Cómputo

El Departamento de Seguridad en Cómputo (ver ubicación en fig. 4.3) se encarga de brindar la máxima seguridad informática a las redes de cómputo de la Facultad de Ingeniería.

El Departamento tiene como objetivos:

- Desarrollo de esquemas de seguridad
- Investigación y desarrollo en tópicos de seguridad informática
- Realización de auditorías
- Manejo de respuesta a incidentes de seguridad informática
- Alertas y anuncios de seguridad

4) CSC: Coordinación de las salas de Cómputo

La Coordinación de las salas de Cómputo tiene como función principal es la de proporcionar el servicio de cómputo y de impresión a los alumnos de la Facultad, para que éstos puedan realizar sus trabajos y tareas de investigación, para lo cual además les proporciona servicio de correo electrónico, acceso a internet y servicios variados de apoyo en materia de cómputo.

Al efecto se cuenta con cuatro salas de atención de usuarios, una en el Edificio Principal (ver ubicación en fig. 4.4), dos en el Anexo de Ingeniería y una en el Edificio de Posgrado.

5) DROS: Departamento de Operación de Servidores

El Departamento de Operación de Servidores (ver ubicación en fig. 4.4) es responsable de la administración, operación, mantenimiento y seguridad de la red de comunicación de la Facultad y de la intercomunicación con la red central de la UNAM; así como del desarrollo e implementación de proyectos para la expansión del servicio. Administra y da mantenimiento a las cuentas de servicios de correo electrónico y de Internet de la Facultad. Unas 6000 cuentas individuales, en promedio anual.

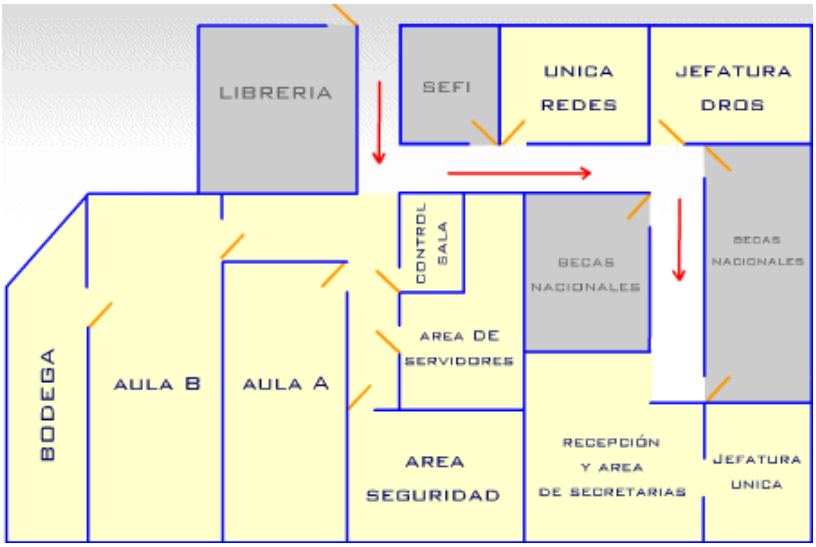


Figura 4.4 Ubicación de salas de cómputo y áreas de UNICA en el edificio Principal, planta baja

b) Laboratorio de Computación sala "A", sala "B" y sala "C"

Las salas "A" y "B" del Laboratorio de Computación son exclusivas para la docencia, se encuentran ubicadas en la planta baja del edificio Luis G. Valdez Vallejo.

Estas salas brindan servicio eficiente tanto a profesores como alumnos de las materias impartidas en la Facultad de Ingeniería a través de la División de Ingeniería Eléctrica (DIE), en las carreras de Ingeniero en Computación, Ingeniero Eléctrico Electrónico e Ingeniero en Telecomunicaciones, así como asesorías al personal que lo requiera y lo solicite.

La Sala "C", la cual es para alumnos ofrece los siguientes servicios: correo electrónico para administrativos, profesores y alumnos, bases de datos, servidor web, mantenimiento a equipos de cómputo que estén asignados a personal de la División, FTP público, sistemas operativos Windows y Linux, así como paquetería que incluye Office, herramientas de edición de imágenes, de CAD, herramientas para el desarrollo de aplicaciones WEB y especializadas de electrónica, internet a alta velocidad, impresión, compiladores y editores de diversos lenguajes de programación, etc. Asimismo, los alumnos pueden acceder vía remota a sus archivos a través de un FTP

c) Laboratorio Microsoft Research

El Laboratorio Microsoft de la Facultad de Ingeniería fue creado en el año 2002 con motivo de la donación de un servidor, ocho PC's, Windows 2000 Server y Visual Studio .NET por el corporativo Microsoft.

El Laboratorio tiene por objetivos:

- Exponer a los estudiantes y académicos de la Facultad de Ingeniería las últimas tecnologías Microsoft disponibles, incorporando su aplicación en asignaturas relacionadas con las carreras de la DIE.
- Desarrollar investigación.
- Desarrollar aplicaciones.
- Formar recursos humanos, Tesis y Servicio Social.
- Organizar cursos intersemestrales sobre tecnologías Microsoft.

d) LINDA: Laboratorio de Investigación para el Desarrollo Académico

LINDA es un grupo de estudiantes, académicos y gente altamente motivada para realizar proyectos de investigación básica en general, así como proyectos de aplicación en Ingeniería. Los proyectos son apoyados por la DIE.

El laboratorio tiene por objetivo:

- Integrar y apoyar a los estudiantes de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México (de cualquier semestre y carrera), que pretendan elevar su nivel académico mediante la realización de proyectos de investigación que ellos elaboren.

e) Laboratorio de Redes y Seguridad

Misión:

- *Proveer* una plataforma de trabajo en hardware y software a los estudiantes y profesores del área de redes y seguridad.
- *Apoyar* al alumno en el desarrollo de habilidades analíticas y funcionales para la creación, diseño, implantación, mantenimiento y administración de redes de datos.
- *Apoyar* al alumno en el desarrollo de habilidades analíticas y funcionales para la creación, diseño, implantación y mantenimiento de esquemas, herramientas y mecanismos de seguridad informática.
- *Auxiliar* a los tesistas en el desarrollo de sus proyectos de titulación poniendo a su disposición el equipo y software necesarios para la realización de éstos.

Visión

- Ser un laboratorio con la capacidad tecnológica y humana necesarias y suficientes para:
  - Fortalecer y difundir el conocimiento que nos lleve a formar los cuerpos de egresados de Ingeniería en Computación en el área de Redes y Seguridad de la más alta calidad que requiere el país.

- Crear nuevo conocimiento que permita el desarrollo de mejores redes, altamente eficientes, rápidas y seguras.
- Llegar a ser un laboratorio de docencia, investigación y desarrollo líder en el campo de las redes y la seguridad informática.
- Formar profesionales éticos, responsables y útiles a la sociedad, que hagan uso de sus conocimientos y habilidades para desarrollar y mantener de manera óptima las redes de datos nacionales e internacionales.

- Convertirse en un laboratorio de excelencia donde se realicen: actividades docentes, proyectos de investigación y desarrollo de alto nivel.

El laboratorio tiene por objetivos:

- Impartir los laboratorios correspondientes a las asignaturas del área de Redes y Seguridad.
- Promover la investigación y el desarrollo de proyectos entre los estudiantes de Ingeniería en Computación que les permitan complementar su formación académica.
- Conformar un grupo de profesores-investigadores interesados en este campo del conocimiento para desarrollar actividades encaminadas a docencia, investigación, creación y desarrollo de proyectos que generen nuevo conocimiento y que el trabajo conjunto sea encaminado a enriquecer cada proyecto con distintas visiones y aprovechar las capacidades y talentos de cada uno de los integrantes del laboratorio.

f) Laboratorio de Multimedia e Internet

El laboratorio está integrado por estudiantes y académicos interesados en preparar personas en diversas áreas, por medio de proyectos que impulsen su necesidad de aprender y resolver problemas.

El laboratorio tiene por objetivo:

- La formación de hombres y mujeres en las áreas de análisis, diseño y desarrollo de proyectos sobre Multimedia e Internet. Es, además, un elemento de servicio a la comunidad universitaria por medio de la impartición de cursos, préstamo de equipo y asesoría en las áreas anteriormente mencionadas.

g) Laboratorio de Intel para la Academia

El laboratorio está destinado a la investigación y a la difusión de temas acerca de Cómputo Distribuido Paralelo, de igual manera se da apoyo a los profesores de la carrera de Ingeniería en Computación para que puedan impartir algunas clases y prácticas de computación.

h) Laboratorio de Java

El laboratorio de IBM hizo un acuerdo con la Facultad de Ingeniería en el que se establece una cooperación tecnológica denominada Iniciativa Académica entre la UNAM e IBM® la cual ofrece la

posibilidad de acceder en forma gratuita a un amplio portafolio de productos de software IBM y a la capacitación de sus docentes.

IBM se comprometió a capacitar al personal docente designado por la Facultad de Ingeniería, en las tecnologías de Linux, Websphere, DB2 y Java.

Por otra parte la Facultad de Ingeniería se comprometió a conformar un centro de capacitación para a académicos y alumnos para impartir temas tecnológicos tales como Java, Linux, y en general Estándares Abiertos.

La misión y visión de este laboratorio se encuentran publicadas oficialmente en su página web "http://ibm.fi-b.unam.mx/gladys/UntitledFrameset-2.ht"

Misión

La misión es proveer la base de conocimientos e infraestructura de cómputo, para difundir los beneficios del desarrollo de software basado en Estándares Abiertos y Productos IBM, promoviendo su uso dentro de la comunidad Universitaria de la UNAM y el Público en General.

Visión

Su visión es establecer un semillero de alumnos, académicos y profesionales de la industria del cómputo, quiénes con los conocimientos aquí generados, aporten desarrollos sobresalientes, investigación e ideas innovadoras a nivel nacional, con impacto y difusión en otros países.

El laboratorio tiene por objetivo:

- La investigación, el desarrollo, la docencia y la difusión de las tecnologías referidas a Java, Linux, estándares abiertos y el resto de los productos IBM de la iniciativa académica.
- Proporcionar apoyo didáctico a las materias de la Facultad que involucren productos de la iniciativa académica.
- Habilitar un espacio para la capacitación del personal docente, alumnos y público en general.

i) Laboratorio de Investigación y desarrollo de Software libre (LIDSOL) y Cómputo Grafico

LIDSOL es un grupo de estudiantes, ex-estudiantes, académicos y entusiastas del software libre que buscan divulgar y crear software libre
También organizan charlas virtuales, conferencias, cursos y material para promover el aprendizaje y uso de software libre. Todo lo que sea software libre es de nuestro interés.

j) Laboratorios de electrónica

Estos laboratorios son de uso docente y se utilizan para la realización de prácticas de las materias de electrónica, así como apoyo a los alumnos para la realización de proyectos académicos.

Estos laboratorios son:

- Dispositivos Lógicos Programables
- Laboratorio de Microcomputadoras
- Laboratorio de Memorias y Periféricos

4.2 Evaluación de la Facultad de Ingeniería

4.2.1 Evaluación de los Laboratorios de la Carrera de Ingeniería en Computación de la Facultad de Ingeniería

La Facultad de Ingeniería es un organismo en constante desarrollo y crecimiento, por ello es importante hacer una evaluación de los laboratorios de la carrera de Ingeniería en Computación con la finalidad de saber cuáles son las condiciones actuales en las que se encuentran dichos laboratorios.

El objetivo de esta evaluación es conocer el espacio físico asignado a cada laboratorio, departamento o sala de Cómputo (que en adelante nos referiremos a los tres como laboratorios); así como, el tipo de personal que labora, herramientas, equipos de cómputo, mobiliario de cada lugar, entre otros, para tener una perspectiva más amplia, la cual nos ayudará a tomar las decisiones pertinentes en nuestra propuesta.

Para lograr este objetivo se diseño un cuestionario enfocado a conocer los recursos materiales, humanos y sus medidas de seguridad de la red y de la información de los laboratorios.

La fase de recolección de información tiene una gran importancia en el desarrollo de esta Propuesta puesto que la información que podamos obtener será la fuente de nuestro análisis y desarrollo.

A continuación se presentan los datos obtenidos a través de la aplicación de dicho cuestionario.

4.2.1.1 Espacio Físico

i) Unidad de Servicios de Cómputo Académico (UNICA)

Nombre: Departamento de Seguridad en Cómputo
Entrevistado: Ing. Rafael Sandoval Vázquez
Dimensiones: Aprox. 28 [m^2]
No. Subdivisiones: 3 salas
Página Web: http://132.248.54.45/unica/

Nombre: Sala 1
Entrevistado: Ing. Cruz Sergio Aguilar Díaz
Dimensiones: Aprox. 10 [m] x 10 [m]
No. Subdivisiones: 3 subdivisiones
Página Web: http://132.248.54.45/unica/

Nombre: Sala 2
Entrevistado: Ing. Cruz Sergio Aguilar Díaz
Dimensiones: Aprox. 15 [m] x 15 [m]
No. Subdivisiones: 5 subdivisiones
Página Web: http://132.248.54.45/unica/




Nombre: Sala 3
Entrevistado: Ing. Cruz Sergio Aguilar Díaz
Dimensiones: Aprox. 25 [m] x 20 [m]
No. Subdivisiones: 5 subdivisiones
Página Web: http://132.248.54.45/unica/



Nombre: Sala 4
Entrevistado: Ing. Cruz Sergio Aguilar Díaz
Dimensiones: Aprox. 6 [m] x 12 [m]
No. Subdivisiones: 2 subdivisiones
Página Web: http://132.248.54.45/unica/

ii) Laboratorio de Computación sala "A" y sala "B"

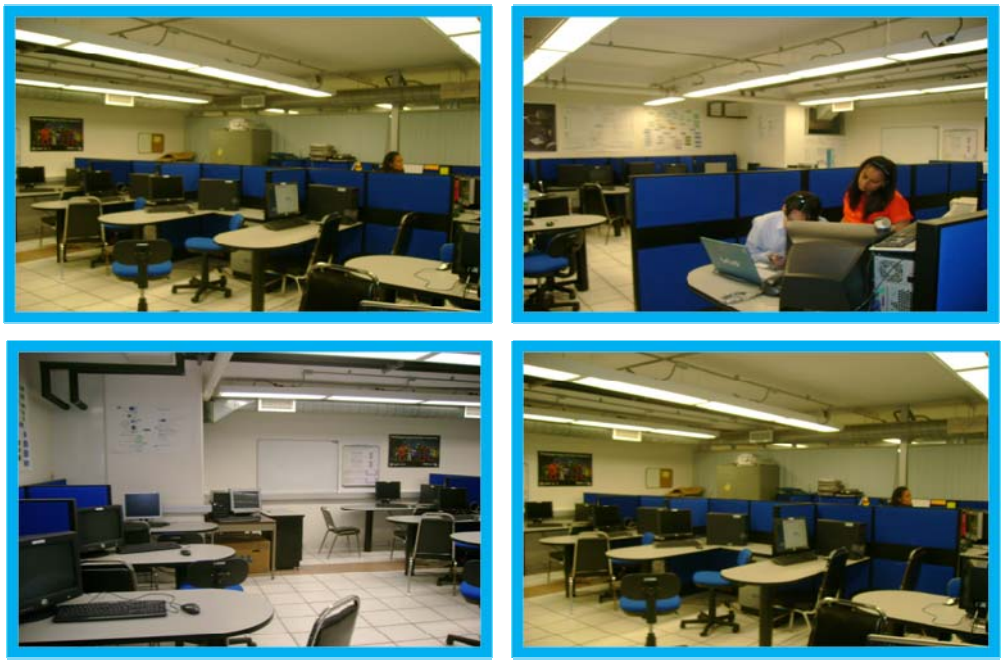
Nombre: Sala A y B
Entrevistado: Ing. Edgar Martínez Meza
Dimensiones: Aprox. 25 [m] x 9 [m]
No. Subdivisiones: 2 laboratorios y 3 cubículos entre laboratorio A y B
Página Web: http://lcp02.fi-b.unam.mx/

iii) Laboratorio Microsoft Research

Dimensiones: Aprox. 10 [m] x 9 [m]
No. Subdivisiones: 2 subdivisiones
Entrevistado: David Abel Herrera Rosales
Página Web: http://microsoft.fib.unam.mx/

iv) Laboratorio de Redes y Seguridad

Dimensiones: Aprox. 7 [m] x 7.5 [m]
Entrevistado: Ing. Alejandra Zúñiga Medel
No. Subdivisiones: 2 subdivisiones
Página Web: http://redyseguridad.fi-p.unam.mx



v) Laboratorio de Multimedia e Internet

Dimensiones: Aprox. 9 [m] x 6 [m]
Entrevistado: Ing. Honorato Saavedra Hernández
No. Subdivisiones: sin subdivisiones
Página Web: http://mmedia1.fi-b.unam.mx




vi) Laboratorio de Intel para la Academia

Dimensiones: Aprox. 8 [m] x 7 [m]
Entrevistado: M.I. Karen Sáenz García
No. Subdivisiones: 2 subdivisiones
Página Web: sin dato


vii) Laboratorio de JAVA

Dimensiones: Aprox. 90 [m^2]
Entrevistado: M.I. Ángel César Govantes Saldívar
No. Subdivisiones: sin subdivisiones
Página Web: http://ibm.fi-b.unam.mx


viii) Laboratorio de Investigación y Desarrollo de Software Libre (LIDSOL) y Cómputo Gráfico

Dimensiones: Aprox. 4 [m] x 8 [m]
Entrevistado: Andrés Hernández Bermúdez
No. Subdivisiones: sin subdivisiones
Página Web: http://wiki.lidsol.org


4.2.1.2 Recursos materiales

Cuando hablamos de Recursos Materiales nos referimos a los bienes físicos que brindan mejores condiciones de trabajo y ayudan a dar continuidad a las actividades de una empresa u organización.

El objetivo de la tabla 4.1 es la recopilación de los recursos materiales con los que cuentan los laboratorios de la Carrera de Ingeniería en Computación de la Facultad de Ingeniería y de esta forma determinar si se tienen los recursos necesarios y suficientes para poder implementar un SGSI y llevar a cabo las actividades de Acreditación y Certificación.

Tabla 4.1 Recursos Materiales de los laboratorios de la Carrera de Ingeniería en Computación

Nombre	*Abierto*	*Salas*	*Mobiliario*
Unidad de Cómputo Académico (Salas de Cómputo)	Si	4	❖ gabinetes de madera ❖ mesas para computadoras y sillas ❖ escritorios y módulos de trabajo ❖ aire acondicionado
Departamento de Seguridad en Cómputo (UNICA)	No	3	❖ gabinetes de madera ❖ escritorios y módulos de trabajo ❖ sillas
Laboratorio de Computación (Salas "A" y "B")	No	2	❖ mesas para computadoras y sillas ❖ escritorios ❖ pizarrones
Laboratorio Microsoft Research	SI	1	❖ gabinete ❖ mesas para computadoras y sillas ❖ pizarrón ❖ televisión ❖ archivero
Laboratorio de Redes y Seguridad	No	1	❖ módulos de trabajo ❖ mesas para computadoras y sillas ❖ pizarrón ❖ gabinete ❖ archivero
Laboratorio de Multimedia e Internet	No	1	❖ mesas para computadoras y sillas ❖ escritorios ❖ archivero ❖ pizarrón ❖ gabinetes ❖ bancos

Laboratorio de Intel para la Academia	No	1	❖ mesas para computadoras y sillas ❖ escritorios ❖ pizarrones ❖ módulos de trabajo ❖ sillas ❖ pizarrón
Laboratorio de JAVA (IBM)	Si	1	
LIDSOL	Si	1	❖ Escritorios ❖ sillas ❖ archivero ❖ gabinete de madera

4.2.1.3 Recursos Tecnológicos

Los datos que se muestran en la tabla 4.2 son importantes para nuestra propuesta ya que incluyen las tecnologías que usan los laboratorios de la Carrera de Ingeniería en Computación como medio para lograr el cumplimiento de sus objetivos, proporcionándoles una ventaja en las actividades que realizan.

Tabla 4.2 Recursos Tecnológicos de los laboratorios de la Carrera de Ingeniería en Computación

Nombre	*Equipo*	*Software*	*Tipo de Red*
Unidad de Cómputo Académico (Salas de Cómputo)	❖ 310 PC's ❖ 12 impresoras ❖ 9 servidores ❖ Fuentes de corriente regulada ❖ Reguladores ❖ Switchs y Hubs	❖ S.O. Windows y Linux ❖ AutoCAD ❖ Visual Basic ❖ Ofimática ❖ C, C++, C#, etc.	LAN Y WLAN
Departamento de Seguridad en Cómputo (UNICA)	❖ 40 PC's ❖ Access Point ❖ Impresoras ❖ Servidores ❖ Switch ❖ Reguladores	❖ S.O. Windows, Linux, Mac OS y UNIX ❖ Ofimática ❖ Herramientas para monitoreo, análisis forense, auditoría y virtualización ❖ Software Libre	LAN y WLAN
Laboratorio de Computación (Salas "A" y "B")	❖ Aprox. 95 PC's ❖ 4 switchs ❖ 1 impresora	❖ S.O Windows y Linux ❖ Ofimática ❖ Herramientas de optimización de Windows ❖ Software especializado para cursos y docencia ❖ Antivirus de Licencia gratuita	LAN

Laboratorio Microsoft Research	❖ 35 PC`s ❖ 6 Tablet PC ❖ 3 Servidores ❖ Access Point ❖ Videoproyectores ❖ Xbox 360 ❖ Robots ❖ Switch	❖ S.O. Windows Vista y XP ❖ Software de Microsoft	LAN y WLAN
Laboratorio de Redes y Seguridad	❖ 15 PC's ❖ 2 Servidores ❖ 5 Switchs	❖ S.O. Windows y Linux ❖ Ofimática ❖ Herramientas de Monitoreo	LAN
Laboratorio de Multimedia e Internet	❖ 9 PC's ❖ 1 Laptop ❖ 1 Servidor ❖ 1 Switch ❖ 1 No-Break ❖ 1 Access Point	❖ S.O. Windows y Linux ❖ Net Beans ❖ PHP y JAVA ❖ Software Libre	LAN y WLAN
Laboratorio de Intel para la Academia	❖ 1 Proyector ❖ 24 PC's ❖ 1 Servidor ❖ 2 Switchs	❖ S.O. Windows y Linux ❖ Compiladores ❖ Herramientas para perfilamiento de código ❖ Software para uso docente	LAN
Laboratorio de JAVA (IBM)	❖ 25 PC's ❖ Switch ❖ Rack ❖ Proyector ❖ Lector biométrico	❖ S.O. Linux distribución Debian ❖ Software de IBM ❖ Eclipse, DB2 ❖ Rational Architect	LAN
LIDSOL	❖ 9 PC's ❖ Rack	❖ S.O. Linux varias distribuciones ❖ Software Libre	LAN

4.2.1.4 Recursos Humanos

Una empresa u organización debe contar con los recursos humanos que estén identificados con las políticas de ésta, para ello es necesario seleccionar, proveer y administrar a las personas que con sus conocimientos, experiencia y competencia colectiva son adecuadas a los objetivos de la empresa u organización llevándola al éxito o al fracaso, es por ello que en la tabla 4.3 se presentan un resumen de los Recursos Humanos de los laboratorios de la Facultad de Ingeniería con el objetivo de determinar el tipo de personal que labora en cada laboratorio, así como su selección y

capacitación. Esto nos servirá para tomar una buena decisión en el momento de determinar y proponer al mejor candidato para la Certificación y Acreditación.

Tabla 4.3 Recursos Humanos de los laboratorios de la Carrera de Ingeniería en Computación

Nombre	*Personal*	*Selección*	*Capacitación*
Unidad de Cómputo Académico (Salas de Cómputo)	❖ 3 Académicos ❖ 1 de base ❖ Aprox. 70 Alumnos de Servicio Social y Prácticas Profesionales	De acuerdo a aptitud y desempeño de los prestadores de Servicio Social y Practicantes	Si
Departamento de Seguridad en Cómputo (UNICA)	❖ 1 Técnico Académico ❖ 3 Ayudantes de Profesor ❖ Becarios (1a, 2a y 3a etapa)	Reclutamiento por parte de UNICA	Si
Laboratorio de Computación (Salas "A" y "B")	❖ 5 Ingenieros ❖ 1 Técnico	No hay proceso de selección	No
Laboratorio Microsoft Research	❖ 3 Ayudantes de Laboratorio ❖ 1 Administrador ❖ 1 Académico	De acuerdo a aptitud y desempeño de los prestadores de Servicio Social y Practicantes	No
Laboratorio de Redes y Seguridad	❖ 1 Administradora ❖ 5 Profesores ❖ 3 Alumnos de Servicio social	Selección a cargo de la Coordinadora del Módulo	Si
Laboratorio de Multimedia e Internet	❖ 4 Ayudantes de Profesor ❖ 4 alumnos de Servicio Social	No hay proceso de selección	No
Laboratorio de Intel para la Academia	❖ 2 Ayudantes de Profesor ❖ 1 Académico	No hay proceso de selección	No
Laboratorio de JAVA (IBM)	❖ No cuenta con personal oficialmente ❖ Alumnos de Servicio Social ❖ 1 Académico	A través de un programa de Servicio Social y recibe apoyo del personal de Programa de Tecnología en Computación (PROTECO)	No
LIDSOL	❖ 1 Administrador ❖ 1 Académico ❖ Alumnos interesados en proyectos	No hay proceso de selección	No

4.2.1.5 Seguridad de las redes y de la información

Con base en los datos de la tabla 4.4 podremos determinar el nivel de seguridad, tanto en las redes como en la información, con el que cuenta cada laboratorio de la Carrera de Ingeniería en Computación de la Facultad de Ingeniería.

Tabla 4.4 Seguridad de las redes y la información de los laboratorios de la Carrera de Ingeniería en Computación

Nombre	*Seguridad*	
	Red	*Información*
Unidad de Cómputo Académico (Salas de Cómputo)	Implementación de un Servidor Firewall por Sala. Implementación de un Servidor que filtra información por Sala.	Implementación de dos Servidores de Aplicaciones por Sala. Implementación de un Área restringida para los Servidores.
Departamento de Seguridad en Cómputo (UNICA)	Implementación de un esquema de Seguridad Perimetral. Monitoreo de la red a través de Sensores de diferentes tipos.	Realización de un análisis de riesgos y estudio de un modelo de seguridad para el departamento.
Laboratorio de Computación (Salas "A" y "B")	Configuración de firewall. Implementación de Servidores con IP virtual. Administración de Switchs.	Almacenamiento de la Información en un Servidor con acceso restringido. Restricción de permisos de acceso. Respaldo de información cada semestre. Realización de planes de contingencia.
Laboratorio Microsoft Research	Configuración de bloqueo de puertos. Configuración de ISA Server 2004 en el Servidor. Configuración de un filtro de Mac Address. Encriptación de transferencia mediante Protocolo WEP.	Manejo de roles para las cuentas de usuario. Restricción de permiso de acceso a los servidores.
Laboratorio de Redes y Seguridad	Monitoreo constante de la red. Implementación y administración de un Swicth con IP virtual. Implementación de un Firewall en el servidor.	Almacenamiento de la información en un servidor con S.O. Linux. Protección de los servidores a través de una chapa.

Laboratorio de Multimedia e Internet	Asignación de nombre de usuario y contraseña a cada usuario. Asignación de una máquina a cada usuario. Protección de red inalámbrica con clave WPA. Implementación de un Proxy para servicio de red. Implementación de un firewall en un Servidor. Implementación de dos Servidores Virtuales.	Almacenamiento de la información en un servidor con S.O. Linux restringido a un solo usuario. Realización de respaldos automáticos semanales.
Laboratorio de Intel para la Academia	Implementación de un firewall en un Servidor. Implementación de un Proxy para servicios de red.	Almacenamiento de la información en un Servidor con S.O. Linux.
Laboratorio de JAVA (IBM)	Implementación de un firewall en un Servidor. Implementación de un Proxy para servicio de red.	No se produce ni maneja información sensible.
LIDSOL	Implementación y configuración de firewall por cada equipo.	Ocultar la información de un equipo de prueba a través de otro equipo.

4.2.2 Análisis de los Laboratorios de la Carrera de Ingeniería en Computación de la Facultad de Ingeniería

Para analizar los datos de las tablas anteriores, relativas a los recursos con los que cuentan los laboratorios de la Carrera de Ingeniería en Computación, los dividimos en dos grupos:

a) Datos Cuantificables

Este grupo consta de aquellos datos que se pueden contar y son fáciles de medir. Estos datos se presentan en la tabla 4.5.

Tabla 4.5 Tabla comparativa de los datos cuantificables de los recursos de los laboratorios de la Carrera de Ingeniería en Computación de la Facultad de Ingeniería

Nombre	*Dimensión [m2]*	*No. Subdivisiones*	*No. Equipo [PC`s]*	*No. Personal*
UNICA (Sala 3)	500	5	161	74
UNICA (Sala 2)	225	5	67	
UNICA (Sala 1)	100	3	25	
UNICA (Sala 4)	72	2	50	

Lab. de Computación (Salas "A" y "B")	225	3	95	6
Lab. Microsoft Research	90	2	41	5
Lab. de JAVA (IBM)	90	0	25	1
Lab. de Intel para la Academia	56	2	24	3
Lab. de Multimedia e Internet	54	0	10	8
Lab. de Redes y Seguridad	52.5	2	15	9
Depto. de Seguridad en Cómputo (UNICA)	28	0	40	12
LIDSOL	12	0	9	5

De la tabla 4.5 podemos observar que:

La sala 3 de UNICA tiene asignado un mayor espacio físico en comparación a los demás laboratorios, pero también podemos apreciar que este laboratorio está subdividido en 5 secciones y que alberga el mayor número de equipos y el mayor número de personal por lo que ya no hay más espacio disponible para albergar mas equipo de computo y personal, además, cabe recordar que el objetivo de esta sala es la de brindar servicios de cómputo a la comunidad estudiantil de la Facultad de Ingeniería.

Los que siguen en cuanto a espacio físico son los Laboratorios de Computación Salas “A” y “B”, el cual está divido en 3 subdivisiones y albergan un número considerable de equipo, sin embargo el personal con el que cuentan es poco, ya que su uso es meramente docente, por lo que no hay espacio para albergar mas equipo de cómputo.

Los laboratorios que siguen son el Laboratorio de Microsoft Research y el Laboratorio de JAVA, qué están destinados a la investigación y docencia, por lo que también el personal que labora formalmente en ambos laboratorios es limitado.

A continuación aparecen los laboratorios de Intel para la Academia y el de Multimedia e Internet, los cuales cuentan con un espacio semejante, pero el Laboratorio de Intel tiene más equipo y menos personal que el de Multimedia e Internet, esto debido a que el laboratorio de Intel está destinado a la Investigación y como apoyo a la docencia, mientras que el de Multimedia e Internet está destinado solo a la investigación, a ambos laboratorios se les puede dar uso a su equipo para nuevos proyectos.

Entre los laboratorios con menor espacio físico se encuentran los laboratorios:

Laboratorio de LIDSOL, es el laboratorio con el menor espacio físico, además, es él que tiene el menor número de equipo y el personal que labora ahí es poco.

Departamento de Seguridad en Cómputo, también cuenta con un espacio físico pequeño ya que este departamento esta subdividido en tres salas y el personal que labora ahí también está dividido, en cuanto al número de equipo de cómputo podemos darnos cuenta que es superior al laboratorio de LIDSOL y al laboratorio de Redes y Seguridad; las actividades que ahí se realizan son de importancia en cuanto a temas de seguridad pero el espacio es muy reducido.

El Laboratorio de Redes y Seguridad, es uno de los laboratorios más pequeños en cuanto a espacio físico. El número de equipo de cómputo así como el número de personal es suficiente para las

actividades que se desempeñan en el laboratorio. Cuenta, además, con dos subdivisiones por lo que no hay espacio para mas equipo.

De los párrafos anteriores podemos deducir que el espacio físico disponible para nuestra propuesta es muy poco, ya que los laboratorios que cuentan con mucho espacio físico están divididos internamente y además su uso es exclusivo para la docencia y servicio a la comunidad estudiantil, por lo que no se pueden ocupar.

Para poder elegir los laboratorios con las más altas probabilidades de realizar las tareas de Acreditación y Certificación, nos interesamos en aquellos que cuentan con el personal mas encaminado a temas de Seguridad de la Información, que cuentan con más experiencia en cuanto a estos temas, y que sean capaces de ir formando recursos humanos con las herramientas y conocimientos necesarios para realizar actividades de Acreditación y Certificación en cuanto a Seguridad de la Información.

b) Datos No Cuantificables

Este grupo consta de los recursos de los cuales no es posible obtener datos que se puedan medir directamente, ya sea por la naturaleza del bien o por que no se cuentan con dichos datos.

Para poder medir estos datos, presentados en la tabla 4.7, recurrimos a una asignación de puntos en la que la escala va del 0 al 1 y los aspectos o características que se tomaron en cuenta para la asignación de puntos se detallan en la tabla 4.6.

Tabla 4.6 Escala y características que se tomaron en cuenta para la asignación de puntos

Escala	Capacitación de Personal	Selección de Personal	Tipo de Seguridad
0	Si el personal del laboratorio no recibe algún tipo de capacitación en cuanto a temas de seguridad en general.	Cuando el laboratorio no tiene un proceso de selección o no hay necesidad de realizar una selección de personal	Cuando el laboratorio tiene implementado un procedimiento para procurar mantener segura la información del laboratorio o mantener segura la red de computadoras.
0.5		Cuando en el laboratorio existe un proceso de selección basado solamente en aptitudes y desempeño.	
1	Si el personal del laboratorio recibe algún tipo de capacitación, ya sea interna o externa, en cuanto a temas de seguridad en general.	Cuando el proceso de selección del personal se basa en un procedimiento definido.	Cuando el laboratorio tiene implementados procedimientos para mantener segura la información del laboratorio así como mantener segura la red de computadoras.

Tabla 4.7 Puntuación asignada a los recursos con los que cuentan los laboratorios de la Carrera de Ingeniería en Computación

Nombre	Capacitación de Personal	Selección de Personal	Tipo de Seguridad
UNICA (Sala 1)	1	0.5	1
UNICA (Sala 2)	1	0.5	1
UNICA (Sala 3)	1	0.5	1
UNICA(Sala 4)	1	0.5	1
Depto. de Seguridad en Cómputo (UNICA)	1	1	1
Lab. de Computación (Salas "A" y "B")	0	0	1
Lab. Microsoft Research	0	0.5	1
Lab. de Redes y Seguridad	1	1	1
Lab. de Multimedia e Internet	0	0	1
Lab. de Intel para la Academia	0	0	1
Lab. de JAVA (IBM)	0	0.5	1
LIDSOL	0	0	1

Después de asignar los puntos (ver tabla 4.7), se procedió a realizar una suma de los puntos obtenidos por cada laboratorio. En la tabla 4.8 se muestran los resultados.

Tabla 4.8 Resultados finales de los laboratorios de la carrera de Ingeniería en Computación

Nombre	*Puntuación Total*
UNICA (Salas de Cómputo)	2.5
Depto. de Seguridad en Cómputo (UNICA)	3
Lab. de Computación (Salas "A" y "B")	1
Lab. Microsoft Research	1.5
Lab. de Redes y Seguridad	3
Lab. de Multimedia e Internet	1
Lab. de Intel para la Academia	1
Lab. de JAVA (IBM)	1.5
LIDSOL	1

Como se puede observar en la tabla 4.8, los laboratorios con una puntuación alta son:

- Departamento de Seguridad en Cómputo.
- Laboratorio de Redes y Seguridad.
- Salas de Cómputo de UNICA.

Por lo que estos laboratorios son los candidatos para nuestra propuesta, ya que son los que cuentan con las mejores condiciones que consideramos pertinentes.

Cabe destacar que en la evaluación de los laboratorios hemos podido comprobar que en todos los laboratorios hay una conciencia y preocupación por mantener la seguridad de la información y en

las redes, y que todos están haciendo algo al respecto. Las diferencias que se dieron en estas puntuaciones no son por la falta de interés o por una mala administración, sino porque cada laboratorio tiene diferentes funciones y la información que manejan algunos laboratorios es más vulnerable que la que se maneja en otros laboratorios y la cantidad de personal y espacio físico son variados.

4.2.2.1 Análisis de la Gestión de la Seguridad de la Información

Con las evaluaciones anteriores hemos determinado que tres laboratorios pueden ser candidatos para nuestra propuesta, por lo que hemos diseñado un segundo cuestionario con el objetivo de conocer los procedimientos y controles de cada laboratorio con el fin de mantener la Seguridad de la Información y cómo el personal contribuye a estos objetivos.

Una vez identificados los tres laboratorios, realizaremos un análisis para poder determinar si cuentan con las bases mínimas en lo que a Seguridad de la Información se refiere. Para lograr dichos objetivos recurrimos a la aplicación del segundo cuestionario a los encargados de cada laboratorio identificados en el tema anterior (ver tabla 4.8), dicho cuestionario nos permitirá conocer si el laboratorio cuenta con una base de implantación de medidas de seguridad así como el flujo de información y las responsabilidades, y también, saber si existe una consciencia acerca de las vulnerabilidades del laboratorio.

El cuestionario está organizado por categorías, el objetivo de cada categoría se explica en la tabla 4.9.

Tabla 4.9 Categorías y objetivos de las categorías empleadas para el análisis de la Gestión de la Seguridad de la Información

Categoría	Objetivo
Evaluación de riesgos de seguridad	Saber si el laboratorio evalúa las amenazas, impactos y vulnerabilidades de la Información y de los medios de tratamiento de la misma así como de su probable ocurrencia.
Política de seguridad	Determinar si el laboratorio establece un compromiso con la seguridad de la información publicando y manteniendo sus políticas de seguridad.
Aspectos organizativos de la seguridad de la información	Determinar si existe una estructura de gestión para iniciar y controlar la implantación de la Seguridad de la Información dentro del laboratorio.
Clasificación y control de activos	Saber si se clasifican y controlan adecuadamente los activos del laboratorio.
Seguridad ligada al personal	Determinar el proceso de desarrollo del personal desde la selección del mismo hasta su capacidad de respuesta a incidentes.
Seguridad física y del entorno	Determinar si existen recursos que eviten accesos físicos no autorizados, daños e intromisiones en las instalaciones y en la información del laboratorio.
Gestión de comunicaciones y operaciones	Determinar si existe una operación correcta y segura de los recursos de tratamiento de información.

Control de accesos	Determinar si el laboratorio cuenta con un control físico y lógico de acceso a la información.
Gestión de continuidad del negocio	Saber si existe una reacción a la interrupción de actividades del laboratorio y si protegen sus procesos críticos frente a grandes fallos o desastres.
Cumplimiento de los requisitos legales	Determinar si el laboratorio tiene disponibles sus registros en caso de que se requiera o se solicite para comprobar que cumple con los requisitos legales.

La información obtenida a través de las entrevistas realizadas se presenta en la tabla 4.10 en donde los laboratorios son identificados por las siguientes siglas:

SCU: Sala de Cómputo de UNICA
DSCU: Departamento de Seguridad de UNICA
LRyS: Laboratorio de Redes y Seguridad

Tabla 4.10 Análisis de las Categorías para la evaluación de la Gestión de la Seguridad de la Información de los laboratorios

	Categoría	SCU	DSCU	LRYS
	EVALUACIÓN DE RIESGOS DE SEGURIDAD			
1	Realiza Evaluación de Riesgos		X	X
2	Programan la evaluación de riesgos			
	POLÍTICA DE SEGURIDAD			
3	Cuenta con Política de Seguridad		X	X
4	Publica y distribuye la Política de Seguridad a todos los empleados y terceros afectados		X	X
	ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN			
5	Existe un Comité que se encargue de la Gestión de la Seguridad de la Información			
6	Asigna responsabilidades relativas a la seguridad de la información		X	
7	Cuenta con ayuda externa o interna de especialistas en Seguridad de la información cuando hay incidencias	X	X	X
	CLASIFICACIÓN Y CONTROL DE ACTIVOS			
8	Cuentan con clasificación de servicios	X	X	X
9	Existe un procedimiento para la clasificación de servicios			
10	Cuenta con clasificación de la información			
11	Existe un procedimiento para la clasificación de información			
12	Cuenta con clasificación de activos físicos	X		X
13	Existe un procedimiento para la clasificación de activos físicos			
14	Cuenta con control de servicios	X	X	

15	Existe un procedimiento para el control de servicios	X	X	
16	Cuenta con control de la información		X	
17	Existe un procedimiento para el control de la información		X	
18	Cuenta con control de activos físicos	X	X	X
19	Existe un procedimiento para el control de activos físicos	X	X	X
	SEGURIDAD LIGADA AL PERSONAL			
20	Existe un proceso de selección del personal	X	X	X
21	Capacita al personal en lo relativo a Seguridad de la información	X	X	X
22	Registra las incidencias de seguridad de la información	X	X	X
23	Existe un procedimiento de información y respuesta a incidencias	X	X	X
24	Documenta el procedimiento de información y respuesta a incidencias	X	X	
	SEGURIDAD FÍSICA Y DEL ENTORNO			
25	Cuenta con perímetro de seguridad	X	X	X
26	Tiene barreras físicas el perímetro de seguridad	X	X	X
27	Cuenta con controles físicos de entrada	X	X	X
28	Cuenta con sistemas de alimentación ininterrumpidas	X	X	
29	Programan el mantenimiento del equipo de cómputo	X	X	X
30	Controla la entrada y salida del equipo de cómputo	X		X
31	Controla la entrada y salida del software			X
32	Controla la entrada y salida de la información			X
	GESTIÓN DE COMUNICACIONES Y OPERACIONES			
33	Documenta procedimientos operativos	X	X	
34	Realiza copias de seguridad de la información	X	X	X
35	Programan la realización de copias de seguridad	X	X	X
36	Existe control en la red de computadoras	X	X	X
37	Existe seguridad en la red de computadoras	X	X	X
	CONTROL DE ACCESOS			
38	Tiene control de acceso	X	X	X
39	Tiene métodos de acceso	X	X	X
40	Gestiona los privilegios		X	X
41	Cuenta con listas de acceso		X	X
42	Actualizan las listas de acceso		X	X
43	Controla el acceso a la red de computadoras	X	X	X
44	Restringe el acceso a la información	X	X	X

45	Aísla los sistemas sensibles	X	X	X
	GESTIÓN DE CONTINUIDAD DEL NEGOCIO			
46	Existe un plan de continuidad de actividades	X	X	
	CUMPLIMIENTO DE LOS REQUISITOS LEGALES			
47	Protegen los registros del laboratorio		X	
48	Tienen un procedimiento para la protección de los registros		X	
49	Protege los datos y privacidad de la información personal			

En la tabla 4.11 se presenta el resultado final de cada una de las categorías que obtuvo cada laboratorio, la cual nos ayudará a visualizar de una mejor manera las condiciones actuales de cada laboratorio en cuanto a Gestión de la Seguridad de la Información se trata.

Tabla 4.11 Análisis de las Categorías para la evaluación de la Gestión de la Seguridad de la Información de los laboratorios

Análisis	SCU	DSCU	LRyS
Evaluación de Riesgos de Seguridad	0	1	1
Política de Seguridad	0	2	2
Aspectos Organizativos de la seguridad de la Información	1	2	1
Clasificación y control de activos	6	7	4
Seguridad ligada al personal	5	5	4
Seguridad Física y del Entorno	6	5	7
Gestión de comunicaciones y operaciones	5	5	4
Control de Accesos	5	8	8
Gestión de continuidad del negocio	1	1	0
Cumplimiento de los requisitos legales	0	2	0

De la tabla 4.11 podemos concluir que:

Los laboratorios DSCU y LRyS, están conscientes de su situación en cuanto a vulnerabilidades y fortalezas, ya que han realizado por lo menos una vez una evaluación de riesgos, además, los dos laboratorios cuentan con una política de seguridad que les ayuda a mantener la seguridad de su información.

En los laboratorios SCU y LRyS habrá que trabajar sobre la designación de responsabilidades del laboratorio en cuanto a la Seguridad de la Información, ya que salieron bajos en la categoría de Aspectos organizativos de la seguridad de la información.

El laboratorio LRyS tiene un área de oportunidad en cuanto a su clasificación y control de activos ya que es una parte importante para la Gestión de la Seguridad de la Información que les permitirá tener un control sobre los activos físicos y lógicos del laboratorio. Por otra parte este laboratorio cuenta con muy poco personal y éste es de confianza, es por ello que salió ligeramente bajo en comparación con los otros dos laboratorios.

En cuanto a Seguridad física y del entorno, el laboratorio LRyS salió con más puntos en comparación con los otros dos laboratorios, esto se debe a que el laboratorio tiene un espacio físico reducido, por lo tanto, todas las medidas de seguridad implementadas son suficientes para lograr un nivel de seguridad deseado. El laboratorio de DSCU salió unos puntos abajo por el hecho de que no distribuyen software y no hay la necesidad de que salga el equipo fuera de las instalaciones del laboratorio, por lo que no tienen controlado esos dos aspectos.

El laboratorio LRyS no documenta sus procedimientos operativos en la categoría de Gestión de comunicaciones y operaciones por lo que es una gran oportunidad para empezar a documentarlos.

El laboratorio SCU salió bajo en cuanto al Control de accesos, esto se debe a que el laboratorio cuenta con muchos registros de acceso por día por lo que no cuenta con listas de acceso y por lo tanto no las actualiza, solo controla los accesos pero no los registra.

En cuanto a la Continuidad del negocio, los laboratorios SCU y DSCU son los que aseguran la continuidad del negocio ante una amenaza.

El laboratorio de DSCU es el único que protegen los registros y tienen un procedimiento para la protección de éstos, para la categoría de Cumplimiento de los requisitos legales.

Con base en los hechos anteriores podemos afirmar que:

El Laboratorio de Redes y Seguridad es el más apto para llevar a cabo las actividades de Acreditación y Certificación bajo la norma ISO/IEC 27001 debido a que:

- El laboratorio de Redes y Seguridad cuenta con las bases necesarias para iniciar la implementación de un SGSI.
- El personal del laboratorio de Redes y Seguridad se capacita constantemente debido a las actividades que se realizan en el laboratorio.
- El laboratorio de Redes y Seguridad es una parte integral del módulo de salida de Redes y Seguridad cuyo objetivo es formar Recursos Humanos con los conocimientos necesarios enmarcados en una base ética para el diseño, desarrollo, mantenimiento y actualización de redes de datos, arquitecturas de seguridad, administración de redes, aplicaciones bajo el esquema cliente/servidor, mecanismos, soluciones y aplicaciones seguros y para la seguridad de la información.

Por otro lado, cabe destacar que en la UNAM hay un organismo que forma parte de la Dirección General de Servicios de Cómputo Académico (DGSCA), el cual lleva por nombre Departamento de Seguridad en Cómputo (DSC) y es uno de los organismos enfocados en temas de seguridad informática y de la información, por lo que a continuación se describe de manera general.

Departamento de Seguridad en Cómputo (DSC), DGSCA

De acuerdo a su página web “http://www.seguridad.unam.mx/servicios/main.dsc”, el DSC es un punto de encuentro al cual puede acudir la comunidad de cómputo para obtener información, asesorías y servicios de seguridad; así como para intercambiar experiencias y puntos de vista, logrando con ello, establecer políticas de seguridad adecuadas, disminuir la cantidad y gravedad de los problemas de seguridad y difundir la cultura de la seguridad en cómputo.

Los servicios otorgados por este Departamento se listan a continuación:

- Análisis de tráfico de red.
- Análisis de vulnerabilidades y pruebas de penetración.
- Análisis de riesgos.
- Creación de políticas de seguridad de la información.
- Implantación de ISMS de acuerdo al estándar ISO 27001.
- Respuesta a incidentes de seguridad de la información.
- Análisis forense.
- Servicios administrados de seguridad.
- Revisión de configuraciones.
- Programas de capacitación.
- Auditoría de código.

Como dato adicional es importante mencionar que el DSC cuenta con certificación bajo la norma ISO/IEC 27001 por la EQA, lo que le permite dar asesoría o consultoría en la Implementación de un SGSI de acuerdo a la norma ISO/IEC 27001, que como se pudo apreciar anteriormente éste es uno de sus servicios.

4.3 Análisis

Con base en los análisis hechos en este capítulo se encontró lo siguiente:

En cuanto a niveles de seguridad:

- Los laboratorios tienen implementadas medidas de seguridad en diferentes niveles y estos niveles dependen de las actividades y recursos de cada laboratorio.

En cuanto a recursos:

- El espacio físico asignado a cada laboratorio es el necesario para albergar el mobiliario y personal que ayudan a realizar las actividades del laboratorio.

- La mayoría del personal involucrado en las actividades del laboratorio tiene los conocimientos necesarios para mantener un nivel de seguridad básica.

CAPÍTULO 5

Propuesta

5.1 Introducción

La información es un activo muy valioso e importante para cualquier organismo. Es por ello que a través del tiempo ha crecido la necesidad de implementar medidas para mantener segura la información, a partir de este hecho surge un concepto muy importante en la actualidad: "Seguridad de la Información".

La seguridad de la Información tiene como objetivo preservar la:

- Confidencialidad, asegurando que sólo quienes estén autorizados pueden acceder a la información.
- Integridad, asegurando que la información y sus métodos de proceso son exactos y completos.
- Disponibilidad, asegurando que los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

Según la norma ISO/IEC 17799:2000, que es un código de buenas prácticas para la Gestión de la Seguridad de la Información, "la Seguridad de la Información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, procedimientos, estructuras organizativas y funciones de software. Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la Organización".

Una forma para mantener la seguridad de la información es a través de la implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) basado en el ciclo de Deming PDCA "Plan-Do-Check-Act (Planificar-Hacer-Verificar-Actuar)". Una norma internacional que sigue el modelo PDCA es la norma ISO/IEC 27001:2005 la cual es una guía para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un SGSI.

Para poder garantizar que el SGSI de cualquier organismo cumple con sus objetivos, es necesario que el SGSI sea evaluado y aprobado por un Organismo de Certificación, es decir, que el SGSI sea certificado.

La certificación es un proceso en el cual se demuestra que el sistema de gestión de un organismo ha cumplido con los requisitos establecidos en una norma nacional o internacional y por lo tanto sus procesos son confiables y competitivos.

El proceso de Certificación sólo puede llevarse a cabo por un Organismo de Certificación debidamente acreditado por un Organismo de Acreditación, el cual se encarga de evaluar si se cumplen con los requisitos establecidos tanto en normas internacionales como nacionales. En México existe un Organismo de Acreditación llamado EMA (Entidad Mexicana de Acreditación).

Actualmente existen una serie de normas enfocadas al proceso de la Seguridad de la Información conocida como la serie ISO/IEC 27000 dentro de las cuales destacan las siguientes:

- Norma ISO/IEC 27001:2005, norma auditable y certificable.
- Norma ISO/IEC 27002:2005, código de buenas prácticas para la Gestión de la Seguridad de la Información.

- Norma ISO/IEC 27006:2007, requisitos para los organismo que realizan actividades de auditoría y certificación de SGSI.

5.2 Antecedentes

La propuesta de crear un Organismo de Certificación bajo la norma ISO/IEC 27001:2005 de origen mexicano surge a través de la realización de un análisis de la situación actual en nuestro país en cuanto a las actividades de certificación bajo la norma ISO/IEC 27001, desarrollado en el Departamento de Ingeniería en Computación de la Facultad de ingeniería dentro del módulo de salida de Redes y Seguridad.

Hoy en día a nivel internacional el primer país con el mayor número de certificaciones bajo la norma ISO/IEC 27001:2005, según la página oficial "http://www.iso27001certificates.com", es Japón con 3321 certificaciones de Sistemas de Gestión de la Seguridad de la Información, México ocupa el lugar número 18 con 27 certificaciones ganándole a Brasil y a Colombia con 13 y 7 certificaciones respectivamente.

En México el número de organismos interesados en mantener la seguridad de la información, ha ido en aumento, por lo tanto ha crecido la demanda en cuanto a certificaciones bajo la Norma ISO/IEC 27001:2005, esto abre oportunidades para impulsar Organismos de Certificación de origen mexicano capaces de cubrir estas necesidades, ya que actualmente sólo existe en México un Organismo de Certificación de origen mexicano que incluye dentro de sus alcances la certificación bajo la norma ISO/IEC 27001:2005.

Un Organismo de Certificación debe brindar confianza y seguridad a todas aquéllas empresas que decidan obtener una certificación nacional o internacional. Estas características las encontramos en nuestra Máxima Casa de Estudios la "Universidad Nacional Autónoma de México" en conjunto con la Carrera de Ingeniería en Computación de la Facultad de Ingeniería, ya que sus antecedentes y su reconocimiento a nivel nacional e internacional la convierten en candidato para ser un Organismo de Certificación de la norma ISO/IEC 27001:2005.

La Facultad de Ingeniería es una institución comprometida con el desarrollo y avance de nuestro país, cuya misión está orientada a la formación de recursos humanos, la investigación y la difusión. Además, tiene como visión ser una institución líder en la formación de profesionales y la generación de nuevos conocimientos a través de la investigación con un impacto óptimo sin dejar atrás el aspecto cultural, humanista y ecológico; dentro de sus políticas contempla a la calidad, la seguridad, el orden y el liderazgo, entre otras.

5.3 Descripción de la Propuesta

5.3.1 Objetivo Final

Proponer que dentro de la Facultad de Ingeniería se instale o adecúe un laboratorio acreditado que realice actividades de certificación bajo la norma ISO/IEC 27001:2005(llamado en adelante solamente Laboratorio), para lograr que la Universidad Nacional Autónoma de México sea uno de los primeros organismos de esta naturaleza.

Para lograr este objetivo se necesitan cubrir los siguientes puntos por parte del Laboratorio:

A. Implementar un SGSI basado en el ciclo de Deming PDCA bajo la norma ISO/IEC 27001:2005
B. Acreditar el Laboratorio para que realice actividades de certificación bajo la norma ISO/IEC 27001:2005
C. Mantener la acreditación del Laboratorio y del SGSI

5.3.2 *Desarrollo de la propuesta*

Con el desarrollo de los tres puntos anteriores quedarán cubiertos los siguientes objetivos generales:

- Ser una organización legalmente constituida, este punto se omitirá por tratarse de una Facultad perteneciente a la Universidad Nacional Autónoma de México.
- Tener implementado un Sistema de Gestión de la Seguridad de la Información.
- Contar con personal calificado para sus actividades.
- Poseer una infraestructura acorde con las funciones que realizan.
- Cumplir con requisitos particulares según el alcance de sus actividades.

A. Implementación de SGSI

Como paso inicial es indispensable y fundamental que los altos directivos de la Facultad de Ingeniería en conjunto con la Carrera de Ingeniería en Computación, estén de acuerdo y comprometidos con el objetivo del Laboratorio.

Además de:

- Comprender el significado de un SGSI.
- Conocer profundamente los riesgos, los procesos afectados, los impactos y la probabilidad de ocurrencia.
- Justificar con un porqué de toda medida de seguridad.
- Establecer procesos de manera cíclica, por ejemplo el ciclo PDCA.
- Apoyarse en las normas de la serie ISO/IEC 27000.
- Establecer métricas ya que: “Lo que no se puede medir no se puede controlar y lo que no se puede controlar no se puede gestionar”.

Al tomar en cuenta los puntos antes mencionados, se logra el verdadero objetivo de un SGSI que es organizar las medidas de seguridad de acuerdo a los objetivos del Laboratorio, reducir los riesgos a niveles aceptables, cambiar el escenario actual del Laboratorio para convertirlo en un Laboratorio más seguro y mejor gestionado.

Para poder llevar a cabo esta tarea es importante contar con asesoría de gente especializada y con experiencia en implementación de un SGSI, pero es conveniente tener presente que solo van a recibir asesorías, ya que si todo el trabajo se deja en manos de los asesores se perderá el objetivo de la implementación y solo ellos tendrán consciencia de lo que han realizado y por lo tanto no se podrá dar seguimiento y mejorar al SGSI.

Cabe mencionar que existe una amplia gama de organismos que ofrecen sus servicios de asesoría y consultoría, los cuales pueden ser consultados a través de su página electrónica.

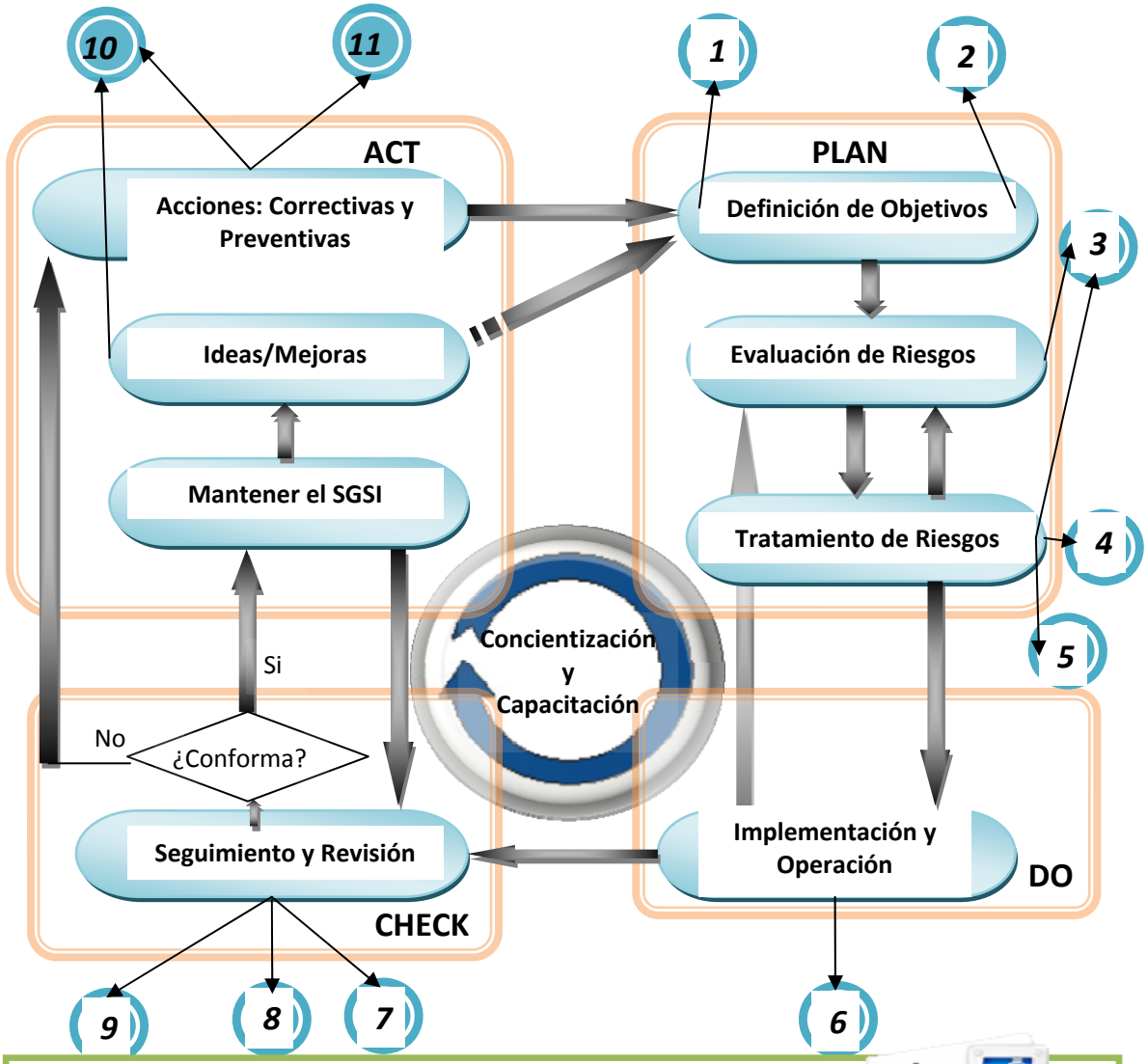
A continuación mencionamos los pasos a seguir para llegar al camino de la implementación del SGSI:

1. Obtener la norma ISO/IEC 27001:2005, para utilizarla como una plantilla guía para definir el SGSI y como una herramienta de mejora. Es conveniente familiarizarse con los requisitos y términos de la norma ISO/IEC 27001:2005.
2. Formar un equipo dedicado al desarrollo e implementación del SGSI.
3. Definir el tipo de capacitación que requieren los integrantes del equipo, con el objetivo de que conozcan con detalle los requisitos aplicables de la norma ISO/IEC 27001:2005. La capacitación puede llevarse a cabo a través de cursos, talleres y seminarios.
4. Elaborar un manual del SGSI, en el cual deberán estar plasmadas las políticas de seguridad, el alcance del SGSI y las operaciones del Laboratorio. A través del manual, se ofrecerá una descripción exacta del Laboratorio y las mejores prácticas adoptadas.
5. Elaborar procedimientos, los cuales describen los procesos del Laboratorio. Estos procedimientos deben tener el mismo formato y responder las siguientes cuestiones:

    - ¿Por qué?
    - ¿Quién?
    - ¿Cuándo?
    - ¿Dónde?
    - ¿Qué?
    - ¿Cómo?

6. Implementar el SGSI, en esta parte se trabajará con los procedimientos elaborados para documentar y demostrar la eficacia del SGSI.

En la fig. 5.1 presentamos una posible metodología que puede llevar a cabo el Laboratorio para la implementación del SGSI por medio del ciclo PDCA.



Entregables de la implementación del SGSI:

1. Alcance del SGSI.
2. Políticas de Seguridad y Objetivos de Control.
3. Reporte de Evaluación de riesgos.
4. Declaración de Aplicabilidad (SOA: The statement of applicability).
5. Indicadores.
6. Plan de tratamiento de riesgos.
7. Registros de cumplimiento y eficiencia.
8. Procedimientos para asegurar la planificación, operación y control de los procesos del Laboratorio.
9. Informe de auditoría.
10. Registros de los resultados de las acciones tomadas.
11. Procedimientos de acciones correctivas y preventivas.

Figura 5.1 Metodología para la implementación de un SGSI y la documentación generada

La documentación que debe existir en la implementación del SGSI del Laboratorio se muestra en la pirámide de 4 niveles de la figura 5.2.

Figura 5.2 Pirámide documental de un SGSI

Con estos 4 niveles de documentación se cubren los documentos (que pueden estar en cualquier formato o tipo de medio) que de manera específica la norma ISO/IEC 27001:2005 pide para la conformación de un SGSI. Estos documentos se muestran en la figura 5.3:

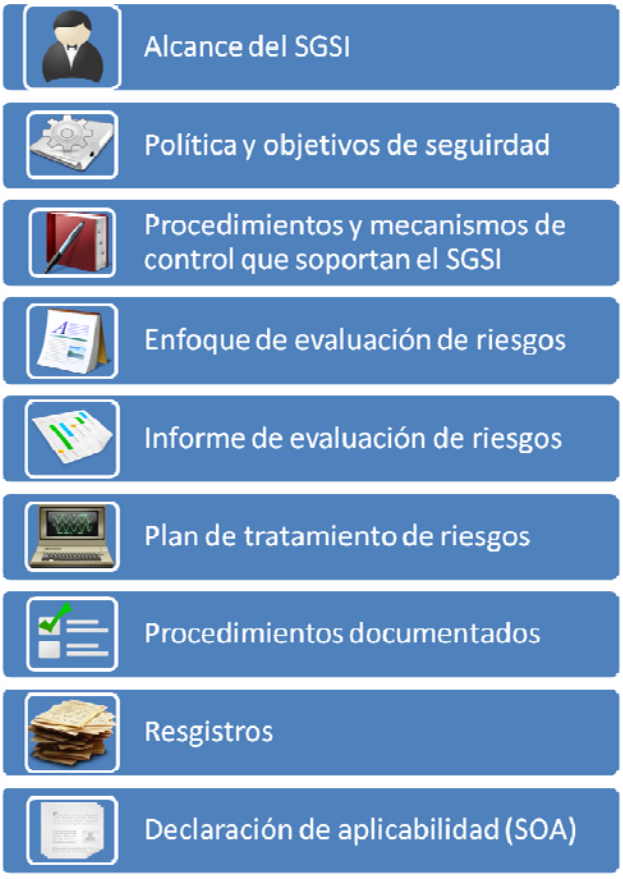


Figura 5.3 Documentos requeridos por la norma ISO/IEC 27001:2005

Una vez terminada la implementación del SGSI, se recomienda solicitar una visita de auditores externos al Laboratorio para realizar una primera evaluación cuyo objetivo es verificar si el SGSI tiene no conformidades (incumplimiento de algún requisito de la norma ISO/IEC 27001:2005) y si es así tomar las acciones correctivas o preventivas pertinentes para la mejora del SGSI.

Análisis de la Situación Actual del Laboratorio

En el capítulo 4. "Evaluación de la Facultad de Ingeniería" se realizó un análisis de los laboratorios y departamentos de la Carrera de Ingeniería en Computación de la Facultad de Ingeniería con la finalidad de elegir a un laboratorio con las características necesarias para llevar a cabo las actividades de acreditación y de certificación: el laboratorio que se consideró adecuado fue el Laboratorio de Redes y Seguridad debido al tipo de actividades que realiza y por ser parte del módulo de salida de Redes y Seguridad entre otras características, pero cabe destacar que también hay otros laboratorios, que es el Departamento de Seguridad en Cómputo de la Unidad de Cómputo Académico y la Salas de Cómputo (ambos pertenecientes a UNICA), capaces de cumplir con estas tareas.
En la tabla 5.1 se realiza un análisis del estado actual del Laboratorio para iniciar la implementación del SGSI:

Tabla 5.1 Análisis del estado actual del Laboratorio para iniciar la implementación del SGSI

DETALLE	RECOMENDACIONES
Normas	El Laboratorio deberá adquirir la norma ISO/IEC 27001:2005. El Laboratorio deberá adquirir la norma ISO/IEC 17799:2005 o la norma ISO/IEC 27002:2005, ya que ambas son la misma pero diferente versión y son normas de consulta para la implementación de controles.
Alcance y Limites	El Laboratorio deberá definir el alcance y los límites del SGSI, en términos de las características de la actividad del Laboratorio, de su organización, su ubicación, sus activos y tecnología, incluyendo los detalles y la justificación de cualquier exclusión del alcance
Políticas	El Laboratorio deberá redefinir su política de seguridad de acuerdo a las características establecidas en la norma ISO/IEC 27001:2005
Enfoque de Evaluación de riesgos	El Laboratorio deberá redefinir y documentar su metodología de evaluación de riesgos adecuada para su SGSI, esta metodología deberá asegurar que las evaluaciones de riesgo generen resultados comparables y reproducibles
En cuanto a riesgos	El Laboratorio deberá realizar las siguientes acciones de acuerdo a la norma ISO/IEC 27001:2005 en conjunto con la norma ISO/IEC 27002:2005: • Identificar los riesgos. • Analizar y valorar los riesgos. • Identificar y Evaluar las opciones para el tratamiento de riesgos. • Seleccionar los objetivos de control y los controles para el tratamiento de riesgos. • Obtener la aprobación, por parte de la Dirección de los riesgos residuales propuestos.
Aprobación de la Dirección	El Laboratorio deberá obtener la autorización de la Dirección para implementar y operar el SGSI

Declaración de Aplicabilidad (SOA)	El Laboratorio deberá realizar una Declaración de Aplicabilidad la cual deberá contener los objetivos de control y los controles contemplados por el SGSI basados en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.
Registros y Procedimientos Documentados	El Laboratorio deberá documentar todos los procedimientos necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implementados. Los registros son documentos del Laboratorio que deberán proporcionar evidencia de la conformidad con los requisitos y funcionamiento eficaz del SGSI.
Recursos Materiales y Tecnológicos	El Laboratorio actualmente no cuenta con espacio físico disponible, ya que el espacio destinado al Laboratorio es reducido y éste está dedicado al uso académico (ver figura 5.4), por lo que, el Laboratorio deberá adecuar (ampliar o construir) un espacio físico disponible para equiparlo con los recursos materiales (mesas, sillas, módulos de trabajo, archiveros, etc.) necesarios para que el equipo encargado de la seguridad de la información lleve a cabo las actividades de implementación de un SGSI y para llevar a cabo las actividades de acreditación. El Laboratorio deberá adquirir el equipo tecnológico (PC's, Switch, Servidores, No-breaks, Notebooks, etc.) necesario para las actividades de implementación del SGSI. Todos estos cambios y adecuaciones deberán estar guiados por los requisitos de la norma ISO/IEC 27001:2005 en el apartado de Gestión de Recursos.
Recursos Humanos	El Laboratorio cuenta solo con una administradora, cinco profesores y tres alumnos de servicio social, por lo que el Laboratorio deberá: • Reclutar por lo menos a cuatro personas más capaces de realizar actividades de implementación de un SGSI. • Capacitar al personal del Laboratorio para que tengan un conocimiento profundo sobre los requisitos de la norma ISO/IEC 27001:2005 y sobre auditorías internas del SGSI. Además, para realizar actividades de certificación. • Redefinir responsabilidades y obligaciones en el equipo de trabajo en cuanto a la Gestión de la Seguridad de la Información. • De ser necesario, el Laboratorio deberá incrementar el número de personas para la realización de actividades antes mencionadas.
Recursos Financieros	El Laboratorio debe obtener los recursos financieros necesarios para sufragar los gastos para ampliar o construir el espacio físico requerido, así como el equipamiento (recursos materiales y tecnológicos) de éste para tener un lugar de trabajo y poder llevar a cabo la implementación del SGSI en el Laboratorio, y así cumplir con los requisitos de la norma ISO/IEC 27001:2005. Además parte de estos recursos financieros deberán estar destinados a los recursos humanos (capacitación, honorarios, etc.) y asesorías externas requeridas.

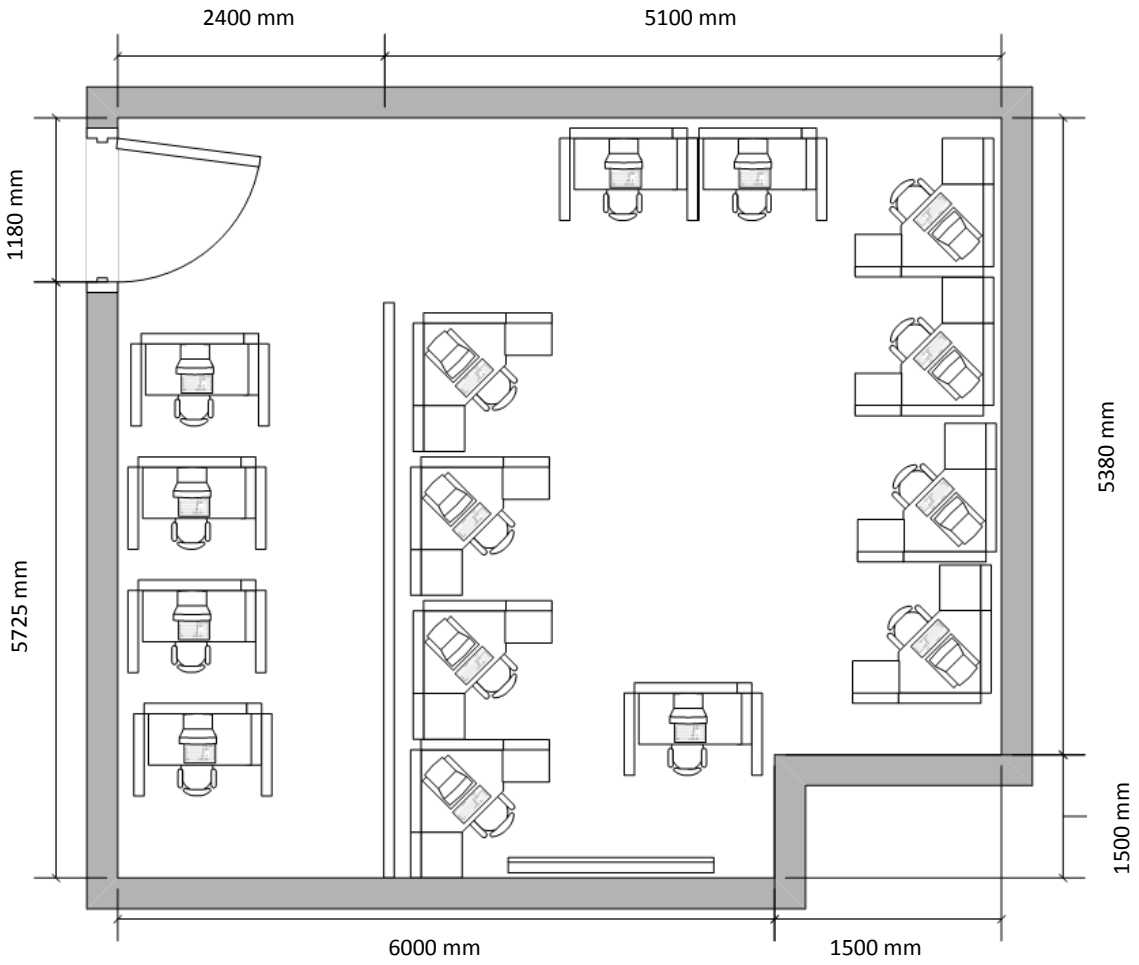


Figura 5.4 Espacio físico asignado al Laboratorio de Redes y Seguridad

Como parte final de la implementación del SGSI es importante mencionar que este proceso de implementación tiene un tiempo aproximado de 12 meses.

B. Acreditación del Laboratorio

Después de haber implementado el SGSI en el Laboratorio con un historial demostrable de al menos tres meses, se puede pasar a la etapa de acreditación del Laboratorio.

Como se menciono anteriormente en México hay un Organismo de Acreditación llamado EMA el cual no incluye a la norma ISO/IEC 27001:2005 dentro de sus alcances, sin embargo, en respuesta a una petición que se les hizo sobre este tema, enviaron lo siguiente:

“La Entidad Mexicana de Acreditación A.C. aun no cuenta con el programa para la acreditación en Sistemas de Gestión de la Seguridad de la Información, este programa será implementado una vez que algún Organismo de Certificación solicite la acreditación bajo este esquema”.

Por lo que esto proporciona una oportunidad para iniciar el proceso de acreditación.

Para empezar el proceso de acreditación, el Laboratorio debe contar con la norma ISO/IEC 27006:2007 que deberá complementarse con la norma ISO/IEC 17021:2006 las cuales son requisitos que deben cumplir los organismos de certificación, estas normas pueden adquirirse en línea a través de la página web:

“http://www.iso.org/iso/search.htm?qt=27006&published=on&active_tab=standards”

Como paso inicial el Laboratorio deberá ingresar a la página web oficial de EMA (http://www.ema.org.mx/), en donde encontrará y conocerá a fondo su proceso de acreditación, el contrato de prestación de servicios del Organismo de Acreditación, requisitos, documentación a entregar, derechos y compromisos que se adquieren antes y después de la acreditación, además del tiempo y costos necesarios para el proceso de acreditación.

En la página web oficial de EMA se encuentra publicado su proceso de acreditación el cual se muestra en la figura 5.5

Figura 5.5 Proceso de acreditación de EMA

Después de leer esta documentación y estar consciente de los requisitos, tiempo y costos del proceso de acreditación, la Dirección y el equipo de trabajo del Laboratorio iniciarán una declaración de intención de acreditación del Laboratorio con la cual todo el personal y la Dirección se comprometen hasta el final de este proceso.

I. Solicitud de acreditación

De acuerdo con el proceso de acreditación de EMA el primer paso es la solicitud de acreditación en la cual el Laboratorio deberá anexar de los siguientes documentos, formando un total de doce anexos:

- Anexo A: Acta Constitutiva, la cual identifica la personalidad jurídica del Laboratorio o de la organización a la que pertenece y relación de la persona o personas físicas o jurídicas que ostentan su propiedad.
- Anexo B: Matriz (Tabla cruzada) de las clausulas de la norma ISO/IEC 17021 e ISO/IEC 27006:2007 con los documentos que demuestren cumplimiento de las mismas.
- Anexo C: Evidencia objetiva de la integración de la estructura técnica funcional (Comité) en la que estén representadas todas las partes significativamente involucradas en el proceso de certificación, incluyendo lista con los nombres de los miembros que la integran, indicando claramente el sector (p.e. industria, consumidor, etc.) al que representan, así como las reglas de funcionamiento de dicha estructura.
- Anexo D: Organigrama que refleje la estructura interna del Laboratorio. En el caso de que el Laboratorio forme parte de una organización superior, señalar claramente las líneas de dependencia entre el Laboratorio y dicha organización.
- Anexo E: Lista de las personas responsables del funcionamiento del Laboratorio.
- Anexo F: Lista actualizada de los documentos del SGSI.
- Anexo G: Procedimientos relacionados con la actividad de certificación, por ejemplo:
  - Gestión de solicitudes.
  - Realización de auditorías de certificación.
  - Criterios para la designación y calificación de auditores.
  - Toma de decisiones de concesión o no de la certificación.
  - Tratamiento de reclamaciones.
  - Utilización de certificados, marcas de conformidad, logotipos, etc.
  - Procedimientos para la supervisión de las certificaciones concedidas.
  - Procedimientos de subcontrataciones y listado actual de subcontratistas.
- Anexo H: Lista de los auditores disponibles indicando los sectores para los que están calificados.
- Anexo I: Copia controlada del Manual de Seguridad asignada a EMA y procedimientos relacionados.
- Anexo J: Lista de todas las certificaciones concedidas. En caso de no haber expedido alguna certificación, debe ingresar un escrito en el que se declare esta situación y la disponibilidad de contar con un cliente potencial para continuar con el proceso.
- Anexo K: Otros documentos que el Laboratorio considere pertinentes, por ejemplo requisitos de convocatorias.
- Anexo L: Comprobante de pago por apertura de expediente.

Cabe recordar que estos documentos deben ser realizados de acuerdo a lo establecido en las normas ISO/IEC 27006:2007 e ISO/IEC 17021:2006.

En la tabla 5.2 se hace una relación entre los anexos que se requieren en la solicitud de acreditación publicada en la página web de EMA y las acciones que deberá realizar el Laboratorio para el cumplimiento de estos requisitos.

Tabla 5.2 Acciones o medidas del Laboratorio para cumplir con los anexos de la solicitud de EMA

Anexo	Documentos	Acciones
A	Acta constitutiva	El Laboratorio deberá conocer la situación jurídica actual de la Facultad de Ingeniería
B	Matriz (Tabla cruzada)	El Laboratorio deberá elaborar una matriz relacionando los requisitos de la norma ISO/IEC 27006:2007 con los documentos que indiquen el cumplimiento de estos
C	Evidencia objetiva de la integración de la estructura técnica funcional (Comité)	El Laboratorio deberá crear un Comité encargado de mantener la imparcialidad de sus actividades relativas a la certificación y deberá presentar los documentos que avalen la formación de este comité
D	Organigrama	El Laboratorio deberá realizar un organigrama de su estructura organizacional incluyendo todas sus dependencias
E	Lista de las personas responsables	El Laboratorio deberá elaborar una lista que incluya a los responsables del funcionamiento del Laboratorio
F	Lista actualizada de los documentos del SGSI	El Laboratorio deberá elaborar una lista de los documentos generados en la implementación del SGSI
G	Procedimientos relacionados con la actividad de certificación (Requisitos de la norma ISO/IEC 27006:2007)	El Laboratorio deberá definir un Proceso de Certificación, mediante el cual certificará o evaluará a los Organismos Solicitantes.
		El Laboratorio deberá contar con procesos y recursos necesarios para determinar la competencia de los auditores y del personal
H	Lista de auditores	El Laboratorio deberá contar con los auditores adecuados para la realización de las auditorías de certificación y deberá elaborar una lista de los nombres de dichos auditores
I	Copia controlada del Manual de Seguridad	El Laboratorio deberá entregar el Manual de seguridad y los procedimientos relacionados generados en la implementación del SGSI
J	Lista de las certificaciones concedidas	El Laboratorio no ha concedido certificaciones por lo que deberá presentar un escrito en el que declare esta situación y también deberá contar con un cliente potencial.
K	Otros documentos	El Laboratorio podrá entregar cualquier documento que sea considerado evidencia objetiva de algún proceso
L	Comprobante de pago	Una vez que el Laboratorio haya solicitado su acreditación deberá pagar su apertura de expediente de acuerdo a las tarifas de EMA y presentar los comprobantes del pago

Después de llenar la solicitud de acreditación el Laboratorio entregará a EMA esta solicitud anexando los documentos requeridos. EMA decidirá si se puede llevar a cabo la evaluación del Laboratorio notificándole esta decisión en un plazo de 5 días hábiles, sin embargo, EMA aún no cuenta con el esquema de acreditación bajo la norma ISO/IEC 27001:2005, por lo que la notificación llegará en un plazo de 15 días hábiles.

II. Revisión Documental

Una vez entregada la solicitud y al haber aceptado EMA evaluar el Laboratorio, EMA pasará a la siguiente etapa la cual consta de revisar la documentación entregada por el Laboratorio. La revisión documental se considerará concluida cuando EMA haya comprobado que la solicitud de acreditación del Laboratorio, está completa y correctamente requisitada, además, que el pago correspondiente se ha realizado.

En caso de que falte algún documento o que esté incorrecta la solicitud, el Laboratorio será informado por medio de un escrito en el que se indicarán los puntos que deben cumplirse en un plazo no mayor a 60 días.

III. Designación del grupo evaluador

Una vez concluida la revisión documental, se pasará a la siguiente etapa la cual consiste en designar y notificar al Laboratorio los nombres de los miembros del grupo evaluador, el cual se encargará de la evaluación documental, de la evaluación en sitio y de la evaluación de seguimiento en caso de requerirse.

El proceso de designación del grupo evaluador deberá llevarse en un periodo máximo de 8 días hábiles.

IV. Evaluación documental

En esta etapa se lleva a cabo la evaluación documental, la cual consiste en la evaluación de los procedimientos técnicos y del SGSI documentados con base en la (s) norma (s) aplicable (s) y sujetas al alcance de la acreditación, con el fin de determinar que el Laboratorio cuenta con los elementos necesarios para una evaluación en sitio. La evaluación documental puede llevarse a cabo en las instalaciones del Laboratorio, en las oficinas de EMA o en las oficinas del evaluador.

La evaluación documental se llevará a cabo en un plazo máximo de 15 días hábiles y el resultado de esta evaluación se notificará al Laboratorio en un plazo de 2 días hábiles.

En caso de existir una o más no conformidades en la evaluación documental, el Laboratorio recibirá un documento con las no conformidades, las cuales deberán ser corregidas satisfactoriamente en un plazo no mayor a los 90 días hábiles (3 meses), después de que EMA reciba estas acciones correctivas, el grupo evaluador deberá revisarlas en un periodo de 10 días hábiles.

V. Preparación de la evaluación en sitio

Una vez dada por concluida la etapa de evaluación documental, EMA preparará todo lo necesario para llevar a cabo la evaluación en sitio. El Laboratorio será informado de la fecha en que se llevará a cabo la evaluación en sitio y el plan de esta evaluación durante los próximos 5 días hábiles después de haber concluido la etapa anterior, y el Laboratorio deberá confirmar a EMA durante los 5 próximos días hábiles después de la notificación.

La etapa de la preparación de la evaluación en sitio tiene una duración estimada de 15 días hábiles y el objetivo principal de esta etapa es lograr un acuerdo entre EMA y el Laboratorio sobre la fecha en la que se llevará a cabo la evaluación en sitio.

VI. Evaluación en sitio

Una vez acordada la fecha de la evaluación en sitio, se pasa a la siguiente etapa en la que el grupo evaluador se encargará de evaluar en las instalaciones del Laboratorio el sistema de gestión y técnico para verificar que se cumple con los requisitos de las normas ISO/IEC 27006:2007 e ISO/IEC 27001:2005.

Al final de la evaluación en sitio el grupo evaluador entregará al Laboratorio un informe final en el cual se detallará el estado en el que se encuentra el sistema de gestión y técnico, así como la operación del mismo, en caso de que se hayan encontrado no conformidades éstas se detallaran en el informe, al igual que el periodo en el cual el Laboratorio deberá corregir estas no conformidades (acciones correctivas), que en este caso será de 60 días hábiles.

Al día siguiente de la entrega de las acciones correctivas se iniciará la etapa de revisión de acciones correctivas y empieza el periodo para realizar la dictaminación.

VII. Dictaminación

En esta etapa EMA decidirá si otorga o niega la acreditación al Laboratorio, por lo que al Laboratorio solo le resta esperar esta decisión, la cual le será enviada en un periodo no mayor a los 32 días hábiles.

Una vez informado el dictamen del Comité de Evaluación, el Laboratorio debe atender los requisitos para continuar con el trámite de acreditación correspondiente.

Visita de testificación

Antes de que EMA otorgue la acreditación inicial al Laboratorio ésta deberá testificar las actividades en sitio de una o más auditorias o evaluaciones dirigidas por el Laboratorio. Esta visita de testificación deberá realizarse dentro de los próximos 180 días naturales después de la notificación de acreditación. La planeación de la visita de testificación es de 15 días hábiles.

Al término de la visita de testificación el grupo evaluador recibirá un informe de la auditoría o evaluación realizada por el Laboratorio, el cual será evaluado por el grupo evaluador quien entregará a EMA un reporte final con las observaciones y no conformidades encontradas, el

tiempo para entregar este informe es de 10 días hábiles a partir de que el grupo evaluador haya recibido el informe de auditoría por parte del Laboratorio.

En caso de que se encuentren no conformidades se definirá el periodo en el que el Laboratorio deberá corregirlas, que por tratarse de una evaluación inicial este periodo será de 60 días hábiles.

Revisión de acciones correctivas

Esta etapa del proceso de acreditación es generada si en la evaluación en sitio o visita de testificación se encuentran no conformidades y el tiempo de revisión de las acciones correctivas es de 15 días hábiles.

VIII. Seguimiento

Las evaluaciones de seguimiento se realizarán cuando:

- Se reciban en EMA quejas o reclamaciones de la actuación del Laboratorio.
- Cuando se notifique a EMA cambios en el Laboratorio.
- Cuando se quiera verificar que han ocurrido cambios no informados en el Laboratorio.
- Después del retiro de una suspensión.
- Cuando el Comité Evaluador requiera corroborar la implementación de alguna acción correctiva de manera anticipada.

El seguimiento podrá realizarse de manera documental o a través de una evaluación en sitio y este proceso deberá llevarse a cabo en un periodo no mayor a 60 días hábiles y el Laboratorio deberá cubrir los gastos correspondientes a este proceso.

Las vistas de monitoreo del desempeño del Laboratorio se realizarán sin previo aviso y se notificaran máximo tres días antes de la realización de la evaluación de monitoreo. Estas evaluaciones no tendrán ningún costo para el Laboratorio.

IX. Concesión de la acreditación

Tras una decisión favorable, EMA emitirá un Certificado de Acreditación, que atestigüe la concesión de la acreditación a favor del Laboratorio firmado por el presidente de EMA.

En dicho certificado se expresarán específicamente los puntos siguientes como mínimo:

- El nombre del Laboratorio y el número de la acreditación concedida.
- Alcance de la acreditación concedida.
- La fecha de entrada en vigor de la acreditación y la vigencia de la misma.

Este documento es propiedad de EMA y por lo tanto está bajo su control. Por lo que, no podrá ser modificado si no es por EMA.

X. Vigilancia

Finalmente el proceso concluye con esta etapa la cual consiste en la evaluación del Laboratorio para verificar que se mantengan las condiciones bajo las cuales se concedió la acreditación.

Estas evaluaciones se realizarán en plazo que va de los 10 a los 14 meses después de entrar en vigencia la acreditación del Laboratorio

A continuación en la tabla 5.3 se detallan los tiempos máximos requeridos para cada etapa del proceso de acreditación, por lo que estos tiempos pueden reducirse dependiendo de las respuestas por parte del Laboratorio, además de considerarse todos los escenarios posibles.

Tabla 5.3 Tiempos máximos requeridos para cada etapa del proceso de acreditación

Etapa	días hábiles	días naturales
Ingreso de solicitud		
Recopilación de la documentación	30	
Aceptación de solicitud y revisión de documentos	15	
Revisión documental		
Revisión de los documentos y solicitud	3	
Plazo para entregar documentos faltantes	60	
Designación del grupo evaluador		
Designación del grupo evaluador	8	
Evaluación documental		
Evaluación documental	15	
Informe de la evaluación documental	2	
Corrección de no conformidades encontradas en la evaluación documental	90	
Evaluación de acciones correctivas	10	
Preparación de la evaluación en sitio		
Informe de plan de evaluación en sitio	5	
Respuesta por parte del Laboratorio	5	
Otros trámites	5	
Evaluación en sitio		
Entrega de acciones correctivas	60	
Dictaminación		
Dictaminación por parte de EMA	32	
Planeación de la visita de testificación	15	
Visitas de testificación		180
Informe de la auditoría realizada por el Laboratorio	10	
Entrega de acciones correctivas	60	
Revisión de acciones correctivas	15	
Total	**440**	**180**

En la tabla 5.3 podemos observar que el tiempo requerido para que el laboratorio se acredite es de aproximadamente 440 días, es decir, aproximadamente un año y seis meses, sin incluir la visita de testificación la cual se realiza después de que EMA dictamine a favor de la acreditación del Laboratorio.

Cabe mencionar que el tiempo estimado en la tabla 5.3 es desde que se inicia el proceso de acreditación con la solicitud, por lo que aquí no se considera el tiempo de selección, reclutamiento y capacitación del personal, además de las adecuaciones que se consideren necesarias al Laboratorio.

C. Mantenimiento de la acreditación

Es importante mencionar que una vez concedida la acreditación al Laboratorio, este deberá iniciar el proceso completo de evaluación para re-evaluar las condiciones bajo las cuales se concedió la acreditación. Este proceso deberá llevarse a cabo antes de que se cumplan cuatro años posteriores a la fecha de inicio de vigencia de la acreditación del Laboratorio.

5.4 Tiempo y Costos

Como parte final de esta propuesta se incluirán el tiempo estimado y los costos necesarios para el desarrollo de este proyecto.

A) Tiempo

El tiempo aproximado para los procesos de implementación y acreditación se muestran en la tabla 5.4, estos tiempos son aproximados ya que pueden variar dependiendo de la rapidez de los procesos y de la disponibilidad de los recursos, entre otros factores.

Tabla 5.4 Tiempo aproximados para la implementación del SGSI y el proceso de acreditación del Laboratorio

Fase	***Tiempo estimado [mes]***
Planeacion del SGSI	5
Implementación del SGSI	3
Mantenimiento del SGSI	4
Planeacion de la acreditación	3
Proceso de acreditación	18
Mantenimeinto de la acreditación	48
Tiempo Total	**81**

En la tabla 5.4 se puede observar que la duración total del proyecto es de 81 meses (6 años y 9 meses), pero hay que tomar en cuenta que el proceso de Mantenimiento de la acreditación incluye la re-evaluación el cual inicia antes de haberse cumplido 4 años después de haberse concedido la acreditación, por lo que el proceso de implementación del SGSI y el de acreditación implicarían un tiempo total aproximado de 33 meses (2 años con nueve meses).

B) Costos

Para llevar a cabo la implementación del SGSI y el proceso de acreditación del Laboratorio es indispensable tener en cuenta la inversión mínima requerida, la cual se detalla en la tabla 5.5 y esta tabla contempla costos al mes de febrero de 2010.

Tabla 5.5 Costos aproximados para la implementación del SGSI y el proceso de acreditación del Laboratorio

DETALLE	COSTO APROXIMADO [MXN]
Norma ISO/IEC 27001:2005	$ 554.00
Norma ISO/IEC 27002:2005 (ISO/IEC 17799:2000)	$ 848.82
Norma ISO/IEC 27006:2007	$ 1,666.00
Norma ISO/IEC 17021:2006	$ 1,373.00
Capacitación	$ 160,000.00*
Apertura de expediente para el proceso de acreditación	$ 54,526.00
TOTAL	**$ 218,967.82**

*Este costo contempla los cinco cursos mínimos indispensables que deben tomar los integrantes del equipo responsable de llevar a cabo el proceso de implementación del SGSI y acreditación del Laboratorio, en la tabla 5.6 se listan estos cursos y el perfil de los integrantes que deben tomar los cursos.

Tabla 5.6 Cursos mínimos e indispensables para el equipo responsable de la implementación del SGSI y acreditación del Laboratorio

Curso	Dirigido a	Objetivo	Recomendación del personal que puede tomar el curso
Fundamentos de SGSI	Directores y responsables de la protección y seguridad de los Sistemas de Información del Laboratorio	Comprender e interpretar los conceptos básicos de las normas ISO/IEC 27001 e ISO/IEC 27002	1 Directivo, 1 Líder de proyecto y 3 Responsables del SGSI
Implementación un SGSI	Personal técnico responsable de implementar las acciones necesarias para asegurar la protección y seguridad de los sistemas de Información	Conocer y aplicar los métodos y procesos del SGSI, así como, aprender a realizar las acciones que permitan implementarlo	1 Líder de proyecto y 3 Responsables del SGSI
Gestión de Riesgos de la Información	Responsables, consultores e implementadores de la gestión de la Seguridad de la Información	Adquirir la capacidad para realizar y planificar una identificación y valoración de riesgos de un SGSI conforme a la norma ISO/IEC 27001	1 Líder de proyecto y 3 Responsables del SGSI

Curso	Dirigido a	Objetivo	Recomendación del personal que puede tomar el curso
Metodología de auditores internos de SGSI	Directores de Seguridad, Técnicos, Auditores y Profesionales familiarizados con las normas ISO/IEC 27001 e ISO/IEC 27002	Adquirir los conocimientos necesarios para la planificación y realización del SGSI y conocer el proceso de certificación	1 Líder de proyecto y 3 Responsables del SGSI
Formación de auditor líder de SGSI	Directores de Seguridad, Técnicos, Auditores y Profesionales familiarizados con las normas ISO/IEC 27001 e ISO/IEC 27002	Adquirir los conocimientos necesarios para la planificación y realización del SGSI y conocer el proceso de certificación y conocer las funciones y las actividades que debe adoptar un auditor en Seguridad de la Información, así como, aprender a identificar y redactar no conformidades	3 Responsables del SGSI

Es recomendable tomar los cursos de acuerdo al orden en que aparecen en la tabla 5.6, ya que de esta manera se van cumpliendo los requisitos solicitados por cada curso.

Cabe mencionar que la información mostrada en la tabla 5.5 no incluye la inversión total del proyecto ya que para esto es necesario tomar en cuenta los gastos requeridos para cubrir los puntos de la tabla 5.1 y de otros gastos que surgirán durante el desarrollo del proyecto.

Algunos de estos gastos necesarios para llevar a cabo las actividades de implementación, acreditación y certificación de SGSI's, que por la naturaleza de estos (ya que dependen de las decisiones que se vayan tomando a los largo del desarrollo del proyecto), no podemos contabilizarlos, pueden ser:

- Construir, ampliar o adecuar un espacio físico.
- Equipar con recursos materiales y tecnológicos (mesas, sillas, escritorios, archiveros, PC's, switch, servidores, software, etc.).
- Reclutamiento y contratación de personal y asesoramiento externo.
- Sueldos y honorarios.
- Visitas de auditoría, evaluación y seguimiento (sueldos y viáticos).
- Capacitación adicional.
- Entre otros.

CONCLUSIONES

Conclusiones

Conclusiones:

En México hay varios Organismos de Certificación, la mayoría de origen extranjero, pero muy pocos están enfocados a la certificación relacionada con la seguridad de la información, verificándose que aún no hay un Organismo de Certificación de origen mexicano que certifique bajo la norma ISO/IEC 27001 ya que actualmente la Entidad Mexicana de Acreditación (EMA), que es el organismo que se encarga de acreditar a los Organismos de Certificación en México, no incluye dentro de sus alcances a la norma ISO/IEC 27001 debido a que ningún Organismo de Certificación ha solicitado la acreditación bajo esta norma, lo que nos da una oportunidad para proponer que en México exista un Organismo Certificador de esta naturaleza.

La UNAM es una institución con reconocimiento a nivel nacional e internacional por lo que en conjunto con algún laboratorio de la Carrera de Ingeniería en Computación de la Facultad de Ingeniería son idóneos para convertirse en un Organismo de Certificación de la norma ISO/IEC 27001 impactando en el desarrollo óptimo del país y de la universidad misma.

En los laboratorios de la Carrera de Ingeniería en Computación de la Facultad de Ingeniería existe una consciencia sobre la seguridad de la información ya que éstos han implementado diferentes métodos y técnicas de seguridad de acuerdo a sus necesidades y actividades, por lo que facilita la realización del proyecto. El laboratorio de Redes y Seguridad es el más apto para llevar a cabo las actividades de Certificación ya que en un análisis realizado en el capítulo 4 tuvo la puntuación más alta pero también influye la experiencia y conocimiento del personal que colabora en éste sobre temas de seguridad así como las actividades de docencia que se realizan. Pero para llevar a cabo este proyecto es necesario obtener recursos tecnológicos, materiales y financieros ya que estos son insuficientes para las necesidades del proyecto, además de los recursos humanos que se necesita contratar y capacitar.

Para llevarse a cabo el proceso de acreditación, es necesario que se involucre todo el personal relacionado con el laboratorio, desde los directivos hasta los colaboradores de servicio social. Todos deben estar conscientes de que la seguridad de la información es responsabilidad de todos y todos deben colaborar para mantenerla, otra parte muy importante es el compromiso el cual debe formalizarse a través de un escrito.

En la elaboración de este proyecto es recomendable que la toma de decisiones las realice la dirección en conjunto con personas de un amplio conocimiento en el tema además de su experiencia (autoridad ganada por expertos) pertenecientes a la Facultad de Ingeniería.

Una parte importante y fundamental en el desarrollo de este proyecto es el proceso de certificación ya que en él se deben definir los procedimientos y criterios para realizar las actividades de Certificación del Laboratorio procurándose los recursos requeridos por la norma ISO/IEC 27006.

Cabe mencionar, que un asesor experto externo en la implementación del SGSI del Laboratorio puede ser el Departamento de Seguridad en Cómputo, ya que éste es un organismo que ha sido certificado de acuerdo a la norma ISO/IEC 27001 por la EQA, por lo que cuenta con la experiencia y conocimiento en el tema.

Por otra parte, con la presente tesis nos dimos cuenta que una parte fundamental en el desarrollo del proyecto corresponde al factor humano y la disposición de éste, ya que el proyecto puede durar aproximadamente tres años en implementarse y los beneficios no se verán reflejados hasta la culminación del mismo.

Además, para el proceso de acreditación y certificación, los auditores forman una parte muy importante, ya que son ellos los encargados de evaluar los Sistemas de Gestión de la Seguridad de la Información, así como, detectar debilidades y fortalezas del SGSI implementado.

Los beneficios a largo plazo de este proyecto son muchos. Una vez lograda la acreditación del Laboratorio, éste puede mantenerse por sí solo, ya que al realizar actividades de Certificación puede obtener recursos financieros que le ayuden a recuperar los costos de la inversión y también sufragar los gastos posteriores.

Otro de los beneficios que se puede obtener con la realización de este proyecto es la posibilidad de certificar a la Unidad de Servicios de Cómputo Administrativos (USECAD), ya que por el papel que tiene dentro de la Facultad de Ingeniería cuenta con información sensible y de mucha importancia, y su certificación le dará a la Facultad de Ingeniería más confianza en sus procesos de administración escolar.

También, este proyecto nos abre una oportunidad para empezar a generar recursos humanos con los conocimientos necesarios para la realización de auditorías e implementación de un SGSI y así colocarse en diferentes empresas. Para lograrlo, es necesario crear programas de capacitación para luego implementarlos en los programas de estudio.

Conjuntamente, en un futuro pueden implementarse otras certificaciones como la relativa a la certificación de auditores.

Finalmente, esperamos que la presente tesis sea tomada en cuenta por los directivos de la Facultad de la Ingeniería para llevar a cabo el proyecto que se propone en la misma y de esta manera nuestra máxima casa de estudios se convierta en un Organismo de Certificación bajo la norma ISO/IEC 27001:2005, siendo un ejemplo a seguir para otras empresas.

Confiamos que nuestro trabajo sea una guía para todos aquellos interesados en salvaguardar la información haciendo uso de las normas internacionales.

GLOSARIO

Glosario

A

Acción Correctiva:
Acción para eliminar la causa de una no conformidad detectada con el fin de prevenir su repetición.

Acción Preventiva:
Medida orientada a prevenir potenciales no-conformidades.

Acreditación:
Es el reconocimiento formal y público por un organismo imparcial y de tercera parte, de la competencia técnica y confiabilidad, de esta forma el Organismo de la Evaluación de la Conformidad recibe un reconocimiento del trabajo realizado correctamente y de acuerdo a una norma apropiada y reconocida internacionalmente.

Activo:
Cualquier bien que tiene valor para la organización.

Alcance:
Ámbito de la organización que queda sometido al SGSI. Definir los límites del trabajo y partes de un proyecto.

Amenaza:
Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos:
Utilización sistemática de la información disponible para identificar peligros y estimar los riesgos.

Auditor Líder:
Auditor responsable de asegurar la conducción y realización eficiente y efectiva de la auditoría, dentro del alcance y del plan de auditoría aprobado por el cliente.

Auditor:
Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área en particular.

Auditoría:
Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio justificado sobre el estado y efectividad de un sistema de gestión de una organización.

Auditoría Interna:
Constituye una función de evaluación que existe en el seno de una organización y bajo la autorización de la dirección con el ánimo de examinar y evaluar las actividades de la organización. Ésta se lleva a cabo con personas pertenecientes a la misma organización.

Auditoría Externa:
Constituye una función de evaluación externa a la organización que se examina. Los profesionales que realizan esta auditoría no forman parte de la organización auditada, es decir son totalmente independientes de la organización y de sus cuadros directivos.

C

Certificación:
Es la confirmación de que una organización ha establecido un sistema de gestión conforme a ciertos requisitos.

Certificado:
Documento expedido por un Organismo de Certificación u Organismo de Acreditación de acuerdo con su proceso de evaluación.

Confidencialidad:
Aseguramiento de que la información es accesible solo para aquellos autorizados a tener acceso.

Control:
Las políticas, procedimientos, prácticas y estructuras organizativas realizadas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Criterio:
Norma para juzgar, estimar o conocer. Juicio o discernimiento. Los criterios deben aplicarse para cada uno de los parámetros y estándares dentro de su respectiva categoría de análisis.

D

Declaración de Aplicabilidad (Statement Of Applicability, SOA):
Declaración documentada que describe los objetivos de control y los controles que son relevantes para el SGSI de la organización y aplicables al mismo.

Disponibilidad:
Aseguramiento de que los usuarios autorizados tienen acceso cuando lo requieran a la información y sus activos asociados.

Documento de Certificación:
Documento que indica que el SGSI y cualquier documentación complementaria prevista en el sistema de la organización cliente, cumple con lo establecido en una norma referente a los SGSI.

E

Eficacia:
Virtud, actividad, fuerza y poder para obrar.

Eficaz:
Se refiere a la descripción o forma de enunciar adecuadamente los requisitos que se deben cumplir, la forma en que se debe proceder y/o las metas por alcanzar.

Eficiencia:
Virtud y facultad con que se logra un objetivo determinado.

Eficiente:
Comprueba que las normas establecidas, los procesos que se llevan a cabo y las metas alcanzadas son las idóneas, han cumplido con los objetivos planteados y han logrado los mejores resultados, haciendo uso óptimo de los recursos.

Estándar:
Lo que sirve como tipo, modelo, norma, patrón, nivel o referencia. Elemento de referencia, previamente establecida, de naturaleza cualitativa.

Estimación de Riesgos:
El proceso de comparación del riesgo estimado con los criterios de riesgo, para así determinar la importancia del riesgo.

Evaluación de la Conformidad:
Cualquier actividad cuyo objeto es determinar directa o indirectamente si se cumplen los requisitos especificados relativos a un producto, proceso, sistema, persona u organismo. La evaluación de la conformidad incluye actividades tales como: muestreo, ensayo, inspección, certificación, así como la acreditación de organismos de evaluación de la conformidad.

Evaluación de riesgos:
Proceso de evaluación de las amenazas, impactos y vulnerabilidades de la información y de los medios de tratamiento de la misma, así como, de su probable ocurrencia.

Evento de Seguridad de la Información:
La ocurrencia detectada en un estado de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad.

Evidencia Objetiva:
Información, registro o declaración de hecho, cualitativa o cuantitativa, verificable y basada en observaciones, medidas o evaluación, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de gestión.

G

Gestión de Riesgos:
Proceso de identificación, control, minimización o eliminación, a un costo aceptable, de los riesgos que afecten a los sistemas de información.

I

Información:
Es un conjunto organizado de datos procesados, que constituyen un mensaje sobre un determinado ente o fenómeno.

IEC (International Electrotechnical Commission):
Organización internacional que pública estándares relacionados con todo tipo de tecnologías eléctricas y electrónicas.

Incidente de la Seguridad de la Información:
Un único evento o una serie de eventos de seguridad de la información, inesperados o no deseados, y que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

Integridad:
Garantía de la exactitud y completitud de la información y los métodos de su procesamiento.
ISMS. Véase Sistema de Gestión de la Seguridad de la Información.

ISO (Organización Internacional de Normalización):
Con sede en Ginebra (Suiza), es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO/IEC 17021:
Requisitos generales para cualquier organismo que realice actividades de certificación. Es certificable

ISO/IEC 17799:
Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, es la antecesora de la ISO/IEC 27002. No es certificable.

ISO/IEC 27001:
Norma para un Sistema de Gestión de la Seguridad de la Información adoptada por ISO transcribiendo la segunda parte de BS7799. Es certificable. Aparece publicada por primera vez en el año 2005.

ISO/IEC 27002:
Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO/IEC 17799). No es certificable.

ISO/IEC 27006:
Requerimientos para organismos que realizan actividades de certificación enfocada a los Sistemas de Gestión de la Seguridad de la Información, basada en la norma ISO/IEC 17021. Es certificable. Publicada por primera vez en el año 2007.

M

Marca:
Símbolo registrado legalmente, que es expedido por un Organismo de Certificación o de Acreditación de acuerdo a normas establecidas, que indica que los sistemas de gestión de un organismo tienen la suficiente confianza y que ha sido demostrada de acuerdo a normas establecidas.

N

No Conformidad:
Incumplimiento de un requisito de cualquier norma auditable.

Norma:
Especificación que reglamenta procesos y productos para garantizar la interoperabilidad.

Normar:
Someter alguna cosa a ciertas normas, reglas o principios.

O

Organismo:
Compañía, corporación, firma, empresa, autoridad o institución, o parte o combinación de ellas, con personalidad jurídica pública o privada, responsable de sus propias funciones y administración, y además, es capaz de garantizar que la seguridad de la información es ejercida.

Organismo de Acreditación:
Empresa que acredita a los Organismos de Certificación com aptos para certificar según diversas normas. Suele haber uno por país, ejemplo: EMA(México), ENAC(España), UKAS (Reino Unido), etc.

Organismo de Certificación:
Empresa acreditada por un Organismo de Acreditación, que evalúa y certifica el SGSI y toda la documentación complementaria prevista en el sistema de una organización cliente que cumple con lo establecido en una norma referente a los SGSI.

Organismo de Evaluación de la Conformidad (OEC):
Organismo que realiza servicios de evaluación de la conformidad y que puede ser objeto de la acreditación.

P

PDCA (Plan-Do-Check-Act):
Modelo de proceso basado en un ciclo continúo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI).

Plan de continuidad del negocio:
Plan orientado a permitir la continuación de las principales funciones del negocio en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos:
Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Políticas:
Es un plan permanente que proporciona guías generales para canalizar el pensamiento administrativo en direcciones específicas. Es el proceso orientado ideológicamente hacia la toma de decisiones para la consecución de los objetivos de un grupo.

Política de seguridad:
Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Contiene las directrices que debe seguir la seguridad de la información, la respuesta a incidentes y definir las responsabilidades.

Procedimientos:
Son los documentos claramente definidos y desarrollados para cumplir con los objetivos marcados por las políticas.

R

Recursos:
Procedimientos o medios de los que se disponen para satisfacer una necesidad, llevara cabo una tarea o conseguir algo.

Recursos Humanos:
Es el conjunto de empleados o colaboradores de una organización.

Recursos Materiales:
Bienes tangibles con los que cuenta o necesita un Organismo para poder ofrecer sus servicios tales como: instalaciones (edificios, maquinaria, equipos, oficinas, terrenos, instrumentos, herramientas, entre otros) y la materia prima(aquellos materiales auxiliares que forman parte del producto, los productos en proceso y los productos terminados, entre otros).

Recursos Tecnológicos:
Bienes, tangibles o intangibles, que hacen uso de la tecnología tales como: equipo de cómputo, switchs, no-breaks, impresoras, software, etc.

Regular:
Hacer que algo funcione o se produzca de acuerdo con un orden, regla o ley, de manera uniforme o bajo control.

Riesgo:
Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo residual:
El riesgo que permanece tras el tratamiento del riesgo.

S

Seguridad:
Podemos entender como seguridad una característica de cualquier sistema (informático o no) que nos indica que ese sistema está libre de todo peligro, daño o riesgo, y que es, en cierta manera, infalible.

Seguridad de la Información:
La preservación de la confidencialidad, integridad y disponibilidad de la información, pudiendo, además, abarcar otras propiedades como la autenticidad, la responsabilidad, la fiabilidad y el no repudio.

Sistemas de Gestión de la Seguridad de la Información (SGSI):
La parte del sistema de gestión general, basado en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información.

Statement Of Applicability (SOA):
Ver Declaración de Aplicabilidad.

T

Tratamiento de Riesgos:
El proceso de selección e implementación de las medidas encaminadas a modificar los riesgos.

V

Vulnerabilidad:
Debilidad de la seguridad de la información de un organismo que potencialmente permite que una amenaza afecte a un activo.

BIBLIOGRAFÍA

Bibliografía

Libros y Normas Consultados

ARIAS, Liana, *Cómo hacer propuestas y proyectos bien pensados* [en línea]. República Dominicana, INTERCOACH, 2008. [Consulta: noviembre 2009]. (Iniciadores de negocios 8). http://www.scribd.com/doc/21449127/4098326-Como-Hacer-Proyectos-y-Propuestas-Bien-Pensados

COMITÉ ASESOR DE CÓMPUTO DE LA FACULTAD DE INGENIERÍA. 2009. *Laboratorios abiertos de cómputo en Ingeniería*. Gaceta de la FI UNAM, 2(12): 10-12.

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION. *Information technology. Security techniques. Information security management systems. Requirements*. España, AENOR, 2007 (ISO/IEC 27001:2005).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION. *Information technology. Code of practice for information security management.* España, AENOR, 2002 (ISO/IEC 17799:2000).

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION, INTERNATIONAL ELECTROTECHNICAL COMMISSION. *Information technology. Security techniques. Requirements for bodies providing audit and certification of information security management systems.* Suiza, ISO, 2007 (ISO/IEC 27006:2007).

[4] CÁMARA DE DIPUTADOS DEL H. CONGRESO DE LA UNIÓN. *Ley Federal sobre Metrología y Normalización*[en línea]. México, 2009. Pp. 3. http://www.cddhcu.gob.mx/LeyesBiblio/pdf/130.pdf

LÓPEZ BARRIENTOS, María Jaquelina y QUEZADA REYES, Cintia. *Fundamentos de Seguridad Informática.* México, UNAM, Facultad de Ingeniería, 2006.

Tríptico *"Módulos de Salida de la carrera de Ingeniería en Computación"* de la Facultad de Ingeniería.

Entrevistas

ENTREVISTA con Alejandra Zúñiga Medel, Encargada del Laboratorio de Redes y Seguridad de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 3 de julio de 2009.

ENTREVISTA con Andrés Hernández Bermúdez, Colaborador del Laboratorio de Investigación y Desarrollo de Software Libre de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 6 de octubre de 2009.

ENTREVISTA con Ángel C. Govantes Saldívar, Responsable del Laboratorio de Estándares Abiertos Java-IBM de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 2 de octubre de 2009.

ENTREVISTA con Cruz S. Aguilar Díaz, Jefe de la Coordinación de las Salas de Cómputo, UNICA de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 1 de julio de 2009.
ENTREVISTA con David A. Herrera Rosales, Colaborador del Laboratorio de Microsoft Research de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 2 de octubre de 2009.

ENTREVISTA con Edgar Martínez Meza, Colaborador del Laboratorio de Computación Salas "A" y "B" de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 28 de septiembre de 2009.

ENTREVISTA con Elba K. Saenz García, Colaborador del Laboratorio de Intel para la Academia de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 14 de septiembre de 2009.

ENTREVISTA con Francisco J. Montoya, Jefe de la Coordinación de las Salas de Cómputo, UNICA de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 1 de julio de 2009.

ENTREVISTA con Honorato Saavedra Hernández, Colaborador del Laboratorio de Multimedia e Internet de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 14 de septiembre de 2009.

ENTREVISTA con Rafael Sandoval Vázquez, Jefe del Departamento de Seguridad en Cómputo, UNICA de la Facultad de Ingeniería de la Universidad Nacional Autónoma de México. México, D. F. 11 de agosto de 2009.

Referencias Electrónicas

AENOR México.
< http://www.aenormexico.com/index.php?op=iso27001>

Certificación Mexicana. Certificación Mexicana.
< http://principal.certificacionmexicana.org/>

Computación. Universidad Nacional Autónoma de México, Facultad de Ingeniería, División de Ingeniería Eléctrica.
<http://www.fi-b.unam.mx/Computacion.aspx>

Corporativo CALMECAC. Corporativo Calidad Mexicana Certificada CALMECAC. 2000.
< http:// www.calmecac.com.mx/>

DIE – División de Ingeniería Eléctrica. Universidad Nacional Autónoma de México, Facultad de Ingeniería, División de Ingeniería Eléctrica. 20 de junio de 2007.
<http://www.fi-b.unam.mx/>

DNV – Servicios. Det Norske Veritas México, S.A. de C.V.
< http://www.dnv.com.mx>

[1] EMA. Entidad Mexicana de Acreditación, a.c.
< http://www.ema.org.mx/ema/ema/>

ENAC – Proceso de Acreditación. Entidad Nacional de Acreditación.
<http://www.enac.es/web/enac/acreditacion-paso-a-paso>

Factual Services, S. C.
< http://factual-services.com.mx>

Facultad de Ingeniería. Universidad Nacional Autónoma de México, Facultad de Ingeniería.
<http://www.ingenieria.unam.mx>

Grupo Bureau Veritas en México: Evaluación de la Conformidad, Certificación, Capacitación y Consultoría. Bureau Veritas. 2007.
< http://www.bureauveritas.com.mx>

Instituto Mexicano de Normalización y Certificación A.C.
<http://www.imnc.org.mx>

[2] Instituto Nacional de Ecología
< http://www2.ine.gob.mx/publicaciones/libros/33/sistema.html>

[3] Organización Interancional para la Estandarización. Wikipedia
< http://es.wikipedia.org/wiki/Organización_Internacional_para_la_Estandarización>

ISO 27001-Sistema de Gestión de Seguridad de la Información – SGSI. Iso27000.es. 2005.
< http://www.iso27000.es/>

ISO/IEC 27001-Wikipedia, la enciclopedia libre. Wikipedia.
< http://es.wikipedia.org/wiki/ISO/IEC_27001>

ISO-ISO Standards. International Organization for Standardization.
< http://www.iso.org/iso/iso_catalogue.htm>

Laboratorio de Computación Salas “A” y “B”. Universidad Nacional Autónoma de México, Facultad de Ingeniería, División Ingeniería Eléctrica.
< http://lcp02.fi-b.unam.mx/>

Laboratorio de Estándares Abiertos Java-IBM. Universidad Nacional Autónoma de México, Facultad de Ingeniería. División de Ingeniería Eléctrica.
<http://ibm.fi-b.unam.mx/index.html>

Laboratorio de Multimedia e Internet. Universidad Nacional Autónoma de México, Facultad de Ingeniería. División de Ingeniería Eléctrica.
<http://mmedia1.fi-b.unam.mx/opencms/opencms/mmedia>

Laboratorio de Redes y Seguridad. Universidad Nacional Autónoma de México, Facultad de Ingeniería, División Ingeniería Eléctrica.
< http://redyseguridad.fi-p.unam.mx/>

Laboratorio Microsoft. Universidad Nacional Autónoma de México, Facultad de Ingeniería, División Ingeniería Eléctrica.
<http://microsoft.fi-b.unam.mx/lmsr/default.aspx/>

LIDSOL. Laboratorio de Investigación y Desarrollo de Software Libre.
<http://wiki.lidsol.org/index.php?title=Portada>

LINDA – Laboratorio de Investigación para el Desarrollo Académico. Universidad Nacional Autónoma de México, Facultad de Ingeniería, División Ingeniería Eléctrica.
<http://www.grupolinda.org>

Unidad de Servicios de Cómputo Académico de la Facultad de Ingeniería. Universidad Nacional Autónoma de México, Facultad de Ingeniería, Unidad de Servicios De Cómputo.
< http://132.248.54.45/unica/>