



UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA
F.E.S. ARAGÓN

“LA IMPORTANCIA DE LA NORMALIZACIÓN”

T E S I S

**PARA OBTENER EL TÍTULO DE:
INGENIERO EN COMPUTACIÓN**

PRESENTA:

FERNANDO VILCHIS VELÁZQUEZ

DIRECTOR DEL TRABAJO DE TITULACIÓN:

**ING. MARIA GABRIELA
GONZÁLEZ HERNÁNDEZ**

MÉXICO

2015



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

Índice

Prologo	1
Agradecimientos	1
Introducción y objetivo	2
Capítulo 1. Conceptos básicos de la normalización	3
1.1 ¿Qué es la normalización?	3
1.2 ¿Qué es una norma?	4
1.3 Beneficios de la normalización	5
1.4 ¿Qué podemos normalizar?	6
1.5 ¿Para qué normalizar?	7
1.6 Tipos, clases y categorías de normas que hay	9
1.7 ¿Quiénes hacen las normas?	12
1.8 ¿Cómo se elaboran las normas?	13
1.9 ¿Quiénes tendrían interés en participar en la normalización y porque?	14
1.10 Difundir o dar a conocer las normas	17
Capítulo 2. La normalización en la seguridad de las tecnologías de la información	23
2.1 El papel de las normas en la seguridad de la información	23
2.2 Organismo internacional que se encarga de realizar las normas en el sector de TI	23
2.3 Normas de seguridad de la información	25
2.4 Adopción de normas en el Organismo Nacional de Normalización "NYCE" (Normalización y Certificación Electrónica, S.C.)	30
2.5 Desarrollo de una NMX-NYCE	31
2.6 Beneficios de adoptar una NMX-NYCE	36
Capítulo 3. Oportunidades de crecimiento para NYCE	37
3.1 Propuestas de mejora	37
3.2 Conclusiones	39
Bibliografía	40

PROLOGO

En el presente trabajo de tesis titulada "La importancia de la normalización" es una descripción de un tema muy importante que nos debe interesar a todos los profesionistas y al público en general.

En el primer capítulo redacto las bases de la normalización para poder adentrarse al tema y verlo reflejado a cualquier caso en particular.

El segundo capítulo pongo como ejemplo la relación que existe entre la normalización y la seguridad de la información tema cotidiano que practico en mi rol del día a día en mi trabajo.

En el tercer capítulo comento los beneficios que ha logrado la empresa en la cual laboro gracias a la normalización.

AGRADECIMIENTOS

A mis Padres:

Dionisio y Apolonia, al final de esta etapa de mi vida no encuentro forma de agradecer todo lo que han hecho por mí. Gracias por darme la vida, por su apoyo incondicional, por sus regaños, por los sí y los no, por enseñarme a luchar con razón, por su ejemplo, amor y confianza. Por el sacrificio en todo momento ya que sin su ayuda no hubiera sido posible la culminación de mi carrera profesional.

A mis hermanos:

Gracias Leticia y Daniel por su ayuda incondicional en todo momento.

Tu Diana que has estado en los momentos difíciles te agradezco tu amor, apoyo y comprensión a lo largo de este camino que no fue fácil.

A ti Demian por ser mi motor para superarme...

A todos los que no menciono por evitar omitir a alguien, pero que me han brindado enseñanza y sabiduría les agradezco infinitamente.

A todos...
GRACIAS

INTRODUCCIÓN

El crecimiento de las sociedades y del comercio mundial ha creado la necesidad de buscar una mejora continua de los productos, servicios y bienes debido al volumen de consumidores. Para ello, es importante la mejora de los procesos productivos de una empresa mediante la optimización de los recursos o medios de los que dispone. A partir de este planteamiento, es necesaria la creación de una estructura organizativa que se dedique a uniformar la producción así como crear normas de calidad aplicables a todas las organizaciones productivas.

Este trabajo es el resultado de una investigación motivada por la necesidad de fomentar la cultura de la normalización entre los mexicanos, aunque podría ser igualmente necesario para otras sociedades con una cultura de normalización similar a la que hay en México. Parte de este trabajo está dirigida, al público en general, a quién no tiene conocimientos previos sobre aspectos de normalización pero que es importante que los tengan, considerando que la mayoría de las personas son productores, todos somos consumidores y todos también somos miembros de una sociedad, a nivel local, regional, nacional, internacional y mundial.

Espero con este trabajo, estar contribuyendo a fomentar la cultura de la normalización; algo que es tan importante para lograr el desarrollo y el equilibrio, en un mundo que demanda cada vez más esfuerzos para establecer justicia y orden en las relaciones entre los hombres, y entre éstos y la naturaleza.

OBJETIVO

Objetivo general

- Crear conciencia de lo importante que es la normalización para el país y porque es conveniente apegarse a ella.

Objetivos específicos

- Describir los conceptos básicos de la Normalización
- Vincular las Tecnologías de la Información y la Normalización
- El beneficio que se obtiene al apegarse a la Normalización

1. CONCEPTOS BÁSICOS DE LA NORMALIZACIÓN

1.1 ¿Qué es la normalización?

Es el proceso de formular y aplicar reglas con el propósito de establecer un orden en una actividad específica, para beneficio y con la cooperación de todos los interesados y, en particular, para la obtención de una economía óptima de conjunto, respetando las exigencias de funcionalidad y seguridad. La Normalización pretende mejorar la calidad y la competitividad de productos y servicios, así como facilitar a la industria la conquista de posiciones en el mercado exterior.

La normalización ocurre si se cumplen esas 4 fases o etapas, esto es, ocurre cuando se cumplen las siguientes condiciones:

- 1.- Que exista una norma esto es el resultado de la fase de formulación de la norma.
- 2.- Que las personas a las que está destinada (la norma) la conozcan y comprendan esto es resultado de la fase de difusión de la norma.
- 3.- Que las personas a las que está destinada (la norma) ajusten su actividad (o el resultado de su actividad) a lo estipulado en ella esto es resultado de la fase de puesta en práctica de la norma.
- 4.- Que se evalúe si se está cumpliendo la condición anterior esto es resultado de la fase de evaluación de la conformidad con la norma.

Si alguna de esas condiciones no se cumple, no se puede decir que algo haya sido normalizado. Esto puede quedar expresado en la siguiente igualdad:

Normalización = norma + su difusión + su aplicación + evaluación de la conformidad

La normalización es un medio u oportunidad para:

- Establecer cómo queremos establecer que se hagan las cosas o que sean las cosas que usamos o consumimos voluntariamente, o que recibimos involuntariamente, mismas que afectan nuestra vida, integridad, salud e intereses y, por lo tanto, nuestro bienestar a nivel de vida;
- Lograr que todos los que hacen algo, de manera común y repetida, que puede afectar nuestro bienestar a nivel de vida, lo hagan de la misma manera, con las mismas características, con la misma calidad y, por lo tanto, con los mismos efectos o consecuencias benéficas para nuestras personas.

Hablar de normalización es hablar de:

- Coordinación, consenso, ponernos de acuerdo
- Trabajo en conjunto, proceso participativo
- Tomar en cuenta todos los puntos de vista, todos los intereses

- Confianza y seguridad en lo que otros hacen
- Ponerse de acuerdo, tener mejor comunicación
- Tener orden, hacer mejor las cosas, ahorrar más, ser más eficiente, ganar más
- Evitar que otros nos pongan en riesgo o nos dañen
- Consumir bienes y servicios de mejor calidad
- Mejorar la calidad de vida
- Proteger y hacer buen uso de recursos escasos y valiosos y de bienes públicos

Favorecer el desarrollo económico y social de la población.

1.2 ¿Qué es una norma?

Existen diferentes tipos de normas: sociales, morales o éticas, religiosas, jurídicas, de calidad, de convivencia, ambientales, tecnológicas, etcétera; y pueden estar escritas o ser transmitidas de forma oral. Cada una de estas tiene objetivos diferentes pero con un punto en común: determinar el comportamiento de una entidad ante una situación. Adicionalmente, una norma puede tener un alcance nacional, internacional, local o regional y por otro lado, siempre tiene una duración, es decir, una norma está sujeta a un marco temporal de tiempo que determina su validez de acuerdo a la evolución de la idiosincrasia de una comunidad. Y que será desechada, eliminada o modificada de acuerdo a las necesidades presentes y futuras. Se puede decir que una norma mantiene un estado del arte del área de conocimiento que describe.

La temporalidad de una norma y su carácter geográfico como alcance, dificultan la elaboración de una norma en la que su aprobación sea reconocida o aceptada por los grupos de interés en los que tiene alcance la norma misma.

Estas dificultades han cambiado drásticamente desde la segunda guerra mundial como resultado de una intensa actividad comercial, fortalecimiento de bloques económicos y el desarrollo industrial; así como algunos acontecimientos como la invención del chip, creación de la Internet, llegada del hombre a la luna, invención de la computadora personal, integración tecnológica en las empresas y el avance tecnológico de las telecomunicaciones.

Como resultado de estos eventos y cambios mencionados, se han realizado esfuerzos significativos en materia de normalización. Estos esfuerzos son dirigidos por entidades que reúnen una amplia gama de representantes para cada sector que mantienen, asegurando una participación ecuaníme para todos los interesados. Así mismo cada entidad lleva a cabo un proceso minucioso en la elaboración, consulta, aprobación, emisión, revisión y modificación de estándares y normas, lo que asegura su validez en la continuidad del tiempo de acuerdo a las necesidades de la comunidad a la que afecta.

Existen diferentes entidades dedicadas en la emisión de normas y estándares, algunos de ellos son:

IEC.- International Electrotechnical Commission.

ISO.- International Standard Organization.

IEEE.- Institute of Electrical and Electronical Engineers.

IATA.- International Air Transport Association.

IETF.- Internet Engineering Task Force.

ANSI.- American National Standards Institute.

ITU.- International Telecommunication Union.

ECN.- European Committee for Standardization.

Una norma tiene diferentes acepciones de acuerdo al entorno en la que se está refiriendo. Para fines de este trabajo y los objetivos que se persiguen, por norma se entenderá lo siguiente:

Una norma es una regulación técnica que establece 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 ¹⁾.

Es importante notar que:

- Una norma puede ser de cumplimiento obligatorio u opcional, por otro lado, una norma puede considerar casos excepcionales que pueden variar su aplicación o implementación, o bien, puede generalizar diferentes escenarios a los que se puede enfrentar el usuario. Así, la implementación, aplicación o adhesión de una norma puede diferir ligeramente del documento que la respalda o de una entidad a otra.

Una norma es un documento que describe un conjunto de especificaciones o algún procedimiento para realizar alguna actividad o la elaboración de un producto. La norma es más estricta en cuanto a los detalles de aplicación o implementación y en caso de considerar diferentes escenarios, todos se encuentran detallados adecuadamente. Finalmente un sistema, producto, servicio o proceso es estándar en el mercado, si su implementación o aplicación es la misma en cada una de las instancias existentes y se encuentra de acuerdo a un documento técnico.

1.3 Beneficios de la normalización

La implementación y gestión de una norma traen consigo cambios sustanciales que pueden cambiar, para bien, el núcleo y la operación de un negocio, y de manera indirecta la estrategia del mismo.

Algunos de los beneficios de la implementación de una norma son:

- Reconocimiento en la implementación de una recomendación emitida por una autoridad reconocida en el ámbito (este reconocimiento es demostrado cuando la organización decide avalar su implementación ante un tercero que determina el cumplimiento de la norma).
- Ventaja competitiva al interior de las operaciones de la organización y al exterior en la entrega de productos o servicios al cliente.
- Confianza del cliente en la operación de la organización.
- Mejora sustancial en la organización e integración de los procesos de acuerdo al ámbito de la norma de una manera consistente, eficiente y eficaz, permitiendo su monitoreo, evaluación, revisión y mejora.
- Confianza al saber que la norma ha sido consultada, revisada documentada y corregida por entidades del sector público y privado alrededor del mundo y que el documento representa la experiencia recabada en los alcances de la misma.

1.4 ¿Qué podemos normalizar?

Conforme a las definiciones de norma mencionadas anteriormente tenemos que el objeto de la normalización es, siempre una actividad o lo que resulta de una actividad. Existen muchos modos de actividad: hay actividades denominadas procesos, también hay actividades denominadas servicios, y hay también modos de llevar a cabo una misma actividad, modos éstos denominados métodos, procedimientos o prácticas. Asimismo, lo que resulta intencionalmente de una actividad suele conocerse como producto, y un producto puede ser un material, una parte o componente de un todo mayor (de un sistema), un equipo, un instrumento, un aparato, un envase, una instalación o información plasmada en forma escrita o gráfica (vocabularios, terminologías, nomenclaturas, diccionarios, simbologías, emblemas, contraseñas, símbolos, información sanitaria, ecológica, de seguridad e higiene sobre los productos y servicios, información comercial de calidad y de publicidad para el consumidor), etc. También hay productos que resultan de una actividad sin que fuera intencional producirlos (denominados productos no intencionales), como pueden ser los gases tóxicos, las aguas residuales contaminantes, los desechos sólidos (basura) o las radiaciones no intencionales, que resultan de alguna actividad o proceso industrial o de la prestación de servicio.

Recientemente se ha considerado también a las personas o individuos como resultados de las actividades o procesos de formación, capacitación, actualización, entrenamiento, educación o enseñanza y aprendizaje, motivo por el cual se han elaborado normas cuyo objeto de normalización es la persona misma, normalizando características tales como su conocimiento acerca de una determinada materia o tema, o su habilidad, capacidad, destreza o aptitud para hacer algo. Esas normas son conocidas como normas de competencias laborales o profesionales.

Todo lo anterior se corrobora también por otro lado, ya que la norma internacional ISO 9000:2015 ²⁾, en sus apartados 3.4.1, 3.4.2 y 3.4.5 define proceso, producto y procedimiento respectivamente, de la siguiente manera:

Proceso es el “conjunto de actividades mutuamente relacionadas o que interactúan, las cuales transforman elementos de entrada en resultados”, agrega, entre otras, la Nota 1 que señala lo siguiente; “los elementos de entrada para un proceso son generalmente resultados de otros procesos” ²⁾.

Producto es el “resultado de un proceso” ²⁾, e incluye las siguientes notas:

Nota 1.- Existen cuatro categorías genéricas de productos:

- Servicios (por ejemplo: transporte);
- Software (por ejemplo: programas de computadora, diccionario);
- Hardware (por ejemplo: parte mecánica de un motor);
- Materiales procesados (por ejemplo: lubricante).

La mayoría de los productos contienen elementos que pertenecen a diferentes categorías genéricas de producto. La denominación del producto en cada caso como servicio, software, hardware o material procesado depende del elemento dominante.

Nota 2.- Un servicio es el resultado de llevar a cabo necesariamente al menos una actividad de la interfaz entre el proveedor y el cliente, y generalmente es intangible. La prestación de un servicio puede implicar, por ejemplo:

- Una actividad realizada sobre un producto tangible suministrado por el cliente (por ejemplo: reparación de un automóvil);
- Una actividad realizada sobre un producto intangible suministrado por el cliente (por ejemplo: la declaración de ingresos necesaria para preparar la devolución de impuestos);
- La entrega de un producto intangible (por ejemplo: la entrega de información en el contexto de la transmisión de conocimiento);
- La creación de una ambientación para el cliente (por ejemplo: en hoteles y restaurantes).

El software consiste de información y generalmente es intangible; puede presentarse bajo la forma de propuestas, transacciones o procedimientos.

El hardware es generalmente tangible y su cantidad es una característica contable. Los materiales procesados generalmente son tangibles y su cantidad es una característica continua. El hardware y los materiales procesados frecuentemente son denominados como bienes.

Nota 3.- El aseguramiento de la calidad está principalmente enfocado en el producto que se pretende.

Nota 4.- En español los términos ingleses "software" y "hardware" tienen un alcance más limitado del que se le da en esta norma, no quedando limitado al campo informático.

Procedimiento Es la "forma especificada para llevar a cabo una actividad o un proceso" ²⁾.

Ahora bien, cuando el objeto de la normalización es un conjunto de productos, o de actividades de esos productos llevadas a cabo con o sin un método o procedimiento especificado, o de procesos, o de varios o todos ellos a la vez, interactuando, estaríamos hablando de que el objeto de la normalización es un sistema.

Para resumir, cualquier actividad o resultado de una actividad puede ser objeto de una norma.

1.5 ¿Para qué normalizar?

Entre los beneficios más importantes que produce la normalización están:

- Hacer que aquello que se normalice (una actividad y/o sus resultados) sea lo más adecuado para cumplir su fin, o sea, que cumpla de la mejor manera los propósitos y funciones para lo que fue concebido.
- Hacer que las actividades humanas (y/o sus resultados), al ser realizadas, busquen alcanzar los fines para los que fueron concebidas, no generen riesgos o daños directa o indirectamente al ser humano aunque sea de manera involuntaria.

Entre las actividades (y/o sus resultados) susceptibles de ser normalizadas, en atención al logro de los beneficios arriba citados, podríamos mencionar las siguientes:

1) Actividades (y/o sus resultados) de las que depende, directa o indirectamente la vida y la salud de las personas; por ejemplo:

- La producción, conservación, manejo y consumo de alimentos y bebidas (naturales y procesados);
- El cuidado, conservación, manejo, tratamiento, distribución y uso del agua;
- La producción, aplicación y uso de medicamentos;
- Las prácticas de salud y sanidad (incluyendo, entre muchas otras, la operación de laboratorios de análisis clínicos);
- Los procesos de emisión intencional y no intencional de sólidos, líquidos y gases contaminantes en los cuerpos de agua, en la atmósfera, en la biósfera y, en general, en el medio ambiente en el que viven las personas y los demás seres vivos;
- Los procesos de emisión intencional y no intencional de radiaciones ionizantes y no ionizantes;
- Las condiciones de protección y seguridad de la vida y la salud de las personas en el medio ambiente general y laboral;
- La producción, distribución, manejo, transporte, conservación y uso de recursos energéticos;
- El manejo, transporte y confinamiento de materiales y residuos industriales peligrosos y de sustancias radioactivas;
- La protección y la salud de la vida animal y vegetal;
- El cuidado, protección y preservación de los recursos naturales y los ecosistemas;
- La protección y cuidado de las vías generales de comunicación;
- Las condiciones de salud, seguridad e higiene en los centros de trabajo, en los centros públicos de reunión, en las viviendas y en las demás obras e instalaciones en las que realizan sus actividades las personas;
- La información sanitaria, ecológica, de seguridad e higiene sobre los productos y servicios; etc.

2) Actividades (y/o sus resultados) que, aún cuando no pudieran poner en riesgo la vida y la salud de las personas de manera directa o indirecta, tienen impacto importante en los intereses de los usuarios o consumidores; por ejemplo:

- Las mediciones de cualquier tipo (su exactitud, precisión y certidumbre, entre otros aspectos)
- La información comercial, de calidad y de publicidad para el consumidor
- El envase y embalaje de productos así como ciertas prácticas comerciales
- Otras actividades (y/o sus resultados) relacionadas con la calidad, funcionalidad, efectividad, capacidad, compatibilidad, intercambiabilidad, control de la variedad - reducción de la diversidad, seguridad, protección del producto, durabilidad, resistencia, exactitud, conformidad, conveniencia, concordancia, etc.

De los ejemplos anteriores podemos ver que la normalización se ha constituido en una respuesta a los requerimientos de la sociedad, atendiendo aspectos fundamentales del bienestar de la población.

Las normas, además:

- Son vehículos de comunicación entre empresas, autoridades, usuarios y consumidores, ya que proporcionan un lenguaje común para definir y establecer criterios, conceptos, objetivos, etc.;
- Facilitan la investigación, la innovación y el cambio tecnológico;
- Favorecen el mantenimiento y preservación de instalaciones y activos;
- Son útiles para la formación y adiestramiento de personal;
- Posibilitan la comparación entre productos, proporcionando a los consumidores información fundamental para tomar mejores decisiones de compra, consumo y uso.

¿Qué consecuencias produce normalizar todo eso?

La normalización de todo lo anterior contribuye al mejor y más rápido desarrollo del ser humano como individuo y como grupo social, ya que:

- Saber que algo es normalizado es saber qué características tiene o qué podemos esperar de ello, y esa certidumbre previa genera confianza entre las personas relacionadas a través del objeto normalizado; se produce una sensación de seguridad en las relaciones entre los individuos y entre los , grupos sociales
- Además, la normalización mejora la comunicación, porque las partes involucradas saben en común de lo que se está hablando, de lo que se espera del objeto normalizado, y ese conocimiento previo permite, por un lado planear mejor las actividades y los recursos, el aprovisionamiento, la producción y la distribución, hacer mejor las cosas, ser más eficientes, más productivos, y en consecuencia tener mayores ahorros, utilidades, ganancias
- Pero también, por otro lado, ese conocimiento previo permite sentir seguridad, tranquilidad y confianza en que lo que están haciendo otros individuos o grupos sociales, aunque no estemos relacionados formalmente con ellos, no nos va a perjudicar, dañar o traer consecuencias nocivas o inconvenientes a nuestras vidas y nuestros intereses, ya que existe la confianza de que están llevando a cabo todas sus actividades con apego a las normas.

1.6 Tipos, clases y categorías de normas que hay

Las normas pueden clasificarse a partir de ciertos criterios. De acuerdo con esto, algunas clases, tipos o categorías de normas serían las siguientes:

- Por la obligatoriedad de su cumplimiento:

Normas obligatorias.- Son aquellas cuya observancia es obligatoria por mandato de ley. También son conocidas como Reglamentos Técnicos o como Regulaciones Técnicas.

Normas voluntarias.- Son aquellas cuya observancia no es obligatoria por mandato de ley o reglamento. También son conocidas como normas contractuales, ya que se convienen voluntariamente entre las partes de un contrato.

- Por el objeto a normalizar:

Normas de producto.- (Ejemplos: normas de material, equipo, aparato, dispositivo, instrumento).

Normas de actividad de proceso.- (Ejemplos: norma de tratamiento de aguas residuales; norma de medición, tasación y facturación del servicio telefónico).

Normas de método.- (Ejemplos: normas de métodos de producción o fabricación; de métodos de operación de servicios; de métodos de prueba; de métodos de evaluación).

Normas de servicio.- (Ejemplos: normas de mantenimiento de equipo e instalaciones; de atención hospitalaria; de transportación de personas; de suministro de gas).

Normas de sistema.- (Ejemplos: normas de sistemas de distribución de energía eléctrica; de sistemas de gestión de la calidad; de sistemas de administración ambiental; de sistemas de administración de la seguridad y la salud en el trabajo; de sistemas de evaluación de la conformidad).

Normas de interface.- (Ejemplos: normas de interface de equipos terminales a redes públicas de telecomunicaciones; de interface hombre -máquina en un sistema informático; de interface producción - distribución de energía eléctrica).

Normas de terminología, de vocabulario, de nomenclatura.- (Ejemplos: normas de vocabulario electrónico; de terminología utilizada en evaluación de la conformidad; de nomenclatura química).

Normas de instalación.- (Ejemplos: normas de instalación de torres y antenas; de instalaciones sanitarias; de instalaciones eléctricas).

Normas de símbolos, de diagramas, de unidades.- (Ejemplos: normas de simbología utilizada en materia de seguridad; de diagramas eléctricos; de unidades de medida).

Normas de competencias laborales o profesionales.- (Ejemplos: norma de auditoría de sistemas de gestión de la calidad y/o ambiental; de soldadura eléctrica; de operación de autotransportes de carga).

- Por el ámbito geográfico, político o económico en que se adopta:

Normas internacionales.- Son aquellas adoptadas por una organización internacional de normalización y que se ponen a disposición del público.

Normas regionales.- Son aquellas adoptadas por una organización regional de normalización y que se ponen a disposición del público.

Normas nacionales.- Son aquellas adoptadas por una organización nacional de normalización y que se ponen a disposición del público.

Normas territoriales.- Son aquellas adoptadas en el nivel de una división territorial de un país y que se ponen a disposición del público. Las normas estatales o provinciales y las normas locales son casos de normas territoriales.

Normas propietarias.- Son aquellas adoptadas en el nivel de una empresa u organización y que no se ponen a disposición del público.

- Por el ámbito de la actividad (y / o sus resultados):

De conformidad con la clasificación Internacional de Normas ³⁾ existen los siguientes campos de normas (se antepone en cada caso el número con el que se clasifica internacionalmente el campo):

- 01 Generalidades. Terminología, Normalización, Documentación.
- 03 Sociología, Servicios, Organización y gestión de empresas, Administración, Transporte.
- 07 Matemáticas, Ciencias naturales.
- 11 Tecnología sanitaria.
- 13 Medio ambiente y protección de la salud. Seguridad.
- 17 Metrología y medición. Fenómenos físicos.
- 19 Ensayos
- 21 Sistemas y componentes mecánicos de uso general.
- 23 Sistemas de fluidos y componentes de uso general.
- 25 Técnicas de fabricación.
- 27 Ingeniería de la energía y transmisión de calor.
- 29 Electrotecnia.
- 31 Electrónica.
- 33 Telecomunicaciones. Técnicas de audio y video.
- 35 Tecnologías de la información. Máquinas de oficina.
- 37 Tecnología de la imagen.
- 39 Mecánica de precisión, Joyería.
- 43 Vehículos de carretera.
- 45 Ferrocarriles.
- 47 Construcción naval y estructuras marinas.
- 49 Aeronáutica y espacio.
- 53 Equipos de manutención para materiales.
- 55 Embalaje y distribución de mercancías.
- 59 Industria textil y tecnología del curtido.
- 61 Industria de la confección.
- 65 Agricultura.
- 67 Tecnología de los alimentos.
- 71 Ingeniería química.
- 73 Minería y minerales.
- 75 Industria del petróleo y tecnologías relacionadas.
- 77 Metalurgia.
- 79 Tecnología de la madera.
- 81 Industrias del vidrio y de la cerámica.
- 83 Industrias de los elastómeros y de los plásticos.
- 85 Tecnologías del papel.

- 87 Industrias de las pinturas y del color.
- 91 Edificación y materiales de construcción.
- 93 Ingeniería civil.
- 95 Ingeniería militar.
- 97 Equipamiento doméstico y comercial, Ocio, Deportes.
- 99 (Sin título).

Cada uno de estos campos se subclasifica en grupos de normas y cada uno de esos grupos se subclasifica a su vez en subgrupos de normas. Así, a manera de ejemplo, se presenta a continuación la subclasificación del grupo 070 servicios móviles, del campo 33 Telecomunicaciones. Técnicas de audio y video, el cual es uno de los 14 grupos en que se subclasifica ese campo de normas (se antepone en cada caso el número con el que se clasifican internacionalmente ese grupo y sus subgrupos en el campo 33):

33 Telecomunicaciones. Técnicas de audio y video.

33.070 Servicios móviles
 33.070.01 Servicios móviles en general
 33.070.10 Radio Troncal Terrestre (Tetra)
 33.070.20 Sistemas de radioescucha

- Incluyendo sistema europeo de radiomensajería (ERMES)
 - 33.070.30 Telecomunicaciones digitales mejoradas sin cordón (DECT)
 - 33.070.40 Satélite
- Incluyendo sistema de posicionamiento global (GPS)
 - 33.070.50 Sistema global para comunicaciones móviles (GSM)
 - 33.070.99 Otros servicios móviles

Como se puede observar, las normas abarcan todos los campos, ramas o sectores de actividad económica, sean de carácter agrícola, pecuario, forestal, pesquero, cinegético, industrial (extractiva y de la transformación) o de toda la gama de servicios.

1.7 ¿Quiénes hacen las normas?

Tal como lo expresamos al definir lo que es una norma, ésta se hace a través de organismos reconocidos. Ahora bien, ¿cuáles son esos organismos reconocidos?

"Son aquellos organismos con actividades de normalización reconocidos a nivel nacional, regional o internacional, que tienen como función principal, en virtud de sus estatutos, la preparación, la aprobación o la adopción de normas que se ponen a disposición del público".

Dependiendo del nivel o ámbito en que son reconocidos, los organismos de normalización pueden ser: organismos nacionales de normalización, organismos regionales de normalización y organismos internacionales de normalización.

Ahora bien, cuando se trata de normas de observancia obligatoria, también conocidas como Reglamentos Técnicos o Regulaciones Técnicas, no son los organismos de normalización los que las preparan, aprueban o adoptan, sino que tales

responsabilidades corresponden a las denominadas autoridades regulatorias o autoridades de reglamentación, las cuales tienen poderes y derechos legales.

Para llevar a cabo las actividades de normalización al interior de los organismos de normalización o de las autoridades regulatorias (o de reglamentación), generalmente se constituyen comités, subcomités o grupos de trabajo o estudio técnicos, los cuales están conformados por (o en los cuales participan) expertos técnicos y/o representantes de los diferentes grupos de interés en las normas (productores, fabricantes, prestadores de servicios, distribuidores, comercializadores, consumidores, colegios de profesionistas, universidades e instituciones de educación superior y científica, centros de investigación científica y desarrollo tecnológico, así como sectores de interés general y sin exclusión de ningún sector de la sociedad que pueda tener interés en las actividades de normalización).

Es altamente deseable y conveniente que los expertos y representantes que participan en las actividades de normalización, posean, fundamentalmente, conocimientos sólidos en una o más de las ciencias básicas (matemáticas, física, química, biología, ecología, psicología ciencias de la salud, etc.) o de las ciencias interdisciplinarias (físicoquímica, bioquímica, biofísica, biomecánica, etc.), así como conocimientos y experiencia acerca de:

- El marco legal y reglamentario de la normalización, regulación técnica, evaluación de la conformidad y metrología.
- Conceptos, métodos y procedimientos de elaboración de normas y/o reglamentos técnicos, incluyendo la manera de evaluar la conformidad (métodos, técnicas, reglas y buenas prácticas de medición, comprobación, muestreo, verificación, inspección, auditoría, certificación, acreditación, etc.).
- Tecnologías: materiales, aparatos, instrumentos, máquinas, instalaciones, procesos y métodos (de diseño y especificación de características, de producción, fabricación, operación, instalación, control de calidad o de especificaciones, de manejo y transformación de materiales y de energía, etc.).
- Conceptos, métodos y procedimientos para la estimación y cálculo de costos y beneficios de la regulación técnica (cuantificables y no cuantificables), así como para la elaboración de manifestaciones de impacto regulatorio o normativo.
- Conceptos, métodos y técnicas de investigación, estimación y evaluación de riesgos, derivados de realizar tal o cual actividad y/o de obtener tales o cuales resultados al llevar a cabo esas actividades.
- Métodos y técnicas de investigación documental y de expresión oral y escrita (en el idioma natal y en al menos un idioma extranjero).
- Tecnologías de información y comunicación TIC (software y hardware).

1.8 Como se elabora una norma

La normalización se lleva a cabo a través de las siguientes actividades:

1. Detección de las necesidades a satisfacer o de los problemas a resolver a través de la normalización; propuesta correspondiente del tema a normalizar y en caso de haber sido aceptado dicho tema su inclusión dentro del programa de normalización del organismo de normalización o de la autoridad regulatoria correspondiente.

2. Investigación, estudio y evaluación del "estado del arte de la normalización" de la normalización nacional e internacional del tema determinado (tanto de las especificaciones y/o características como de los procedimientos de evaluación de la conformidad correspondientes).
3. Decisión sobre la adopción o adaptación de normas internacionales, regionales, de otros países y de organismos de normalización especializados (tanto de las especificaciones y/o características como de los procedimientos de evaluación de la conformidad correspondientes), para la elaboración de la norma.
4. Redacción, estructuración y presentación de un anteproyecto (o borrador) de la norma (sea obligatoria o voluntaria).
5. Participación en la elaboración de la norma a través de comités, subcomités y/o grupos de trabajo del organismo de normalización o de la autoridad regulatoria.
6. Para el caso de las normas obligatorias (o reglamentos técnicos), estudio y evaluación de los beneficios (incluyendo el grado de satisfacción de las necesidades económicas y sociales), los costos y el impacto regulatorio de la aplicación de la norma.
7. Aprobación o adopción y puesta en vigor de la norma, de acuerdo con las reglas, procedimientos y demás disposiciones legales o administrativas que apliquen al organismo de normalización o a la autoridad regulatoria.
8. Difusión y facilitación de la comprensión de la importancia, beneficios y correcta interpretación y aplicación de la norma.
9. Uso, aplicación, evaluación de la conformidad y cumplimiento de la norma.

Existen técnicas, métodos y prácticas específicas para llevar a cabo cada una de las actividades de normalización antes descritas. Sin embargo, es conveniente hacer mención que ha sido necesario y conveniente hacer normas, especificaciones técnicas, códigos de buena práctica y reglamentos sobre la manera de llevar a cabo las actividades de normalización.

1.9 ¿Quiénes tendrían interés en participar en la normalización y porque?

A continuación se describen esos sectores de interés que debieran participar en la formulación, difusión, puesta en práctica y evaluación de la conformidad de las normas, describiéndolos e indicando en cada caso porque deben o les conviene participar:

- Los productores

Son las personas que realizan la actividad normalizada o sus resultados; en la rama agropecuaria, forestal o pesquero; los fabricantes o productores industriales; los productores o prestadores de servicios; los que van a proveer de insumos a otros productores o de bienes y servicios a los consumidores finales.

Les conviene participar en la normalización de sus productos y de sus insumos productivos; porque al asegurarse de la calidad o cualidades de sus insumos, podrán facilitarse el aseguramiento de una determinada calidad en sus productos, situación

ésta que pueden garantizar a sus clientes, usuarios o consumidores, repercutiendo en su confianza hacia el producto y en su lealtad al mismo, manteniendo e incrementando su demanda.

- **Los comerciantes**

Son las personas que tienen la responsabilidad de hacer llegar al consumidor intermedio y final los bienes y servicios que tienen que cumplir con normas de observancia obligatoria (regulaciones técnicas) o con normas que, de manera voluntaria, el productor declara cumplir (al declararlo lo convierte en una norma de cumplimiento obligatorio aunque no sea una regulación).

En una gran cantidad de casos, los comerciantes adquieren o le compran a los productores o distribuidores o comercializadores mayoristas del producto, sin estar seguros de que lo que compran cumple con las normas que están obligados a observar, y como son ellos los que van a hacer el contacto final del consumidor, son a quienes se les va a responsabilizar en caso de algún incumplimiento normativo.

Les conviene participar en la normalización de los bienes y servicios que comercializan para familiarizarse con las cualidades normalizadas de esos productos y con las normas que deben cumplir; así sabrán de qué van a ser responsables ante el consumidor por razón del cumplimiento de cualidades normalizadas del producto que están comercializando, y estarán preparados para hacer frente a las responsabilidades contractuales que tengan que ver con el asunto.

- **Los consumidores**

Son las personas que reciben los efectos institucionales o no intencionales de la actividad normalizada (o sus resultados), los que consumen o utilizan los objetos normalizados, ya sea como consumidores intermedios de insumos productivos o como consumidores finales.

Les conviene participar en la normalización de los bienes y servicios que consumen o utilizan para conocer, y asegurarse de que tengan, las cualidades o atributos que satisfagan de la mejor manera sus necesidades o expectativas, y para asegurarse también de que esos bienes y servicios no vayan a causarles algún daño a su vida, a su salud o a sus intereses legítimos.

- **Los expertos: profesionistas, peritos, especialistas y investigadores académicos**

Son las personas que saben más de la materia o de la actividad que se va a normalizar. Las normas constituyen reglas de tecnología reconocida (reconocida por una mayoría de expertos representativos), por lo que el trabajo de normalización requiere de un profundo conocimiento y experiencia en el campo de conocimiento que domina al objeto que se normaliza.

Les conviene participar en la normalización porque es una actividad en la que pueden poner en juego su conocimiento experto, incrementándolo con la discusión y el trabajo grupal de otros expertos en el campo de su especialidad, lo que hace que estén al día en un asunto de la materia de su especialidad que busca garantizar un nivel de orden óptimo en un contexto dado. En general, y de materia natural, los otros sectores de

interés (productores, comerciantes, consumidores, autoridades regulatorias) van a requerir de los servicios de los expertos a participar en las actividades de normalización, de manera que puedan contar con su conocimiento experto para salvaguardar los intereses de sector ante las posiciones y argumentaciones que presentan los demás expertos, representantes de otros sectores, los cuales no siempre van a defender los mismos interés.

- **Autoridades regulatorias**

Son las personas que tienen la responsabilidad legal de garantizarle a la población en general su protección contra actividades (o sus resultados) que pongan o puedan poner en riesgo de su vida, salud e intereses legítimos, a través de la elaboración y expedición de normas o regulaciones técnicas de observancia obligatoria así como de la religiosa vigilancia de su cumplimiento.

En este caso no es precisamente que le convenga participar en la normalización, sino que están obligados a hacerlo por mandato de ley (en el caso de las normas, regulaciones técnicas obligatorias).

- **Los expertos en evaluación de la conformidad**

Son las personas que realizan las actividades para determinar si se cumplen los requisitos contenidos en las normas. Su participación es muy importante porque, por la naturaleza de su actividad, estarán siempre atentos a que los requisitos que se establezcan en las normas se puedan medir o evaluar objetivamente una vez que la norma esté vigente, además, jugarán un papel fundamental en la formulación de los métodos y procedimientos de evaluación de la conformidad de los requisitos, cuando las normas así lo demanden, y con mayor razón cuando se trate de hacer normas cuyo objeto sean esos métodos o procedimientos.

Les conviene participar en la normalización, además de por los motivos mencionados en el caso de los expertos, para familiarizarse con las cualidades normalizadas de los objetos normalizados y con los métodos o procedimientos de evaluación de la conformidad que más adelante tendrían que aplicar, ya sea como integrantes de organismos de evaluación de la conformidad (laboratorios de pruebas, organismos de certificación, unidades de verificación, entre otros), de primera parte (contratados por, o formando parte integrante de, los mismos productores, comercializadores o proveedores del objeto normalizado); de segunda parte (contratados por, o formando parte integrante de las personas u organizaciones que tienen interés como usuarios consumidores del objeto normalizado), o de tercera parte (contratados por una persona u organismo que es independiente de la persona u organización que provee el objeto y también de los intereses del usuario en dicho objeto).

- **Los académicos de las instituciones educativas**

Son personas que tienen la responsabilidad de difundir o divulgar el conocimiento científico y tecnológico a los educandos que asisten a esas instituciones a través de actividades de enseñanza – aprendizaje y a la sociedad en general a través de actividades de extensión o difusión del conocimiento, todo ello con el fin de formar nuevas generaciones de ciudadanos comprometidos con el desarrollo económico, social y cultural de la sociedad y de la humanidad en su conjunto.

Le conviene participar en la normalización, además de por los motivos mencionados arriba, en la parte correspondiente a la participación de los expertos, porque es una actividad propicia para estar actualizados en la forma en que se están atendiendo necesidades, problemas y expectativas de la sociedad, buscando siempre garantizar un nivel de orden óptimo en un contexto dado; de esa manera estarán en mejores condiciones para reproducir ese conocimiento actualizado entre sus alumnos y entre los demás beneficiarios de las actividades de divulgación del conocimiento científico y tecnológico propias de las instituciones a las que pertenecen, fomentando así mismo en el contexto social una cultura de la calidad.

1.10 Difundir o dar a conocer las normas

En primer lugar debemos tener muy en claro quiénes deben conocer las normas (incluyendo, desde luego, las regulaciones técnicas de observancia obligatoria), qué de ellas deben conocer y para que deben conocerlas; enseguida plantearnos quienes son los más abocados para llevar a cabo esa difusión o divulgación de las normas y, finalmente proponer de qué maneras se podrán llevar a cabo esa divulgación.

Recordando a esos grupos de interés, dijimos que eran:

- Los productores (de bienes y servicios);
- Los comerciantes;
- Los consumidores;
- Los expertos: profesionistas, peritos, especialistas, investigadores, académicos;
- Las autoridades regulatorias;
- Los expertos en la evaluación de la conformidad;
- Los académicos de las instituciones educativas.

A continuación plantearemos, para cada uno de esos grupos de interés, lo que deben conocer acerca de las normas, para qué fines, quiénes debieran proveer ese conocimiento y de qué manera.

Difundir o dar a conocer **a los productores** (de bienes y servicios):

Que	Para qué	Quién	Cómo
Normas obligatorias aplicables a sus productos	Para cumplir con requisitos legales y evitar ser sancionados	Dependencias, agencias o autoridades regulatorias, en colaboración con expertos y con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	Con programas de capacitación, actualización y divulgación para los productores (cursos, seminarios, publicaciones y otros medios idóneos)
Normas voluntarias aplicables a sus productos establecidas por los clientes	Para cumplir con los requisitos de los clientes	Organismos de normalización reconocidos en colaboración con expertos y con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	
Normas voluntarias aplicables a sus productos no establecidas por los clientes pero necesarias para el uso previsto del producto	Para ofrecerle buena calidad de sus productos a los clientes (como una ventaja comparativa)		
Normas voluntarias aplicables a sus insumos productivos, cuyo cumplimiento exigirán a sus proveedores, y los modos de atestación aceptables de esas normas voluntarias	Para exigir su cumplimiento a los proveedores, contribuir a elevar la calidad de sus productos y poder garantizar que estos satisfagan el uso provisto por los clientes		
Normas obligatorias aplicables a sus insumos productivos, y los modos de atestación aceptables de esas normas obligatorias	Para exigir su cumplimiento a los proveedores	Dependencias, agencias o autoridades regulatorias, en colaboración con expertos y con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	

Los procedimientos de evaluación de la conformidad de todas las normas arriba mencionadas	Para aplicarlos y/o asegurarse de que los insumos que utilizan y productos que generan cumplan con las normas arriba mencionadas	Dependencias, agencias o autoridades regulatorias, u organismos de normalización reconocidos, en colaboración con expertos y con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	
---	--	---	--

Difundir o dar a conocer **a los comerciantes:**

Que	Para qué	Quién	Cómo
Normas obligatorias aplicables a los productos que comercializan, y los modos de atestación aceptables de esas normas obligatorias	Para asegurarse que los productos que van a comerciar cumplen con requisitos legales y así evitar ser sancionados	Dependencias, agencias o autoridades regulatorias, en colaboración con expertos y con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	Con programas de capacitación, actualización y divulgación para los productores (cursos, seminarios, publicaciones y otros medios idóneos)
Normas voluntarias que el productor declara que su producto cumple, y los modos de atestación aceptables de esas normas voluntarias	Para asegurarse de que los productos que va a comerciar cumplen con esas normas, ya que al declarar el productor que las cumple se convierten en obligación, y así evitar ser sancionado	Organismos de normalización reconocidos en colaboración con expertos y con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	

Difundir o dar a conocer **a los consumidores:**

Que	Para qué	Quién	Cómo
Normas obligatorias aplicables a los productos que compran, adquieren, utilizan o consumen, y los modos de atestación aceptables de esas normas obligatorias	Para cerciorarse de que están comprando, adquiriendo, utilizando o consumiendo productos que cumplen con disposiciones destinadas a proteger su vida, o salud, o sus intereses legítimos	Dependencias, agencias o autoridades regulatorias, o responsables de procurar el bienestar y la protección del consumidor y/o organismos de normalización reconocidos, en colaboración con expertos y con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios, así como de organizaciones o asociaciones de consumidores	Con programas de capacitación, actualización y divulgación para los productores (cursos, seminarios, publicaciones y otros medios idóneos)
Normas voluntarias que el productor declara que su producto cumple, y los modos de atestación aceptables de esas normas voluntarias	Para cerciorarse de que están comprando, adquiriendo, utilizando o consumiendo productos (bienes o servicios) que cumplen con características que mejoran su calidad, satisfaciendo de mejor manera su necesidad o expectativa		

Difundir o dar a conocer **a los expertos: profesionistas, peritos, especialistas, investigadores, académicos:**

Que	Para qué	Quién	Cómo
Normas obligatorias, normas voluntarias, procedimientos de evaluación de la conformidad aplicables y en particular, los modos de atestación aceptables para todas las normas	Para que asesoren capaciten a su vez y ayuden profesionalmente a los productores en el cumplimiento de dichas normas y en la aplicación de los procedimientos de evaluación de la conformidad respectivos	Dependencias, agencias o autoridades regulatorias u organismos de normalización reconocidos, en colaboración con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	Con programas de capacitación, actualización y divulgación para los productores (cursos, seminarios, publicaciones y otros medios idóneos)

Difundir o dar a conocer **a las autoridades regulatorias o responsables de procurar el bienestar y la protección del consumidor** encargadas de vigilar que se cumplan las normas:

Que	Para qué	Quién	Cómo
Normas obligatorias, procedimientos de evaluación de la conformidad aplicables y en particular, los modos de atestación aceptables para esas normas	Para exigir y vigilar su aplicación y cumplimiento	Dependencias, agencias o autoridades regulatorias en colaboración con expertos y asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	Con programas de capacitación, actualización y divulgación para los productores (cursos, seminarios, publicaciones y otros medios idóneos)

Difundir o dar a conocer **a los expertos en evaluación de la conformidad**:

Que	Para qué	Quién	Cómo
Normas obligatorias, normas voluntarias, procedimientos de evaluación de la conformidad aplicables y en particular, los modos de atestación aceptables para todas esas normas	Para que asesoren, capaciten a su vez y ayuden profesionalmente a los productores en el cumplimiento de dichas normas, en la aplicación de los procedimientos de evaluación de la conformidad respectivos y, particularmente en la aplicación de los métodos y procedimientos de ensayo/prueba y/o medición	Dependencias, agencias o autoridades regulatorias u organismos de normalización reconocidos, en colaboración con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	Con programas de capacitación, actualización y divulgación para los productores (cursos, seminarios, publicaciones y otros medios idóneos)

Difundir o dar a conocer **a los académicos de las instituciones educativas:**

Que	Para qué	Quién	Cómo
Normas obligatorias, normas voluntarias, procedimientos de evaluación de la conformidad aplicables y en particular, los modos de atestación aceptables para todas esas normas	Para que lo enseñen a sus alumnos en los programas regulares de cursos de diferentes niveles educativos (educación básica, media, superior, de extensión académica o de divulgación, entre otros)	Dependencias, agencias o autoridades regulatorias u organismos de normalización reconocidos, en colaboración con asociaciones, cámaras y sindicatos empresariales, industriales, de comercio o de servicios	Con programas de capacitación, actualización y divulgación para los productores y expertos (cursos, seminarios, publicaciones y otros medios idóneos)

En este capítulo, la actividad de difusión de las normas y de los procedimientos de evaluación de la conformidad es fundamental si aspiramos a que ciertas actividades o sus resultados se normalicen real y efectivamente.

2.LA NORMALIZACIÓN EN LA SEGURIDAD DE LAS TECNOLOGÍAS DE LA INFORMACIÓN

2.1 El papel de las normas en la seguridad de la información

En años recientes el avance de la tecnología en sus diferentes áreas ha tenido un impacto sin precedentes en la historia de la humanidad, no puede transcurrir un día sin que tengamos algún contacto significativo con alguno de los avances tecnológicos que mantienen funcionando nuestro entorno social al cual nos unimos al despertar y en muchos casos no termina durante el sueño.

Esta dependencia tecnológica es la misma que nos hace vulnerables a un fallo en los mecanismos destinados a mantener los aspectos fundamentales de seguridad de la información. Con este problema en escena tenemos algunos actores como el gobierno, bancos, empresas, iniciativa privada y otros más que están preocupados en una de las áreas con mayor interés en los años recientes en el campo de cómputo: La Seguridad Informática.

Derivado a esta problemática se han establecido leyes, marcos de trabajo, buenas prácticas y normas que permiten la confianza entre distintas entidades en materia de gestión de la seguridad de la información y en el cumplimiento de los requisitos mínimos de seguridad, que permitan ganar una ventaja frente a sus competidores siendo este el tema a ser tratado en el desarrollo del presente trabajo.

En los últimos años, la mayor parte de la información reside en equipos informáticos, redes de datos y medios de almacenamiento, en el mundo de la electrónica y el ciberespacio, hemos necesitado cada vez más hacer frente al impacto en materia de seguridad y privacidad. Las tecnologías de la información aportan un nivel de desafíos, que son motivo de preocupación para los individuos y empresas, así como a las administraciones.

Así que, mediante el intercambio de mejores prácticas y especificando el estado de las técnicas y mecanismos, se puede ayudar a mejorar la calidad de los procesos y también la calidad de las soluciones, las normas de seguridad puede ayudar a empresas, administraciones, y particulares. Lo especial es que la seguridad es un área horizontal en que se aplica a básicamente todo y debe ser considerado esencialmente en todas partes.

Se ha visto la importancia del papel que juega la Seguridad para cualquier organización; y es este interés lo que ha llevado a diferentes entidades a elaborar programas de capacitación, foros, comités, congresos, grupos de trabajo, instituciones, etcétera; dedicados al intercambio y fortalecimiento del conocimiento relacionado a este tema.

Particularmente la seguridad en cómputo no es una ciencia y con esto, tampoco lo es la seguridad de la información; aunque se han hecho muchos esfuerzos para poder evaluar o valorar la seguridad de un sistema, aplicación, producto o servicio. Algunos ejemplos de estos esfuerzos son las normas, las buenas prácticas, las publicaciones, los marcos de trabajo, los métodos, los manuales, las guías, los lineamientos y directrices que buscan integrar y estandarizar el conocimiento y poder así medir la seguridad cuantitativamente.

2.2 Organismo internacional que se encarga de realizar las normas en el sector de TI

La actividad comercial internacional ha establecido la necesidad de tomar como referencia las normas que son acordadas por consenso mundial dentro de organismos internacionales. Surge

así un foro que crea un lenguaje común y un mínimo a exigir en lo que se integra al comercio mundial; con el fin de evitar barreras técnicas o una competencia injusta.

Por tal motivo la ISO ⁴⁾ es el mayor desarrollador mundial de las normas internacionales voluntarias. Fue fundada en 1947, y desde entonces ha publicado más de 19 500 Normas Internacionales que abarca casi todos los aspectos de la tecnología y los negocios.

ISO es una organización independiente, no gubernamental compuesta por miembros de los organismos nacionales de normalización de 163 países. Dichos miembros desempeñan un papel vital en nuestra forma de actuar, se reúnen una vez al año para una Asamblea General que decide sobre los objetivos estratégicos en diferentes áreas.

Las normas ISO hacen una contribución positiva al mundo en que vivimos, facilitan el comercio, diseminan el conocimiento, difunden los avances innovadores en tecnología, y comparten buenas prácticas de gestión y de evaluación de la conformidad.

Las normas ISO proporcionan soluciones y logran beneficios para casi todos los sectores de actividad, incluida la agricultura, la construcción, la ingeniería mecánica, la fabricación, la distribución, el transporte, los dispositivos médicos, el medio ambiente, la energía, la gestión de calidad, la evaluación de la conformidad y las tecnologías de la información y comunicación.

ISO desarrolla sólo normas para las cuales existe un requerimiento indiscutible en el mercado. El trabajo se lleva a cabo por expertos en el tema provenientes directamente de sectores industriales, técnicos y empresariales que han identificado la necesidad de una norma, y que posteriormente la utilizan. A estos expertos se les pueden unir otras personas con conocimientos pertinentes, tales como representantes de agencias gubernamentales, laboratorios de pruebas, asociaciones de consumidores y el mundo académico, y por organizaciones internacionales gubernamentales y no gubernamentales.

2.2.1 ¿Qué es el ISO / IEC JTC 1 / SC 27 Security techniques?

Es un subcomité del Comité Mixto Técnico ISO / IEC JTC 1 de la ISO y la Comisión Electrotécnica Internacional (IEC), que desarrolla y facilita las Normas Internacionales, informes y especificaciones técnicas en el campo de las técnicas de seguridad de TI.

La actividad de normalización de este subcomité incluye métodos generales, técnicas y directrices para abordar tanto los aspectos de seguridad y privacidad. Los borradores de las Normas Internacionales del ISO / IEC JTC 1 o de cualquiera de sus subcomités son enviados para que participen los organismos nacionales de normalización para la votación, comentarios y aportaciones. La publicación como Norma Internacional ISO / IEC requiere la aprobación de un mínimo del 75% de los organismos nacionales con derecho a voto.

El ISO / IEC JTC 1 / SC 27 se estableció en 1990, cuando el ISO / TC 97 / SC 20, cubría la normalización en el campo de las técnicas de seguridad, tales como "técnicas de clave secreta" (ISO / TC 97 / SC 20 / WG 1) y "técnicas de clave pública" (ISO / TC 97 / SC 20 / WG 2), hasta que toman la decisión de parar las actividades de estos 2 WG's. Esto permitió que el ISO / IEC JTC 1 / SC 27 se hiciera cargo de la labor que tenía el ISO / TC 97 / SC 20 del WG 1 y del WG 2, así como para ampliar su ámbito de aplicación a otras áreas dentro del campo de las técnicas de seguridad informática.

El subcomité amplió su estructura con el tiempo para tener cinco WG's, modificando su alcance para satisfacer las demandas actuales de normalización.

El ámbito de aplicación de las normas del ISO / IEC JTC 1 / SC 27 es "El desarrollo de normas para la protección de la información y las TIC. Esto incluye métodos genéricos, técnicas y directrices para abordar tanto los aspectos de seguridad y privacidad, como por ejemplo:

- Los requisitos de seguridad;
- La gestión de la seguridad de la información y las TIC; en particular los sistemas de gestión de seguridad de la información (SGSI), los procesos de seguridad, los controles y servicios de seguridad;
- Mecanismos de seguridad de cifrado y otros, incluyendo pero no limitado a mecanismos de protección de la rendición de cuentas, la disponibilidad, integridad y confidencialidad de la información;
- Documentación para la gestión de la seguridad, incluida la terminología, las directrices, así como los procedimientos para el registro de los componentes de seguridad;
- Aspectos de seguridad de la gestión de identidad, biometría y la privacidad;
- La evaluación de la conformidad, requisitos de acreditación y auditoría en el ámbito de la seguridad de la información;
- Criterios de seguridad y la metodología de evaluación.

El ISO / IEC JTC 1 / SC 27 se dedica a la coordinación y colaboración activa con los organismos pertinentes para garantizar el correcto desarrollo y aplicación de las normas e informes técnicos en los ámbitos pertinentes.

El ISO / IEC JTC 1 / SC 27 se compone de cinco grupos de trabajo, cada uno de los cuales lleva a cabo tareas específicas en el desarrollo de normas en el ámbito de las técnicas de seguridad de TI. El enfoque de cada grupo de trabajo se describe en los términos de referencia del grupo.

Los grupos son:

Grupo de Trabajo	Área de Trabajo
ISO / IEC JTC 1 / SC 27 / WG 1	Sistemas de gestión de seguridad de la información
ISO / IEC JTC 1 / SC 27 / WG 2	Mecanismos de criptografía y de seguridad
ISO / IEC JTC 1 / SC 27 / WG 3	Evaluación de la seguridad, pruebas y especificaciones
ISO / IEC JTC 1 / SC 27 / WG 4	Controles y servicios de seguridad
ISO / IEC JTC 1 / SC 27 / WG 5	Gestión de la identidad y tecnologías de privacidad

2.3 Normas de seguridad de la información

La familia de normas de seguridad de la información más conocida es la serie 27000, que son normas que están relacionadas entre sí; algunas ya se encuentran publicadas o en desarrollo y que contienen una serie de componentes estructurales importantes.

Estos componentes se centran en normas regulatorias para describir los requisitos de un SGSI (ISO/IEC 27001) y los requisitos para los organismos de certificación (ISO/IEC 27006) que certifiquen la conformidad con la norma 27001.

Otras normas ofrecen directrices para los diversos aspectos de la implementación de un SGSI, dirigiéndose a un proceso genérico, guías para los controles relacionados de seguridad, así como de sectores específicos.

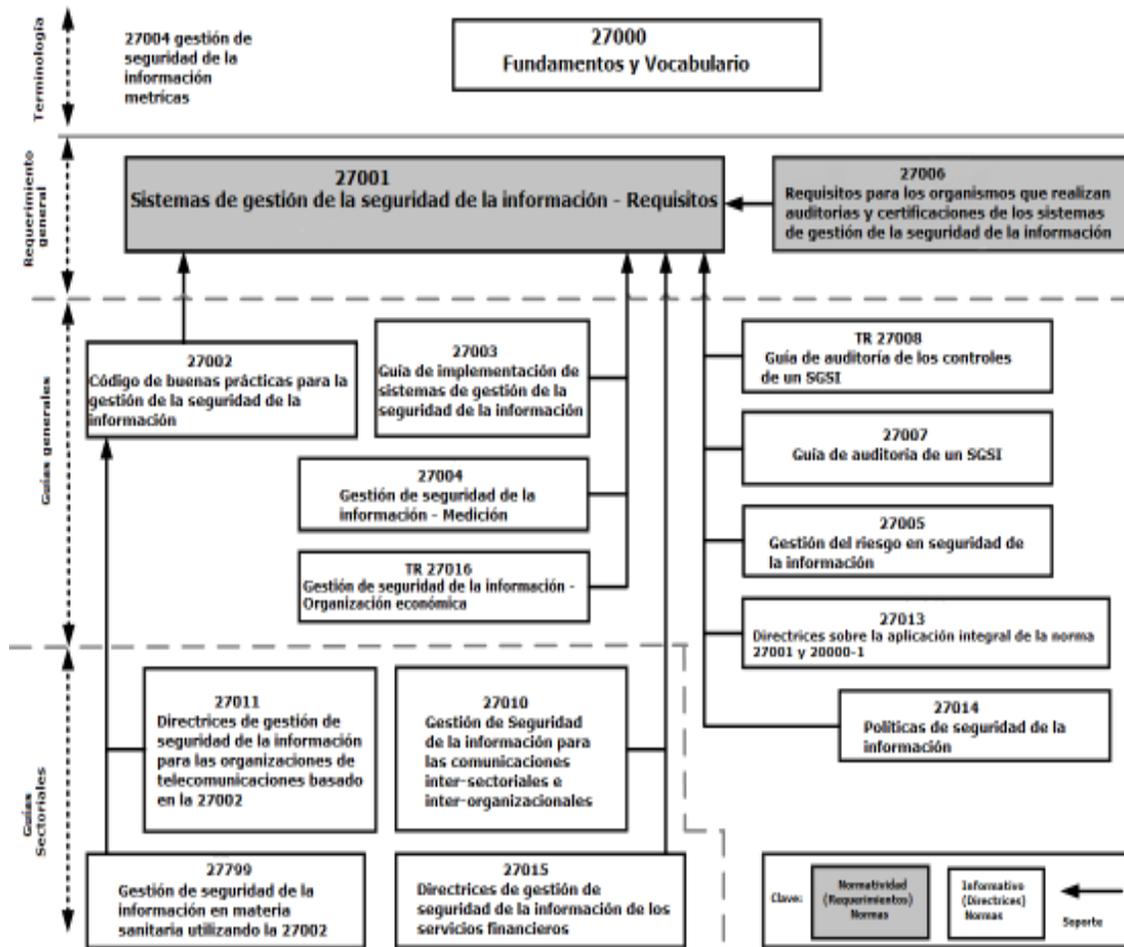


Figura 1 Relaciones entre las normas de la familia 27000

Las normas que proporcionan un apoyo directo, una guía detallada y/o una interpretación de los procesos generales del Plan-Do-Check-Act, (Planear-Hacer-Verificar-Actuar); y los requisitos específicos de la norma ISO/IEC 27001 son:

ISO/IEC 27000	Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary
ISO/IEC 27002	Information technology -- Security techniques -- Code of practice for information security controls
ISO/IEC 27003	Information technology -- Security techniques -- Information security management system implementation guidance
ISO/IEC 27004	Information technology -- Security techniques -- Information security management – Measurement
ISO/IEC 27005	Information technology -- Security techniques -- Information security risk management
ISO/IEC 27007	Information technology -- Security techniques -- Guidelines for information security management systems auditing
ISO/IEC 27013	Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1

ISO/IEC 27014	Information technology -- Security techniques -- Governance of information security
ISO/IEC 27016	Information technology -- Security techniques -- Information security management -- Organizational economics

La norma que proporciona apoyo directo, una orientación y/o interpretación detallada de los controles especificados en la ISO/IEC 27002 es:

ISO/IEC 27008	Information technology -- Security techniques -- Guidelines for auditors on information security controls
---------------	---

La norma que se ocupa de los requisitos de los organismos que realizan las certificaciones del SGSI es:

ISO/IEC 27006	Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems
---------------	---

Las normas que describen las directrices sectoriales orientadas para un SGSI son:

ISO/IEC 27010	Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications
ISO/IEC 27011	Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002
ISO/IEC 27015	Information technology -- Security techniques -- Information security management guidelines for financial services
ISO/IEC 27799	Health informatics -- Information security management in health using ISO/IEC 27002

La familia de normas de la serie 27000 mantiene relaciones con muchas normas ISO/IEC, además se clasifican y se describen ya sea:

- a) Normas que describen una visión general y terminología;
- b) Normas que especifican los requisitos;
- c) Normas que describen los lineamientos generales;
- d) Normas que describen directrices específicas por sector.

2.3.1 Normas que describen una visión general y terminología

ISO/IEC 27000:2014 – Tecnologías de la Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Información general y vocabulario, proporciona la visión general de los Sistemas de Gestión de Seguridad de la Información (SGSI), y los términos y las definiciones utilizadas en la familia de normas 27000. Es aplicable a todos los tipos y tamaños de organización (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro).

2.3.2 Normas que especifican los requisitos

ISO/IEC 27001:2013 - Tecnologías de la Información – Técnicas de seguridad – Sistemas de Gestión de Seguridad de la Información – Requisitos, especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un SGSI en el contexto de la organización. También incluye los requisitos para la evaluación y el tratamiento de los riesgos de seguridad de información adaptados a las necesidades de la organización. Los requisitos establecidos son genéricos y se pretende que sean aplicables a todas las organizaciones, sin importar su tipo, tamaño o naturaleza.

ISO/IEC 27006:2011 – Tecnologías de la Información – Técnicas de seguridad - Requisitos para los organismos que realizan la auditoría y la certificación de Sistemas de Gestión de Seguridad de la Información, especifica los requisitos y proporciona una guía para los organismos que realizan la auditoría y la certificación de un Sistema de Gestión de Seguridad de la Información (SGSI), además de los requisitos contenidos en la norma ISO/IEC 17021 e ISO/IEC 27001. Está pensado principalmente para apoyar a la acreditación de los organismos de certificación que ofrecen la certificación del SGSI.

2.3.3 Normas que describen las directrices generales

ISO/IEC 27002:2013 - Tecnologías de la Información – Técnicas de seguridad – Código de buenas prácticas para los controles de seguridad de la información, proporciona directrices para las normas de seguridad de la información de la organización y las prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de los controles, teniendo en cuenta el medio ambiente de riesgos de seguridad de información de la organización.

ISO/IEC 27003:2010 – Tecnologías de la Información – Técnicas de seguridad – Guía de implementación de Sistemas de Gestión de Seguridad de la Información, se centra en los aspectos críticos necesarios para el éxito del diseño e implementación de un SGSI según la norma ISO/IEC 27001:2013. En ella se describe el proceso de especificación del Sistema de Gestión de Seguridad de la Información y el diseño desde el inicio hasta la producción de los planes de ejecución. En ella se describe el proceso de obtener la aprobación de la gerencia para implementar un SGSI, se define un proyecto para implementar un SGSI (mencionadas en la norma ISO/IEC 27003:2010 como el proyecto de SGSI), y proporciona orientación sobre cómo planificar el proyecto del SGSI, resultando en un plan final del SGSI como un proyecto de implementación.

ISO/IEC 27004:2009 - Tecnologías de la Información – Técnicas de seguridad – Gestión de seguridad de la información– Medición, proporciona orientación sobre el desarrollo y uso de las medidas y la medición con el fin de evaluar la eficacia de un Sistema de Gestión de Seguridad de la Información, implementado los controles o grupos de controles, como se especifica en la norma ISO/IEC 27001:2013 y es aplicable a todos los tipos y tamaños de organización.

La ISO/IEC 27005:2011 – Tecnologías de la información – Técnicas de seguridad – Gestión de riesgos de seguridad de la información, proporciona directrices para la gestión de riesgos de seguridad de la información, es compatible con los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro), que tienen la intención de gestionar los riesgos que podrían comprometer la seguridad de la información de la organización.

ISO/IEC 27007:2011 - Tecnologías de la información – Técnicas de seguridad - Directrices para la auditoría de sistemas de gestión de seguridad de la información, proporciona orientación sobre el manejo de un sistema de gestión de seguridad de la información y el programa de auditoría, en la realización de las auditorías, y en la competencia de los auditores de un SGSI, además de las directrices contenidas en la norma ISO 19011. Es aplicable para aquellos que necesitan comprender o realizar auditorías internas o externas de un SGSI o para gestionar un programa de auditorías de un SGSI.

La ISO/IEC TR 27008:2011 - Tecnologías de la información – Técnicas de seguridad - Directrices para los auditores sobre los controles de seguridad de la información, proporciona orientación sobre la revisión de la implementación y operación de los controles, incluyendo la comprobación del cumplimiento técnico de los controles del sistema de información, de conformidad con las normas establecidas de seguridad de la información de una organización. Es aplicable a todos los tipos y tamaños de organizaciones, incluidas las empresas públicas y privadas, entidades gubernamentales y organizaciones sin fines de lucro que lleven a cabo revisiones de seguridad de la información y los controles de conformidad técnica.

La ISO/IEC 27013:2012 - Tecnologías de la información – Técnicas de seguridad - Guía para la aplicación integrada de la norma ISO / IEC 27001 e ISO / IEC 20000-1, proporciona directrices sobre la aplicación integrada de la ISO/IEC 27001 e ISO / IEC 20000-1 para las organizaciones que tienen la intención de:

- a) Implementar la norma ISO / IEC 27001 para la ISO / IEC 20000-1 que ya está implementada, o viceversa;
- b) Aplicar las normas ISO / IEC 27001 e ISO / IEC 20000-1 juntas;
- c) Integrar la norma ISO / IEC 27001 vigente y la ISO / IEC 20000-1 en los sistemas de gestión.

La ISO/IEC 27013:2012 se centra exclusivamente en la aplicación integrada de la ISO/IEC 27001 e ISO / IEC 20000-1.

La ISO/IEC 27014:2013 – Tecnologías de la información – Técnicas de seguridad – Gobierno de seguridad de la información, proporciona orientación sobre los conceptos y principios para el gobierno de la seguridad de la información, mediante el cual las organizaciones pueden evaluar, dirigir, controlar y comunicar las actividades relacionadas con la seguridad de la información dentro de la organización, es aplicable a todos los tipos y tamaños de organizaciones.

ISO/IEC TR 27016:2014 - Tecnologías de la información – Técnicas de seguridad - Gestión de la seguridad de la información - Economía de las organizaciones, proporciona directrices sobre cómo una organización puede tomar decisiones para proteger la información y entender las consecuencias económicas de estas decisiones en el contexto de las necesidades que compiten por los recursos, es aplicable a todos los tipos y tamaños de organizaciones y proporciona información para que las decisiones económicas en la gestión de seguridad de la información de la alta dirección que tenga la responsabilidad de las decisiones de seguridad de la información.

2.3.4 Normas que describen las directrices específicas del sector

ISO/IEC 27010:2012 - Tecnologías de la información – Técnicas de seguridad - Gestión de la seguridad de la información para las comunicaciones inter-sectoriales e inter-organizacionales, proporciona directrices, además de la orientación que figuran en las normas de la familia 27000 para la aplicación de la gestión de seguridad de la información dentro de las comunidades de intercambio de información. Además proporciona controles y orientaciones relativas específicamente a iniciar, implementar, mantener y mejorar la seguridad de la información en las comunicaciones interinstitucionales e intersectoriales, es aplicable a todas las formas de intercambio y difusión de información sensible, tanto pública como privada, nacional e internacional, dentro de la misma industria o sector del mercado o entre sectores. En particular, puede ser aplicable a los intercambios de información y el intercambio en relación con el suministro, el mantenimiento y la protección de una organización de la infraestructura crítica o del estado-nación.

ISO/IEC 27011:2008 - Tecnologías de la información – Técnicas de seguridad - Directrices de gestión de seguridad de información para las organizaciones de telecomunicaciones basados en la norma ISO / IEC 27002, el alcance de esta recomendación es definir directrices que fomenten la aplicación de la gestión de seguridad de la información en las organizaciones de telecomunicaciones. La adopción de esta norma permitirá a las organizaciones de telecomunicaciones satisfacer las necesidades de gestión de seguridad de la información de línea de base de la confidencialidad, integridad, disponibilidad y cualquier otra propiedad de seguridad pertinentes.

ISO/IEC TR 27015:2012 - Tecnologías de la información – Técnicas de seguridad - Directrices de gestión de seguridad de información para los servicios financieros, proporciona información de seguridad complementación orientación y, además de los controles de seguridad de la información definidos en la norma ISO / IEC 27002 para iniciar, implementar, mantener y mejorar la seguridad de la información dentro de las organizaciones que prestan servicios financieros.

ISO/IEC 27799:2008 - Informática sanitaria – Gestión de seguridad de la información en materia de salud mediante la norma ISO / IEC 27002, especifica un conjunto de controles detallados para la gestión de seguridad de la información sanitaria y ofrece directrices sobre mejores prácticas. Mediante la implementación de esta norma internacional, las organizaciones sanitarias serán capaces de garantizar un nivel mínimo de seguridad requerido que sea apropiado a las circunstancias de su organización y que va a mantener la confidencialidad, integridad y disponibilidad de la información, se aplica a la información sanitaria en todos sus aspectos; cualquiera de las formas en las que se presente la información (palabras y números, grabaciones sonoras, dibujos, vídeos e imágenes médicas), cualquier medio que usen para almacenarla (impresión o escritura en papel o de almacenamiento electrónico) y cualquier medio que utilicen para transmitirlo (a mano, por fax, a través de redes informáticas o por correo), ya que la información siempre debe ser protegida de manera apropiada.

2.4 Adopción de normas en el Organismo Nacional de Normalización "NYCE" (Normalización y Certificación Electrónica, S.C.)

Normalización y Certificación Electrónica, S.C., NYCE, es el organismo responsable, en México, del desarrollo de las normas de Electrónica, Telecomunicaciones y Tecnologías de la Información, así como el organismo líder en la prestación de servicios de evaluación de la conformidad para estos sectores y muchos otros, contribuyendo a la sociedad mediante estas actividades que son herramientas para lograr la competitividad de los productos y servicios, su

adecuado acceso a mercados, así como para garantizar que todos los concurrentes participan con las mismas reglas del juego.

NYCE fue creado en noviembre de 1994 por 35 empresas líderes de la rama electrónica, de telecomunicaciones y tecnologías de información. Se encuentra acreditado y aprobado con base en la Ley Federal sobre Metrología y Normalización, por las instancias legales conducentes, para brindar servicios de normalización y evaluación de la conformidad.

Entre las principales actividades de NYCE destaca la elaboración de Normas Mexicanas (NMX) y la coordinación de actividades para que nuestro país participe en la elaboración de normas internacionales, en los ámbitos de la electrónica, tecnologías de la información y telecomunicaciones. Las NMX y las normas internacionales son importantes porque detonan diversos factores para los consumidores y para la industria, tales como:

- Facilitar el diseño y manufactura
- Racionalizar procesos y operaciones
- Promover economía con calidad
- Simplificar la comunicación y el comercio
- Inspirar confianza en el fabricante por parte de los consumidores

NYCE cuenta dentro de su estructura organizacional con Comités Técnicos Nacionales de Normalización (CTNN), Subcomités y Grupos de trabajo para la elaboración de NMX y Subcomités para la participación de nuestro país en la elaboración de normas internacionales.

Los Comités Técnicos Nacionales de Normalización para la elaboración de NMX y los Subcomités para la participación de nuestro país en la elaboración de normas internacionales, se conforman con la participación voluntaria de todos los actores involucrados en el tema: academia, industria, gobierno, consumidores, proveedores, distribuidores, entre otros.

NYCE debe garantizar que en la elaboración de sus NMX y de las posiciones que emanen de nuestro país para la elaboración de normas internacionales, se tomen en cuenta la opinión de los actores involucrados.

2.5 Desarrollo de una NMX-NYCE

Como se menciona en el capítulo anterior NYCE tiene a su cargo subcomités que se encargan de la elaboración de Normas Mexicanas, en este caso nos enfocaremos al subcomité de "Seguridad de TI" el cual está constituido por un coordinador, un secretario técnico (un servidor) y una serie de representantes de (academia, industria, gobierno, consumidores, proveedores, distribuidores, entre otros).

A continuación cuento paso a paso como son adoptadas las Normas Mexicanas, en las cuales describo la manera en la que participo y el papel que desarrollo en el organismo en 10 etapas:

1.- Definición de viabilidad del Anteproyecto:

El secretariado técnico comienza convocando al subcomité de "Seguridad de TI" con la finalidad de identificar las necesidades de los temas a desarrollar en el año corriente.

2.- Inscripción del tema en el PNN o el SPNN:

Una vez que identificamos los temas, estos se deben de inscribir en el Programa Nacional de Normalización (PNN) el cual debe estar estructurado con los temas nuevos a desarrollar,

modificar, reprogramar o cancelar. Una vez que se tiene estructurado el PNN, éste se debe entregar a la Dirección General de Normas (DGN) el último día del mes de noviembre para que la DGN gestione su publicación en el Diario Oficial de la Federación (DOF) y una vez publicado tenemos un lapso de un año para desarrollar los temas inscritos.

El Suplemento del Programa Nacional de Normalización (SPNN) es básicamente el mismo proceso que el antes descrito, a diferencia que en este se incluyen los temas que por alguna razón no pudieron ser inscritos en el PNN y este debe ser entregado a la DGN el último día de junio para que de igual manera sea publicado en el DOF.

3.- Elaboración de los Anteproyectos:

En la elaboración de un Anteproyecto se verifica que exista una norma internacional que nos pueda ayudar a desarrollar el tema, si existe la norma entonces se transcribe a lo que es llamado formato Z13; de no existir norma se debe realizar una investigación bien documentada que cubra los puntos a normalizar y de igual forma se debe pasar a formato Z13. Una vez que se tiene terminado el Anteproyecto en Z13 se debe verificar que se cumple con lo establecido en la ley federal de metrología y normalización y a lo establecido en la Z13.

Ya que se realizó la revisión se somete el Anteproyecto ante el subcomité de "Seguridad de TI" y se establece una fecha límite para su revisión y envío de comentarios ante el secretariado técnico.

Una vez que se vence la fecha establecida de revisión se verifica si hubo comentarios, si hay comentarios se hace un concentrado de ellos y se convoca al subcomité con la finalidad de desahogarlos.

De no existir comentarios se pasa a la siguiente etapa.

Nota 1: El formato Z13 se refiere a la norma establecida para realizar normas.

Nota 2: Un Anteproyecto es el borrador inicial con el que empezamos a cubrir los puntos a normalizar.

4.- Aprobación de proyecto para Consulta Pública

Una vez que nuestro Anteproyecto ya no tiene ningún comentario por parte del subcomité, el secretariado técnico convoca a una reunión con la finalidad de rubricar el Anteproyecto.

Ya que se cuenta con el Proyecto rubricado por parte del subcomité de "Seguridad de TI", el secretariado técnico debe solicitar al COTENNETIC (Comité Técnico de Normalización Nacional de Electrónica y Tecnologías de la Información y Comunicación) la aprobación de su publicación de Consulta Pública del Proyecto.

Nota 3: Un Anteproyecto pasa a Proyecto una vez que se rúbrica para que sea enviado a Consulta Pública.

Nota 4: El COTENNETIC es un comité conformado por el coordinador de cada subcomité que coordina NYCE, dicho comité se encarga de revisar los trabajos de cada subcomité que tiene a su cargo NYCE.

5.- Gestión de publicación del PROY-NMX en el DOF por parte de DGN

Una vez que el Proyecto fue aprobado el secretariado técnico gestiona ante la DGN dicha publicación, entregándole un ejemplar el cual lo revisa y emite comentarios; si es el caso donde hay comentarios el secretariado técnico debe atenderlos lo más pronto posible para no postergar la publicación, de no existir comentarios la DGN solicita al DOF la publicación de su Consulta Pública del Proyecto.

6.- Aviso de Consulta Pública

Una vez que se publica el Proyecto en el DOF, los próximos 60 días naturales el Proyecto estará expuesto a que cualquier persona lo revise y emita comentarios técnicos bien sustentados.

Después de transcurrir los 60 días:

- 1) Si no se reciben comentarios se pasa al siguiente paso.
- 2) Si se emitieron comentarios, el secretariado técnico debe informarle al subcomité de "Seguridad de TI" que el Proyecto recibió comentarios y se deben atender. El secretariado técnico convoca a una reunión del subcomité con la persona que emite los comentarios; se atienden los comentarios que procedan y tengan un sustento confiable, los comentarios que no proceden no se toman en cuenta, dichas modificaciones se deben incorporar al Proyecto.

7.- Aprobación de proyecto para Declaratoria de Vigencia

Para este paso ya contamos con un Proyecto al cual se le hicieron modificaciones o no según sea el caso como se describió en el paso anterior.

Nuevamente el secretariado técnico convoca al subcomité de "Seguridad de TI" a una reunión para rubricar dicho Proyecto, ya que se tiene rubricada la Norma el secretariado técnico solicita al COTENNETIC su aprobación para que se gestione ante la DGN la publicación en el DOF la Declaratoria de Vigencia de la Norma.

8.- Gestión de publicación de la NMX en el DOF por parte de DGN

Una vez que la Norma5 fue aprobada el secretariado técnico entrega un ejemplar a la DGN la cual revisará y emitirá comentarios; si es el caso donde hay comentarios el secretariado técnico debe atenderlos lo más pronto posible para no postergar la publicación, de no existir comentarios la DGN solicita al DOF la publicación de la Declaratoria de Vigencia de la Norma.

Nota 5: Un Proyecto se vuelve Norma una vez que se rúbrica el Proyecto para que sea enviado a Declaratoria de Vigencia.

9.- Publicación de NMX definitiva en el DOF

Una vez que se publica la Norma en el DOF, los próximos 60 días naturales la Norma estará expuesta a que cualquier persona la revise y emita comentarios técnicos bien sustentados.

Después de transcurrir los 60 días:

- 1) De no haber recibido comentarios, se pasa al siguiente paso.

- 2) De ser el caso que se hayan emitido comentarios el secretariado técnico debe informarle al subcomité de "Seguridad de TI" que la Norma recibió comentarios y se deben atender. El secretariado técnico convoca a una reunión del subcomité con la persona que emite los comentarios; se atienden los comentarios que proceden y tengan un sustento confiable, los comentarios que no proceden no se toman en cuenta, dichas modificaciones se deben incorporar en la Norma.
- 3) Si las modificaciones que se incorporaron a la Norma son muy drásticas, se debe solicitar a la DGN que se repita nuevamente el paso anterior.

10.- Entrada en vigor de la NMX

Ya que transcurrieron los 60 días naturales y la Norma no recibió comentarios, entonces esta Norma se considera como un documento vigente el cual podrá ser utilizado por las organizaciones y las dependencias de gobierno que lo soliciten.

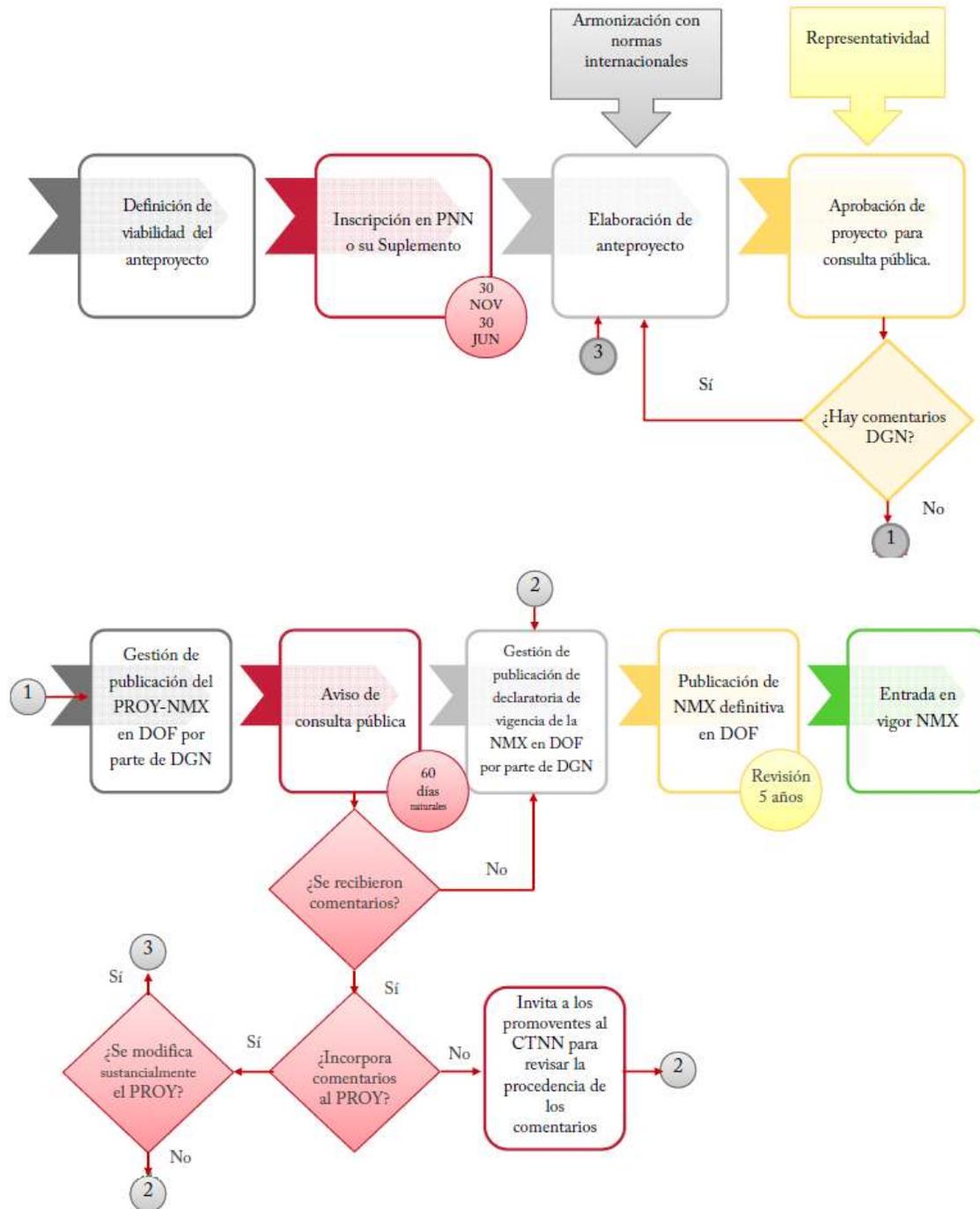


Figura 2 Desarrollo de una NMX-NYCE

2.6 Beneficios de adoptar NMX-NYCE

El sistema nacional de normalización mexicano debe existir apoyado por las industrias y el sector gubernamental para conseguir que los productos nacionales se fabriquen en condiciones tales que cumplan satisfactoriamente con los requisitos que demandan las economías globalizadas.

La NMX puede convertirse en un documento de observancia obligatoria cuando se hace referencia a él en un instrumento legal de observancia obligatoria; por ejemplo, en un reglamento o en una NOM. Como compromiso del "código de buena conducta para la elaboración, adopción y aplicación de Normas" del Acuerdo sobre Obstáculos Técnicos al Comercio de la OMC, en la mayoría de los casos, NYCE trabaja en la armonización de sus Normas Mexicanas, traduciendo las normas internacionales para adecuarlas a las necesidades del país, respetando los derechos de propiedad intelectual que existan sobre ellas.

Algunas ventajas para el país son:

- Medio eficaz y adecuado técnicamente para la protección del consumidor
- Instrumento de transferencia de tecnología
- Factor fundamental para el aumento de la productividad
- Elemento que permite el acceso a mercados internacionales

Ventajas para los consumidores:

- Garantía de intercambiabilidad y calidad
- Facilidad en la formulación de pedidos
- Acceso a datos técnicos antes dispersos o inciertos
- Bases técnicas para licitaciones

Y por último las ventajas para las empresas:

- Información como mecanismo de comunicación
- Enriquecimiento tecnológico
- Intercambiabilidad
- Estabilidad y mejoramiento de la calidad
- Simplificación y reducción de costos

3. OPORTUNIDADES DE CRECIMIENTO PARA NYCE

3.1 Propuestas de mejora

A lo largo de estos 3 años en el organismo, he podido notar una serie de deficiencias que son importantes y que están siendo atendidas. Como en toda organización se busca mejorar día con día los servicios que ofrece el organismo, con la finalidad de tener la lealtad de los usuarios.

Estas son las insuficiencias con las que cuenta el organismo:

- El organismo cuenta con procedimientos obsoletos, derivado de esto existen anomalías y retardos en los procesos de revisión y emisión de NMX
- Los ingresos económicos que tiene el organismo son gracias a la certificación electrónica, pero las normas con las que son verificadas las certificaciones son NMX que son obsoletas
- Existe poco personal calificado para la atención de elaboración de NOM´s
- Los servicios que ofrece NYCE se ven limitados a falta de certificación de nuevas normas
- Ser un organismo que certifica procedimientos de TI y no contar con uno, disminuye la credibilidad con el usuario
- Falta de motivación por parte de NYCE con los trabajadores

Estas son solo algunas de las problemáticas que tiene el organismo y se han estado atendiendo de la siguiente forma demostrando el beneficio que se obtiene.

- El organismo no tiene claro sus procedimientos internos de normalización
- Las normas que son importantes para NYCE no están actualizadas
- Hay poca participación en los subcomités que coordina NYCE
- Las normas tardaban demasiado en su procedimiento de revisión por parte de los subcomités
- En la parte internacional se distribuyen muchos documentos, por lo cual saturamos las bandejas de correo de los miembros que pertenecen al subcomité
- El organismo no cumple con las fechas establecidas para la emisión de votaciones
- El organismo no tiene mucha participación en la elaboración de NOM´s
- La página web con la que cuenta el organismo, no tiene información relevante a los trabajos de normalización
- Se detectaron anomalías en el catálogo de normas
- Cuando los integrantes del departamento salen atender reuniones de trabajo el departamento de normalización se queda solo y no existe alguien que pueda apoyar a los usuarios con información sobre las normas
- El mismo personal del organismo no conoce sobre la normalización
- Los servicios que ofrece NYCE se han visto limitados a falta de más normas

Estas deficiencias son en las que nos hemos enfocado a corregir, ya que vemos oportunidades de mejora y crecimiento para el organismo.

- El organismo no tiene claro sus procedimientos internos de normalización

Solución

Se realizó un análisis a detalle del procedimiento normalización, y se descubrió porque el departamento tenía inconsistencias a la hora de realizar normas, por tal motivo se reestructuraron los procedimientos

- Las normas que son importantes para NYCE no están actualizadas

Solución

Se actualizaron las normas más importantes para NYCE y con esto se logra que nuestra NMX sea referenciada en una NOM

- Hay poca participación en los subcomités que coordina NYCE

Solución

La solución ha sido la de difundir lo que es la normalización y los beneficios que se alcanzan con esta, ya que en cierta forma comprueban que los servicios que ofrecen se apegan a las regulaciones y brindan mayor confianza a sus clientes

- Las normas tardaban demasiado en su procedimiento de revisión por parte de los subcomités

Solución

Tras analizar el procedimiento de revisión por parte del subcomité se detectó que se llevaba en un lapso de 4 a 6 meses, ya que no respetaban las fechas y acuerdos para realizar los avances de las normas. Se modificaron los lineamientos de los subcomités y ahora la revisión de cada norma se lleva en un máximo de 2 meses.

- En la parte internacional se distribuyen muchos documentos, por lo cual saturamos las bandejas de correo de los miembros que pertenecen al subcomité

Solución

Para la parte de distribución de documentos internacionales, primero se optó por filtrar los documentos correspondientes a cada WG, era una labor muy compleja ya que ahora se tenían que revisar los documentos uno por uno y canalizarlos a cada WG. Después de buscar soluciones se solicitó a nivel internacional se concediera a los integrantes tener acceso a los documentos y que estos ya fueran descargados por los mismos miembros

- El organismo no cumple con las fechas establecidas para la emisión de votaciones

Solución

Para atender las votaciones sin que se tuviera incumplimiento por rebasar la fecha establecida, se acordó darles una fecha límite y de no cumplir con ella se emite la votación a favor sin comentarios

- El organismo no tiene mucha participación en la elaboración de NOM's

Solución

Para aumentar la participación en la elaboración de NOM's, el organismo busca internamente quién puede participar y que cuente con la competencia adecuada para lograr que nuestras NMX sean referenciadas en las NOM's para que estas sean obligatorias. De no contar con alguno, se le manda capacitar para que pueda atender la elaboración de la NOM

- La página web con la que cuenta el organismo, no tiene información relevante a los trabajos de normalización

Solución

Nuestra página web se actualiza constantemente con las normas que demanda la industria, y se les informa de los avances que tienen los Proyectos y las NMX

Entre las mejoras que se han hecho para el departamento de normalización han sido las siguientes:

- Se estructuraron los procedimientos internos para tener un control adecuado sobre las NMX-NYCE.
- Se revisó detalladamente el ciclo de una norma con la finalidad de agilizar los procesos que conlleva a tener una norma NYCE.
- Se actualizaron las normas con más demanda por los usuarios, para estar a la vanguardia y competencia con mercados internacionales.
- Se creó un mecanismo interno para atender las votaciones relacionadas con la normalización internacional.
- Se apoya cada vez más a las dependencias de gobierno para que las NMX-NYCE sean referenciadas en las NOM para que sean de cumplimiento obligatorio en aduanas y fronteras.
- Se busca estar a la vanguardia con temas actuales, como por ejemplo la NMX-J-C-I-489-ANCE-ONNCCE-NYCE-2014, Centros de datos de alto desempeño - Sustentable y energético - Requisitos y métodos de comprobación.
- Gracias a la normalización se busca ampliar el catálogo de servicios que ofrece NYCE, ejemplo la NMX-I-291-NYCE-2013, Digitalización documental con valor agregado.
- Las licitaciones que ofrecen las dependencias de gobierno obligan a que las empresas competidoras estén certificadas con las NMX, en nuestro caso NMX-NYCE.

3.2 Conclusiones

La elaboración de este trabajo me ha permitido exponer una temática de interés creciente hoy en día en el terreno de la normalización, también me ha permitido consolidar el conocimiento de diferentes enfoques entorno a este tema, exponiendo la importancia para enfrentar una problemática actual.

Aunque el alcance de este trabajo se ha considerado en la parte de normalización, considero que la información que he presentado a lo largo del texto, es la más adecuada para guiar al lector a que se interese en estos temas, ya que hay muy poca difusión de lo que es este tema.

Así mismo hago una reflexión, y expongo a las futuras generaciones a que se interesen en estos temas.

La información que ha sido encontrada por el autor respecto algunos temas contemplados en este trabajo es escasa y en algunas circunstancias escritas por autores hispanoamericanos con una falta de conocimiento en profundidad de este tema, lo que indica una falta de personal experimentado o con conocimientos sólidos en la materia. Esta situación indudablemente cambiará con el tiempo, sin embargo; el tiempo requerido en este cambio marcará a futuro la capacidad de respuesta de las organizaciones para enfrentar pares internacionales con una capacidad y una experiencia mayor. Ejemplo de esto, es el caso de Japón y México con una razón de certificación en la norma ISO/IEC 27001:2005 de 123 empresas por cada empresa certificada en México.

La percepción de la seguridad de la información como soporte a la organización con un alcance en la infraestructura tecnológica ha cambiado en los últimos diez años para ser concebida como un socio y habilitador de negocio, sin embargo; por experiencia propia del autor aún persisten organizaciones en las que la dirección/subdirección de tecnologías de la información y/o seguridad de la información son vistas como un impedimento en el alcance de objetivos. En la medida en la que esta concepción cambie en los siguientes años, permitirá el aprovechamiento máximo de las bondades que ofrecen las tecnologías de la información y en última instancia la seguridad informática.

FUENTES DE INFORMACIÓN

BIBLIOGRAFÍA

Leyes y reglamentos:

- Ley Federal sobre metrología y Normalización. Publicada en el Diario Oficial de la Federación (DOF) el 1 de julio de 1992 y reformada por decretos publicados en el DOF los días 24 de diciembre de 1996, 20 de mayo de 1997 y el 19 de mayo de 1999.
- Reglamento de la Ley Federal sobre Metrología y Normalización. Publicado en el Diario Oficial de la Federación (DOF) el 14 de enero de 1999.

Sitios de internet:

- 1) "Normalización nacional" en: <http://www.economia.gob.mx/comunidad-negocios/competitividad-normatividad/normalizacion/nacional> [accesado el día 07 de septiembre de 2015].
 - 3) "ICS, por sus siglas en inglés" en: http://www.iso.org/iso/international_classification_for_standards.pdf [Última edición en 2005].
 - 4) "Organización Internacional de Normalización" se encuentra en <http://www.iso.org/iso/home.htm> [accesado el día 07 de septiembre de 2015].
- www.iec.ch
 - www.iso.org
 - <https://www.ieee.org>
 - <http://www.iata.org>
 - <https://www.ietf.org>
 - www.ansi.org
 - <http://www.itu.int>
 - <https://www.cen.eu>
 - www.bsi-global.com
 - www.economia.gob.mx
 - www.ema.org.mx

Normas y guías:

- 2) ISO:9000:2015, "Sistemas de gestión de la calidad – Fundamentos y vocabulario" en http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42180 [última edición en 2015].

Directivas ISO/IEC, Parte 2: Reglas para la estructura y realización en borrador de normas internacionales. 2002, 91 pp.

ISO/IEC Directives, Part 1: Procedures for the technical work. Cuarta edición, 2001, 61 pp.

ISO 9001 Quality management Systems – Requirements. 2015.

ISO/IEC 27000 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary, 2014.

ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems – Requirements, 2014.

ISO/IEC 27002 Information technology -- Security techniques -- Code of practice for information security controls, 2014.

ISO/IEC 27003 Information technology -- Security techniques -- Information security management system implementation guidance, 2010.

ISO/IEC 27004 Information technology -- Security techniques -- Information security management – Measurement, 2009.

ISO/IEC 27005 Information technology -- Security techniques -- Information security risk management, 2011.

ISO/IEC 27006 Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems, 2011.

ISO/IEC 27007 Information technology -- Security techniques -- Guidelines for information security management systems auditing, 2011.

ISO/IEC TR 27008 Information technology -- Security techniques -- Guidelines for auditors on information security controls, 2011.

ISO/IEC 27010 Information technology -- Security techniques -- Information security management for inter-sector and inter-organizational communications, 2012.

ISO/IEC 27011 Information technology -- Security techniques -- Information security management guidelines for telecommunications organizations based on ISO/IEC 27002, 2008.

ISO/IEC 27013 Information technology -- Security techniques -- Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1, 2012.

ISO/IEC 27014 Information technology -- Security techniques -- Governance of information security, 2013.

ISO/IEC TR 27015 Information technology -- Security techniques -- Information security management guidelines for financial services, 2012.

ISO/IEC TR 27016 Information technology -- Security techniques -- Information security management -- Organizational economics, 2014.

ISO 27799 Health informatics -- Information security management in health using ISO/IEC 27002, 2008.

NMX-Z-13/1-1977 Guía para la redacción, estructuración y presentación de las normas mexicanas. México, Secretaría de Comercio y Fomento Industrial / Dirección General de Normas, octubre 1977.

NMX-Z-109-1992 Términos generales y sus definiciones referentes a la normalización y actividades conexas. México, Secretaría de Comercio y Fomento Industrial / Dirección General de Normas, junio 1992.