NORMAS ISO Y SU COBERTURA

Introducción

Boletín #1

Organización Internacional de Estandarización

La Organización Internacional de Estandarización, ISO, es una organización sin ánimo de lucro de carácter no gubernamental creada el 23 de Febrero de 1947 que promueve el desarrollo y la implementación de normas a nivel internacional, tanto de fabricación como de servicios. El objetivo de esta organización es brindar herramientas para facilitar las transacciones a nivel internacional tanto de objetos, bienes y servicios como de desarrollos científicos, actividades intelectuales, tecnológicas y económicas.

La organización está constituida por 180 Comités Técnicos y las actividades técnicas se encuentran descentralizada en unos 2700 Comités, subcomité y grupo de trabajo. Los aspectos que abarcan son de lo más diversos, desde el tamaño de las hojas de papel hasta lo último en telecomunicaciones.

ISO International Organization for Standardization

Contenido:

Niveles de normas de acuerdo a su alcance

Empresarial: Son normas editadas e implantadas en una compañía gubernamental o de iniciativa privada, originadas y reconocidas por el cuerpo directivo, en las que se establece una serie de características o directrices particulares relacionadas con el giro o actividad de la misma, con el fin de hacer más efectiva su tarea a través del control y simplificación de actividades y procesos.

Sectorial: Son normas editadas y reconocidas por un conjunto de empresas relacionado en algún campo industrial determinado.
El objeto primordial de estas normas es el de evitar competencias desleales entre los fabricantes, y se formulan por un grupo representativo de estos aprovechando las experiencias comunes al sector industrial.

Nacional: Las normas nacionales son promulgadas después de consultar a todos los intereses afectados en un país, esto es en los sectores productores, consumidores, centros de investigación, gobierno de interés general, a través de una organización Nacional de Normalización, que puede ser privada ó gubernamental. En algunas ocasiones los países desarrollados son los que emiten dichas normas y posteriormente los países en vías de desarrollo adoptan homologan y validan las mismas.

Estas Normas facilitan el comercio Internacional a medida que dicha actividad adopta formas más complejas de realización, la importancia de las normas se acrecienta; hoy en día no podríamos pensar en un mercado común sin Normalizar los productos a intercambiar (GÓMEZ & RAVE, 2008)

Regional: Son normas editadas e implantadas por algunos organismos, reuniendo un grupo de países que por su finalidad geográfica comercial, industrial, económica, etc., establecen una serie de características o directrices particulares, con el fin de facilitar un mejor intercambio tanto económico como de transferencia tecnológica entre los países pertenecientes a una región.

Internacional: Es el nivel de Normalización que presenta el esquema de aplicación más amplia y cuyas normas son el resultado, en muchas ocasiones de arduas sesiones para conciliar los intereses de todos los países que intervienen en el proceso, actualmente el organismo que agrupa la gran mayoría de los países del orbe (82) es la ISO (International StandardOrganization).

ISO (Organización Internacional de Normalización)

La familia de las ISO se clasifican en varias series que pretenden estandarizar temas variados, en esta introducción se establecerá genéricamente la cobertura de cada una de las series ISO que luego se desarrollaran a profundidad en las siguientes entregas.

Serie ISO 9000

ISO 9000: es un conjunto de normas sobre calidad y gestión de calidad que especifican los elementos y como deben funcionar el conjunto de estos elementos para asegura la calidad de los bienes y servicios que produce la Organización .

Está conformada por:

ISO 9000: Sistemas de Gestión de la Calidad − Fundamentos y Vocabulario. En ella se definen términos relacionados con la calidad y establece Lineamientos generales para los Sistemas de Gestión de la Calidad.

ISO 9001: Sistemas de Gestión de la Calidad − Requisitos. Establece los requisitos mínimos que debe cumplir un Sistema de Gestión de la Calidad. Puede utilizarse para su aplicación interna, para certificación o para fines contractuales.

Versión 2015: realiza cambios enfocando el tema a la Administración de Riesgo y la Organización por procesos.

ISO 9002: Sistema de Calidad. Modelo para el aseguramiento de la calidad en la producción; instalación y el servicio posventa.

ISO 9004: Sistemas de Gestión de la Calidad −Directrices para la Mejora del desempeño.

ISO 9011:2002: Directrices para la auditoría ambiental y de la calidad.

Serie ISO 14000

ISO 14000: Es un Estándar Internacional que contiene una serie de normas que establecen los lineamientos para la aplicación de un Sistema de Gestión Ambiental (SGA).

La serie 14000 está constituido por la siguientes normas:

ISO 14001:2004 Sistemas de gestión ambiental. Requisitos con orientación para su uso.

ISO 14004:2004 Sistemas de gestión ambiental. Directrices generales sobre principios, sistemas y técnicas de apoyo.

ISO 14006:2011 Sistemas de gestión ambiental. Directrices para la incorporación del ecodiseño.

ISO 14011:2002: Guía para las auditorías de sistemas de gestión de calidad o ambiental.

ISO 14020: Etiquetado y declaraciones ambientales - Principios Generales

ISO 14021: Etiquetado y declaraciones ambientales – Autodeclaraciones

ISO 14024: Etiquetado y declaraciones ambientales

ISO/TR 14025: Etiquetado y declaraciones ambientales

ISO 14031:1999: Gestión ambiental. Evaluación del rendimiento ambiental. Directrices.

ISO/TR 14032:1999 Gestión ambiental - Ejemplos de evaluación del rendimiento ambiental (ERA)

ISO 14040:2006: Gestión ambiental - Evaluación del ciclo de vida - Principios y marco de referencia.

ISO 14044:2006: Gestión ambiental - Análisis del ciclo de vida - Requisitos y directrices.

ISO/TR 14047: Gestión ambiental - Evaluación del impacto del ciclo de vida. Ejemplos de aplicación de ISO 14042.

ISO/TS 14048: Gestión ambiental - Evaluación del ciclo de vida. Formato de documentación de datos.

ISO/TR 14049: Gestión ambiental - Evaluación del ciclo de vida. Ejemplos de la aplicación de ISO 14041 a la definición de objetivo y alcance y análisis de inventario.

ISO 14050:2009: Gestión ambiental – Vocabulario.

ISO/TR 14062:2002: Gestión ambiental - Integración de los aspectos ambientales en el diseño y desarrollo de los productos.

ISO 14063:2006: Comunicación ambiental - Directrices y ejemplos (Libre, 2014)

Serie ISO 19000

ISO 19000: A partir de esta entrega vamos a empezar a explorar a cerca de Normas Internacionales que impactan a los Sistemas de Gestión (NTC- ISO – 19011)

La ISO 19000 es el marco normativo de referencia para realizar auditorías internas y externas, básicamente de Sistemas de Gestión de la Calidad basados en la norma internacional ISO 9001:2008.

NTC- ISO – 19011 DIRECTRICES PARA LA AUDITORÍA DE LOS SIETMAS DE GESTIÓN

INTRODUCCIÓN

Esta Norma Internacional aplicada a la legislación Colombiana pretende que se aplique a un amplio de usuario potenciales, incluyendo auditores, Organizaciones que implementan sistemas de gestión y quienes requieran la realización de Auditorías de Sistema de Gestión por razones fiduciarias y de reglamentación. Otra visión que podemos aplicar a esta norma es solo para efectos del desarrollo de mejores prácticas Corporativas o para empresas que participan en formación de auditores o certificación de personas.

El riesgo de Auditoria es un componente a tener en cuenta, pues se refiere al riesgo a los riesgos del proceso de Auditoria para lograr las metas trazadas como al riesgo de interferir con las actividades propias del personal responsable del proceso a Auditar. También esta norma específica el esfuerzo conjunto dos o más Sistemas de Gestión de disciplinas diferentes, lo que llamaremos más adelante como “auditoría combinada” y se aplica cuando existen integración en un único sistema de Gestión.

OBJETO Y CAMPO DE APLICACIÓN DE LA NORMA

Esta norma pretende llegar a la Organizaciones como un marco de mejores prácticas sobre la auditoría de los sistemas de Gestión donde esboza los principios de la auditoría, la gestión de un programa de auditoría, la realización del programa y las competencias de las personas que desarrollan, gestionan el programa y los equipos de auditores conformados para este fin.

REFERENCIAS NORMATIVAS

Para este capítulo no existen referenciaciones, pero se conserva este capítulo para conservar la misma estructura utilizada en otras normas.

TERMINOS Y DEFINICIONES

En cada entrega vamos a dar algunos términos y definiciones hasta completar la totalidad en la última entrega:

Auditoría: “Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría”

Criterios de Auditoría: “Conjuntos de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia de la auditoría”

Evidencia de Auditoría: “Registros, declaraciones de hechos o cualquier otra información que es pertinente para los criterios de Auditoria”

ISO 19113: establece los conceptos a considerar para la descripción de la calidad de los datos geográficos y establece los elementos de información de calidad para la presentación de informes.

ISO 19114 : principios de calidad

ISO 19131: establece las especificaciones de todos los productos de datos que utilizan los datos geográficos

ISO 19138 define los componentes y la estructura de contenido para un registro de medidas de calidad de los datos.

ISO 19115 a 19139: *Normas de metadatos.*

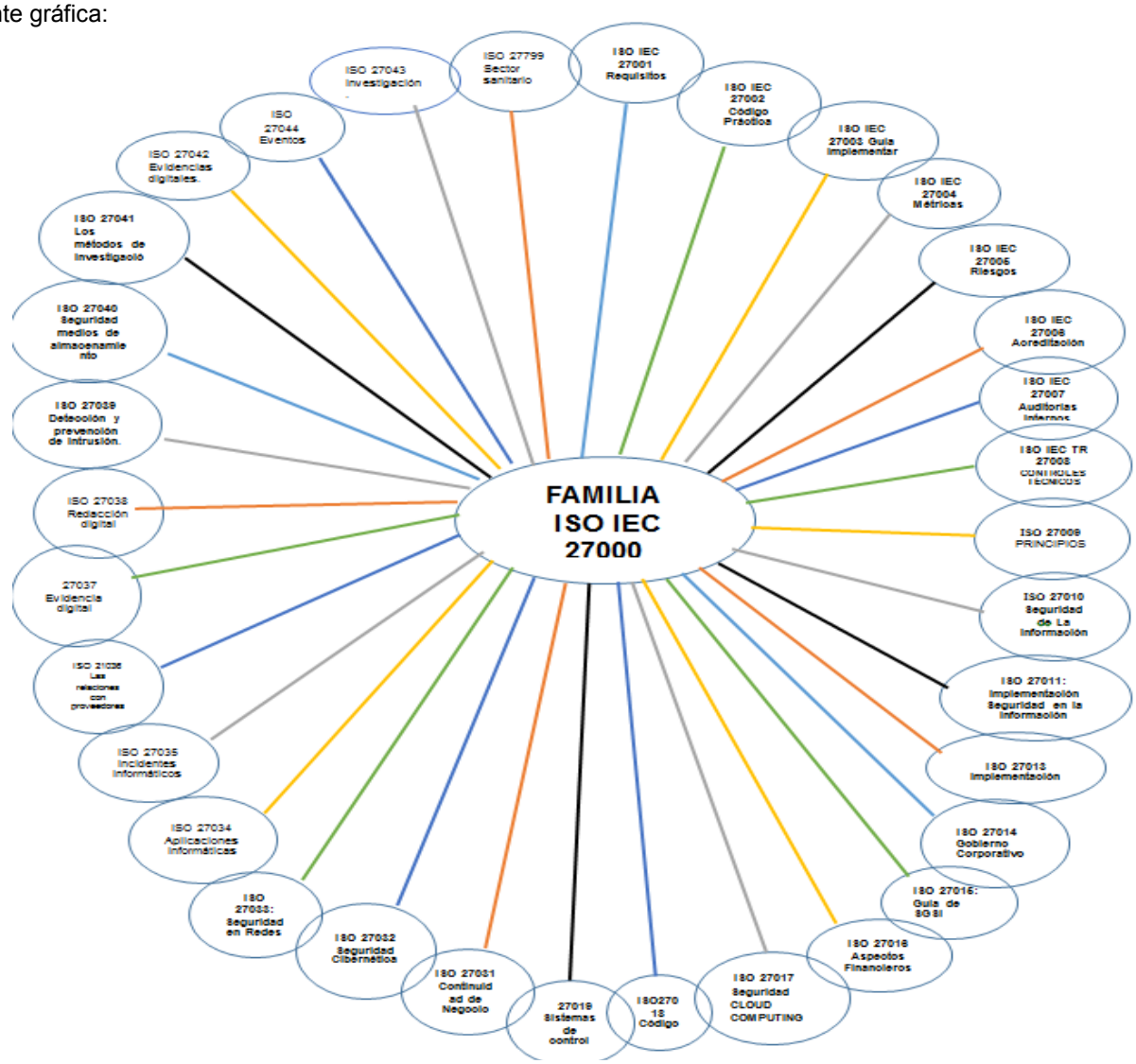
Serie ISO 27000

A partir de esta entrega vamos a empezar a explorar a cerca de Normas Internacionales de Técnicas de Seguridad de Tecnología de la Información (NTC-ISO-IEC 27000).

TÉCNICAS DE SEGURIDAD DE TECNOLOGÍA DE LA INFORMACIÓN (NTC-ISO-IEC 27000).

La norma Internacional **ISO/IEC 27000** es un compendio de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que brindan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de Organización de múltiples sectores de la Economía, pues la Información es el foco importante a proteger.

Existen entonces diferentes normas que componen la serie ISO 27000 y se indica cómo puede una Organización implementar un Sistema de Gestión de Seguridad de la Información (SGSI) basado en ISO 27001 como guía de requisitos del SGSI y la ISO IEC 27002 como código de práctica en conjunto con otras normas de la serie 27000, que veremos en la siguiente gráfica:



Serie ISO 27000

Esta norma fue publicada en Octubre de 2005, revisada en Septiembre de 2013 y publicada en Diciembre de 2013. Esta norma contiene los requisitos del sistema de gestión de seguridad de la información. Tiene su origen en la BS (British Stándar) 7799-2:2002 y es la norma a certificar por auditores externos del SGSI de las organizaciones. Contiene el Anexo A, en el que resumen los 14 objetivos de control y 114 controles que desarrolla la ISO IEC 27002:2005, la cual brinda las guías de implementación del SGSI con un nivel de detalle para ser seleccionados y aplicados por las organizaciones en todas las etapas del SGSI.

ISO 27001: Contiene los requisitos del sistema de gestión de seguridad de la información

ISO 27002: Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.

ISO 27003: Guía de implementación de SGSI e información acerca del uso del modelo PDCA y de los requerimientos de sus diferentes fases.

ISO 27005: Proporciona las directrices para la gestión del riesgo en la seguridad de la información.

ISO 27006: Especifica los requisitos para la acreditación de entidades de auditoría y certificación de sistemas de gestión de seguridad de la información.

ISO 27007: Es una guía de auditoría de un SGSI, como complemento a lo especificado en ISO 19011.

ISO 27008: Guía de auditoría de los controles seleccionados en el marco de implantación de un SGSI

ISO 27009 Es una guía sobre el uso y aplicación de los principios de ISO/IEC 27001 para el sector servicios específicos en emisión de certificaciones acreditadas de tercera parte. (Esta en desarrollo).

ISO 27010: Guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores.

ISO 27011: Guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002:2005

ISO 27013 : Guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

ISO 27014: Guía de gobierno corporativo de la seguridad de la información.

Serie ISO 27000

ISO 27015: Es una guía de SGSI orientada a organizaciones del sector financiero y de seguros y como complemento a ISO/IEC 27002:2005.

ISO 27016: Guía de valoración de los aspectos financieros de la seguridad de la información.

ISO 27017: Guía de seguridad para Cloud Computing.

ISO 27018: Es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

ISO 27019: Guía para el proceso de sistemas de control específicos relacionados con el sector de la industria de la energía

ISO 27031: Guía de continuidad de negocio en cuanto a tecnologías de la información y comunicaciones.

ISO 27032: Proporciona orientación para la mejora del estado de seguridad cibernética.

ISO 27033: Norma dedicada a la seguridad en redes, consistente en 7 partes: gestión de seguridad de redes, arquitectura de seguridad de redes, escenarios de redes de referencia, aseguramiento de las comunicaciones entre redes mediante gateways, acceso remoto, aseguramiento de comunicaciones en redes mediante VPNs y diseño e implementación de seguridad en redes.

ISO 27034: Norma dedicada la seguridad en aplicaciones informáticas, consistente en 6 partes: conceptos generales, marco normativo de la organización , proceso de gestión de seguridad en aplicaciones, validación de la seguridad en aplicaciones , estructura de datos y protocolos y controles de seguridad de aplicaciones , guía de seguridad para aplicaciones de uso específico.

ISO 27035: guía sobre la gestión de incidentes de seguridad en la información.

ISO 27036: guía sobre la seguridad en las relaciones con proveedores, consiste en cuatro partes: visión general y conceptos, requisitos comunes, seguridad en la cadena de suministro TIC, seguridad en entornos de servicios Cloud.

ISO 27037: Guía para la Identificación, recolección, adquisición y preservación de evidencia digital.

ISO 2738: Guía de especificación para seguridad en la redacción digital.

ISO 2739: Guía para la selección, despliegue y operativa de sistemas de detección y prevención de intrusión

Serie ISO 27000

ISO 27040: Guía para la seguridad en medios de almacenamiento.

ISO 27041: Orientación para garantizar la idoneidad y adecuación de los métodos de investigación.

ISO 27042: Orientaciones con directrices para el análisis e interpretación de las evidencias digitales.

ISO 27043: Desarrollará principios y procesos de investigación.

ISO 27044: Gestión de eventos y de la seguridad de la información - Security Información and Event Management (SIEM).

ISO 27799: Es un estándar de gestión de seguridad que proporciona directrices para apoyar la interpretación y aplicación en el sector sanitario de ISO/IEC 27002:2005, en cuanto a la seguridad de la información sobre los datos de salud de los pacientes.

Serie ISO 31000

ISO 31000: Principios y directrices genéricas sobre gestión de riesgos para todos los sectores.

ISO 31010: Es una norma de apoyo de la norma ISO 31000, trata sobre las directrices de Gestión de riesgos, Técnicas y evaluación de riesgos.

Bibliografía

GÓMEZ , M., & RAVE, M. (24 de Octubre de 2008). *LA NORMALIZACIÓN: UNA SOCIEDAD SIN NORMAS, NO ES SOCIEDAD*. Obtenido de NIVELES DE NORMAS: http://gaenormalizacion.blogspot.com/2008/10/niveles-de-normas.html

©, W. (s.f.). *WWW.ISO27000.ES ©*. Obtenido de ISO 27000 : http://www.iso27000.es/download/doc_iso27000_all.pdf

Libre, C. d. (21 de SEPTIEMBRE de 2014). *WIKIPEDIA: La Encciclopedia Libre* . Obtenido de ISO 14000: http://es.wikipedia.org/wiki/ISO_14000

PriteshGupta.com. (s.f.). *ISO 27000.es*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es/iso27000.html

QCONSULTORES. (2014). *QCONSULTORES*. Obtenido de PREPARACIÓN PARA CERTIFICACIONES Y ACREDITACIONES: http://www.qconsultores.com/nsite/qconsultores/index.php?option=com_content&view=article&id=59:sistemas-de-la-calidad&Itemid=75